CIS Center for Internet Security®

CIS Controls

Controlli CIS

Versione 8

V8

Controlli CIS Versione 8

Maggio 2021

Ringraziamenti

CIS ringrazia tutti gli esperti in sicurezza che volontariamente dedicano il loro tempo e le loro capacità per supportare CIS Controls e tutto il resto del lavoro di CIS. I prodotti CIS rappresentano lo sforzo di un vero esercito di volontari del settore che generosamente donano il loro tempo e le loro capacità in nome di una esperienza online sempre più sicura per tutti.

Translated by Giacomo Lunardon, Italian Ministry of Public Education

Contenuti

Glossario

Account amministratore	Account dedicati con privilegi elevati e utilizzati per la gestione di un computer, dominio o dell'intera infrastruttura informatica aziendale. I più comuni sottotipi di account amministratore includono: account root, account amministratore locale, account amministratore di dominio e account amministrativi dedicati alla rete o ai vari strumenti di sicurezza.
Applicazione	Applicazione: un programma o un gruppo di programmi ospitati sulle risorse aziendali e progettati per l'utente finale. In questo documento le applicazioni sono considerate una risorsa software. Alcuni esempi includono applicazioni Web, database, mobili, basate sul cloud.
Sistemi di autenticazione	Un sistema o meccanismo utilizzato peri identificare un utente mediante l'associazione di una richiesta a un insieme di credenziali di identificazione. Le credenziali fornite vengono confrontate con quelle presenti in un database contenente le informazioni dell'utente autorizzato su un sistema operativo locale, servizio di directory utente o all'interno di un server di autenticazione. Alcuni sistemi di autenticazione includono ad esempio Active Directory, Autenticazione Multi Fattore (MFA), biometria e i token.
Sistemi di autorizzazione	Un sistema o un meccanismo utilizzato per determinare i livelli di accesso o i privilegi utente / client relativi alle risorse di sistema, inclusi file, servizi, programmi, dati e funzionalità delle applicazioni. Un sistema di autorizzazione permette o nega l'accesso a una risorsa in base all'identità dell'utente. Alcuni sistemi di autorizzazione includono ad esempio Active Directory, elenchi di controllo degli accessi ed elenchi di controllo degli accessi basati sui ruoli.
Ambiente cloud	Un ambiente virtualizzato che fornisce un comodo accesso su richiesta, tramite la rete, ad un insieme di risorse condivise configurabili come rete, elaborazione, archiviazione, applicazioni e servizi. Le cinque caratteristiche principali di un ambiente cloud sono: self-service su richiesta, accesso alla rete, pool di risorse, elasticità immediata e misurazione del servizio. Alcuni servizi offerti tramite ambienti cloud includono Software as a Service (SaaS), Platform as a Service (PaaS) e Infrastructure as a Service (IaaS).
Database	Insieme organizzato di dati, generalmente gestito e consultabile in modo elettronico, da parte di un sistema informatico. Il database può risiedere in remoto o in locale. In questo documento i sistemi di gestione dei database (DMSs) vengono utilizzati per la loro amministrazione e non sono considerati parte del database stesso.
Dispositivi dell'utente finale	Risorse delle tecnologie dell'informazione (IT) utilizzate dal personale di un'impresa durante il lavoro, al di fuori di esso e per qualsiasi altro scopo. I dispositivi degli utenti finali includono dispositivi mobili e portatili come laptop, smartphone e tablet, nonché desktop e workstation. Ai fini di questo documento, i dispositivi dell'utente finale sono considerati un sottoinsieme delle risorse aziendali.
Risorse aziendali	Risorse con la possibilità di archiviare o elaborare dati. Ai fini del presente documento, le risorse aziendali includono dispositivi degli utenti finali, dispositivi di rete, dispositivi non informatici / Internet of Things (IoT) e server, in ambienti virtuali, cloud e fisici.
Risorse aziendali accessibili esternamente	Si fa riferimento alle risorse aziendali rivolte al pubblico e rilevabili tramite il riconoscimento del sistema dei nomi di dominio e tramite la scansione della rete Internet dall'esterno della rete aziendale.

Risorse aziendali interne	Si fa riferimento alle risorse aziendali non pubbliche che possono essere identificate solo tramite scansioni di rete e ricognizione dall'interno della rete aziendale tramite accesso autorizzato autenticato o non autenticato.
Libreria	Codice scritto in precedenza, classi, procedure, scripts, dati di configurazione, ed altro, utilizzabili per lo sviluppo di software, programmi e applicazioni. È progettata per aiutare sia il programmatore sia il compilatore del linguaggio utilizzato, per la compilazione ed esecuzione del software.
Dispositivi mobili dell'utente finale	Dispositivi per l'utente finale rilasciati dall'azienda, di piccole dimensioni con capacità wireless intrinseca, come smartphone e tablet. Tali dispositivi mobili sono un sottoinsieme dei dispositivi portatili per gli utenti finali, compresi i laptop, che potrebbero richiedere hardware esterno per la connettività. Ai fini di questo documento, i dispositivi mobili sono un sottoinsieme dei dispositivi degli utenti finali.
Dispositivi di rete	Dispositivi elettronici necessari per la comunicazione e l'interazione tra dispositivi su una rete di computer. I dispositivi di rete includono punti di accesso wireless, firewall, gateway fisici / virtuali, router e switch. Questi dispositivi sono costituiti da hardware fisico, così come da dispositivi virtuali e basati su cloud. Ai fini di questo documento, i dispositivi di rete sono un sottoinsieme delle risorse aziendali.
Infrastruttura di rete	Si fa riferimento a tutte le risorse di una rete che rendono possibile la connettività di rete o Internet, la gestione, le operazioni aziendali e la comunicazione. È costituita da hardware e software, sistemi, dispositivi e permette l'elaborazione e la comunicazione tra utenti, servizi, applicazioni e processi. L'infrastruttura di rete può essere cloud, fisica o virtuale.
Dispositivi non informatici / Internet of Things (IoT)	Dispositivi integrati con sensori, software e altre tecnologie con lo scopo di connettere, archiviare e scambiare dati con altri dispositivi e sistemi su Internet. Sebbene non siano utilizzati per processi di calcolo, supportano l'azienda nello svolgimento dei processi aziendali. Esempi di questi dispositivi includono stampanti, schermi intelligenti, sensori di sicurezza fisica, sistemi di controllo industriali e sensori della tecnologia dell'informazione. Ai fini di questo documento, i dispositivi non informatici / IoT sonio un sottoinsieme delle risorse aziendali.
Sistema operativo	Sistema software installato sulle risorse aziendali che gestisce l'hardware e il software del computer fornendo servizi comuni per i programmi. I sistemi operativi sono considerati una risorsa software e possono essere single e multi-tasking, single e multi-user, distribuiti, basati su modelli, incorporati, in tempo reale e librerie.
Ambiente fisico	Parti hardware che costituiscono una rete inclusi cavi e router. L'hardware è necessario per la comunicazione e l'interazione tra i vari dispositivi connessi alla rete.
Dispositivi portatili dell'utente finale	Dispositivi trasportabili per l'utente finale con capacità di connessione a una rete in modalità wireless. Ai fini di questo documento, i dispositivi portatili dell'utente finale, che possono includere laptop e dispositivi mobili tipo smartphone e tablet, sono un sottoinsieme delle risorse aziendali.
Dispositivi remoti	Qualsiasi risorsa aziendale in grado di connettersi a una rete da remoto, di solito da Internet. Sono incluse le risorse aziendali come i dispositivi dell'utente finale, dispositivi di rete, dispositivi non informatici / Internet of Things (IoT) e server.
File system remoto	Permette ad una applicazione di funzionare su una risorsa aziendale permettendo l'accesso ai file archiviati su una risorsa diversa. I file system remoti spesso rendono accessibili ad una risorsa altri dispositivi non informatici remoti. L'accesso ai file remoti avviene utilizzando una qualsiasi forma di rete locale, rete geografica, punto a punto o altro sistema di comunicazione. Spesso ci si riferisce a questi file system come file system di rete o file system distribuiti.

Media rimovibile	Qualsiasi tipo di dispositivo di archiviazione che può essere rimosso da un computer mentre il sistema è in esecuzione che consente di spostare i dati da un sistema all'altro. Esempi di supporto rimovibile includono compact disc (CD), dischi versatili digitali (DVD) e dischi Blu-ray, backup su nastro, nonché dischetti e unità USB (Universal Serial Bus).
Server	Un dispositivo o un sistema che fornisce risorse, dati, servizi o programmi ad altri dispositivi su una rete locale o su una rete geografica. I server possono fornire risorse e utilizzarle contemporaneamente da un altro sistema. Gli esempi includono server Web, applicazioni server, server di posta e file server.
Account di servizio	Un account dedicato con privilegi elevati utilizzato per l'esecuzione di applicazioni e altri processi. Gli account di servizio possono anche essere creati solo per ottenere la proprietà su dati e file di configurazione. Non sono destinati ad essere utilizzati, se non per l'esecuzione di operazioni amministrative.
Servizio	Si fa riferimento ad una o più funzionalità software, come il recupero di informazioni specifiche o l'esecuzione di una serie di operazioni. I servizi forniscono un meccanismo per consentire l'accesso a una o più funzionalità, nel caso in cui l'accesso venga fornito utilizzando un'interfaccia prestabilita e basata sull'identità del richiedente in funzione delle regole aziendali.
Social engineering	Si fa riferimento ad una vasta gamma di attività ingannevoli realizzate per mezzo dell'interazione umana sfruttando varie piattaforme, come e-mail o telefono. Si basa sulla manipolazione psicologica per indurre gli utenti a commettere errori di sicurezza o a divulgare informazioni sensibili.
Risorsa software	Indicata anche come software in questo documento, si fa riferimento ai programmi ed altre informazioni operative utilizzate all'interno di una risorsa aziendale. Le risorse software includono sistemi operativi e applicazioni.
Account utente	Un'identità creata per una persona in un computer o in un sistema informatico. Ai fini di questo documento, gli account utente si riferiscono agli account utente "standard" o "interattivi" con privilegi limitati che vengono utilizzati per attività generali come la lettura di e-mail e la navigazione sul Web. Gli account utente con privilegi elevati rientrano tra gli account amministrativi.
Ambiente virtuale	Simulando l'hardware consente l'esecuzione di un ambiente software senza la necessità di utilizzare molto hardware reale. Gli ambienti virtualizzati vengono utilizzati in modo che un numero limitato di risorse agisca come una quantità elevata di capacità computazionale, memoria, archiviazione e capacità di rete. La virtualizzazione è una tecnologia di funzionamento fondamentale per il cloud computing.

Acronimi e Abbreviazioni

AAA	Authentication, Authorization, and Auditing	Autenticazione, Autorizzazione e Auditing
ACL	Access Control List	Lista di Controllo degli Accessi
AD	Active Directory	Active Directory
AoC	Attestation of Compliance	Attestato di Conformità
API	Application Programming Interface	Interfaccia di Programmazione di un'Applicazione
BEC	Business Email Compromise	Compromissione Email Aziendale
C2	Command and Control	Comando e Controllo
CCE	Common Configuration Enumeration	Enumerazione Comune di Configurazione
CDM	Community Defense Model	Modello di Difesa CIS Community
CIA	Confidentiality, Integrity, and Availability	Riservatezza, integrità e disponibilità
CIS	Center for Internet Security	Centro per la Sicurezza Internet
CIS –CAT	CIS Configuration Assessment Tool	CIS Strumento di Valutazione della Configurazione
COTS	Commercial off-the-Shelf	Prodotto Commerciale Adattabile su Richiesta
CPE	Common Platform Enumeration	Piattaforma Comune di Enumerazione
CREST	Council of Registered Security Testers	Consiglio dei Tester Sicurezza Autorizzati
CSA	Cloud Security Alliance	Cloud Security Alliance
CSP	Cloud Service Provider	Fornitore Servizi Cloud
CVE	Common Vulnerabilities and Exposures	Vulnerabilità ed Esposizioni Comuni
CVSS	Common Vulnerability Scoring System	Sistema di Punteggio delle Vulnerabilità Comuni
DBIR	Data Breach Investigations Report	Rapporto di Investigazione sula Violazione dei Dati
DEP	Data Execution Prevention	Prevenzione di Esecuzione in area Dati
DG	Development Group	Gruppo di Sviluppo
DHCP	Dynamic Host Configuration Protocol	Protocollo Dinamico di Configurazione Host
DKIM	DomainKeys Identified Mail	Chiave Identificativa Dominio Mail
DLP	Data Loss Prevention	
DMARC	Domain-based Message Authentication, Reporting, and Conformance	Autenticazione Messaggi Reportistica e Conformità dei Messaggi di Dominio
DMS	Database Management System	Gestione Sistema Database
DNS	Domain Name System	Sistema dei Nomi di Dominio
DPI	Deep Packet Inspection	Ispezione Approfondita dei Pacchetti
EDR	Endpoint Detection and Response	Endpoint di Rilevamento e Risposta
EOL	End of Life	Fine Ciclo di Vita
FFIEC	Federal Financial Institutions Examination Council	Consiglio di Valutazione delle Istituzioni Finanziarie Federali
FISMA	Federal Information Security Modernization Act	Legge Federale di Modernizzazione della Sicurezza delle Informazioni
GRC	Governance Risk and Compliance	Rischio di Governance e Conformità
HECVAT	Higher Education Community Vendor Assessment Toolkit	Strumento di Valutazione dei Fornitori dell'Educazione Superiore

HIPAA	Health Insurance Portability and Accountability Act	Accordi sulla Responsabilità e Portabilità dell'Assicurazione Sanitaria
HTTP	Hypertext Transfer Protocol	Protocollo di Trasferimento Ipertestuale
HTTPS	Hypertext Transfer Protocol Secure	Protocollo di Trasferimento Ipertestuale Sicuro
IaaS	Infrastructure as a Service	Infrastructure as a Service
IAM	Identity and Access Management	Gestione degli Accessi e dell'Identità
IDS	Intrusion Detection System	Sistema di Rilevamento delle Intrusioni
IG	Implementation Group	Gruppo di Implementazione
IOCs	Indicators of Compromise	Indicatori di Compromissione
IoT	Internet of Things	Internet of Things
IP	Internet Protocol	Protocollo Internet
IPS	Intrusion Prevention System	Sistema di Prevenzione delle Intrusioni
ISAC	Information Sharing and Analysis Center	Centro di Condivisione e Analisi delle Informazioni
ISO	International Organization for Standardization	Organizzazione Internazionale per la Standardizzazione
IT	Information Technology	Tecnologia dell'Informazione
LotL	Living off the Land	Uso di Strumenti Sicuri per la Diffusione Malware
MDM	Mobile Device Management	Gestione dei Dispositivi Mobili
MFA	Multi-Factor Authentication	Autenticazione Multi Fattore
MITRE ATT&CK	MITRE Adversarial Tactics, Techniques, and Common Knowledge®	MITRE Tattiche Antagoniste, Tecniche e Conoscenza Comune®
MS-ISAC	Multi-State Information Sharing and Analysis Center	Centro Interstatale di Analisi e Condivisione delle Informazioni
NaaS	Network-as-a-Service	Network-as-a-Service
NCSA	National Cyber Security Alliance	National Cyber Security Alliance
NIDS	Network Intrusion Detection System	Sistema di Rete per il Rilevamento delle Intrusioni
NIST	National Institute of Standards and Technology	Istituto Nazionale degli Standard Tecnologici
OS	Operating System	Sistema Operativo
OSS	Open Source Software	Software Open Source
OVAL	Open Vulnerability and Assessment Language	Linguaggio Open per la Valutazione delle Vulnerabilità
OWASP	Open Web Application Security Project	Open Web Application Security Project
PaaS	Platform as a Service	Platform as a Service
PAM	Privileged Access Management	Gestione degli Accessi Privilegiati
PCI	Payment Card Industry	Settore delle Carte di Pagamento
SaaS	Software as a Service	Software come Servizio
SAFECode	Software Assurance Forum for Excellence in Code	Software Assurance Forum for Excellence in Code
SCADA	Supervisory Control and Data Acquisition	Controllo di supervisione e acquisizione dati
SCAP	Security Content Automation Protocol	Protocollo di Automazione dei Contenuti di Sicurezza
SIEM	Security Information and Event Management	Gestione Informazioni di Sicurezza ed Eventi
SIP	System Integrity Protection	Protezione di Integrità del Sistema

SMS	Short Messaging Service	Servizio Messaggistica Veloce
SOC	Security Operations Center	Centro Operativo per la Sicurezza
SOC 2	Service Organization Control 2	Servizio di Controllo Organizzazione 2
SPAM	Something Posing as Mail	Spam / Posta Indesiderata
SPF	Sender Policy Framework	Sender Policy Framework
SQL	Structured Query Language	Linguaggio di Query Strutturato
SSDF	Secure Software Development Framework	Framework di Sviluppo Software Sicuro
SSH	Secure Shell	Secure Shell
SSO	Single Sign-On	Single Sign-On
Telnet	Teletype Network	Teletype Network
TLS	Transport Layer Security	Protocollo Comunicazione Telnet
TTPs	Tactics, Techniques, and Procedures	Tattiche, Tecniche e Procedure
U.K.	United Kingdom	Regno Unito
URL	Uniform Resource Locator	Uniform Resource Locator
USB	Universal Serial Bus	Universal Serial Bus
VPN	Virtual Private Network	Rete Privata Virtuale
WDEG	Windows Defender Exploit Guard	Windows Defender Exploit Guard
WPA2	Wi-Fi Protected Access 2	Protocollo di Accesso Wi-Fi 2
XCCDF	Extensible Configuration Checklist Description Format	Formato Descrittivo Elenco di Controllo Configurazione

Introduzione

I Controlli CIS® iniziano come una semplice attività di base per identificare i più comun i ed importanti cyber-attacchi che avvengono quotidianamente nel mondo reale a danno delle aziende, traducendo quelle conoscenze ed esperienze in azioni positive e costruttive per chi si difende, condividendo tutte queste informazioni con una più vasta platea. Gli obiettivi originali erano modesti—aiutare persone ed aziende concentrando la loro attenzione per iniziare i passi più importanti per difendersi dagli attacchi veramente importanti.

Guidati dal Center for Internet Security® (CIS®), i Controlli CIS sono maturati nell'ambito di una comunità internazionale di persone ed istituzioni che volontariamente:

- Condividono approfondimenti sugli attacchi e sugli attaccanti, identificando le cause principali e traducendo tutto questo in classi di azioni difensive
- Creano e condividono strumenti, utili, storie di adozione e di problem solving
- Mappano i Controlli CIS per l'adeguamento normativo e la conformità ai frameworks al fine di assicurarne l'allineamento e conferendo loro l'attenzione e la priorità collettiva
- Identificano i problemi comuni e gli ostacoli (valutazione iniziale, raodmap di implementazione), risolvendoli come comunità

I Controlli CIS riflettono l'esperienza combinata di esperti di ogni parte dell'ecosistema (società enti governativi, singoli individui), con svariati ruoli (threat responders, analisti, tecnici, operatori e difensori della tecnologia dell'informazione IT, cercatori di vulnerabilità, produttori di strumenti, fornitori di soluzioni, utenti, responsabili delle policy, revisori, ecc.), provenienti da molteplici settori (governativo, energetico, difesa, finanza, trasporti, università, consulenza, sicurezza IT, ecc.) che si sono uniti per creare, adottare e supportare i Controlli CIS

Evoluzione dei Controlli CIS

I Controlli CIS sono iniziati come molte altre attività simili—abbiamo riunito esperti, condiviso e discusso fino a raggiungere un accordo. Questo può essere molto utile, a seconda delle persone al tavolo e della loro esperienza. Attraverso la documentazione e la condivisione dei risultati, tutte le imprese possono beneficiare del lavoro di persone che non potrebbero assumere o neppure incontrare. Si può migliorare il risultato (e la tua fiducia in esso) selezionando esperti che rappresentino un'ampia gamma di conoscenze, che rendano congruente il processo e garantiscano l'uso delle migliori informazioni disponibili (soprattutto sugli attacchi). In sintesi, tutto dipende dal buon senso di un gruppo relativamente piccolo di persone, che collaborano in modo informale nell'ambito di una azione descrittiva.

In CIS abbiamo intrapreso un percorso pluriennale per portare più dati, rigore e trasparenza nel processo di raccomandazione delle migliori pratiche (i CIS Benchmarks™ e i CIS Controls). Tutti questi elementi sono essenziali per maturare una scienza alla base della cyber difesa; inoltre sono tutti necessari per consentire la personalizzazione e la "negoziazione" delle azioni di sicurezza applicabili in casi specifici così come richiesto da specifici framework di sicurezza, regolamenti ed altri schemi di supervisione simili.

Nelle prime versioni dei Controlli CIS, abbiamo utilizzato un elenco standard di attacchi pubblicamente noti come semplice test informale dell'utilità di specifiche raccomandazioni. A partire dal 2013, abbiamo collaborato con il team di Verizon per Rapporto sulle Indagini di Violazione dei Dati (DBIR) per mappare i risultati della loro analisi dei dati su larga scala, direttamente sui Controlli CIS, abbinando i loro riepiloghi degli attacchi in un programma standard per il miglioramento difensivo.

CIS ha pubblicato recentemente il Modello di Difesa CIS Community (CDM), che è il nostro approccio maggiormente "guidato dai dati", Nella sua versione iniziale, il CDM guarda alle conclusioni del più recente DBIR di Verizon, insieme ai dati del Centro Interstatale di Analisi e Condivisione delle Informazioni® (MS-ISAC®), al fine di identificare quelli che crediamo siano i cinque tipi attacchi più importanti. Li descriviamo utilizzando il framework MITRE Tattiche Antagoniste, Tecniche e Conoscenza Comune® (MITRE ATT&CK®) Framework al fine di creare pattern di attacco (o specifiche combinazioni di tattiche e tecniche utilizzate in questi attacchi). Ciò ci permette di analizzare il valore delle azioni difensive (es. Salvaguardie[1]) messe in atto per contrastarli. Nello specifico fornisce anche un modo congruo e spiegabile per esaminare il valore di sicurezza di un insieme di azioni difensive durante il ciclo di vita dell'attaccante e fornisce una base per le strategie come la difesa "in-depht". I dettagli di questa analisi sono disponibili sul sito Web CIS. L'elemento di base è quello di aver compiuto un passo importante verso l'identificazione del valore di sicurezza dei controlli CIS o di qualsiasi loro sottoinsieme. Mentre queste idee sono ancora in evoluzione, in CIS ci impegniamo per fornire raccomandazioni sulla sicurezza basate sui dati e presentate in modo trasparente. Per ulteriori informazioni si faccia riferimento a https://www.cisecurity.org/controls/v8/.

Queste attività assicurano che le "best practices" di sicurezza CIS (che includono i Controlli CIS e i Benchmark CIS) siano più di un elenco di "cose buone da fare" o "cose che potrebbero aiutare"; si tratta invece di un insieme di azioni prescrittive, prioritarie e altamente mirate che si basano su una rete di supporto della community per renderle implementabili, utilizzabili, scalabili e in linea con tutti i requisiti di sicurezza dei settori industriali e governativi.

[1] Le "Salvaguardie" erano note come "Sotto-Controlli" precedentemente alla Versione 8 dei Controlli CIS.

Questa versione dei controlli CIS

Quando iniziamo il lavoro su una nuova versione, prima ci riuniamo per stabilire i "principi di progettazione" che verranno utilizzati per guidare il processo. Questo serve come "pietra di paragone" decisionale per ricordarci che cosa è veramente importante e quali sono gli obiettivi dei Controlli CIS. Sebbene questi siano stati piuttosto coerenti fin dalle prime versioni dei controlli CIS, abbiamo affinato il nostro pensiero sulle ultime due versioni per concentrarci sul ruolo che i Controlli CIS svolgono nel quadro complessivo della sicurezza aziendale.

I nostri principi di progettazione prevedono:

- L'attacco informa la Difesa
  - I Controlli CIS vengono selezionati, eliminati e prioritizzati in base ai dati e alla conoscenza specifica del comportamento dell'attaccante e su come fermarlo
- Focalizzare
  - Aiutare i difensori nell'identificare gli elementi più importanti di cui necessitano per fermare gli attacchi più importanti
  - Evitare dall'essere tentato di risolvere ogni problema di sicurezza – evitare di aggiungere "cose buone da fare" o "cose che potresti fare"
- Fattibilità
  - Tutte le singole raccomandazioni (Salvaguardie) devono essere specifiche ed implementabili in modo pratico
- Misurabilità
  - Tutti i Controlli CIS, specialmente per il Gruppo Implementazione 1, devono essere misurabili
  - Semplificare o eliminare le ambiguità linguistiche per evitare interpretazioni non coerenti
  - Alcune Salvaguardie possono avere una soglia
- Allineamento
  - Creare e dimostrare una "convivenza pacifica" con altri regolamenti, amministrazioni, processi gestionali, frameworks e strutture
  - Cooperare puntando ad altri standard e raccomandazioni di sicurezza se esistenti ad esempio Istituto Nazionale degli Standard Tecnologici (NIST®), Cloud Security Alliance (CSA), Software Assurance Forum for Excellence in Code (SAFECode), ATT&CK, Open Web Application Security Project® (OWASP®)

Inoltre, dalla versione 7, abbiamo tutti assistito a cambiamenti significativi della tecnologia e dell'ecosistema della sicurezza informatica. Il passaggio al cloud computing, alla virtualizzazione, alla mobilità, all'outsourcing, al lavoro da casa e al cambiamento delle tattiche degli aggressori sono stati al centro di ogni discussione. I dispositivi fisici, i confini fissi e le isole felici di implementazione della sicurezza sono meno importanti e quindi riportiamo tutto questo nella Versione 8, attraverso la revisione della terminologia e il raggruppamento in Salvaguardie. Inoltre, per guidare gli utenti nell'implementazione della Versione 8, CIS ha creato un glossario per evitare ambiguità nella terminologia. Alcune idee sono state combinate o raggruppate differentemente per riflettere in modo più naturale l'evoluzione tecnologica, piuttosto che codificare l'organizzazione dei team o delle responsabilità aziendali, facendo sempre riferimento ai nostri principi guida.

Il testo del documento Controlli CIS è solo una fase di un processo per progettare, implementare, misurare, relazionare e gestire la sicurezza aziendale. Tenendo conto di questo intero flusso di lavoro mentre scriviamo i Controlli CIS, possiamo supportare l'intero processo di gestione aziendale: assicurandoci che ogni Salvaguardia richieda "una cosa", ove possibile, con chiarezza ed in modo che richieda un'interpretazione minima; concentrandoci su azioni misurabili e definendone la misurazione come parte del processo; semplificando il linguaggio per evitare ripetizioni.

In CIS, abbiamo sempre cercato di essere consapevoli nell'equilibrio tra l'affrontare temi attuali e la stabilità di un programma complessivo di miglioramento difensivo. Abbiamo sempre cercato di concentrarci sui fondamenti di una buona difesa informatica, tenendo d'occhio le nuove tecnologie difensive emergenti, evitando la "sindrome del giocattolo nuovo" o le tecnologie complesse fuori dalla portata della maggior parte delle aziende.

L'ecosistema dei Controlli CIS ("Non è solo un elenco")

Sia che utilizzi i Controlli CIS e/o un altro modo per condurre il tuo programma di miglioramento della sicurezza, dovresti riconoscere che "non è un problema di elenco». È possibile ottenere un elenco affidabile di consigli sulla sicurezza da molte fonti ma è meglio considerarlo come un punto di partenza. È importante osservare l'ecosistema che cresce intorno alla lista. Dove posso ottenere formazione, informazioni aggiuntive, spiegazioni; in che modo gli altri hanno implementato e utilizzato queste raccomandazioni; esiste un mercato di strumenti e servizi tra cui scegliere; come misurerò il progresso o la maturità; tutto questo come si allinea con la miriade norme e framework di conformità applicabili al mio caso? Il vero potere dei Controlli CIS non è quello di creare la lista migliore, bensì quello di sfruttare l'esperienza di una comunità di individui e imprese per apportare miglioramenti effettivi alla sicurezza attraverso la condivisione di idee, strumenti, lezioni e azioni collettive.

A sostengo di tutto questo, CIS agisce come catalizzatore e centro di coordinamento per aiutare tutti noi a imparare gli uni dagli altri. Dalla Versione 6, c'è stata un'esplosione di informazioni aggiuntive, prodotti e servizi messi a disposizione da CIS e dall'industria in generale. I materiali di supporto e vari aiuti per questo tipo di attività, sono disponibili nella pagina dedicata https://www.cisecurity.org/controls/v8/

- Mappatura dei Controlli CIS ad una vasta gamma di framework di gestione del rischio (tipo NIST®, Legge Federale di Modernizzazione della Sicurezza delle Informazioni–FISMA, Organizzazione Internazionale per la Standardizzazione–ISO, ecc.)
- Casi pratici di utilizzo in ambito aziendale
- Un elenco di riferimenti ai Controlli CIS negli standard nazionali e internazionali, nella legislazione e nei regolamenti statali e nazionali, nelle associazioni professionali e di categoria, ecc.
- Informazioni personalizzate per piccole e medie imprese
- Misure e metriche dei Controlli CIS
- Riferimenti a varie pagine informative dei rivenditori ed altri materiali a supporto dei Controlli CIS
- Documentazione riguardante l'allineamento al framework di sicurezza informatica NIST®

Come iniziare

Storicamente, i controlli CIS sono stati ordinati in sequenza per concentrare le attività di sicurezza informatica di un'azienda, con un sottoinsieme dei primi sei Controlli CIS denominato "igiene informatica". Tuttavia, questo si è dimostrato troppo semplicistico. Le aziende, specialmente quelle di piccole dimensioni, potevano incontrare difficoltà con alcune delle prime salvaguardie non riuscendo nell'implementazione dei Controlli CIS successivi (ad esempio, avere una strategia di backup per consentire il recupero dal ransomware). Di conseguenza, a partire dalla versione 7.1, abbiamo creato nei Controlli CIS i Gruppi di Implementazione (IG) come nuova guida consigliata per dare priorità all'implementazione.

I Gruppi di Implementazione dei Controlli CIS sono categorie di autovalutazione per le imprese. Ciascun IG identifica un sottoinsieme dei Controlli CIS che la comunità ha ampiamente valutato come applicabili a un'impresa con un profilo di rischio simile e con risorse disponibili per implementarli. Questi Gruppi di Implementazione rappresentano uno sguardo orizzontale che percorre i Controlli CIS organizzandoli su misura per diversi tipi di imprese. Nello specifico, abbiamo definito IG1 una "igiene informatica di base", l'insieme fondamentale delle garanzie di difesa informatica che ogni azienda dovrebbe applicare per proteggersi dagli attacchi più comuni (https://www.cisecurity.org/controls/v8/). Ciascun IG si basa quindi sul precedente: IG2 include IG1 e IG3 include tutte le salvaguardie CIS presenti in IG1 e IG2.

Utilizzo o Transizione dalla versione precedente dei Controlli CIS

Riteniamo che la Versione 8 dei Controlli CIS sia la migliore mai prodotta. Sappiamo inoltre che le aziende che utilizzano attivamente versioni precedenti dei Controlli CIS come parte fondamentale della loro strategia difensiva, potrebbero essere riluttanti a passare alla Versione 8. La nostra raccomandazione è che se si utilizza la Versione 7 o 7.1, si stia seguendo un piano di sicurezza efficace e utilizzabile e, nel tempo, si dovrebbe considerare la possibilità di passare alla Versione 8. Se si utilizza la versione 6 (o precedente), il consiglio e quello di iniziare a pianificare una transizione alla Versione 8 non appena possibile.

Per le versioni precedenti dei controlli CIS, siamo stati in grado di fornire solo gli strumenti più semplici per facilitare la transizione dalle versioni precedenti, fondamentalmente foglio di calcolo come registro delle modifiche intercorse. Per la Versione 8, abbiamo adottato un approccio molto più sinergico, lavorando con molti partner per garantire che l'ecosistema dei Controlli CIS sia pronto a supportare la transizione (https://www.cisecurity.org/controls/v8/).

Struttura dei Controlli CIS

La presentazione di ogni Controllo in questo documento include i seguenti elementi:

- **Panoramica:** Una breve descrizione degli obiettivi del Controllo e la sua utilità come azione difensiva
- **Perché questo controllo è importante?** Una descrizione della rilevanza del Controllo per bloccare, mitigare o identificare gli attacchi ed una spiegazione di come gli attaccanti possano effettivamente colpire in sua assenza
- **Procedure e strumenti:** Una descrizione tecnica dei processi e delle tecnologie che permettono l'implementazione e l'automazione del Controllo
- **Salvaguardie:** Una tabella di azioni specifiche che l'azienda dovrebbe applicare per implementare il Controllo

Profili

IG1

Un'impresa IG1 è di piccole o medie dimensioni con competenze IT e di sicurezza informatica limitate da dedicare alla protezione delle risorse e del personale. L'obiettivo principale di queste aziende è continuare ad essere operative, in quanto presentano una bassa tolleranza dei tempi di inattività. La sensibilità dei dati che proteggono è bassa e riguarda principalmente le informazioni finanziarie e dei dipendenti.

Le Salvaguardie previste in IG1 dovrebbero essere implementabili con limitate esperienze di sicurezza informatica e mirate a contrastare gli attacchi generici non mirati. Queste Salvaguardie sono in genere progettate per funzionare in combinazione con hardware e software commerciale (COTS) di piccoli uffici aziendali o domestici.

IG2 (Includes IG1)

Un'impresa IG2 impiega personale responsabile della gestione e della protezione dell'infrastruttura IT. Queste aziende supportano vari reparti con diversi profili di rischio in base alla funzione lavorativi e relativi obiettivi. Alcuni piccoli settori aziendali potrebbero avere anche obblighi di rispetto normativo. Le aziende IG2 spesso archiviano ed elaborano informazioni sensibili sui clienti o sull'azienda e possono sopportare brevi interruzioni del servizio. Una delle principali preoccupazioni è la perdita di credibilità in caso di violazione.

Le Salvaguardie previste in IG2 aiutano i team di sicurezza nel fronteggiare una maggiore complessità operativa. L'applicabilità delle Salvaguardie dipenderà dal livello tecnologico dell'azienda e dalle competenze disponibili, necessarie per le corrette installazioni e configurazioni.

IG3 (Includes IG1 and IG2)

Una azienda in IG3 impiega esperti di sicurezza specializzati nei vari aspetti della sicurezza informatica (es. gestione del rischio, test di penetrazione, sicurezza delle applicazioni). Le risorse e i dati in IG3 contengono informazioni sensibili o funzioni soggette a al rispetto normativo e di conformità. Un'impresa IG3 deve garantire la disponibilità dei servizi e la riservatezza ed integrità dei dati sensibili. Gli attacchi riusciti possono causare danni significativi ad un vasto pubblico.

Le Salvaguardie previste in IG3 devono ridurre drasticamente gli attacchi mirati di un avversario sofisticato e contenere l'impatto degli attacchi zero-day.

CONTROLLI 01

Inventario e Controllo delle Risorse Aziendali

SAFEGUARDS TOTAL	5	IG1	2/5	IG2	4/5	IG3	5/5

Panoramica

Gestire attivamente (inventariare, tracciare e correggere) tutte le risorse aziendali (dispositivi dell'utente finale, mobili e portatili inclusi, dispositivi di rete, dispositivi non informatici/ Internet of Things – IoT e server) connessi all'infrastruttura fisicamente, virtualmente, in remoto e quelli in ambienti cloud, per conoscere con precisione la totalità delle risorse che devono essere monitorate e protette in azienda. Ciò aiuterà anche nell'identificare quelle non autorizzate e non gestite, da rimuovere o aggiornare.

Perché questo controllo è importante?

Le aziende non possono difendere ciò che non sanno di avere. Il controllo gestito di tutte le risorse aziendali svolge anche un ruolo fondamentale nel monitoraggio della sicurezza, nella risposta agli incidenti, nel backup e ripristino del sistema. Le aziende dovrebbero sapere quali dati sono fondamentali per loro e una corretta gestione delle risorse aiuterà a identificare quelle che contengono o gestiscono questi dati critici, in modo che possano essere applicati i controlli di sicurezza più appropriati.

Gli aggressori esterni scansionano continuamente gli indirizzi Internet delle aziende target, siano essi in sede o nel cloud, identificando risorse potenzialmente non protette collegate alla rete aziendale. Gli aggressori possono sfruttare le nuove risorse installate, ma non ancora aggiornate e configurate in modo sicuro. Internamente, le risorse non identificate possono anche avere configurazioni di sicurezza deboli tali da renderle vulnerabili a malware basato su Web o e-mail; gli avversari possono sfruttare questi punti deboli per spostarsi nella rete, una volta entrati.

Altre risorse che si connettono alla rete aziendale (esempio sistemi dimostrativi, sistemi di test temporanei, reti ospiti) devono essere identificate e / o isolate per evitare che l'accesso di un avversario influisca sulla sicurezza delle operazioni aziendali.

Ovviamente le aziende grandi, complesse e dinamiche, devono affrontare la sfida della gestione di ambienti complessi ed in rapida evoluzione. Comunque, gli aggressori hanno dimostrato la capacità, la pazienza e la volontà di "inventariare e controllare" le nostre risorse aziendali su vasta scala per raggiungere i loro obiettivi.

Altra sfida è quella dei dispositivi portatili degli utenti finali che si collegheranno e disconnetteranno alla rete, rendendo dinamico l'inventario delle risorse in essere. Similmente, gli ambienti cloud e le macchine virtuali possono essere difficili da tracciare negli inventari delle risorse in caso di disattivazione o messa in pausa.

Un altro vantaggio della gestione completa delle risorse aziendali è il supporto in risposta agli incidenti, sia quando si indaga sull'origine del traffico di rete da una risorsa, sia quando si identificano le risorse simili per tipologia o collocazione, potenzialmente vulnerabili o interessate, durante un incidente.

Procedure e strumenti

Questo Controllo CIS richiede azioni tecniche e procedurali, unite in un processo che tenga conto e gestisca l'inventario delle risorse aziendali e di tutti i dati associati durante il suo ciclo di vita. Si collega inoltre all'amministrazione aziendale stabilendo proprietari di dati / risorse responsabili per ogni elemento di un processo aziendale. Le aziende possono utilizzare prodotti completi e professionali per mantenere gli inventari delle risorse IT. Le aziende più piccole possono sfruttare gli strumenti di sicurezza già installati sulle risorse aziendali o utilizzati sulla rete per raccogliere questi dati. Si includo l'esecuzione di una scansione di rilevamento della rete con uno scanner di vulnerabilità, il controllo dei log anti-malware, i log dei portali di sicurezza degli endpoint, i log di rete degli switch o i log di autenticazione; la gestione dei risultati può avvenire tramite un foglio di calcolo o utilizzando un database.

Mantenere una panoramica aggiornata e accurata delle risorse aziendali è un processo continuo e dinamico. Anche per le aziende, raramente esiste un'unica fonte certa, in quanto le risorse aziendali non sempre vengono fornite o installate dal reparto IT. La realtà è che una vasta gamma di informazioni deve essere reperita come "crowd-sourced" per determinare un inventario affidabile delle risorse aziendali. Le aziende possono scansionare attivamente e regolarmente, inviando vari tipi di pacchetti per identificare le risorse connesse alla rete. Oltre alle fonti di risorse valide per le piccole imprese, le aziende più grandi possono raccogliere dati da portali cloud e dai log delle piattaforme aziendali come: Active Directory (AD), Single Sign-On (SSO), Autenticazione Multi Fattore (MFA), Rete Privata Virtuale (VPN), Sistema di Rilevamento delle Intrusioni (IDS), Ispezione Approfondita dei Pacchetti (DPI), Gestione dei Dispositivi Mobili (MDM) e strumenti di scansione delle vulnerabilità. Database, sistemi di tracciamento degli ordini, elenchi di inventario locali, sono altre fonti di dati per determinare quali dispositivi siano collegati. Esistono strumenti e metodi che normalizzano i dati di queste fonti per identificare i dispositivi in modo univoco.

→ **Per una guida specifica dedicata al cloud si faccia riferimento al Cloud Companion di CIS Controls:** https://www.cisecurity.org/controls/v8/

→ **Per una guida specifica dedicata a tablet e smartphone si faccia riferimento al Mobile Companion di CIS Controls:** https://www.cisecurity.org/controls/v8/

→ **Per una guida specifica dedicata al IoT si faccia riferimento al Internet of Things Companion di CIS Controls:** https://www.cisecurity.org/controls/v8/

→ **Per una guida specifica dedicata ai Sistemi di Controllo Industriali, si faccia riferimento al ICS Implementation di CIS Controls:** https://www.cisecurity.org/controls/v8/

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
1.1	**Stabilire e Mantenere un Inventario Dettagliato delle Risorse Aziendali**	**Dispositivi**	**Identificare**	●	●	●
	Stabilire e mantenere un inventario accurato, dettagliato e aggiornato di tutte le risorse aziendali con la possibilità di archiviazione o elaborazione dati, includendo: dispositivi dell'utente finale (compresi portatili e mobili), dispositivi di rete, dispositivi non informatici/IoT e server. Assicurare che l'inventario registri l'indirizzo di rete (se statico), l'indirizzo hardware, il nome del computer, il proprietario della risorsa aziendale, il reparto per ogni risorsa e se la risorsa è stata approvata per la connessione alla rete. Per i dispositivi mobili degli utenti finali, gli strumenti di tipo MDM possono supportare questo processo. Questo inventario include le risorse connesse all'infrastruttura fisica, virtuale, remota e quelle all'interno di ambienti cloud. Include inoltre le risorse che sono regolarmente connesse all'infrastruttura di rete dell'impresa, anche se non sono sotto il suo controllo. Rivedere e aggiornare l'inventario di tutte le risorse aziendali semestralmente o più frequentemente.					
1.2	**Trattare le Risorse non Autorizzate**	**Dispositivi**	**Rispondere**	●	●	●
	Assicurare la presenza di un processo per trattare le risorse non autorizzate su base settimanale. L'azienda può scegliere di rimuovere la risorsa dalla rete, bloccarne la connessione remota o metterla in quarantena.					
1.3	**Utilizzare uno Strumento di Rilevamento Attivo**	**Dispositivi**	**Rilevare**		●	●
	Utilizzare uno strumento di rilevamento attivo per identificare le risorse connesse alla rete aziendale. Configurarlo per l'esecuzione quotidiana o più frequente.					
1.4	**Utilizzare i log del Protocollo Dinamico di Configurazione Host (DHCP)**	**Dispositivi**	**Identificare**		●	●
	Utilizzare i log su tutti i server DHCP o altri strumenti di gestione degli indirizzi IP (Internet Protocol) per aggiornare l'inventario delle risorse aziendali. Rivedere ed utilizzare i registri per aggiornare l'inventario delle risorse settimanalmente o più frequentemente.					
1.5	**Utilizzare uno Strumento di Rilevazione Passiva**	**Dispositivi**	**Rilevare**			●
	Utilizzare uno strumento di rilevazione passiva per identificare le risorse connesse alla rete aziendale. Rivedere e utilizzare le scansioni per aggiornare l'inventario delle risorse almeno una volta alla settimana o più frequentemente.					

CONTROLLI 02

Inventario e Controllo delle Risorse Software

SAFEGUARDS TOTAL	7	IG1	3/7	IG2	6/7	IG3	7/7

Panoramica

Gestire attivamente (inventariare, tracciare e correggere) tutto il software (sistemi operativi e applicazioni) sulla rete in modo che solo il software autorizzato possa essere installato ed eseguito e che il software non autorizzato e non gestito venga trovato impedendone l'installazione o l'esecuzione.

Perché questo controllo è importante?

Un inventario software completo è una base fondamentale per prevenire gli attacchi. Gli aggressori scansionano continuamente le aziende bersaglio cercando versioni vulnerabili di software che possono essere sfruttate da remoto. Ad esempio, se un utente apre un sito Web o un allegato dannoso con un browser vulnerabile, un malintenzionato può spesso installare programmi e bot backdoor che consentono il controllo del sistema a lungo termine. Gli aggressori possono anche utilizzare questo accesso per spostarsi lateralmente attraverso la rete. Una delle principali difese contro questi attacchi è l'aggiornamento e l'applicazione di patch al software. Comunque, senza un inventario completo delle risorse software, un'azienda non può determinare se esse siano vulnerabili o se siano presenti potenziali violazioni delle licenze.

Anche se una patch non è ancora disponibile, un inventario completo del software consente ad un'azienda di proteggersi dagli attacchi noti fino al rilascio della patch. Alcuni aggressori sofisticati utilizzano gli "exploit zero-day," che sfruttano vulnerabilità precedentemente sconosciute e che devono ancora ricevere una patch rilasciata dal fornitore del software. In funzione della gravità dell'exploit, un'azienda può implementare misure di mitigazione temporanee per proteggersi dagli attacchi fino al rilascio della patch.

La gestione delle risorse software è importante anche per identificare i rischi superflui per la sicurezza. Un'azienda dovrebbe aggiornare il proprio inventario software per identificare eventuali risorse aziendali che eseguano software non necessario. Ad esempio, una dotazione aziendale può essere installata con un software predefinito in grado di generare un potenziale rischio per la sicurezza senza fornire alcun vantaggio. È fondamentale inventariare, capire, valutare e gestire tutto il software connesso all'infrastruttura di un'impresa.

Procedure e strumenti

Un elenco delle autorizzazioni può essere implementato utilizzando la combinazione di strumenti commerciali, criteri o strumenti di esecuzione delle applicazioni forniti con le suite anti-malware e i sistemi operativi più diffusi. Attualmente i software commerciali di inventario sono ampiamente disponibili e utilizzati in molte aziende. Il migliore di questi strumenti fornisce un controllo dell'inventario di centinaia di software comuni utilizzati nelle aziende. Gli strumenti raccolgono informazioni sul livello di patch di ciascun programma installato per garantire che si tratti della versione più recente sfruttando i nomi delle applicazioni standardizzati, come quelli trovati nel Sistema Strutturato di Nomenclatura (CPE). Un esempio di un metodo che può essere utilizzato è il Protocollo di Automazione dei Contenuti di Sicurezza (SCAP). Ulteriori informazioni sono disponibili al link https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf

Le funzionalità che implementano le liste di autorizzazione consentite sono incluse in molte moderne suite di sicurezza degli endpoint ed anche implementate in modo nativo in alcune versioni dei principali sistemi operativi. Inoltre, le soluzioni commerciali combinano sempre più soluzioni anti-malware, anti-spyware, firewall personali e IDS basati sugli host e sistemi di prevenzione delle intrusioni (IPS), unitamente all'elenco delle applicazioni consentite o bloccate. In particolare, molte soluzioni per la sicurezza degli endpoint possono esaminare il nome, la posizione nel file system e/o l'hash crittografico di un eseguibile per determinare se l'applicazione possa essere autorizzata a funzionare sulla macchina protetta. Il più efficace di questi strumenti offre liste consentite personalizzabili basate sui percorsi eseguibili, hash o sulla corrispondenza delle espressioni di controllo. Alcuni includono anche una funzione applicativa non dannosa, ma non approvata, che consente agli amministratori di definire regole per l'esecuzione di software specifiche per determinati utenti e in determinate ore del giorno.

- **Per una guida specifica dedicata al cloud si faccia riferimento al Cloud Companion di CIS Controls:** https://www.cisecurity.org/controls/v8/
- **Per una guida specifica dedicata a tablet e smartphone si faccia riferimento al Mobile Companion di CIS Controls:** https://www.cisecurity.org/controls/v8/
- **Per una guida specifica dedicata al IoT si faccia riferimento al Internet of Things Companion di CIS Controls:** https://www.cisecurity.org/controls/v8/
- **Per una guida specifica dedicata ai Sistemi di Controllo Industriali, si faccia riferimento al ICS Implementation di CIS Controls:** https://www.cisecurity.org/controls/v8/

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
2.1	**Stabilire e Mantenere un Inventario Software** Stabilire e mantenere un inventario dettagliato di tutto il software con licenza installato sulle risorse aziendali. L'inventario del software deve documentare il titolo, l'editore, la data di installazione/utilizzo iniziale e la sua finalità; se opportuno, includere URL, app store, versione(i), distribuzione e data di disattivazione. Rivedere e aggiornare l'inventario del software semestralmente o più frequentemente.	Applicazioni	Identificare	●	●	●
2.2	**Accertare il Supporto del Software Autorizzato** Assicurare che solo il software attualmente supportato sia individuato come autorizzato nell'inventario software delle risorse aziendali. Se il software non è supportato, ma è necessario per gli scopi aziendali, documentare un'eccezione che riporti la mitigazione dei controlli l'accettabilità del rischio residuo. Qualsiasi software non supportato privo di documentazione di eccezione, deve essere indicato come non autorizzato. Rivedere l'elenco del software per verificarne il supporto almeno mensilmente o più frequentemente.	Applicazioni	Identificare	●	●	●
2.3	**Trattare il Software non Autorizzato** Assicurare che il software non autorizzato venga rimosso dalle risorse aziendali o riceva un'eccezione documentata. Rivedere mensilmente o più frequentemente.	Applicazioni	Rispondere	●	●	●
2.4	**Utilizzare Strumenti Automatici per l'Inventario del Software** Utilizzare strumenti di inventario del software, quando possibile, in tutta l'azienda per automatizzare l'individuazione e la documentazione del software installato.	Applicazioni	Rilevare		●	●
2.5	**Elenco del Software Consentito** Utilizzare i controlli tecnici, come l'elenco delle applicazioni autorizzate, per garantire che solo il software consentito possa essere accessibile o eseguibile Aggiornare semestralmente o più frequentemente.	Applicazioni	Proteggere		●	●
2.6	**Elenco delle Librerie Consentite** Utilizzare controlli tecnici per garantire che solo le specifiche librerie software autorizzate, come file .dll, .ocx, .so, ecc., possano essere caricate in un processo di sistema. Impedire il caricamento delle librerie non autorizzate in un processo di sistema. Rivalutare semestralmente o più frequentemente.	Applicazioni	Proteggere		●	●
2.7	**Elenco degli Script Consentiti** Utilizzare controlli tecnici, come le firme digitali e controllo di versione, per garantire che solo gli script autorizzati, come file .ps1, .py, ecc., possano essere eseguiti. Impedire l'esecuzione di script non autorizzati. Rivalutare semestralmente o più frequentemente.	Applicazioni	Proteggere			●

CONTROLLI 03

Protezione dei Dati

SAFEGUARDS TOTAL	14	IG1	6/14	IG2	12/14	IG3	14/14

Panoramica

Sviluppare processi e controlli tecnici per identificare, classificare, elaborare in sicurezza, conservare ed eliminare i dati.

Perché questo controllo è importante?

I dati non sono più contenuti solo all'interno dei confini aziendali; sono in cloud, sui dispositivi portatili degli utenti finali utilizzati per il lavoro da casa, spesso in condivisione con partner o servizi online che potrebbero trovarsi in qualsiasi parte del mondo. Oltre ai dati sensibili aziendali riguardanti aspetti finanziari, proprietà intellettuale, dati dei clienti, potrebbero esserci anche numerose normative internazionali per la protezione dei dati personali da rispettare. La riservatezza dei dati è diventata sempre più importante e le aziende stanno imparando che la privacy riguarda l'uso e la gestione appropriata dei dati, non solo la crittografia. I dati devono essere gestiti in modo appropriato durante l'intero ciclo di vita. Queste regole sulla privacy possono essere complicate per le imprese multinazionali di qualsiasi dimensione; tuttavia, esistono elementi fondamentali che possono essere sempre applicati.

Quando gli aggressori sono penetrati nell'infrastruttura aziendale, una delle prime attività è trovare ed esfiltrare i dati. Le aziende potrebbero non essere consapevoli che i dati sensibili stanno lasciando il loro ambiente perché non monitorano i flussi dei dati in uscita.

Mentre molti attacchi avvengono sulla rete, altri comportano il furto fisico dei dispositivi portatili dell'utente finale oppure colpiscono i fornitori di servizi o altri partner che detengono dati sensibili. Altre risorse aziendali sensibili possono inoltre includere i dispositivi non informatici di gestione e controllo dei sistemi fisici, come i sistemi SCADA (Controllo di Supervisione e Acquisizione Dati).

La perdita di controllo da parte dell'azienda sui dati protetti o sensibili provoca un impatto importante serio e spesso rilevante. Mentre alcuni dati vengono compromessi o persi a causa di furto o spionaggio, la grande maggioranza è il risultato di errori dell'utente e di regole di gestione dei dati poco comprese. L'adozione della crittografia dei dati, sia in transito che a riposo, può fornire una mitigazione contro la compromissione dei dati e, cosa ancora più importante, spesso si tratta di un requisito normativo applicabile alla maggior parte dei dati controllati.

Procedure e Strumenti

È importante che l'azienda sviluppi un processo di amministrazione dei dati che includa un framework di gestione, linee guida di classificazione, requisiti di protezione, gestione, conservazione ed eliminazione. Dovrebbe esserci anche una procedura in caso di violazione dei dati che si inserisca nel piano di risposta agli incidenti e nei piani di conformità e comunicazione. Per determinare i livelli di sensibilità dei dati, le aziende devono catalogare i loro tipi chiave di dati definendone la criticità complessiva (impatto sulla loro perdita o danneggiamento). Questa analisi dovrebbe essere utilizzata per creare uno schema generale di classificazione dei dati per l'impresa. Le aziende possono utilizzare etichette, come "Sensibile", "Riservato" e "Pubblico" per classificare le informazioni in base a questi elementi.

Una volta definita la sensibilità dei dati, è necessario creare un inventario o una mappatura che identifichi il software che vi accede, i vari livelli di sensibilità nonché le risorse aziendali che ospitano tali applicazioni. Idealmente, la rete dovrebbe essere separata in modo che le risorse aziendali dello stesso livello di sensibilità si trovino sulla stessa rete e di conseguenza separate dalle altre risorse aziendali (con diversi livelli di sensibilità). Se possibile, i firewall dovrebbero controllare l'accesso a ciascun segmento applicando regole agli utenti per autorizzare solo a chi ne abbia l'esigenza.

Per un approfondimento su questo argomento, si suggeriscono le seguenti risorse che possono aiutare l'azienda nel processo di protezione dei dati

- **NIST® SP 800-88r1 Linee Guida per la Sanificazione dei Media:** https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
- **NIST® FIPS 140-2:** https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
- **NIST® FIPS 140-3:** https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf
- **Per una guida specifica dedicata al cloud si faccia riferimento al Cloud Companion di CIS Controls:** https://www.cisecurity.org/controls/v8/
- **Per una guida specifica dedicata a tablet e smartphone si faccia riferimento al Mobile Companion di CIS Controls:** https://www.cisecurity.org/controls/v8/

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
3.1	**Stabilire e Mantenere una Procedura di Gestione dei Dati** Stabilire e mantenere una procedura di gestione dei dati. Considerarne la sensibilità, il proprietario, la gestione, i limiti di conservazione e i requisiti di rimozione, in base agli standard aziendali di riservatezza e conservazione. Rivedere e aggiornare la documentazione ogni anno o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.	Dati	Identificare	●	●	●
3.2	**Stabilire e Mantenere un Inventario dei Dati** Stabilire e mantenere un inventario dei dati, basato sulla procedura di gestione aziendale dei dati. Inventariare come minimo i dati sensibili. Rivedere e aggiornare l'inventario almeno una volta all'anno, dando priorità a quest'ultimi.	Dati	Identificare	●	●	●
3.3	**Configurare le Liste di Controllo degli Accessi** Configurare le liste di controllo degli accessi ai dati in base alle esigenze di conoscenza di un utente. Utilizzare queste liste, note anche come permessi di accesso, a file system locali e remoti, database e applicazioni	Dati	Proteggere	●	●	●

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
3.4	**Determinare la Conservazione dei Dati**	Dati	Proteggere	●	●	●
	Conservare i dati secondo la procedura aziendale di gestione dei dati. La conservazione dei dati deve includere tempi minimi e massimi.					
3.5	**Rimozione Sicura dei Dati**	Dati	Proteggere	●	●	●
	Eliminare i dati in modo sicuro secondo la procedura aziendale di gestione dei dati Assicurare che il processo ed il metodo di eliminazione siano commisurati alla loro sensibilità.					
3.6	**Crittografare i Dati sui Dispositivi degli Utenti Finali**	Dispositivi	Proteggere	●	●	●
	Crittografare i dati sui dispositivi degli utenti finali contenenti dati sensibili. Le implementazioni possono includere ad esempio: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.					
3.7	**Stabilire e Mantenere un Sistema di Classificazione dei Dati**	Dati	Identificare		●	●
	Stabilire e mantenere uno schema generale di classificazione dei dati aziendali. Le aziende possono utilizzare etichette, come “Sensibile”, “Riservato” e “Pubblico” per classificare i propri dati in base a tali elementi. Rivedere e aggiornare lo schema di classificazione annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.					
3.8	**Documentare il Flusso dei Dati**	Dati	Identificare		●	●
	Documentare il flusso dei dati. La documentazione include i flussi di dati dei fornitori di servizi e dovrebbe essere basata sulla procedura gestionale dei dati aziendali Rivedere e aggiornare la documentazione ogni anno o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.					
3.9	**Crittografare i Dati sui Media Rimovibili**	Dati	Proteggere		●	●
	Crittografare i dati sui media rimovibili.					
3.10	**Crittografare i Dati Sensibili in Transito**	Dati	Proteggere		●	●
	Crittografare i dati in transito. Esempi di implementazione includono: Transport Layer Security (TLS) e Open Secure Shell (OpenSSH).					
3.11	**Crittografare i Dati Sensibili a Riposo**	Dati	Proteggere		●	●
	Crittografare i dati sensibili a riposo su server, applicazioni e database. La crittografia a livello di archiviazione, nota anche come crittografia lato server, soddisfa i requisiti minimi di questa Salvaguardia. Ulteriori metodi di crittografia possono includere quella a livello di applicazione, nota anche come crittografia lato client, in cui l’accesso ai dispositivi di archiviazione non permette l’accesso ai dati in chiaro					
3.12	**Segmentare Elaborazione ed Archiviazione dei Dati secondo la Sensibilità**	Rete	Proteggere		●	●
	Segmentare elaborazione ed archiviazione dei dati in base alla sensibilità. Non elaborare dati sensibili utilizzando risorse aziendali predisposte per livelli inferiori di sensibilità.					
3.13	**Adottare una Soluzione per la Prevenzione della Perdita dei Dati**	Dati	Proteggere			●
	Implementare uno strumento automatizzato, di prevenzione della perdita di dati (DLP) basato su host, per identificare tutti i dati sensibili archiviati, elaborati o trasmessi attraverso le risorse aziendali, compresi quelli in locale o presso un fornitore di servizi remoto, aggiornando l’inventario dei dati sensibili.					
3.14	**Mantenere un Log di Accesso ai Dati Sensibili**	Dati	Rilevare			●
	Mantenere un log che registri l’accesso ai dati sensibili, inclusa la loro modifica e l’eliminazione.					

CONTROLLI 04

Configurazione Sicura delle Risorse Aziendali e del Software

SAFEGUARDS TOTAL	12	IG1	7/12	IG2	11/12	IG3	12/12

Panoramica

Stabilire e mantenere la configurazione sicura delle risorse aziendali (dispositivi dell'utente finale, inclusi portatili e mobili, dispositivi di rete, dispositivi non informatici / IoT, server) e software (sistemi operativi e applicazioni).

Perché questo controllo è importante?

Così come fornite da produttori e rivenditori, le configurazioni predefinite per risorse e software aziendali sono normalmente orientate alla facilità di implementazione e di utilizzo piuttosto che alla sicurezza. Controlli di base, servizi e porte aperte, account o password predefiniti, impostazioni DNS (Sistema dei Nomi di Dominio) predefinite, protocolli meno recenti (vulnerabili) e preinstallazione di software non necessario possono essere tutti sfruttabili se mantenuti con valori di default. Inoltre, questi aggiornamenti della configurazione della sicurezza devono essere gestiti e mantenuti durante l'intero ciclo di vita delle risorse e dei software aziendali. Gli aggiornamenti della configurazione devono essere tracciati e approvati attraverso la gestione del flusso di lavoro di delle configurazioni per mantenere una valida traccia che può essere rivista per la conformità, sfruttata per la risposta agli incidenti e per supportare gli audit. Questo Controllo CIS è importante sia per i dispositivi locali sia per quelli remoti, per i dispositivi di rete e per gli ambienti cloud.

I fornitori di servizi svolgono un ruolo chiave nelle infrastrutture moderne, specialmente per le piccole imprese. Spesso però non sono impostati di default nella configurazione più sicura, al fine di fornire una certa flessibilità ai clienti perché possano applicare i loro criteri di sicurezza. Pertanto, la presenza di account o password predefiniti, accessi diffusi o servizi non necessari sono frequenti nelle configurazioni predefinite. Questo potrebbe generare punti deboli direttamente attribuibili all'azienda che utilizza il software, piuttosto che al fornitore di servizi. Ciò si estende alla gestione degli aggiornamenti, in quanto alcuni sistemi Platform as a Service (PaaS) coinvolgono solo il sistema operativo, mentre l'applicazione di patch e l'aggiornamento delle applicazioni ospitate rimane sotto la responsabilità dell'azienda.

Anche se una configurazione iniziale affidabile è stata sviluppata e applicata, deve essere continuamente gestita per evitare il decadimento del livello di sicurezza quando il software viene aggiornato o corretto, quando vengono segnalate nuove vulnerabilità di sicurezza e quando le configurazioni vengono modificate per consentire l'installazione di nuovo software o supportare nuove esigenze operative.

Procedure e strumenti

Ci sono molti criteri standard di sicurezza disponibili per ogni sistema. Le aziende dovrebbero iniziare con questi benchmark, guide di sicurezza ed elenchi di controlli che sono sviluppati pubblicamente, controllati e supportati. Alcune risorse includono:

- **Il Programma CIS Benchmark™:** http://www.cisecurity.org/cis-benchmarks/
- **L'Istituto Nazionale degli Standard Tecnologici (NIST®) Archivio Nazionale delle Checklist:** https://nvd.nist.gov/ncp/repository

Le aziende dovrebbero aumentare o adeguare questi criteri di base per soddisfare le politiche di sicurezza aziendale e i requisiti normativi settoriali e governativi. Le deviazioni dai criteri standard delle configurazioni dovrebbero essere documentate per facilitare revisioni o audit futuri.

Per un'impresa più grande o più complessa, saranno disponibili più configurazioni di base della sicurezza in funzione dei requisiti o alla classificazione dei dati presenti sulle risorse aziendali. Ecco un esempio dei passaggi per creare un'immagine di base sicura:

01 Determinare una classificazione del rischio dei dati gestiti / memorizzati sulla risorsa aziendale (es. rischio alto, moderato, basso).

02 Creare uno script di configurazione della sicurezza che definisca le impostazioni di sicurezza del sistema per soddisfare i requisiti di protezione dei dati utilizzati sulla risorsa aziendale. Utilizzare benchmark, come quelli descritti in precedenza in questa sezione.

03 Installare il software del sistema operativo di base.

04 Applicare le patch di sicurezza del sistema operativo.

05 Installare le applicazioni software, strumenti ed utilità varie.

06 Applicare gli aggiornamenti al software installato al punto 4.

07 Installare gli script di personalizzazione a questa immagine.

08 Eseguire lo script di sicurezza creato al punto 2 per applicare il dovuto livello di sicurezza.

09 Eseguire uno strumento di conformità SCAP per registrare / valutare l'impostazione di sistema dell'immagine di base.

10 Eseguire un test per garantire il livello di qualità della sicurezza.

11 Salvare l'immagine di base in un luogo sicuro.

È possibile utilizzare strumenti di gestione della configurazione commerciali o gratuiti, come il Modello CIS di Valutazione della Configurazione (CIS-CAT®) https://learn.cisecurity.org/cis-cat-lite, per valutare le impostazioni dei sistemi operativi e delle applicazioni dei computer gestiti per cercare deviazioni dalle configurazioni delle immagini standard. Gli strumenti commerciali di gestione della configurazione utilizzano una combinazione di un "agent" installato su ciascun sistema gestito oppure l'analisi dei sistemi senza "agent", tramite l'accesso remoto a ciascuna risorsa aziendale con l'utilizzo di credenziali amministrative. Inoltre, a volte viene utilizzato una modalità ibrida in base alla quale viene avviata una sessione remota, distribuito un "agent" temporaneo o dinamico sul sistema di destinazione, che poi viene rimosso dopo la scansione.

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
4.1	**Stabilire e Mantenere una Procedura di Configurazione Sicura** Stabilire e mantenere una procedura di configurazione sicura per le risorse aziendali (dispositivi dell'utente finale inclusi portatili e mobili, dispositivi non informatici / IoT) e per il software (sistemi operativi ed applicazioni). Rivedere e aggiornare la documentazione annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.	Applicazioni	Proteggere	●	●	●
4.2	**Stabilire e Mantenere una Procedura di Configurazione Sicura per l'Infrastruttura di Rete** Stabilire e mantenere una procedura di configurazione sicura per i dispositivi di rete. Rivedere e aggiornare la documentazione annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.	Rete	Proteggere	●	●	●
4.3	**Configurare il Blocco Automatico della Sessione sulle Risorse Aziendali** Configurare il blocco automatico della sessione sulle risorse aziendali dopo un periodo di inattività definito. Per i sistemi operativi generici, il periodo non deve superare i 15 minuti. Per i dispositivi mobili dell'utente finale, il periodo non deve superare i 2 minuti.	Utenti	Proteggere	●	●	●
4.4	**Implementare e Gestire un Firewall sui Server** Implementare e gestire un firewall sui server, quando supportato. Esempi di implementazione includono un firewall virtuale, un firewall del sistema operativo o un agent firewall di terze parti.	Dispositivi	Proteggere	●	●	●
4.5	**Implementare e Gestire un Firewall sui Dispositivi dell'Utente Finale** Implementare e gestire un firewall basato su host o uno strumento di filtraggio delle porte sui dispositivi degli utenti finali, con una regola predefinita di negazione che elimina tutto il traffico ad eccezione di porte e servizi esplicitamente consentiti.	Dispositivi	Proteggere	●	●	●
4.6	**Gestire in modo Sicuro Risorse e Software Aziendali** Gestire in modo sicuro risorse e software aziendali. Esempi di implementazione includono la gestione della configurazione tramite il controllo di versione dell'infrastruttura tramite codice e l'accesso alle interfacce amministrative utilizzando protocolli di rete sicuri, come Secure Shell (SSH) e Protocollo di trasferimento Ipertestuale Sicuro (HTTPS). Non utilizzare protocolli di gestione non sicuri, come Telnet (Teletype Network) e HTTP, a meno che non siano essenziali dal punto di vista operativo.	Rete	Proteggere	●	●	●
4.7	**Gestire gli Account Predefiniti di Risorse e Software Aziendali** Gestire gli account predefiniti di risorse e software aziendali, come root, amministratore e altri account preconfigurati rilasciati dal fornitore. Esempi di implementazione includono: disabilitare o rendere inutilizzabili gli account predefiniti.	Utenti	Proteggere	●	●	●
4.8	**Disinstallare o Disabilitare Servizi e Software non Necessari sulle Risorse Aziendali** Disinstallare o disabilitare servizi e software non necessari sulle risorse aziendali, come un servizio di condivisione file inutilizzato, un modulo di applicazione Web o una funzione di servizio.	Dispositivi	Proteggere		●	●
4.9	**Configurare Server DNS Sicuri sulle Risorse Aziendali** Configurare server DNS sicuri sulle risorse aziendali. Esempi di implementazione includono: configurazione delle risorse affinché utilizzino server DNS controllati dall'azienda o accesso a server DNS esterni affidabili.	Dispositivi	Proteggere		●	●
4.10	**Abilitare il Blocco Automatico sui Dispositivi Portatili dell'Utente Finale** Abilitare il blocco automatico del dispositivo portatile dell'utente finale dopo una soglia stabilita di tentativi di autenticazione non riusciti, ove supportato. Per i laptop, non consentire più di 20 tentativi di autenticazione falliti; per tablet e smartphone, non più di 10. Esempi di implementazione includono: Microsoft® InTune Device Lock e Apple® Configuration Profile maxFailedAttempts.	Dispositivi	Rispondere		●	●
4.11	**Abilitare la Cancellazione da Remoto sui Dispositivi Portatili dell'Utente Finale** Cancellare da remoto i dati aziendali dai dispositivi portatili di proprietà dell'utente finale quando è necessario, ad esempio dispositivi smarriti o rubati, o quando una persona lascia l'azienda.	Dispositivi	Proteggere		●	●
4.12	**Separare gli Spazi di Lavoro Aziendali sui Dispositivi Portatili dell'Utente Finale** Assicurare che gli spazi di lavoro aziendali sui dispositivi mobili degli utenti finali siano separati, ove supportato. Esempi di implementazione includono: l'utilizzo di Apple® Configuration Profile, Android™ Work Profile per separare applicazioni e dati aziendali da quelli personali.	Dispositivi	Proteggere			●

CONTROLLI 05

Gestione degli Account

SAFEGUARDS TOTAL	6	IG1	4/6	IG2	6/6	IG3	6/6

Panoramica

Utilizzare procedure e strumenti per assegnare e gestire l'autorizzazione delle credenziali a risorse e software aziendali, per gli account utente, inclusi quelli amministrativi e di servizio.

Perché questo controllo è importante?

È più facile per un malintenzionato esterno o interno ottenere l'accesso non autorizzato alle risorse o ai dati aziendali utilizzando credenziali utente valide piuttosto che "hackerando" l'ambiente. Esistono molti modi per ottenere in modo furtivo l'accesso agli account utente, tra cui: password deboli, account attivi di un utente che lascia l'azienda, account di prova inattivi o persistenti, account condivisi non modificati da mesi o anni, account di servizio incorporati nelle applicazioni per gli script, utenti che usano la stessa password per un account online compromesso (dump pubblico di password), social engineering finalizzato al rilascio della password o uso di malware per acquisire password o token in memoria o sulla rete.

Gli account amministrativi o con privilegi elevati sono un obiettivo particolare, perché consentono agli aggressori di aggiungere altri account o modificare le risorse per renderle più vulnerabili ad altri attacchi. Anche gli account di servizio sono sensibili, poiché sono spesso condivisi tra i team, interni ed esterni all'azienda, e talvolta non censiti, che vengono poi scoperti negli audit di gestione degli account.

Infine, la registrazione e il monitoraggio degli account sono una componente fondamentale delle operazioni di sicurezza. Sebbene siano trattati nei Controlli CIS 8 (Gestione dei Log di Controllo), sono importanti nello sviluppo di un programma completo di Gestione degli Accessi e delle Identità (IAM).

Procedure e strumenti

Le credenziali sono risorse che devono essere inventariate e tracciate come le risorse e software aziendali, poiché sono il punto di ingresso principale nell'azienda. Dovrebbero essere sviluppati criteri di password appropriati e linee guida per non riutilizzarle. Per indicazioni sulla creazione e l'utilizzo delle password, si faccia riferimento alla Guida ai Criteri delle Password di CIS: https://www.cisecurity.org/white-papers/cis-password-policy-guide/.

Anche gli account devono essere tracciati; tutti gli account inattivi devono essere disabilitati ed eventualmente rimossi dal sistema. Si dovrebbero effettuare controlli periodici per garantire che tutti gli account attivi siano riconducibili ad utenti autorizzati alle risorse aziendali. Cercare i nuovi account aggiunti in seguito

alla precedente revisione, in particolare gli account amministrativi e di servizio. Occorre prestare molta attenzione per identificare e tenere traccia degli account amministrativi, privilegiati e di servizio.

Gli utenti con accesso amministrativo o altri privilegiati dovrebbero avere account separati per le attività che richiedono livelli autorizzativi superiori. Questi account dovrebbero essere utilizzati solo durante l'esecuzione di tali attività o per l'accesso a dati particolarmente sensibili, per ridurre il rischio nel caso in cui l'account solitamente usato venga compromesso. Per gli utenti con più account, quello di base, utilizzato quotidianamente per attività non amministrative, non dovrebbe avere alcun privilegio elevato.

Il Single Sign-On (SSO) è comodo e sicuro quando un'azienda dispone di molte applicazioni, comprese quelle cloud, in quanto permette una riduzione del numero di password gestite da un utente. Si consiglia agli utenti di utilizzare applicazioni di gestione delle password per archiviarle in modo sicuro ma dovrebbero ricevere anche istruzioni chiare per non conservarle in fogli di calcolo o file di testo sui propri computer. Per l'accesso remoto si consiglia l'autenticazione MFA.

Gli utenti devono inoltre essere disconnessi automaticamente dal sistema dopo un periodo di inattività ed istruiti per bloccare lo schermo quando lasciano il dispositivo al fine di ridurre al minimo la possibilità che qualcun altro nelle vicinanze acceda ai loro sistemi, alle applicazioni e ai dati.

→ **Ottime Risorse NIST® sono le Linee Guida all'Identità Digitale:** https://pages.nist.gov/800-63-3/.

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
5.1	**Stabilire e Mantenere un Inventario degli Account**	Utenti	Identificare	●	●	●
	Stabilire e mantenere un inventario di tutti gli account aziendali. L'inventario deve includere account utenti e amministrativi. L'inventario, dovrebbe contenere almeno il nome della persona, il nome utente, le date di inizio/fine e l'area lavorativa. Assicurare che tutti gli account attivi siano autorizzati, con una pianificazione almeno trimestrale o più frequentemente.					
5.2	**Utilizzare Password Univoche**	Utenti	Proteggere	●	●	●
	Utilizzare password univoche per tutte le risorse aziendali. L'implementazione delle "best practice" prevede, come minimo, una password di 8 caratteri per gli account che utilizzano l'autenticazione multi fattore e una password di 14 caratteri per gli account che non la prevedono.					
5.3	**Disabilitare gli Account Dormienti**	Utenti	Rispondere	●	●	●
	Cancellare o disabilitare tutti gli account dormienti dopo un periodo di 45 giorni di inattività, quando supportato.					
5.4	**Limitare i Privilegi Amministrativi agli Account dell'Amministratore**	Utenti	Proteggere	●	●	●
	Limitare i privilegi amministrativi agli account di amministratore riservati alle risorse aziendali. Effettuare attività informatiche generali, navigazione in Internet, posta elettronica ed uso delle suite di produttività, da un account utente non privilegiato.					
5.5	**Stabilire e Mantenere un Inventario degli Account di Servizio**	Utenti	Identificare		●	●
	Stabilire e mantenere un inventario degli account di servizio. L'inventario, deve contenere almeno il referente dell'area lavorativa, data di revisione e scopo. Eseguire revisioni degli account di servizio per verificare che tutti quelli attivi siano autorizzati, con una pianificazione ricorrente almeno trimestrale o più frequentemente.					
5.6	**Centralizzare la Gestione degli Account**	Utenti	Proteggere		●	●
	Centralizzare la gestione degli account con un servizio di directory o identità.					

CONTROLLI 06

Gestione del Controllo degli Accessi

SAFEGUARDS TOTAL	8	IG1	5/8	IG2	7/8	IG3	8/8

Panoramica

Utilizzare processi e strumenti per creare, assegnare, gestire e revocare credenziali di accesso e privilegi per gli account utenti, amministratori, di servizio per le risorse e i software aziendali.

Perché questo controllo è importante?

Mentre i Controlli CIS 5 si occupano specificamente della gestione degli account, i Controlli CIS 6 si concentrano sulla gestione dell'accesso di questi ultimi, garantendo che gli utenti abbiano l'autorizzazione solo ai dati o alle risorse aziendali necessari per il loro ruolo e garantendo che sia presente un'autenticazione di tipo forte per funzioni o dati di particolare sensibilità o criticità. Gli account dovrebbero avere solo l'autorizzazione minima necessaria per il ruolo. Definire diritti di accesso coerenti per ogni ruolo ed assegnarli ai singoli utenti è una best practice. È importante anche lo sviluppo di una procedura di conferimento e revoca degli accessi. Centralizzare questa funzione è l'ideale.

Esistono alcune attività degli utenti che rappresentano un rischio maggiore per l'azienda, sia per la possibilità di accesso da reti mobili non sicure, sia per lo svolgimento di funzioni amministrative che consentono aggiunta, modifica, rimozione di altri account sia pe la modifica della configurazione dei sistemi operativi o delle applicazioni rendendoli meno sicuri. Ciò rafforza anche l'importanza di utilizzare gli strumenti MFA e di Gestione degli Accessi Privilegiati (PAM).

Alcuni utenti hanno accesso a risorse aziendali o dati di cui non necessitano per il loro ruolo; ciò potrebbe essere dovuto a una procedura generalizzata che concede a tutti gli utenti gli accessi o a un accesso prolungato nel tempo, anche quando gli utenti cambiano ruolo all'interno dell'azienda. Inoltre i privilegi di amministratore locale sui laptop degli utenti sono un problema, in quanto qualsiasi codice dannoso installato o scaricato dall'utente, può avere un impatto maggiore sulle risorse aziendali quando eseguito come amministratore. L'accesso di utenti, amministratori e account di servizio, deve essere basato sul ruolo e sulle esigenze aziendali.

Procedure e strumenti

Dovrebbe essere previsto una procedura in cui i privilegi vengano concessi e revocati per gli account utente. Questo si basa, idealmente, sul ruolo aziendale e sulle necessità di accesso basato sui ruoli. Quest'ultimo è un sistema per definire e gestire i requisiti per ciascun account in base a: necessità di conoscenza, privilegi

minimi, requisiti di privacy e / o separazione dei compiti. Esistono strumenti tecnologici che aiutano a gestire questo processo. Tuttavia, si potrebbe prevedere un accesso più granulare o temporaneo in base alle necessità.

L'autenticazione multi fattore dovrebbe essere estesa a tutti gli account con privilegi o amministrativi. Esistono molti strumenti che dispongono di applicazioni per smartphone per svolgere questa funzione e sono facili da implementare. L'utilizzo della funzione di generazione di numeri è più sicuro rispetto all'invio di un messaggio SMS (Servizio Messaggistica Veloce) con un codice monouso o rispetto alla richiesta di un avviso "push" accettato dall'utente. Tuttavia, nessuno è consigliato per l'autenticazione multi fattore con privilegi. Gli strumenti PAM sono disponibili per il controllo degli account privilegiati e forniscono una password monouso che viene verificata per ogni utilizzo. Per una maggiore sicurezza nell'amministrazione dei sistemi, si consiglia di utilizzare soluzioni "jump-box" o soluzioni di gestione "out-of-Band".

La revoca completa dell'account è importante. Molte aziende dispongono di processi coerenti e ripetibili per rimuovere l'accesso quando i dipendenti lasciano l'azienda. Tuttavia, questa procedura non è sempre adatta per i fornitori e deve essere prevista nel processo standard di revoca. Le aziende dovrebbero anche inventariare e tenere traccia degli account di servizio, poiché un errore comune è lasciare token o password nel codice, poi pubblicato in repository su cloud pubblici.

Gli account con privilegi elevati non dovrebbero essere utilizzati per l'uso quotidiano, come la navigazione sul Web e la lettura della posta elettronica. Gli amministratori dovrebbero avere account separati senza privilegi elevati per l'uso quotidiano in ufficio e dovrebbero accedere agli account amministrativi solo quando si eseguono funzioni di amministratore che richiedono quel livello di autorizzazione. Il personale addetto alla sicurezza dovrebbe raccogliere periodicamente un elenco dei processi in esecuzione per determinare se eventuali browser o programmi di posta elettronica siano in esecuzione con privilegi elevati.

→ **Ottime risorse NIST® sono le Linee Guida all'Identità Digitale:** https://pages.nist.gov/800-63-3/.

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
6.1	**Stabilire una Procedura di Concessione degli Accessi**	Utenti	Proteggere	●	●	●
	Stabilire e seguire una procedura, preferibilmente automatizzata, per concedere l'accesso alle risorse aziendali in caso di nuova assunzione, attribuzione di diritti o cambio di ruolo di un utente.					
6.2	**Stabilire una Procedura di Revoca degli Accessi**	Utenti	Proteggere	●	●	●
	Stabilire e seguire una procedura, preferibilmente automatizzata, per revocare l'accesso alle risorse aziendali, disabilitando gli account immediatamente dopo la cessazione, la revoca dei diritti o il cambio di ruolo di un utente. La disattivazione degli account, piuttosto che la loro eliminazione, potrebbe essere necessaria per consentire gli audit di tracciamento.					
6.3	**Richiedere MFA per le Applicazioni Esposte Esternamente**	Utenti	Proteggere	●	●	●
	Richiedere che tutte le applicazioni aziendali o di terze parti esposte esternamente applichino l'autenticazione multi fattore, ove supportata. Il suo utilizzo tramite un servizio di directory o un provider SSO è un'implementazione					
6.4	**Richiedere MFA per l'Accesso di Rete Remoto**	Utenti	Proteggere	●	●	●
	Richiedere l'autenticazione multi fattore per l'accesso di rete da remoto					

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
6.5	**Richiedere MFA per l'Accesso Amministrativo** Richiedere l'autenticazione multi fattore per l'accesso di tutti gli account amministrativi, se supportata, per tutte le risorse aziendali, sia gestite in locale sia utilizzando un fornitore esterno	Utenti	Proteggere	●	●	●
6.6	**Stabilire e Mantenere un Inventario dei Sistemi di Autenticazione ed Autorizzazione** Stabilire e mantenere un inventario dei sistemi di autenticazione ed autorizzazione aziendali, inclusi quelli ospitati in locale o presso un fornitore di servizi remoto. Rivedere e aggiornare l'inventario, come minimo, annualmente o più frequentemente.	Utenti	Identificare		●	●
6.7	**Centralizzare il Controllo degli Accessi** Centralizzare il controllo degli accessi per tutte le risorse aziendali tramite un servizio di directory o un provider SSO, se supportato.	Utenti	Proteggere		●	●
6.8	**Definire e Mantenere un Controllo degli Accessi Basato sui Ruoli** Definire e mantenere il controllo degli accessi basato sui ruoli, determinando e documentando i diritti di accesso necessari per ciascun ruolo aziendale per consentire lo svolgimento dei compiti assegnati. Esegui le revisioni del controllo degli accessi delle risorse aziendali per assicurare che tutti i privilegi siano autorizzati, secondo una pianificazione almeno annuale o più frequentemente.	Dati	Proteggere			●

CONTROLLI 07

Gestione Continua delle Vulnerabilità

SAFEGUARDS TOTAL	7	IG1	4/7	IG2	7/7	IG3	7/7

Panoramica

Sviluppare un piano per valutare e monitorare costantemente le vulnerabilità su tutte le risorse aziendali all'interno dell'infrastruttura, al fine di rimediare e ridurre al minimo la finestra di opportunità per gli aggressori. Monitorare le fonti di informazione del settore pubblico e privato per conoscere le più recenti minacce e vulnerabilità.

Perché questo controllo è importante?

La difesa informatica è costantemente sfidata da aggressori che cercano vulnerabilità all'interno dell'infrastruttura da sfruttare per ottenerne l'accesso. I difensori devono avere a loro disposizione informazioni tempestive sulle minacce riguardanti: aggiornamenti software, patch, avvisi di sicurezza, bollettini, ecc., e dovrebbero rivedere con regolarità i loro ambienti per individuare le vulnerabilità prima che lo facciano gli attaccanti. Comprendere e gestire le vulnerabilità è un'attività continua, che richiede tempo, attenzione e risorse.

Gli aggressori hanno accesso alle stesse informazioni e spesso possono sfruttare le vulnerabilità più velocemente di quanto un'azienda possa porvi rimedio. Sebbene trascorra un intervallo di tempo tra la conoscenza di una vulnerabilità e l'applicazione della patch, i difensori possono dare la priorità alle vulnerabilità più impattanti per l'azienda o che possono essere sfruttate per prime a causa della facilità d'uso. Ad esempio, quando i ricercatori o la comunità segnalano nuove vulnerabilità, i fornitori devono sviluppare e distribuire patch, indicatori di compromissione (IOC) e aggiornamenti. I difensori dovranno valutare il rischio della nuova vulnerabilità per l'azienda, verificare le patch tramite un preventivo test di regressione, quindi installarle.

In questo processo non esiste la perfezione. Gli aggressori potrebbero utilizzare un exploit per una vulnerabilità che non è conosciuta dalla comunità della sicurezza, o anche aver sviluppato un exploit per questa debolezza denominato "zero-day". Una volta che la vulnerabilità è nota nella comunità, inizia il processo sopra citato. Pertanto, i difensori devono tenere presente che un exploit potrebbe esistere già, quando la vulnerabilità è ampiamente socializzata. A volte le vulnerabilità potrebbero essere note all'interno di una comunità ristretta (ad esempio, un fornitore che sta ancora sviluppando una correzione) per settimane, mesi o anni prima che vengano divulgate pubblicamente. I difensori devono essere consapevoli che potrebbero sempre esserci vulnerabilità non rimediabili, dovendo ricorrere quindi ad altri controlli per mitigare.

Le aziende che non valutano la propria infrastruttura per le vulnerabilità e fronteggiano in modo proattivo i difetti scoperti, affrontano una probabilità significativa di vedere compromesse le risorse aziendali. I difensori inoltre, affrontano sfide particolari nell'ottimizzare le azioni correttive in un'intera azienda e nel dare la precedenza a diverse azioni con uguale priorità, senza che ciò incida sull'attività o sugli scopi aziendali.

Procedure e strumenti

Sono disponibili numerosi strumenti di scansione delle vulnerabilità per valutare la configurazione della sicurezza delle risorse aziendali. Alcune aziende hanno anche riscontrato che i servizi commerciali che utilizzano dispositivi di scansione gestiti in remoto sono efficaci. Per aiutare a standardizzare le definizioni delle vulnerabilità scoperte in un'azienda, è preferibile utilizzare strumenti di scansione che le mappano ad uno o più dei seguenti schemi e linguaggi di vulnerabilità, configurazione e classificazione riconosciuti dal settore: Vulnerabilità ed Esposizioni Comuni (CVE®), Enumerazione Comune di Configurazione (CCE), Linguaggio Open per la Valutazione delle Vulnerabilità (OVAL®), Piattaforma Comune di Enumerazione (CPE), Sistema di Punteggio delle Vulnerabilità Comuni (CVSS), e / Formato Descrittivo Elenco di Controllo Configurazione (XCCDF). Tali schemi e linguaggi sono componenti del protocollo SCAP. Ulteriori informazioni su SCAP sono disponibili qui: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf

La frequenza delle attività di scansione dovrebbe aumentare con l'aumentare della diversità delle risorse aziendali, in considerazione dei diversi cicli di patch di ogni fornitore. Gli strumenti avanzati di scansione delle vulnerabilità possono essere configurati con le credenziali utente per eseguire l'autenticazione sulle risorse aziendali ed effettuare analisi più complete che vengono definite "scansioni autenticate".

Oltre agli strumenti di scansione che controllano le vulnerabilità e le configurazioni errate attraverso la rete, vari strumenti gratuiti e commerciali possono valutare le impostazioni di sicurezza e le configurazioni delle risorse aziendali. Questi strumenti possono fornire informazioni dettagliate su modifiche non autorizzate nella configurazione o sull'introduzione involontaria di punti deboli della sicurezza da parte degli amministratori.

Le aziende più efficienti collegano i loro scanner di vulnerabilità con sistemi di gestione ticketing che ne tengono traccia, registrandone i progressi nella risoluzione. Ciò può aiutare a collegare vulnerabilità critiche non attenuate al responsabile della gestione affinché vengano risolte. Le aziende possono anche tenere traccia del tempo impiegato per porre rimedio a una vulnerabilità, dopo l'identificazione o l'emissione di una patch. Tali elementi possono supportare vari requisiti di conformità sia interni, sia del settore. Alcune aziende con maggior esperienza esamineranno questi rapporti nelle riunioni del comitato direttivo per la sicurezza IT, riunendo i responsabili dell'area IT e business per dare priorità alle azioni, in base all'impatto aziendale.

Nella selezione delle vulnerabilità da correggere o delle patch da applicare, un'azienda dovrebbe integrare il Sistema di Punteggio delle Vulnerabilità Comuni (CVSS) del NIST® con i dati riguardanti la probabilità che un attaccante utilizzi una vulnerabilità oppure considerando il potenziale impatto aziendale derivante da un exploit. Anche le informazioni sulla probabilità di sfruttamento di queste minacce, dovrebbero essere periodicamente aggiornate sulla base delle informazioni più

recenti. Ad esempio, il rilascio di un nuovo exploit, o di nuove informazioni relative allo sfruttamento della vulnerabilità, dovrebbe cambiarne la priorità di considerazione relativamente all'applicazione della patch. Sono disponibili vari sistemi commerciali per consentire a un'azienda di automatizzare e mantenere questo processo in modo scalabile.

Gli strumenti di scansione delle vulnerabilità più efficaci confrontano i risultati dell'ultima scansione con quelle precedenti per determinare come le vulnerabilità nell'ambiente siano cambiate nel tempo. Il personale addetto alla sicurezza utilizza queste funzionalità per valutare l'andamento delle vulnerabilità di mese in mese.

Infine, dovrebbe esserci un valido processo che garantisca la verifica degli aggiornamenti delle configurazioni o che le patch siano implementate correttamente, in tutte le risorse aziendali rilevanti.

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
7.1	**Stabilire e Mantenere una Procedura di Gestione delle Vulnerabilità.** Stabilire e mantenere una procedura di gestione delle vulnerabilità documentata. Rivedere ed aggiornare la documentazione annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.	Applicazioni	Proteggere	●	●	●
7.2	**Stabilire e Mantenere una Procedura di Correzione** Stabilire e mantenere una strategia di correzione documentata basata sul rischio nell'ambito di una procedura di correzione, rivedendola mensilmente o più frequentemente.	Applicazioni	Rispondere	●	●	●
7.3	**Gestire l'Aggiornamento Automatico del Sistema Operativo** Eseguire gli aggiornamenti del sistema operativo delle risorse aziendali per mezzo di un sistema automatizzato, mensilmente o più frequentemente.	Applicazioni	Proteggere	●	●	●
7.4	**Gestire l'Aggiornamento Automatico delle Applicazioni** Eseguire gli aggiornamenti delle applicazioni delle risorse aziendali per mezzo di un sistema automatizzato di installazione delle patch, mensilmente o più frequentemente.	Applicazioni	Proteggere	●	●	●
7.5	**Eseguire Scansioni di Vulnerabilità delle Risorse Aziendali Interne** Eseguire scansioni automatizzate delle vulnerabilità delle risorse aziendali interne, trimestralmente o più frequentemente. Effettuare scansioni sia autenticate che non, utilizzando uno strumento di scansione delle vulnerabilità compatibile SCAP.	Applicazioni	Identificare		●	●
7.6	**Eseguire Scansioni di Vulnerabilità delle Risorse Aziendali Esposte Esternamente** Eseguire scansioni automatizzate delle vulnerabilità delle risorse aziendali esposte esternamente utilizzando uno strumento conforme SCAP, mensilmente o più frequentemente.	Applicazioni	Identificare		●	●
7.7	**Correggere le Vulnerabilità Rilevate** Correggere le vulnerabilità rilevate nel software per mezzo di strumenti e procedure, mensilmente o più frequentemente, secondo la procedura di correzione.	Applicazioni	Rispondere		●	●

CONTROLLI 08

Gestione dei Log di Controllo

SAFEGUARDS TOTAL	12	IG1	3/12	IG2	11/12	IG3	12/12

Panoramica

Raccogliere, avvisare, esaminare e conservare i log di controllo degli eventi che potrebbero aiutare a rilevare, comprendere o rimediare in seguito ad un attacco.

Perché questo controllo è importante?

Raccolta ed analisi dei log sono fondamentali per la capacità di un'azienda nel rilevare rapidamente attività dannose. A volte i record di audit sono l'unica prova di un attacco riuscito. Gli aggressori sanno che molte aziende conservano registri di controllo per ragioni di conformità, ma raramente li analizzano. Gli aggressori, consapevoli di ciò, se ne avvalgono per nascondere la propria posizione, il software dannoso e le attività sui computer delle vittime. A causa delle analisi dei log scadenti o inesistenti, gli aggressori a volte mantengono il controllo delle macchine vittime per mesi o anni senza che nessuno nell'azienda colpita lo sappia.

Esistono due tipi di log generalmente trattati e spesso configurati in modo indipendente: log di sistema e log di controllo. I primi in genere forniscono eventi a livello di sistema che mostrano vari orari di inizio / fine del processo, arresti anomali, ecc.; questi sono nativi e richiedono meno configurazione per l'attivazione. I secondi in genere includono eventi a livello di utente (quando un utente si è collegato, ha eseguito un accesso a un file, ecc.) e richiedono più pianificazione ed impegno per la loro impostazione.

Anche i record di logging sono fondamentali per la risposta agli incidenti. Dopo aver rilevato un attacco, l'analisi dei log può aiutare le aziende a comprenderne l'entità. I record di logging completi possono mostrare, ad esempio, quando e come si è verificato l'attacco, a quali informazioni è stato effettuato l'accesso e se i dati sono stati esfiltrati. La conservazione dei log è fondamentale anche nel caso in cui sia necessaria un'indagine di follow-up o se un attacco non è stato rilevato per un lungo periodo di tempo.

Procedure e strumenti

La maggior parte delle risorse e dei software aziendali offre funzionalità di logging. Tale registrazione dovrebbe essere attivata, inviando i registri a server centralizzati. Firewall, proxy e sistemi di accesso remoto (Rete Privata Virtuale—VPN, dial-up, ecc.) dovrebbero essere tutti configurati per il logging dettagliato, se utile. La conservazione dei dati di logging è importante anche nel caso in cui sia necessaria un'indagine sull'incidente.

Inoltre, tutte le risorse aziendali dovrebbero essere configurate per creare i log degli accessi quando un utente tenta l'utilizzo delle risorse senza i privilegi appropriati. Per valutare se tale registrazione è in atto, un'azienda dovrebbe scansionare periodicamente i propri registri e confrontarli con l'inventario delle risorse aziendali organizzato come previsto nei Controlli CIS 1, per assicurarsi che ogni risorsa gestita attivamente connessa alla rete generi periodicamente i log.

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
8.1	**Stabilire e Mantenere una Procedura di Gestione dei Log di Controllo** Stabilire e mantenere una procedura di gestione dei log di controllo che soddisfi i requisiti di registrazione. Come minimo, salvare i log delle risorse aziendali, per la loro revisione e conservazione. Rivedere e aggiornare la documentazione ogni anno o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.	Rete	Proteggere	●	●	●
8.2	**Raccogliere i Log di Controllo** Raccogliere i log di controllo. Assicurare che la procedura aziendale di gestione dei log sia attivata su tutti i dispostivi aziendali .	Rete	Rilevare	●	●	●
8.3	**Assicurare un Spazio Adeguato per l'Archiviazione dei Log** Assicurare che le destinazioni di archiviazione dei log mantengano uno spazio adeguato per adattarsi al processo aziendale di gestione dei log di controllo.	Rete	Proteggere	●	●	●
8.4	**Standardizzare la Sincronizzazione dell'Orario** Standardizzare la sincronizzazione dell'orario. Configurare almeno due sorgenti orarie sulle risorse aziendali, se supportato.	Rete	Proteggere		●	●
8.5	**Raccogliere i Log di Controllo Dettagliati** Configurare il logging dettagliato per le risorse aziendali che contengono dati sensibili. Includere l'origine dell'evento, data, nome utente, marca temporale, indirizzo di origine e di destinazione, ed altri elementi utili che potrebbero aiutare in una indagine forense.	Rete	Rilevare		●	●
8.6	**Raccogliere i Log di Controllo del DNS** Raccogliere i log di controllo delle query DNS sulle risorse aziendali, ove appropriato e supportato..	Rete	Rilevare		●	●
8.7	**Raccogliere i Log di Controllo delle Richieste URL** Raccogliere i log di controllo delle richieste URL, ove appropriato e supportato.	Rete	Rilevare		●	●
8.8	**Raccogliere i Log di Controllo dai Command-Line** Raccogliere i log di controllo delle interfacce command-line. Esempi di implementazione includono la raccolta dei log di PowerShell®, BASH™, e terminali di amministrazione remota.	Dispositivi	Rilevare		●	●
8.9	**Centralizzare i Log di Controllo** Centralizzare, per quanto possibile, raccolta e conservazione dei log di controllo delle risorse aziendali.	Rete	Rilevare		●	●
8.10	**Conservare i Log di Controllo** Conservare i log di controllo delle risorse aziendali per un minimo di 90 giorni.	Rete	Proteggere		●	●
8.11	**Effettuare le Revisioni dei Log di Controllo** Effettuare le revisioni dei log di controllo per rilevare anomalie o eventi inconsueti che potrebbero indicare una potenziale minaccia. Attuare i controlli su base settimanale o più frequentemente.	Rete	Rilevare		●	●
8.12	**Raccogliere i Log dei Fornitori di Servizi** Raccogliere i log dei fornitori di servizi, se supportati. Esempi di implementazione includono la raccolta di eventi di autenticazione e autorizzazione, eventi di creazione ed eliminazione di dati ed eventi di gestione degli utenti.	Dati	Rilevare			●

CONTROLLI 09

Protezione della Posta elettronica e del Browser Web

SAFEGUARDS TOTAL	7	IG1	2/7	IG2	6/7	IG3	7/7

Panoramica

Migliorare le protezioni ed il rilevamento delle minacce provenienti dalle e-mail e da vettori web, che danno l'opportunità agli aggressori di manipolare il comportamento umano sfruttandone il diretto coinvolgimento.

Perché questo controllo è importante?

I browser Web e i client di posta elettronica sono punti di accesso molto comuni per gli aggressori a causa della loro interazione diretta con gli utenti che operano in azienda. Il contenuto può essere creato per invogliare o indurre gli utenti nel divulgare di credenziali, fornire dati sensibili o aprire un canale per consentire agli aggressori di ottenere l'accesso, aumentando così il rischio per l'azienda. Considerando che e-mail e Web sono i mezzi principali con cui gli utenti interagiscono con persone ed ambienti esterni non attendibili, diventano obiettivi primari sia per il codice dannoso sia per il social engineering. Inoltre, le aziende preferendo la posta elettronica basata sul Web o all'accesso all'e-mail mobile, indirizzano gli utenti verso l'abbandono dei più i tradizionali client completi di posta elettronica, che forniscono controlli di sicurezza incorporati come la crittografia della connessione, l'autenticazione avanzata e i pulsanti di segnalazione del phishing.

Procedure e strumenti

Browser Web

I criminali informatici possono sfruttare i browser Web in vari modi. Avendo accesso agli exploit dei browser vulnerabili, possono creare pagine Web dannose in grado di sfruttare tali debolezze quando esplorate con un software non sicuro o non aggiornato. In alternativa, possono provare a prendere di mira un qualsiasi plug-in di terze parti che potrebbe consentire loro di collegarsi al browser o anche direttamente al sistema operativo o all'applicazione. Questi plugin, proprio come qualsiasi altro software all'interno di un ambiente, necessitano di revisioni per individuare vulnerabilità, controlli e manutenzione per l'aggiornamento con le ultime patch o versioni. Molti provengono da fonti non attendibili e alcuni sono addirittura scritti per essere dannosi. Per questo, è meglio impedire agli utenti di installare più o meno intenzionalmente i malware che potrebbero nascondersi in alcuni di questi plug-in, estensioni e componenti aggiuntivi. Semplici aggiornamenti della configurazione del browser possono rendere molto più difficile l'installazione di malware riducendo la capacità di aggiungere componenti / plug-in /estensioni e bloccando l'esecuzione automatica di tipi specifici di contenuti.

I browser più diffusi utilizzano un database di siti di phishing e / o malware per proteggersi dalle minacce più comuni. Una buona pratica consiste nell'abilitare questi filtri di contenuto ed attivare i blocchi dei pop-up. I pop-up non sono solo fastidiosi; possono anche includere direttamente il malware o indurre gli utenti a cliccare i collegamenti utilizzando trucchi di social engineering. Per migliorare nel blocco dei domini dannosi noti, si prenda in considerazione anche la sottoscrizione ai servizi di filtro DNS per impedire i tentativi di accesso a questi siti Web a livello di rete.

Posta Elettronica

La posta elettronica rappresenta una delle maggiori modalità lavorative con cui il personale interagisce con le risorse aziendali; la formazione e l'incoraggiamento al comportamento corretto sono importanti quanto le impostazioni tecniche. La posta elettronica è il vettore di minaccia più comune contro le aziende attraverso tattiche come il phishing e la Compromissione dell'E-mail Aziendale (BEC).

L'utilizzo di uno strumento di filtraggio della posta indesiderata e della scansione del malware nel gateway di posta elettronica riduce il numero di e-mail ed allegati dannosi che entrano nella rete aziendale. L'utilizzo delle policy di autenticazione e dei rapporti di conformità dei messaggi basati sul dominio (DMARC) aiuta a ridurre le attività di spam e phishing. L'installazione di uno strumento di crittografia per proteggere la posta elettronica e le comunicazioni aggiunge un ulteriore elemento di sicurezza a livello utente e di rete. Oltre al blocco basato sul mittente, è opportuno consentire solo i tipi di file necessari allo svolgimento del lavoro. Ciò richiederà il coordinamento con diverse unità aziendali per capire quali tipi di file siano ricevuti via e-mail per garantire che non vi siano interruzioni dell'attività lavorativa.

Poiché le tecniche phishing basate sull'e-mail si evolvono continuamente per eludere le regole dei filtri per la posta indesiderata (SPAM), è importante addestrare gli utenti ad identificare il phishing e informare la sicurezza IT quando lo rilevano. Esistono molte piattaforme che eseguono test di phishing che aiutano ed istruiscono gli utenti nel rilevarli, presentando vari esempi e monitorando il loro miglioramento nel tempo. La conoscenza condivisa sul come segnalare i tentativi di phishing ai team di sicurezza IT aiuta a migliorare le protezioni e i rilevamenti delle minacce basate sulla posta elettronica.

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
9.1	**Assicurare l'Utilizzo di Client E-mail e di Browser Pienamente Supportati**	Applicazioni	Proteggere	●	●	●
	Assicurare che venga permessa l'esecuzione solo di client di posta elettronica e di browser pienamente supportati ed aggiornati alla versione più recente rilasciata dal fornitore.					
9.2	**Utilizzare Servizi di Filtro DNS**	Rete	Proteggere	●	●	●
	Utilizzare i servizi di filtro DNS su tutte le risorse aziendali per bloccare l'accesso ai domini riconosciuti come pericolosi.					
9.3	**Mantenere ed Applicare i Filtri URL di Rete**	Rete	Proteggere		●	●
	Applicare ed aggiornare i filtri URL di rete per limitare la connessione di una risorsa aziendale a siti Web potenzialmente dannosi o non approvati. Esempi di implementazione includono i filtri basati sulla categoria, i filtri basati sulla reputazione o tramite l'uso di elenchi di blocco. Applicare i filtri su tutte le risorse aziendali.					

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
9.4	**Limitare le Estensioni di Browser e Client E-Mail non Necessarie o non Autorizzate**	**Applicazioni**	**Proteggere**		●	●
	Limitare, disinstallando o disattivando dal browser o dal client di posta elettronica, qualsiasi estensione, plug-in e applicazione add-on, non autorizzata o non necessaria.					
9.5	**Implementare DMARC**	**Rete**	**Proteggere**		●	●
	Per ridurre la possibilità di e-mail contraffatte o modificate da domini validi, implementare le policy e le verifiche DMARC, iniziando con l'implementazione del Sender Policy Framework (SPF) e degli standard di Chiave Identificativa Dominio Mail (DKIM).					
9.6	**Bloccare i Tipi di File non Necessari**	**Rete**	**Proteggere**		●	●
	Bloccare i tipi di file non necessari in ingresso sul gateway di posta elettronica aziendale.					
9.7	**Installare e Mantenere le Protezioni Anti-Malware del Server di Posta**	**Rete**	**Proteggere**			●
	Installare e mantenere le protezioni anti-malware del server di posta, esempio scansione degli allegati e/o sandboxing.					

CONTROLLI 10

Difesa dal Malware

SAFEGUARDS TOTAL	7	IG1	3/7	IG2	7/7	IG3	7/7

Panoramica

Prevenire o controllare installazione, diffusione ed esecuzione di applicazioni, codici o script dannosi sulle risorse aziendali.

Perché questo controllo è importante?

Il software dannoso (definito anche come virus o trojan) è un aspetto integrante e pericoloso delle minacce provenienti da Internet. Possono avere molti scopi: acquisizione di credenziali, furto di dati, identificazione di altri obiettivi all'interno della rete, crittografia o distruzione dei dati. Il malware è in continua evoluzione ed adattivo, in quanto le varianti moderne sfruttano le tecniche di apprendimento automatico.

Il malware entra in un'azienda sfruttando le debolezze presenti nei dispositivi degli utenti finali, allegati e-mail, pagine Web, servizi cloud, dispositivi mobili e supporti rimovibili. Il malware spesso si basa su comportamenti non sicuri dell'utente finale, come cliccare su collegamenti, aprire allegati, installare software o profili, inserire drive USB (Universal Serial Bus). Il malware moderno è progettato per evitare, ingannare o disabilitare le difese.

Le difese antimalware devono essere in grado di agire in questo ambiente dinamico per mezzo dell'automazione, l'aggiornamento costante e rapido ed integrandosi con altri processi come la gestione delle vulnerabilità e la risposta agli incidenti. Devono essere implementate in tutti i possibili punti di ingresso e risorse aziendali per rilevare, prevenire la diffusione o controllare l'esecuzione di software o codice dannoso.

Procedure e strumenti

La protezione efficace contro il malware include le tradizionali suite di prevenzione e rilevamento del malware sugli endpoint. Per garantire che gli Indicatori di Compromissione (IOC) del malware siano aggiornati, le aziende possono ricevere aggiornamenti automatici dal fornitore per arricchire altri dati su vulnerabilità o minacce. Questi strumenti sono gestiti al meglio in modo centralizzato, per fornire coerenza nell'infrastruttura.

La capacità di bloccare o identificare il malware è solo una parte di questo Controllo CIS; è presente anche un approfondimento sulla raccolta centralizzata dei log per supportare gli avvisi, l'identificazione e la risposta agli incidenti. Mentre i malintenzionati continuano a sviluppare le loro metodologie, molti stanno cominciando ad adottare l'uso di strumenti sicuri per la diffusione malware ("living-

off-the-land"—LotL) per ridurre al minimo la probabilità di essere scoperti. Questo approccio si riferisce al comportamento dell'attaccante che usa strumenti o funzionalità già esistenti nell'ambiente di destinazione. L'abilitazione dei log, sulla base delle Salvaguardie nei Controlli CIS 8, renderà molto più semplice per l'azienda seguire gli eventi per capire cosa è successo e perché.

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
10.1	**Distribuire e Mantenere il Software Anti-Malware**	**Dispositivi**	**Proteggere**	●	●	●
	Distribuire e mantenere il software anti-malware su tutte le risorse aziendali.					
10.2	**Configurare gli Aggiornamenti Automatici delle Firme Anti-Malware**	**Dispositivi**	**Proteggere**	●	●	●
	Configurare gli aggiornamenti automatici dei file delle firme anti-malware su tutte le risorse aziendali.					
10.3	**Disabilitare Esecuzione e Riproduzione Automatica per i Supporti Rimovibili**	**Dispositivi**	**Proteggere**	●	●	●
	Disabilitare l'esecuzione e la riproduzione automatica per i supporti rimovibili.					
10.4	**Configurare la Scansione Automatica dei Supporti Rimovibili**	**Dispositivi**	**Rilevare**		●	●
	Configurare il software anti-malware per la scansione automatica dei supporti rimovibili.					
10.5	**Abilitare le Funzioni Anti-Exploit**	**Dispositivi**	**Proteggere**		●	●
	Abilitare le funzioni anti-exploit sui software e sui dispositivi aziendali, se possibile, come ad esempio Microsoft® Prevenzione di Esecuzione in area Dati (DEP), Windows® Defender Exploit Guard (WDEG), Apple® Protezione di Integrità del Sistema (SIP), Gatekeeper™.					
10.6	**Gestire Centralmente il Software Anti-Malware**	**Dispositivi**	**Proteggere**		●	●
	Gestire in modo centralizzato il software anti-malware.					
10.7	**Utilizzare un Software Anti-Malware Basato sul Comportamento**	**Dispositivi**	**Rilevare**		●	●
	Utilizzare un software anti-malware basato sul comportamento.					

CONTROLLI 11

Recupero dei Dati

SAFEGUARDS TOTAL	5	IG1	4/5	IG2	5/5	IG3	5/5

Panoramica

Stabilire e mantenere sufficienti procedure di ripristino dei dati per riportare le risorse aziendali in funzione ad uno stato attendibile di pre-incidente.

Perché questo controllo è importante?

Nel triangolo della sicurezza informatica—Riservatezza, Integrità e Disponibilità (CIA)—la disponibilità dei dati è, in alcuni casi, più critica della loro riservatezza. Le aziende hanno bisogno di molti tipi di dati per prendere le loro decisioni e, quando tali dati non sono disponibili o non sono attendibili, potrebbero avere un impatto sull'attività. Un semplice esempio sono le informazioni meteorologiche per un'impresa di trasporti.

Quando gli aggressori compromettono le risorse, modificano le configurazioni, aggiungono account e spesso aggiungono software o script. Questi cambiamenti non sono sempre facili da identificare, poiché gli aggressori potrebbero aver danneggiato o sostituito applicazioni attendibili con versioni dannose oppure le modifiche potrebbero sembrare nomi di account standard. Le modifiche delle configurazioni possono includere l'aggiunta o la modifica di voci di registro, l'apertura di porte, la disattivazione dei servizi di sicurezza, l'eliminazione dei log o altre azioni dannose che rendono insicuro un sistema. Queste azioni non devono essere intenzionali ma anche l'errore umano può esserne la causa. Per questo è importante avere la disponibilità di backup o repliche recenti per ripristinare le risorse e dati aziendali in uno stato sicuro ed attendibile.

Negli ultimi anni c'è stato un aumento esponenziale del ransomware. Non è una nuova minaccia ma è diventata più commercializzata ed organizzata come tecnica affidabile per gli aggressori per guadagnare denaro. Se un malintenzionato crittografa i dati di un'azienda e chiede un riscatto per la restituzione, può essere utile disporre di un backup recente per ripristinare uno stato sicuro ed attendibile. Col tempo il ransomware si è evoluto diventando anche una tecnica di estorsione, in cui i dati aziendali vengono esfiltrati prima di essere crittografati per richiederne poi il pagamento per il ripristino nonché per impedirne la vendita o la diffusione. In questo caso però, il ripristino risolverebbe solo il problema del recupero dei sistemi in uno stato attendibile e del proseguimento delle attività. L'utilizzo della guida all'interno dei Controlli CIS aiuterà a ridurre il rischio di ransomware per mezzo di una migliore igiene informatica, dato che gli aggressori utilizzano di solito exploit elementari o più datati sui sistemi non sicuri.

Procedure e strumenti

Le procedure di recupero dei dati dovrebbero essere definite nel processo di gestione dei dati descritto nei Controlli CIS 3, Protezione dei Dati. Si dovrebbero includere procedure di backup basate sul valore, sensibilità e requisiti di conservazione dei dati. Ciò aiuterà nel definire la frequenza e il tipo di backup (completo o incrementale).

Trimestralmente (oppure ogni volta che viene introdotto un nuovo processo o tecnologia di backup), un team di controllo dovrebbe valutare un campione casuale di backup tentandone il ripristino in un ambiente di prova. I backup ripristinati devono essere verificati per garantire che il sistema operativo, l'applicazione e i dati provenienti dal backup siano tutti integri e funzionanti.

In caso di attacco malware, le procedure di ripristino dovrebbero utilizzare una versione del backup che si ritiene preceda l'infezione iniziale.

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
11.1	**Stabilire e Mantenere una Procedura di Recupero dei Dati** Stabilire e mantenere una procedura di recupero dei dati. Definire l'ambito delle attività di ripristino dei dati, la priorità del ripristino e la sicurezza dei dati di backup. Rivedere e aggiornare la documentazione annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.	Dati	Recuperare	●	●	●
11.2	**Eseguire Backup Automatizzati** Eseguire backup automatizzati delle risorse aziendali in funzione. Eseguire il backup settimanalmente o più frequentemente, in base alla sensibilità dei dati.	Dati	Recuperare	●	●	●
11.3	**Proteggere i Dati di Ripristino** Proteggere i dati di ripristino con controlli equivalenti ai dati originali. Applicare la crittografia necessaria o separare i dati in funzione dei requisiti.	Dati	Proteggere	●	●	●
11.4	**Stabilire e Mantenere una Istanza Isolata dei Dati di Ripristino** Stabilire e mantenere un'istanza isolata dei dati di ripristino. Le implementazioni di esempio includono il controllo della versione delle destinazioni di backup tramite sistemi o servizi offline, cloud e off-site.	Dati	Recuperare	●	●	●
11.5	**Recupero Dati di Prova** Testare il ripristino del backup trimestralmente, o con maggiore frequenza, per un campione di risorse aziendali in funzione.	Dati	Recuperare		●	●

CONTROLLI 12

Gestione dell'Infrastruttura di Rete

SAFEGUARDS TOTAL	8	IG1	1/8	IG2	7/8	IG3	8/8

Panoramica

Stabilire, implementare e gestire attivamente (tracciando, segnalando, correggendo) i dispositivi di rete, al fine di impedire agli aggressori di sfruttarne servizi e punti di accesso vulnerabili.

Perché questo controllo è importante?

L'infrastruttura di rete sicura è una difesa essenziale contro gli attacchi. Ciò include un'architettura di sicurezza appropriata, che affronti le vulnerabilità che sono spesso introdotte con le impostazioni predefinite, monitorando le modifiche e rivalutando le configurazioni correnti. L'infrastruttura di rete include dispositivi come gateway fisici e virtualizzati, firewall, punti di accesso wireless, router e switch.

Le configurazioni predefinite dei dispositivi di rete sono orientate alla facilità di distribuzione e di uso, non alla sicurezza. Le potenziali vulnerabilità predefinite comprendono servizi e porte aperte, account e password di default (inclusi gli account di servizio), supporto di protocolli meno recenti e vulnerabili, preinstallazione di software non necessario. Gli aggressori cercano impostazioni predefinite vulnerabili, lacune o incongruenze nelle regole dei firewall, router e switch utilizzando tali falle per penetrare nelle difese. Sfruttano i difetti in questi dispositivi per ottenere l'accesso alle reti, reindirizzare il traffico su una rete e intercettare i dati in trasmissione.

La sicurezza della rete è un ambiente in continua evoluzione e necessita di una rivalutazione regolare di diagrammi dell'architettura, configurazioni, controlli di accesso e flussi di traffico consentiti. Gli aggressori sfruttano le configurazioni dei dispositivi di rete che diventano meno sicure nel tempo quando gli utenti richiedono delle eccezioni per esigenze aziendali specifiche: a volte le eccezioni vengono applicate, ma non rimosse quando non sono più necessarie. In alcuni casi, il rischio per la sicurezza di un'eccezione può cambiare nel tempo, quando non viene analizzato correttamente, né valutato in funzione delle esigenze aziendali correlate.

Procedure e strumenti

Le aziende dovrebbero garantire che l'infrastruttura di rete sia completamente documentata e che i diagrammi dell'architettura siano aggiornati. È importante che i componenti chiave dell'infrastruttura siano supportati dal fornitore per le patch e gli aggiornamenti delle funzionalità. È importante aggiornare i componenti a fine ciclo di vita (EOL) prima della data in cui non saranno più supportati o applicare i controlli di mitigazione per isolarli. Le aziende devono monitorare le versioni e le configurazioni dell'infrastruttura per individuare vulnerabilità che richiedono l'aggiornamento dei dispositivi di rete all'ultima versione sicura e stabile che non influisca sull'infrastruttura.

Un diagramma dell'architettura di rete aggiornato, compreso quello dell'architettura di sicurezza, è una base importante per la gestione dell'infrastruttura. A seguire, disporre di una gestione completa degli account per il controllo degli accessi, il logging e il monitoraggio. Infine, l'amministrazione dell'infrastruttura dovrebbe essere eseguita utilizzando solo protocolli sicuri, con autenticazione forte (MFA per PAM) e da reti e dispositivi amministrativi dedicati.

Gli strumenti commerciali possono essere utili per valutare l'insieme di regole dei dispositivi di filtraggio di rete per determinare se sono coerenti o in conflitto, fornendo un controllo automatico dell'integrità. Questi strumenti cercano errori nei set di regole o nelle liste di controllo degli accessi (ACL) che possono consentire servizi non previsti nei dispositivi di rete. Tali strumenti dovrebbero essere eseguiti ogni volta che vengono apportate modifiche significative all'insieme di regole del firewall, ACL del router o ad altre tecnologie di filtraggio.

→ **Per la guida al lavoro a distanza e per i piccoli uffici, si faccia riferimento a CIS Controls Telework and Small Office Network Security Guide:** https://www.cisecurity.org/controls/v8/

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
12.1	**Assicurare l'Aggiornamento dell'Infrastruttura di Rete**	Rete	Proteggere	●	●	●
	Assicurare che l'infrastruttura di rete sia sempre aggiornata. Esempi di implementazione includono l'esecuzione dell'ultima versione stabile del software e / o l'utilizzo delle potenzialità NaaS (network-as-a-service) attualmente disponibili. Rivedere le versioni del software mensilmente o più frequentemente per verificarne il supporto					
12.2	**Stabilire e Mantenere una Architettura di Rete Sicura**	Rete	Proteggere		●	●
	Stabilire e mantenere un'architettura di rete sicura. Un'architettura di rete sicura deve prevedere almeno la segmentazione, i privilegi minimi e la disponibilità.					
12.3	**Gestione Sicura dell'Infrastruttura di Rete**	Rete	Proteggere		●	●
	Gestire in sicurezza l'infrastruttura di rete. Esempi di implementazione includono il controllo di versione dell'infrastruttura tramite codice e l'uso di protocolli di rete sicuri, come SSH e HTTPS.					
12.4	**Stabilire e Mantenere il / i Diagramma / i dell'Architettura**	Rete	Identificare		●	●
	Stabilire e mantenere i diagrammi dell'architettura e / o altra documentazione del sistema di rete. Rivedere e aggiornare la documentazione ogni anno o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.					
12.5	**Centralizzare Autenticazione, Autorizzazione e Auditing di Rete**	Rete	Proteggere		●	●
	Centralizzare AAA di rete.					
12.6	**Utilizzare Protocolli Sicuri di Gestione e Comunicazione della Rete**	Rete	Proteggere		●	●
	Utilizzare protocolli sicuri di gestione e comunicazione della rete (esempio 802.1X, Protocollo di Accesso Wi-Fi 2–WPA2 versione Enterprise o superiore)					
12.7	**Assicurare l'Utilizzo di VPN per i Dispositivi Remoti e Connessione AAA all'Infrastruttura Aziendale**	Dispositivi	Proteggere		●	●
	Richiedere agli utenti l'autenticazione alla VPN aziendale e ai servizi di autenticazione prima dell'accesso alle risorse aziendali dai dispositivi degli utenti finali.					
12.8	**Stabilire e Mantenere Risorse Informatiche Dedicate per tutto il Lavoro Amministrativo**	Dispositivi	Proteggere			●
	Stabilire e mantenere risorse informatiche dedicate, fisicamente o logicamente separate, per tutte le attività amministrative o che richiedano l'accesso amministrativo. Le risorse informatiche dovrebbero essere segmentate dalla rete primaria dell'azienda e non avere accesso a Internet.					

CONTROLLI 13

Monitoraggio e Difesa della Rete

SAFEGUARDS TOTAL	11	IG1	0/11	IG2	6/11	IG3	11/11

Panoramica

Adottare processi e strumenti per stabilire e mantenere un monitoraggio completo della rete e una difesa contro le minacce alla sicurezza dell'infrastruttura di rete aziendale e agli utenti.

Perché questo controllo è importante?

Non è possibile affidarsi ad una difesa di rete perfetta. Gli avversari continuano ad evolversi e maturare, mentre condividono o vendono informazioni nelle loro comunità su exploit e bypass dei controlli di sicurezza. Anche se gli strumenti di sicurezza funzionano "come pubblicizzato", è necessario comprendere il livello di rischio aziendale per configurarli, ottimizzarli e tracciarli al fine di renderli efficaci. Spesso, errate configurazioni dovute a errori umani o conoscenza carente delle capacità degli strumenti, danno alle aziende un falso senso di sicurezza.

Gli strumenti di sicurezza possono essere efficaci solo se supportano una procedura di monitoraggio continuo che consente agli addetti di essere avvisati e di rispondere rapidamente agli incidenti di sicurezza. Le aziende che adottano una soluzione esclusivamente tecnologica affronteranno anche più falsi positivi, dovuti all'eccessiva dipendenza dagli avvisi derivanti da questo tipo di approccio. L'identificazione e la risposta a queste minacce richiedono visione d'insieme su tutti i vettori di minacce dell'infrastruttura impiegando persone nel processo di rilevamento, analisi e risposta. È fondamentale per le grandi aziende o per quelle fortemente esposte, di disporre di una capacità operativa di sicurezza al fine di prevenire, rilevare e rispondere rapidamente alle minacce informatiche prima che possano avere un impatto sull'azienda. Questo processo genererà rapporti di attività e metriche che aiuteranno a migliorare i criteri di sicurezza, supportando molte aziende per la conformità normativa.

Come abbiamo visto più volte sulla stampa, le aziende sono state compromesse per settimane, mesi o anni prima di venirne a conoscenza. Il vantaggio principale di avere una completa consapevolezza situazionale si esprime con l'aumento della velocità di rilevamento e risposta. Questo è fondamentale per agire rapidamente quando viene scoperto un malware, quando vengono rubate credenziali o quando i dati sensibili vengono compromessi, al fine di ridurre l'impatto sull'azienda.

Avendo una buona consapevolezza della situazione (ad esempio operazioni di sicurezza), le aziende identificheranno e catalogheranno Tattiche, Tecniche e Procedure (TTP) degli aggressori, inclusi i loro IOC, che aiuteranno l'azienda a diventare più proattiva nell'identificare minacce o incidenti futuri. Il ripristino può essere più rapido quando la risposta ha accesso a informazioni complete sull'ambiente e sulla struttura aziendale per sviluppare strategie di risposta efficienti.

Procedure e strumenti

Molte aziende non ha bisogno di allestire un Centro Operativo per la Sicurezza (SOC) per ottenere una certa consapevolezza della situazione. Si può iniziare con la comprensione delle funzioni aziendali critiche, l'architettura di rete e server, dati e flussi, servizi dei fornitori e connessione con i partner commerciali, dispositivi degli utenti finali e account. Queste informazioni contribuiscono allo sviluppo di un'architettura di sicurezza, controlli tecnici, log, monitoraggio e procedure di risposta.

Al centro di questo processo c'è un gruppo formato e organizzato che implementa processi per il rilevamento, l'analisi e la mitigazione degli incidenti; queste funzioni possono essere svolte internamente, tramite consulenti o un fornitore di servizi gestiti. Per queste procedure le aziende dovrebbero includere le attività di rete, le risorse aziendali, le credenziali utente e di accesso ai dati. La tecnologia svolgerà un ruolo fondamentale per raccogliere ed analizzare tutti i dati monitorando reti e risorse aziendali all'interno e all'esterno dell'impresa. Le aziende dovrebbero anche includere la visibilità delle piattaforme cloud che potrebbero non essere in linea con le tecnologie di sicurezza locale.

L'inoltro di tutti i log importanti ai programmi di analisi, come le soluzioni SIEM (Gestione Informazioni di Sicurezza ed Eventi), può essere importante, ma non in grado di fornire un quadro completo. Sono necessarie revisioni settimanali dei log per ottimizzare le soglie e identificare eventi anomali. Gli strumenti di correlazione possono rendere i registri di controllo più utili per la successiva ispezione manuale. Questi strumenti non sostituiscono il personale specializzato nella sicurezza delle informazioni e gli amministratori di sistema. Anche con gli strumenti di analisi dei log automatizzati, spesso sono necessarie competenze umane e intuizione per identificare e comprendere gli attacchi.

Con la crescita di questo processo, le aziende potranno creare, mantenere ed evolvere una conoscenza di base che aiuterà a comprendere e valutare i rischi, sviluppando una capacità di intelligence sulle minacce interne rappresentata da una raccolta di Tattiche Tecniche e Procedure (TTP) estrapolata da incidenti ed avversari. A tal fine, un programma di consapevolezza della situazione definirà e valuterà quali fonti di informazioni siano significative per rilevare, segnalare e gestire gli attacchi. Le aziende più preparate potranno passare alla ricerca delle minacce, attuata da personale qualificato in grado di esaminare manualmente i log di sistema ed utente, i flussi di dati e i modelli di traffico per trovare anomalie.

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
13.1	**Centralizzare gli Avvisi degli Eventi di Sicurezza** Centralizzare gli avvisi degli eventi di sicurezza delle risorse aziendali per la correlazione ed analisi dei log. L'implementazione delle best practice prevede l'uso di un SIEM, che includa gli avvisi di correlazione degli eventi definiti dal fornitore. Anche una piattaforma di analisi dei log configurata con avvisi di sicurezza correlati e rilevanti soddisfa questa salvaguardia.	Rete	Rilevare		●	●
13.2	**Adottare una Soluzione di Rilevamento Intrusioni Basata su Host** Adottare una soluzione di rilevamento delle Intrusioni basata su host sulle risorse aziendali, ove appropriato e/o supportato	Dispositivi	Rilevare		●	●
13.3	**Adottare una Soluzione di Rilevamento Intrusioni Basata sulla Rete** Adottare una soluzione di rilevamento delle intrusioni basata sulla rete sulle risorse aziendali, ove appropriato. Esempi di implementazione includono l'utilizzo di un Sistema di Rete per il Rilevamento delle Intrusioni (NIDS) o un servizio fornito in cloud equivalente (CSP)	Rete	Rilevare		●	●
13.4	**Filtrare il Traffico tra i Segmenti di Rete** Filtrare il traffico tra i segmenti di rete ove appropriato	Rete	Proteggere		●	●
13.5	**Gestire il Controllo degli Accessi per le Risorse Remote** Gestire il controllo degli accessi per le risorse che si connettono da remoto alle dotazioni aziendali. Determinare il numero di accessi in base a: software anti-malware aggiornato installato, conformità della configurazione sicura relativamente al processo definito dall'azienda, verifica di aggiornamento del sistema operativo e delle applicazioni.	Dispositivi	Proteggere		●	●
13.6	**Salvare i Log del Flusso di Traffico di Rete** Salvare i log del flusso di traffico di rete e / o il traffico di rete per esaminare e inviare avvisi dai dispositivi di rete.	Rete	Rilevare		●	●
13.7	**Adottare una Soluzione di Prevenzione delle Intrusioni Basata su Host** Adottare una soluzione di prevenzione delle intrusioni basata su host sulle risorse aziendali, ove appropriato e / o supportato. Esempi di implementazione includono l'uso di un client Endpoint di Rilevamento e Risposta (EDR) o di un agent IPS basato su host.	Dispositivi	Proteggere			●
13.8	**Adottare una Soluzione di Prevenzione delle Intrusioni Basata sulla Rete** Adottare una soluzione di prevenzione delle intrusioni di rete, ove appropriato. Esempi di implementazione includono l'uso di un sistema di prevenzione delle intrusioni di rete (NIPS) o di un servizio CSP equivalente.	Rete	Proteggere			●
13.9	**Implementare il Controllo degli Accessi a Livello di Porta** Adottare il controllo degli accessi a livello di porta che utilizzi 802.1x o protocolli di controllo di accesso alla rete simili, come i certificati, includendo l'autenticazione dell'utente e / o del dispositivo.	Dispositivi	Proteggere			●
13.10	**Eseguire il Filtraggio a Livello di Applicazione** Eseguire il filtraggio a livello di applicazione. Esempi di implementazione includono un proxy di filtraggio, un firewall a livello di applicazione o un gateway.	Rete	Proteggere			●
13.11	**Perfezionare le Soglie di Avviso degli Eventi di Sicurezza** Ottimizzare le soglie di avviso degli eventi di sicurezza mensilmente o più.	Rete	Rilevare			●

CONTROLLI 14

Sensibilizzazione e Formazione sulle Competenze di Sicurezza

SAFEGUARDS TOTAL	9	IG1	8/9	IG2	9/9	IG3	9/9

Panoramica

Stabilire e mantenere un programma di sensibilizzazione alla sicurezza per istruire il personale affinché sia consapevole ed adeguatamente preparato per ridurre i rischi di sicurezza informatica aziendali.

Perché questo controllo è importante?

Le azioni delle persone svolgono un ruolo fondamentale per il successo o il fallimento del programma di sicurezza aziendale. È più facile per un malintenzionato indurre un utente a cliccare su un collegamento o aprire un allegato di posta elettronica per installare un malware al fine di entrare in un'azienda, piuttosto che trovare un exploit di rete per farlo direttamente.

Gli utenti stessi, più o meno intenzionalmente, possono causare incidenti a causa del non adeguato trattamento dei dati sensibili, inviando una e-mail con dati sensibili al destinatario sbagliato, smarrendo un dispositivo portatile, utilizzando password deboli o impiegando la stessa password che utilizzano su siti pubblici.

Nessun programma di sicurezza può fronteggiare efficacemente il rischio informatico senza affrontare questa fondamentale vulnerabilità umana. Gli utenti aziendali a ogni livello hanno rischi diversi: ad esempio i dirigenti gestiscono dati più sensibili, gli amministratori di sistema hanno la capacità di controllare l'accesso a sistemi e applicazioni, infine gli utenti dei settori finanziario, risorse umane e contratti hanno tutti accesso a diversi tipi di informazioni riservate che possono renderli obiettivi.

La preparazione dovrebbe essere aggiornata regolarmente per aumentare la conoscenza in materia di sicurezza e scoraggiare rischiose alternative.

Procedure e strumenti

Un efficace programma di formazione sulla consapevolezza della sicurezza non dovrebbe ridursi ad un annuale video di formazione preconfezionato, abbinato a regolari test di phishing. Nonostante sia necessaria una formazione annuale, dovrebbero anche essere fornite frequentemente informative e notifiche aggiornate sulla sicurezza. Ciò potrebbe includere messaggi su: uso di password forti in coincidenza con una segnalazione sui media di una compromissione di password, aumento del phishing durante periodi particolari (fiscale), maggiore consapevolezza di e-mail dannose collegate alle spedizioni durante periodi particolari (festività).

La formazione aziendale dovrebbe anche considerare la posizione normativa e l'esposizione alle minacce. Le società finanziarie potrebbero avere una formazione più orientata alla conformità nell'uso e gestione dei dati, le imprese sanitarie sulla gestione delle informazioni sanitarie e quelle commerciali sui dati relativi alle carte di credito.

La formazione per il "social engineering" oltre ai test di phishing, dovrebbe includere anche la consapevolezza delle tattiche adottate per i diversi ruoli. Ad esempio, il team finanziario potrebbe ricevere messaggi da e-mail aziendali compromesse (BEC) che si spacciano per dirigenti contenenti richieste di trasferimento di denaro oppure e-mail da partner o fornitori compromessi che chiedono la modifica delle informazioni del conto bancario per il loro prossimo pagamento.

Per un approfondimento di questo argomento, le risorse seguenti sono utili per creare un programma efficace di sensibilizzazione alla sicurezza:

- **NIST® SP 800-50 Infosec Formazione sulla Consapevolezza:** https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf
- **Centro Nazionale per la Sicurezza Informatica (UK):** https://www.ncsc.gov.uk/guidance/10-steps-user-education-and-awareness
- **EDUCAUSE:** https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/awareness-campaigns
- **National Cyber Security Alliance (NCSA):** https://staysafeonline.org/
- **SANS:** https://www.sans.org/security-awareness-training/resources
- **Per la guida alla configurazione dei routers domestici, si faccia riferimento a CIS Controls Telework and Small Office Network Security Guide:** https://www.cisecurity.org/white-papers/cis-controls-telework-and-small-office-network-security-guide/

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
14.1	**Stabilire e Mantenere un Programma di Sensibilizzazione alla Sicurezza**	N/A	Proteggere	●	●	●
	Stabilire e mantenere un programma di sensibilizzazione alla sicurezza. Lo scopo è quello di istruire il personale su come interagire con le risorse e i dati aziendali in modo sicuro. Effettuare la formazione al momento dell'assunzione e, come minimo, annualmente. Rivedere e aggiornare i contenuti annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.					
14.2	**Formare il Personale nel Riconoscimento degli Attacchi Social Engineering**	N/A	Proteggere	●	●	●
	Formare il personale nel riconoscimento degli attacchi social engineering, come il phishing, pre-texting e tailgating.					
14.3	**Formare il Personale sulle Migliori Tecniche di Autenticazione**	N/A	Proteggere	●	●	●
	Formare il personale sulle migliori tecniche di autenticazione. Alcuni esempi includono MFA, composizione delle password e gestione delle credenziali.					
14.4	**Formare il Personale sulle Migliori Tecniche di Gestione dei Dati**	N/A	Proteggere	●	●	●
	Formare il personale su come identificare, salvare trasferire, archiviare e cancellare in modo appropriato i dati sensibili. È compresa la formazione del personale sulla disattivazione dello schermo quando viene lasciata la postazione, sulla cancellazione di lavagne fisiche o virtuali a fine riunione, sull'archiviazione sicura di dati e risorse					

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
14.5	**Formare il Personale sulle Cause di Esposizione Involontaria di Dati** Formare il personale sulle cause di esposizione involontaria di dati. Alcuni esempi includono l'errato trasferimento di dati sensibili, la perdita di un dispositivo portatile dell'utente finale o la pubblicazione di dati non dovuta.	N/A	Proteggere	●	●	●
14.6	**Formare il Personale sul Riconoscimento e Segnalazione degli Incidenti di Sicurezza** Formare il personale affinché riconosca un potenziale incidente e possa segnalarlo	N/A	Proteggere	●	●	●
14.7	**Formare il Personale su Identificazione e Segnalazione di Mancati Aggiornamenti dei Dispositivi Aziendali** Formare il personale per capire come verificare e segnalare un mancato aggiornamento automatizzato di uno strumento o procedura. Parte di questa formazione dovrebbe prevedere la modalità di segnalazione al personale IT di qualsiasi malfunzionamento di strumenti o procedure automatizzati.	N/A	Proteggere	●	●	●
14.8	**Formare il Personale sui Pericoli di Connessione e Trasmissione di Dati Aziendali su Reti non Sicure** Formare il personale sui pericoli della connessione e della trasmissione di dati su reti non sicure per le attività aziendali. Se l'azienda dispone di lavoratori remoti, la formazione deve includere le indicazioni per garantire che tutti gli utenti configurino in modo sicuro la propria infrastruttura di rete domestica.	N/A	Proteggere	●	●	●
14.9	**Effettuare una Formazione Specifica sulla Competenze e per la Sensibilizzazione sulla Sicurezza** Effettuare una formazione specifica sulle competenze e per la sensibilizzazione sulla sicurezza. Esempi di implementazione includono corsi di amministrazione sicura dei sistemi per il personale IT (OWASP® Top 10 sulla consapevolezza e prevenzione delle vulnerabilità per sviluppatori di applicazioni Web e formazione avanzata sulla sensibilizzazione social engineering per ruoli di alto profilo).	N/A	Proteggere		●	●

CONTROLLI 15

Gestione dei Service Provider

SAFEGUARDS TOTAL	7	IG1	1/7	IG2	4/7	IG3	7/7

Panoramica

Sviluppare una procedura per valutare i Service Provider che detengono dati sensibili o sono responsabili delle piattaforme o dei processi IT aziendali più importanti, per assicurarsi che proteggano tali piattaforme ed i dati in modo appropriato.

Perché questo controllo è importante?

Nel nostro mondo, moderno e connesso, le aziende si affidano a fornitori e partner per gestire i propri dati o si affidano a infrastrutture di terze parti per le principali funzioni o applicazioni.

Ci sono stati numerosi esempi in cui le violazioni subite da terzi hanno determinato significativi impatti aziendali; ad esempio, già alla fine degli anni 2000, le carte di pagamento sono state compromesse dopo che gli aggressori si erano infiltrati tra i fornitori di terze parti, nella vendita al dettaglio. Esempi più recenti includono attacchi ransomware che producono un impatto indiretto su un'azienda, dovuto al blocco di uno dei service provider, causando l'interruzione dell'attività. Ancor peggio, in caso di connessione diretta, un attacco ransomware potrebbe crittografare anche i dati della sede aziendale.

La maggior parte delle norme sulla sicurezza dei dati e sulla privacy richiedono che la protezione si estenda ai service provider di terze parti, come previsto dagli Accordi sulla Responsabilità e Portabilità dell'Assicurazione Sanitaria (HIPAA) nel settore sanitario, i requisiti del Consiglio di Valutazione delle Istituzioni Finanziarie Federali (FFIEC) per il settore finanziario e il Cyber Essentials per il Regno Unito. L'affidabilità di terze parti è una funzione fondamentale per il Rischio di Governance e Conformità (GRC), in quanto i rischi non gestiti all'interno dell'azienda, vengono trasferiti a strutture esterne.

Nonostante l'aggiornamento della sicurezza attuato da terze parti sia un'attività consolidata da decenni, non esiste uno standard universale di valutazione della sicurezza; inoltre molti service provider vengono controllati dai loro clienti più volte al mese, con inevitabili ripercussioni sulla produttività; questo avviene in quanto ogni azienda segue una diversa "checklist" o un insieme di standard per valutare il service provider. Esistono solo pochi standard di settore, ad esempio nella finanza con il programma Shared Assessments, o nell'istruzione superiore, con lo Strumento di Valutazione dei Fornitori dell'Educazione Superiore (HECVAT). Anche le compagnie assicurative che vendono polizze di sicurezza informatica hanno i propri criteri.

Mentre una grande azienda può essere interessata alle grandi società di hosting o cloud perché già ospitano la posta elettronica o altre applicazioni aziendali vitali, le aziende più piccole sono spesso soggette ad un rischio maggiore. Sovente, un fornitore di servizi di terze parti stipula ulteriori contratti con altre strutture per fornire diversi plug-in o servizi, ad esempio, quando venga utilizzata una piattaforma o un prodotto di "quarte parti" per supportare l'impresa principale.

Procedure e strumenti

La maggior parte delle aziende ha utilizzato abitualmente liste di controllo standard, come quelle della ISO 27001 o dei Controlli CIS. Spesso, questo processo viene gestito tramite fogli di calcolo, tuttavia oggi sono disponibili piattaforme online che consentono la gestione centralizzata di questo processo. L'attenzione di questo Controllo CIS non è però rivolta alla lista di controllo ma ai fondamenti del programma. Assicurare l'aggiornamento annualmente, poiché relazioni e dati potrebbero cambiare.

Indipendentemente dalle dimensioni aziendali, dovrebbe esserci un criterio di revisione dei service provider con relativo inventario ed e una valutazione del rischio associata al potenziale impatto sull'azienda in caso di incidente. Dovrebbe esserci anche un riferimento contrattuale per evidenziarne la responsabilità in caso di incidente con conseguente impatto sull'attività lavorativa.

Esistono piattaforme di valutazione di terzi che dispongono di un inventario di migliaia di service provider, che possono fornire una visione complessiva del settore, aiutando le aziende a prendere decisioni più informate sui rischi. Queste piattaforme adottano un sistema di punteggio di rischio dinamico per i service provider, basato (di solito) su valutazioni tecniche passive o completato da ulteriori valutazioni aziendali di terzi.

Quando si eseguono le revisioni, bisogna concentrarsi sui servizi o i reparti aziendali supportati dal provider. Un terzo che abbia un contratto per il servizio di gestione della sicurezza, o un intermediario, che abbia un'assicurazione sulla sicurezza informatica, può aiutare nella riduzione del rischio.

È anche importante disattivare in modo sicuro i service provider alla scadenza o risoluzione contrattuale. Le attività di interruzione possono includere la disattivazione degli account utente e di servizio, la sospensione dei flussi di dati e l'eliminazione sicura delle informazioni aziendali.

→ **Nel caso, fare riferimento a NIST® 800-88r1:** Linee Guida Sanificazione dei Media: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf.

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
15.1	**Stabilire e Mantenere un Inventario dei Service Providers**	N/A	Identificare	●	●	●
	Stabilire e mantenere un inventario dei service providers. L'inventario deve riportare tutti i service providers conosciuti, compresa la classificazione e il contatto aziendale designato. Rivedere ed aggiornare l'inventario annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.					
15.2	**Stabilire e Mantenere un Criterio di Gestione del Service Provider**	N/A	Identificare		●	●
	Stabilire e mantenere un criterio di gestione del service provider. Garantire che i criteri includano la classificazione, l'inventario, la valutazione, il monitoraggio e la disattivazione dei service provider. Rivedere ed aggiornare i criteri annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.					
15.3	**Classificare i Service Providers**	N/A	Identificare		●	●
	Classificare i service provider. La classificazione può includere una o più caratteristiche, come la sensibilità dei dati, volume dei dati, requisiti di disponibilità, normative applicabili, rischio intrinseco e rischio mitigato. Rivedere ed aggiornare la classificazione annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.					
15.4	**Garantire che i Contratti dei Service Provider Includano Requisiti di Sicurezza**	N/A	Proteggere		●	●
	Garantire che i contratti dei service provider includano i requisiti di sicurezza. Esempi di requisiti possono includere: requisiti minimi del programma di sicurezza, notifica e risposta di incidenti di sicurezza e / o violazione dei dati, requisiti di crittografia dei dati e procedure di dismissione dei dati. Questi requisiti di sicurezza devono essere coerenti con la politica di gestione del service provider aziendale. Rivedere i contratti del service provider annualmente per garantire la presenza di tali requisiti.					
15.5	**Valutare i Service Provider**	N/A	Identificare			●
	Valutare i service provider aziendali in coerenza con i relativi criteri di gestione. La valutazione può variare in base alle classificazioni e può includere la revisione di rapporti di valutazione standardizzati, come il Servizio di Controllo Organizzazione 2 (SOC 2) e l'Attestato di Conformità (AoC) del Settore delle Carte di Pagamento (PCI), questionari personalizzati o altre adeguate e rigorose procedure. Rivalutare i fornitori di servizi annualmente o in occasione nuovo contratto o di suo di rinnovo.					
15.6	**Controllare i Service Providers**	Dati	Rilevare			●
	Controllare i service provider aziendali in coerenza con i relativi criteri di gestione. Il monitoraggio può includere una rivalutazione periodica della conformità, il monitoraggio delle note di rilascio e il monitoraggio del dark web.					
15.7	**Disattivazione Sicura dei Service Providers**	Dati	Proteggere			●
	Disattivazione sicura dei service providers. Esempi di considerazioni includono la disattivazione degli account utente e di servizio, l'interruzione dei flussi di dati e la rimozione sicura dei dati aziendali dai sistemi.					

CONTROLLI 16

Sicurezza degli Applicativi

SAFEGUARDS TOTAL	14	IG1	0/14	IG2	11/14	IG3	14/14

Panoramica

Gestire la sicurezza del ciclo di vita del software sviluppato in proprio, ospitato o acquistato per prevenire, rilevare e rimediare ai punti deboli di sicurezza prima che possano impattare sull'azienda.

Perché questo controllo è importante?

Le applicazioni forniscono un'interfaccia di facile utilizzo per consentire agli utenti di accedere e gestire i dati a seconda delle funzioni aziendali. Riducono inoltre al minimo la necessità per gli utenti di occuparsi direttamente di funzioni di sistema complesse (e potenzialmente a rischio di errori), come l'accesso a un database per inserire o modificare file. Le aziende utilizzano le applicazioni per gestire i dati più sensibili e controllare l'accesso alle risorse di sistema. Quindi, un utente malintenzionato può utilizzare l'applicazione medesima per compromettere i dati, invece di adottare una complessa sequenza di hacking di rete e di sistema per aggirarne i controlli e i sensori di sicurezza. Questo è il motivo per cui è così importante proteggere le credenziali dell'utente (in particolare le credenziali dell'applicazione) definite nei Controlli CIS 6.

Se mancano le credenziali, i difetti delle applicazioni diventano il primo vettore di attacco. Tuttavia, le applicazioni moderne vengono sviluppate, gestite e mantenute in un ambiente molto complesso, diversificato e dinamico. Le applicazioni sono disponibili per più piattaforme: web, mobile, cloud, ecc., con architetture applicative più complesse rispetto alle strutture più obsolete client-server o database-web server. I cicli di vita dello sviluppo sono diventati più brevi, passando da mesi o anni in lunghe metodologie a cascata, a cicli DevOps con frequenti aggiornamenti del codice. Inoltre, le applicazioni vengono raramente create da zero e spesso vengono "assemblate" in un complesso mix di framework di sviluppo, librerie, codice esistente e nuovo. Esistono anche moderne normative in evoluzione sulla protezione dei dati che si occupano della privacy degli utenti. Tutto ciò può richiedere la conformità a requisiti di protezione dei dati a livello regionale o per specifici settori.

Questi fattori rendono gli approcci tradizionali alla sicurezza, come il controllo (processi, codici sorgente, ambiente di runtime, ecc.), l'ispezione e la verifica, molto più impegnativi. Inoltre, il rischio introdotto da una vulnerabilità di un'applicazione potrebbe non essere compreso, se non in un contesto specifico o operativo.

Le vulnerabilità delle applicazioni possono essere presenti per varie ragioni: progettazione non sicura, infrastruttura non sicura, errori di codice, autenticazione debole ed errori di verifica in condizioni insolite o impreviste. Gli aggressori possono sfruttare vulnerabilità specifiche, tra cui buffer overflow, esposizione a iniezione

SQL (Linguaggio di Query Strutturato), scripting tra siti, richieste falsificate tra siti e clickjacking del codice per ottenere l'accesso a dati sensibili o assumere il controllo di risorse vulnerabili all'interno dell'infrastruttura come base di partenza per ulteriori attacchi.

Le applicazioni e i siti Web possono essere utilizzati anche per raccogliere credenziali, dati o tentare di installare malware sulle utenze che vi accedono.

Infine, ora è più comune acquisire piattaforme Software come Servizio (SaaS), in cui il software viene sviluppato e gestito direttamente da terzi. Questi potrebbero essere ospitati in qualsiasi parte del mondo. Le aziende devono quindi affrontare la sfida nel riconoscere quali rischi stanno accettando con l'utilizzo di queste piattaforme, spesso non avendo alcuna visibilità sullo sviluppo e sulle pratiche di sicurezza delle applicazioni. Alcune di queste piattaforme SaaS consentono la personalizzazione delle loro interfacce e dei database. Le aziende che adottano tali applicazioni dovrebbero seguire questo Controllo CIS, come se stessero effettuando uno sviluppo ex-novo per il cliente.

Procedure e strumenti

Per la Versione 8, CIS ha collaborato con SAFECode per aiutare a sviluppare le procedure e le salvaguardie per l'aggiornamento di questo controllo di sicurezza del software applicativo. Tuttavia, tale ambito è per natura un argomento vasto e quindi (coerentemente con i principi generali dei Controlli CIS), ci concentriamo sulle Salvaguardie più importanti. Queste derivano da un documento complementare sulla sicurezza del software applicativo sviluppato da SAFECode (riportato di seguito), che fornisce una trattazione più approfondita dell'argomento ed è coerente con gli attuali contenuti di SAFECode.

SAFECode ha sviluppato un approccio a tre livelli per aiutare i lettori a identificare in quale gruppo di sviluppo (Development Group) si collocano come livello di maturità per i programmi di sviluppo. I tre livelli CIS IG utilizzati nelle Salvaguardie hanno ispirato il loro approccio per i DG seguenti:

Gruppo di Sviluppo (DG) 1

- L'azienda utilizza soprattutto software standard o Open Source (OSS) e pacchetti con solo l'aggiunta occasionale di piccole applicazioni o codice di siti web. L'impresa è in grado di applicare le migliori pratiche operative e procedurali di base e di gestire la sicurezza del software fornito dal fornitore seguendo la guida dei Controlli CIS.

Gruppo di Sviluppo (DG) 2

- L'azienda utilizza alcune applicazioni web personalizzate (sviluppate in proprio o da un appaltatore) e / o in codice nativo integrando componenti di terze parti, che vengono eseguite in locale o in cloud. L'azienda dispone di uno staff di sviluppo che applica le migliori pratiche di sviluppo del software. L'impresa è attenta alla qualità e alla manutenzione del codice open source o commerciale di terzi parti da cui dipende.

Gruppo di Sviluppo (DG) 3

- L'azienda effettua un investimento importante nel software personalizzato necessario per gestire la propria attività e servire i clienti. Può ospitare software sulla propria infrastruttura, nel cloud o su entrambi e può integrare un'ampia gamma di componenti software commerciali e open source di terzi. I fornitori di software e le aziende che forniscono SaaS dovrebbero considerare il Gruppo di Sviluppo 3 come un insieme minimo di requisiti.

Il primo passo nello sviluppo di un programma di sicurezza delle applicazioni consiste nell'implementare una procedura di gestione delle vulnerabilità. Questa deve integrarsi nel ciclo di vita dello sviluppo e dovrebbe essere di semplice inserimento nel processo standard di correzione dei bug. La procedura dovrebbe includere l'analisi della causa principale per correggere i difetti derivanti, in modo da ridurre le vulnerabilità future ed un livello di gravità per dare una priorità agli interventi di correzione.

Gli sviluppatori devono essere formati sui concetti di sicurezza delle applicazioni e sulle pratiche di codifica sicura, includendo un processo per acquisire o valutare software, moduli e librerie di terze parti utilizzati nell'applicazione garantendo che non introducano difetti di sicurezza. Gli sviluppatori dovrebbero ricevere una formazione su quali tipi di moduli si possono utilizzare in modo sicuro, dove possono essere acquisiti in sicurezza e quali componenti possano sviluppare autonomamente (ad esempio la crittografia) oppure no.

Le debolezze dell'infrastruttura che supporta queste applicazioni possono introdurre dei rischi. I Controlli CIS e il concetto di minimizzare la superficie di attacco possono aiutare a proteggere reti, sistemi e account utilizzati all'interno dell'applicazione. Una guida specifica è disponibile nei Controlli CIS 1-7, 12 e 13.

Il programma di sicurezza delle applicazioni ideale è quello che la introduce il prima possibile nel ciclo di vita dello sviluppo del software. La gestione dei problemi di sicurezza dovrebbe essere coerente e integrata con la gestione standard di difetti / bug del software, piuttosto che prevista in un processo separato di competenza del sistema di sviluppo. I gruppi di sviluppo più grandi o più evoluti dovrebbero prendere in considerazione la pratica della modellazione delle minacce nella fase di progettazione. Le vulnerabilità a livello di progettazione sono meno comuni delle vulnerabilità a livello di codice; tuttavia, spesso sono molto gravi e molto più difficili da risolvere rapidamente. La modellazione delle minacce è il processo di identificazione e risoluzione dei difetti di progettazione della sicurezza delle applicazioni prima che il codice venga creato. Tale modellazione richiede una formazione specifica, conoscenze tecniche e aziendali. Meglio sarebbe se fosse eseguita da "campioni della sicurezza" in ogni gruppo di sviluppo, per guidare le attività di modellazione delle minacce per il software di quel team. Fornisce inoltre un contesto prezioso per le successive attività, come l'analisi della causa principale e i test di sicurezza.

I gruppi di sviluppo più grandi o commerciali possono anche prendere in considerazione un programma di "caccia al bug" in cui si possono pagare addetti al fine di trovare difetti nelle loro applicazioni. Tale programma viene utilizzato al meglio per integrare una procedura interna di sviluppo sicura e può fornire un modo efficiente per identificare le classi di vulnerabilità su cui tale procedura deve concentrarsi.

Infine, nel 2020 il NIST® ha pubblicato il suo Framework di Sviluppo Software Sicuro (SSDF), che ha riunito ciò che il settore ha appreso sulla sicurezza del software negli ultimi vent'anni creando un framework di sviluppo del software sicuro per la pianificazione, valutazione e comunicazione delle attività di sicurezza sul software. Le aziende che acquisiscono software o servizi possono utilizzare questo framework per creare i propri requisiti di sicurezza e capire se la procedura di sviluppo di un fornitore di software segue le best practice.

Alcune risorse per la sicurezza delle applicazioni:

- **SAFECode Supplemento sulla Sicurezza delle Applicazioni:** https://safecode.org/cis-controls/
- **NIST® SSDF:** https://csrc.nist.gov/News/2020/mitigating-risk-of-software-vulns-ssdf
- **The Software Alliance:** https://www.bsa.org/reports/updated-bsa-framework-for-secure-software
- **OWASP®:** https://owasp.org/

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
16.1	**Stabilire e Mantenere una Procedura di Sviluppo Sicuro delle Applicazioni** Stabilire e mantenere una procedura di sviluppo sicuro delle applicazioni. In questo procedimento si considerino elementi quali: standard di progettazione di applicazioni sicure, pratiche di codifica sicura, formazione per gli sviluppatori, gestione delle vulnerabilità, sicurezza del codice di terze parti e procedure di test di sicurezza delle applicazioni. Rivedere e aggiornare la documentazione annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero avere un impatto su questa Salvaguardia.	Applicazioni	Proteggere		●	●
16.2	**Stabilire e Mantenere una Procedura di Accettazione e Risoluzione delle Vulnerabilità** Stabilire e mantenere una procedura di accettazione e risoluzione delle segnalazioni di vulnerabilità del software, inclusa quella dedicata per la segnalazione da parte di entità esterne. Il procedimento deve includere elementi quali: un criterio di gestione delle vulnerabilità che identifichi il processo di segnalazione, il responsabile della gestione delle segnalazioni di vulnerabilità e un sistema per la presa in carico, l'assegnazione, la risoluzione e la relativa verifica. Come parte del processo, utilizzare un sistema di rilevamento delle vulnerabilità che includa livelli di gravità e metriche per misurarne i tempi di identificazione, analisi e correzione. Rivedere e aggiornare la documentazione annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero avere un impatto su questa salvaguardia. Gli sviluppatori di applicazioni di terze parti devono rendere pubblici questi criteri al fine di soddisfare le aspettative delle parti interessate	Applicazioni	Proteggere		●	●
16.3	**Eseguire l'Analisi della Causa Principale sulle Vulnerabilità della Sicurezza** Eseguire l'analisi della causa principale sulle vulnerabilità della sicurezza. Quando si esaminano le vulnerabilità, l'analisi della causa principale è il lavoro di valutazione dell'origine sottostante che crea il punto debole nel codice permettendo ai team di sviluppo di andare oltre la semplice correzione dei singoli problemi quando si presentano.	Applicazioni	Proteggere		●	●
16.4	**Stabilire e Gestire un Inventario di Componenti Software di Terze Parti** Stabilire e gestire un inventario aggiornato dei componenti di terze parti utilizzati nello sviluppo, spesso indicato come "distinta del materiale", nonché dei componenti previsti per un uso futuro. Questo inventario deve includere i rischi che ogni componente di terzi potrebbe comportare. Valutare l'elenco almeno mensilmente per identificare eventuali modifiche o aggiornamenti a questi componenti e verificarne il corrente supporto.	Applicazioni	Proteggere		●	●
16.5	**Utilizzare Componenti Software di Terze Parti Aggiornati** Utilizzare componenti software di terze parti aggiornati e affidabili. Quando possibile, scegliere framework e librerie consolidati e comprovati che forniscano una sicurezza adeguata. Acquisire questi componenti da fonti attendibili o valutare le vulnerabilità del software prima dell'uso.	Applicazioni	Proteggere		●	●

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
16.6	**Stabilire e Mantenere un Sistema di Valutazione della Gravità e una Procedura per le Vulnerabilità delle Applicazioni** Stabilire e mantenere un sistema di valutazione della gravità e una procedura per le vulnerabilità delle applicazioni che faciliti la priorità dell'ordine in cui vengono scoperte e risolte. Questo processo include la definizione di un livello minimo di accettabilità di sicurezza per il rilascio di codice o applicazioni. I livelli di gravità offrono un modo sistematico di valutazione delle vulnerabilità che migliorano la gestione del rischio e aiutano a garantire che i bug più gravi vengano corretti per primi. Rivedere e aggiornare il sistema e la procedura annualmente.	Applicazioni	Proteggere		●	●
16.7	**Utilizzare Modelli di Hardening Standard per la Configurazione dell'Infrastruttura Applicativa** Utilizzare modelli di hardening standard di tipo industriale per la configurazione dei componenti dell'infrastruttura applicativa. Ciò include i relativi server, i database, i server web e si applica ai contenitori cloud, ai componenti Platform as a Service (PaaS) e ai componenti SaaS. Non consentire al software sviluppato internamente di indebolire l'hardening della configurazione.	Applicazioni	Proteggere		●	●
16.8	**Separare i Sistemi in Produzione e da quelli non in Produzione** Mantenere ambienti separati tra i sistemi in produzione e quelli non in produzione	Applicazioni	Proteggere		●	●
16.9	**Formare gli Sviluppatori sui Concetti di Sicurezza delle Applicazioni e sulla Codifica Sicura** Garantire che tutto il personale di sviluppo software riceva formazione sulla scrittura di codice sicuro per il proprio ambiente di sviluppo e le proprie responsabilità. La formazione può includere principi generali di sicurezza e pratiche standard di sicurezza delle applicazioni. Predisporre la formazione almeno annualmente e progettandola in modo da promuovere la sicurezza all'interno del team di sviluppo e favorire la cultura della sicurezza tra gli sviluppatori.	Applicazioni	Proteggere		●	●
16.10	**Applicare Principi di Progettazione Sicura nelle Architetture Applicative** Applicare principi di progettazione sicura nelle architetture applicative. I principi di progettazione sicura includono il concetto di privilegio minimo e l'applicazione della mediazione per validare ogni operazione eseguita dall'utente, applicando il concetto di "non fidarsi mai dell'input dell'utente". Gli esempi includono la garanzia che il controllo degli errori espliciti venga eseguito e documentato per tutti gli input, inclusi dimensioni, tipi di dati, intervalli o formati accettabili. Progettazione sicura significa anche ridurre al minimo la superficie di attacco dell'infrastruttura dell'applicazione, disattivando porte e servizi non protetti, rimuovendo programmi e file non necessari e rinominando o rimuovendo gli account predefiniti..	Applicazioni	Proteggere		●	●
16.11	**Utilizzare Moduli o Servizi Controllati per i Componenti di Sicurezza delle Applicazioni** Utilizzare moduli o servizi controllati per i componenti di sicurezza delle applicazioni, come la gestione delle identità, la crittografia, il controllo e il logging. L'utilizzo delle funzionalità della piattaforma nelle funzioni di sicurezza più importanti ridurrà il carico di lavoro degli sviluppatori e ridurrà al minimo la probabilità di errori di progettazione o implementazione. I sistemi operativi moderni forniscono meccanismi efficaci per l'identificazione, l'autenticazione e l'autorizzazione e li rendono disponibili per le applicazioni. Utilizzare solo algoritmi di crittografia standardizzati, attualmente accettati e ampiamente controllati. I sistemi operativi forniscono anche meccanismi per creare e mantenere i log di controllo	Applicazioni	Proteggere		●	●
16.12	**Implementare Controlli di Sicurezza a Livello di Codice** Applicare strumenti di analisi statica e dinamica nel ciclo di vita dell'applicazione per verificare che vengano seguite pratiche di codifica sicura.	Applicazioni	Proteggere			●
16.13	**Effettuare Test di Penetrazione sull'Applicazione** Effettuare test di penetrazione sulle applicazioni. Per le applicazioni critiche, i test di penetrazione autenticati sono più adatti per trovare vulnerabilità rispetto alla scansione del codice e ai test di sicurezza automatizzati. Il test di penetrazione si basa sull'abilità del tester di manipolare un'applicazione come utente autenticato e non autenticato.	Applicazioni	Proteggere			●
16.14	**Effettuare la Modellazione delle Minacce** Effettuare la modellazione delle minacce. Consiste nell'identificazione e risoluzione dei difetti di progettazione della sicurezza delle applicazioni all'interno di un progetto, prima della creazione del codice. Viene realizzata attraverso personale appositamente addestrato che valuta la progettazione dell'applicazione misurando i rischi per la sicurezza per ogni punto di ingresso e livello di accesso. L'obiettivo è mappare l'applicazione, l'architettura e l'infrastruttura in modo strutturato per comprenderne i punti deboli.	Applicazioni	Proteggere			●

CONTROLLI 17

Gestione e Risposta agli Incidenti

SAFEGUARDS TOTAL	9	IG1	3/9	IG2	8/9	IG3	9/9

Panoramica

Stabilire un programma per sviluppare e mantenere una capacità di risposta agli incidenti (ad esempio criteri, piani, procedure, ruoli definiti, formazione e comunicazioni) per prepararsi a rilevare e rispondere rapidamente ad un attacco.

Perché questo controllo è importante?

Un programma completo di sicurezza informatica include protezione, rilevamento, risposta e capacità di ripristino. Spesso, gli ultimi due vengono trascurati nelle imprese meno evolute, oppure la tecnica di risposta adottata per i sistemi compromessi consiste semplicemente nel ripristino allo stato originale per poter ripartire. L'obiettivo principale della risposta agli incidenti è identificare le minacce all'interno dell'azienda, rispondere prima che si diffondano e rimediare prima che possano causare danni. Non comprendendo completamente l'ambito di un incidente, come si è verificato e cosa si può fare per evitare che accada di nuovo, i difensori ripeteranno sempre e soltanto uno schema come nel gioco "colpisci la talpa".

Non possiamo attendere un'efficacia al 100% delle nostre protezioni. Quando si verifica un incidente, se un'impresa non dispone di un piano documentato, anche con personale preparato, è quasi impossibile conoscere le corrette procedure investigative, rapporti, raccolta dati, responsabilità di gestione, aspetti legali e strategia di comunicazione che consentiranno all'impresa di comprendere, gestire e recuperare con successo.

Oltre al rilevamento, al contenimento e all'eradicazione, la comunicazione con le parti interessate è fondamentale. Volendo ridurre la probabilità di un impatto tangibile dovuto a un evento informatico, la leadership aziendale deve sapere quale conseguenza potenziale potrebbe verificarsi, al fine di dare priorità alle decisioni di riparazione o ripristino che meglio si addicono all'azienda. Queste decisioni potrebbero basarsi sul rispetto normativo, regole di divulgazione, accordi sul livello di servizio con partner o clienti, aspetti economici o impatti sugli obiettivi aziendali.

Il tempo trascorso da quando si verifica un attacco a quando viene identificato può essere di giorni, settimane o mesi. Quanto più a lungo l'aggressore si trova nell'infrastruttura aziendale, tanto più diventerà integrato, sviluppando vari modi per mantenere l'accesso permanente anche quando verrà scoperto. Con il diffondersi del ransomware, che è una fonte di guadagno stabile per gli aggressori, il tempo di permanenza è fondamentale, soprattutto con le moderne tattiche di furto dei dati e successiva crittografia a scopo di riscatto.

Procedure e strumenti

Anche se un'azienda non dispone delle risorse per affrontare la risposta agli incidenti, è comunque fondamentale disporre di un piano. Ciò dovrebbe includere i meccanismi di protezioni e di rilevamento, l'elenco per le chiamate di assistenza e i modelli di comunicazione ovvero come trasmettere le informazioni a leadership, dipendenti, enti regolatori, partner e clienti.

Avendo definito le procedure di risposta agli incidenti, il team dedicato, o una terza parte, dovrebbe impegnarsi in una formazione periodica basata su scenari, lavorando attraverso una serie di circostanze di attacco basate sulle potenziali minacce che l'azienda potrebbe dover affrontare. Queste condizioni possono far comprendere alla leadership aziendale e i membri del team tecnico il loro ruolo nella procedura di gestione e risposta agli incidenti. È inevitabile che gli scenari di esempio e formazione identifichino lacune nei piani e nei processi, con correlazioni impreviste, che potranno tornare utili per l'aggiornamento del piano.

Le aziende più evolute dovrebbero includere l'intelligence sulle minacce e / o la loro ricerca nella procedura di risposta agli incidenti. Ciò aiuterà il team a diventare più proattivo, identificando gli aggressori chiave o principali della propria azienda, o settore, monitorando o cercando tra le proprie TTP. Ciò aiuterà a delineare i rilevamenti e definire le procedure di risposta per identificare e rimediare più rapidamente.

Le azioni nei Controlli CIS 17 forniscono sequenze specifiche ad alta priorità che possono migliorare la sicurezza aziendale e che dovrebbero far parte di qualsiasi piano di risposta agli incidenti. Inoltre, consigliamo la seguente risorsa dedicata a questo argomento:

→ **Consiglio dei Tester Sicurezza Autorizzati (CREST):** Guida per Risposta agli Incidenti di Cyber Sicurezza—che fornisce indicazioni, standard, e informazioni su una vasta gamma di argomenti riguardanti la difesa informatica: https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
17.1	**Designare il Personale Incaricato per la Gestione degli Incidenti** Designare una persona chiave e almeno un sostituto che dirigerà la procedura di gestione degli incidenti. Il personale di gestione è responsabile del coordinamento e della documentazione delle attività di risposta e agli incidenti e relativo ripristino; ci si può avvalere di dipendenti interni, terzi o scegliendo una soluzione ibrida. Se si utilizza un fornitore di terze parti, designare almeno una persona interna all'azienda per supervisionarne il lavoro. Rivedere annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero avere un impatto su questa Salvaguardia.	N/A	Rispondere	●	●	●
17.2	**Stabilire e Mantenere le Informazioni di Contatto per la Segnalazione degli Incidenti di Sicurezza** Stabilire e mantenere l'elenco delle figure che devono essere informate degli incidenti di sicurezza. I contatti possono includere personale interno, fornitori di terze parti, forze dell'ordine, compagnie di assicurazione informatica, agenzie governative, partner del Centro di Condivisione e Analisi delle Informazioni (ISAC) o altre parti interessate. Verificare i contatti annualmente per garantire che le informazioni siano aggiornate.	N/A	Rispondere	●	●	●

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
17.3	**Stabilire e Mantenere una Procedura Aziendale di Segnalazione degli Incidenti** Stabilire e mantenere una procedura per il personale aziendale per segnalare gli incidenti di sicurezza. Sono inclusi i tempi di segnalazione, il personale di riferimento, il meccanismo di segnalazione e le informazioni minime da riportare. Assicurare che il procedimento sia disponibile pubblicamente per tutto il personale. Rivedere annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero avere un impatto su questa Salvaguardia.	N/A	Rispondere	●	●	●
17.4	**Stabilire e Mantenere una Procedura di Risposta agli Incidenti** Stabilire e mantenere una procedura di risposta agli incidenti che preveda ruoli e responsabilità, requisiti di conformità e un piano di comunicazione. Rivedere annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero avere un impatto su questa Salvaguardia.	N/A	Rispondere		●	●
17.5	**Assegnare Ruoli Chiave e Responsabilità** Assegnare ruoli chiave e responsabilità per la risposta agli incidenti, incluso il personale legale, IT, sicurezza delle informazioni, strutture, pubbliche relazioni, risorse umane, referenti di incidenti e analisti, se possibile. Rivedere annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero avere un impatto su questa Salvaguardia.	N/A	Rispondere		●	●
17.6	**Definire i Meccanismi di Comunicazione Durante la Risposta agli Incidenti** Determinare quali modalità primarie e secondarie verranno utilizzati per comunicare e segnalare durante un incidente di sicurezza. I meccanismi possono includere telefonate, e-mail o lettere. Tenere presente che determinati meccanismi, come le e-mail, potrebbero non funzionare in seguito ad un incidente di sicurezza. Rivedere annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero avere un impatto su questa Salvaguardia.	N/A	Rispondere		●	●
17.7	**Condurre Esercizi di Routine in Risposta agli Incidenti** Pianificare e condurre esercizi di routine e scenari in risposta agli incidenti per il personale chiave coinvolto nella procedura per prepararlo a fronteggiare l'eventualità in casi reali. Gli esercizi devono testare i canali di comunicazione, il processo decisionale e i flussi di lavoro. Effettuare test almeno su base annuale.	N/A	Recuperare		●	●
17.8	**Effettuare Revisioni Post-Incidente** Effettuare revisioni post-incidente. Le revisioni post-incidente aiutano a prevenire il ripetersi di incidenti attraverso l'identificazione delle lezioni apprese e l'azione di follow-up.	N/A	Recuperare		●	●
17.9	**Stabilire e Mantenere i Livelli per gli Incidenti di Sicurezza** Stabilire e mantenere i livelli per gli incidenti di sicurezza, inclusa, come minimo, la differenziazione tra un incidente e un evento. Gli esempi possono includere: attività anomale, vulnerabilità della sicurezza, debolezza della sicurezza, violazione dei dati, incidente di privacy, ecc. Rivedere annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero avere un impatto su questa Salvaguardia.	N/A	Recuperare			●

CONTROLLI 18

Test di Penetrazione

SAFEGUARDS TOTAL	5	IG1	0/5	IG2	3/5	IG3	5/5

Panoramica

Verificare l'efficacia e la resilienza delle risorse aziendali identificando e sfruttando i punti deboli nei controlli (persone, processi e tecnologia) e simulando obiettivi ed azioni di un utente malintenzionato.

Perché questo controllo è importante?

Un atteggiamento difensivo di successo richiede un programma completo di criteri e amministrazione efficace, difese tecniche solide, combinate con un atteggiamento adeguato da parte delle persone. Tuttavia raramente si raggiunge la perfezione. In un ambiente complesso in cui la tecnologia è in continua evoluzione e con la comparsa regolare di nuovi aggressori, le aziende dovrebbero testare periodicamente i propri controlli per identificare le lacune e valutare la resilienza. Questo test può essere condotto dal punto di vista della rete esterna, della rete interna, dell'applicazione, del sistema o del dispositivo. Può includere il social engineering degli utenti o il bypass del controllo per l'accesso fisico.

Spesso i test di penetrazione vengono eseguiti per scopi specifici:

- Come dimostrazione concreta di un attacco, di solito per convincere i responsabili delle debolezze aziendali
- Come mezzo per testare il corretto funzionamento delle difese aziendali ("verifica")
- Per verificare prima di tutto che l'impresa abbia costruito le giuste difese ("convalida")

I test di penetrazione indipendenti possono fornire informazioni utili e oggettive sull'esistenza di vulnerabilità nelle risorse aziendali e nelle persone ma anche sull'efficacia delle difese e dei controlli di mitigazione per la protezione dagli impatti negativi a danno dell'azienda. Sono inoltre parte di un più completo e continuo programma di gestione e miglioramento della sicurezza. Possono anche rivelare punti deboli del processo, come la gestione incompleta o incoerente della configurazione o la formazione degli utenti finali.

I test di penetrazione sono diversi dal test di vulnerabilità, descritti nei Controlli CIS 7. I test di vulnerabilità controllano soltanto la presenza di risorse aziendali note non sicure, non oltre. I test di penetrazione si spingono più avanti per sfruttare tali punti deboli e vedere fino a che punto potrebbe arrivare un utente malintenzionato e quali processi o dati aziendali potrebbero essere coinvolti dallo sfruttamento di tali vulnerabilità. Questo è un dettaglio importante e spesso i test di penetrazione

e i test di vulnerabilità vengono utilizzati in modo errato o intercambiabile. I test di vulnerabilità sono soltanto una scansione automatizzata con una saltuaria convalida manuale dei falsi positivi, mentre i test di penetrazione richiedono maggior coinvolgimento ed analisi da parte umana, a volte con l'ausilio di strumenti o script personalizzati. Comunque, i test di vulnerabilità, sono spesso un punto di partenza per i test di penetrazione.

Un altro termine comune sono le esercitazioni del "Red Team": sono simili ai test di penetrazione in quanto vengono sfruttate le vulnerabilità tuttavia, la differenza, è il focus. I "Red Team" simulano specifiche TTP degli aggressori per valutare come l'ambiente aziendale possa resistere ad un attacco da parte di un aggressore specifico o di una categoria di avversari.

Procedure e strumenti

I test di penetrazione iniziano con l'ispezione dell'impresa e dell'ambiente e con la scansione per identificare le vulnerabilità che possono essere utilizzate come punti di acceso. È importante assicurarsi che vengano individuate tutte le risorse nell'ambito aziendale, non basandosi solo su un elenco statico, che potrebbe essere datato o incompleto; successivamente, verranno identificate le vulnerabilità in questi obiettivi. Gli exploit vengono eseguiti per dimostrare in modo specifico come un avversario possa sia minare gli obiettivi di sicurezza dell'azienda (esempio la protezione di dati sensibili specifici) sia raggiungere obiettivi specifici (esempio l'attivazione di una infrastruttura segreta di Comando e Controllo—C2). I risultati forniscono informazioni approfondite, dimostrando i rischi aziendali dovuti alle varie vulnerabilità. Questa azione può essere mirata ai controlli di accesso fisico, alla rete, al sistema o ai livelli dell'applicazione, includendo spesso componenti di social engineering.

I test di penetrazione sono costosi, complessi e potenzialmente introducono rischi intrinseci. Devono essere condotti da fornitori affidabili con personale esperto. Alcuni rischi includono l'arresto improvviso di sistemi che potrebbero essere instabili, alcuni exploit potrebbero cancellare o modificare dati e configurazioni. L'esito di un rapporto di test deve inoltre essere protetto a sua volta, dato che fornisce istruzioni passo passo su come entrare in l'azienda e colpire risorse o dati critici.

Ogni azienda dovrebbe definire obiettivi chiari e regole di ingaggio per i test di penetrazione. L'ambito di queste attività dovrebbe includere, come minimo, le risorse aziendali con le informazioni di maggior valore e la funzionalità della produzione. Anche altri sistemi di minor valore possono essere testati per capire se possano essere usati come punti di partenza per compromettere obiettivi di valore superiore. Le regole di ingaggio per le analisi dei test di penetrazione dovrebbero descrivere, come minimo, momenti della giornata per il test, la durata e l'approccio generale. Solo poche persone nell'azienda dovrebbero sapere quando viene eseguito un test di penetrazione e in caso di problemi dovrebbe essere designato un contatto principale in azienda. Di recente si sta diffondendo la pratica di condurre i test di penetrazione tramite consulenti legali di terze parti per proteggere i rapporti dalla divulgazione.

Le salvaguardie in questo Controllo CIS forniscono passaggi specifici ad alta priorità che possono migliorare la sicurezza aziendale e dovrebbero far parte di qualsiasi test di penetrazione. Inoltre, si suggeriscono le ottime ed esaurienti risorse dedicate a questo argomento per supportare la pianificazione, la gestione e il reporting dei test di sicurezza:

→ **OWASP Metodologie dei Test di Penetrazione:** https://www.owasp.org/index.php/Penetration_testing_methodologies

→ **PCI Consiglio per gli Standard di Sicurezza:** https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf

Salvaguardie

SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
18.1	**Stabilire e Mantenere un Programma di Test di Penetrazione**	N/A	Identificare		●	●
	Stabilire e mantenere un programma di test di penetrazione adeguato alle dimensioni, alla complessità e alla maturità dell'azienda. Le caratteristiche del programma di test di penetrazione includono ambiti di rete, applicazioni Web, API (Interfaccia di Programmazione di un'Applicazione), servizi ospitati e controlli della sede fisica; frequenza, limitazioni (come orari accettabili e tipi di attacco esclusi), informazioni sul punto di contatto, azioni di rimedio (come i risultati verranno indirizzati internamente), requisiti retroattivi.					
18.2	**Eseguire Periodicamente Test di Penetrazione Esterni**	Rete	Identificare		●	●
	Eseguire periodicamente test di penetrazione esterni basati sui requisiti del programma, almeno annualmente. I test di penetrazione esterni devono includere l'ispezione dell'impresa e dell'ambiente per rilevare le informazioni soggette ad exploit. Questi test richiedono competenze ed esperienze specifiche e devono essere condotti da personale qualificato. I test possono avvenire in modalità "clear box" oppure "opaque box".					
18.3	**Correggere Considerando i Risultati del Test di Penetrazione**	Rete	Proteggere		●	●
	Rimediare in base ai risultati dei test di penetrazione considerando i criteri aziendali riferiti all'ambito di correzione ed ai livelli di priorità.					
18.4	**Convalidare le Misure di Sicurezza**	Rete	Proteggere			●
	Convalidare le misure di sicurezza dopo ogni test di penetrazione. Se si ritiene necessario, modificare i set di regole e le capacità di rilevamento delle tecniche utilizzate durante i test.					
18.5	**Eseguire Periodicamente Test di Penetrazione Interni**	N/A	Identificare			●
	Eseguire periodicamente i test di penetrazione interni basati sui requisiti del programma, almeno annualmente. I test possono avvenire in modalità "clear box" oppure "opaque box".					

APPENDICE A

Risorse e Riferimenti

Programma CIS Benchmarks™: http://www.cisecurity.org/cis-benchmarks/

Controlli CIS Guida Cloud Companion: https://www.cisecurity.org/controls/v8/

Modello di Difesa CIS Community (CDM): https://www.cisecurity.org/controls/v8/

Modello CIS di Valutazione della Configurazione (CIS-CAT®): https://learn.cisecurity.org/cis-cat-lite

CIS Specifiche di Valutazione dei Controlli: https://controls-assessment-specification.readthedocs.io/en/latest/

Controlli CIS Gruppi di Implementazione: https://www.cisecurity.org/controls/v8/

Controlli CIS Guida di Implementazione dei Sistemi di Controllo Industriali: https://www.cisecurity.org/controls/v8/

Controlli CIS Guida Internet of Things Companion: https://www.cisecurity.org/controls/v8/

Controlli CIS Guida Mobile Companion: https://www.cisecurity.org/controls/v8/

CIS Metodologia di Valutazione del Rischio (RAM): https://www.cisecurity.org/controls/v8/

Controlli CIS Strumento di Autovalutazione (CSAT): https://www.cisecurity.org/blog/cis-csat-free-tool-assessing-implementation-of-cis-controls/

Controlli CIS Guida alla Sicurezza di Rete e Telelavoro negli Uffici di Piccole Dimensioni: https://www.cisecurity.org/controls/v8/

CIS Guida per i Criteri delle Password: https://www.cisecurity.org/white-papers/cis-password-policy-guide/

Cloud Security Alliance (CSA): https://cloudsecurityalliance.org/

Consiglio dei Tester Sicurezza Autorizzati (CREST) Guida alla risposta degli Incidenti di Cyber Sicurezza: CREST: https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf

EDUCAUSE: https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/awareness-campaigns

Organizzazione Internazionale per la Standardizzazione: https://www.iso.org/home.html

Centro Nazionale per la Sicurezza Informatica (U.K.): https://www.ncsc.gov.uk/guidance/10-steps-user-education-and-awareness

Istituto Nazionale degli Standard Tecnologici (NIST®): https://www.nist.gov/

Istituto Nazionale degli Standard Tecnologici (NIST®) SSDF: https://csrc.nist.gov/News/2020/mitigating-risk-of-software-vulns-ssdf

Istituto Nazionale degli Standard Tecnologici (NIST®) National Checklist Program Repository: https://nvd.nist.gov/ncp/repository

Istituto Nazionale degli Standard Tecnologici (NIST®) Linee Guida Identità Digitale: https://pages.nist.gov/800-63-3/

Istituto Nazionale degli Standard Tecnologici (NIST®) FIPS 140-2: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

Istituto Nazionale degli Standard Tecnologici (NIST®) FIPS 140-3: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf

Istituto Nazionale degli Standard Tecnologici (NIST®) SP 800-50 Infosec Formazione sulla Consapevolezza: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf

Istituto Nazionale degli Standard Tecnologici (NIST®) SP 800-88r1 – Linee Guida per la Sanificazione dei Media: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

National Cyber Security Alliance (NCSA): https://staysafeonline.org/

OWASP®: https://owasp.org/

OWASP® Metodologie dei Test di Penetrazione: https://www.owasp.org/index.php/Penetration_testing_methodologies

PCI Consiglio per gli Standard di Sicurezza: https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf

SANS: https://www.sans.org/security-awareness-training/resources

SAFECode Supplemento sulla Sicurezza delle Applicazioni: https://safecode.org/cis-controls/

Istituto Nazionale degli Standard Tecnologici (NIST®) SP 800-126r3 Specifiche Tecniche per il Protocollo di Automazione dei Contenuti di Sicurezza (SCAP): https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-126r3.pdf

The Software Alliance: https://www.bsa.org/reports/updated-bsa-framework-for-secure-software

Verizon Rapporto sulle Indagini di Violazione dei Dati: https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf

APPENDICE B

Controls and Safeguards Index

CONTROLLI 01 / SALVAGUARDIE 1.1 — CONTROLLI 02 / SALVAGUARDIE 2.2

CONTROLLI	SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
01		**Inventario e Controllo delle Risorse Aziendali** Gestire attivamente (inventariare, tracciare e correggere) tutte le risorse aziendali (dispositivi dell'utente finale, mobili e portatili inclusi, dispositivi di rete, dispositivi non informatici/Internet of Things—IoT e server) connessi all'infrastruttura fisicamente, virtualmente, in remoto e quelli in ambienti cloud, per conoscere con precisione la totalità delle risorse che devono essere monitorate e protette in azienda. Ciò aiuterà anche nell'identificare quelle non autorizzate e non gestite, da rimuovere o aggiornare.					
	1.1	**Stabilire e Mantenere un Inventario Dettagliato delle Risorse Aziendali** Stabilire e mantenere un inventario accurato, dettagliato e aggiornato di tutte le risorse aziendali con la possibilità di archiviazione o elaborazione dati, includendo: dispositivi dell'utente finale (compresi portatili e mobili), dispositivi di rete, dispositivi non informatici/IoT e server. Assicurare che l'inventario registri l'indirizzo di rete (se statico), l'indirizzo hardware, il nome del computer, il proprietario della risorsa aziendale, il reparto per ogni risorsa e se la risorsa è stata approvata per la connessione alla rete. Per i dispositivi mobili degli utenti finali, gli strumenti di tipo MDM possono supportare questo processo. Questo inventario include le risorse connesse all'infrastruttura fisica, virtuale, remota e quelle all'interno di ambienti cloud. Include inoltre le risorse che sono regolarmente connesse all'infrastruttura di rete dell'impresa, anche se non sono sotto il suo controllo. Rivedere e aggiornare l'inventario di tutte le risorse aziendali semestralmente o più frequentemente.	Dispositivi	Identificare	●	●	●
	1.2	**Trattare le Risorse non Autorizzate** Assicurare la presenza di un processo per trattare le risorse non autorizzate su base settimanale. L'azienda può scegliere di rimuovere la risorsa dalla rete, bloccarne la connessione remota o metterla in quarantena.	Dispositivi	Rispondere	●	●	●
	1.3	**Utilizzare uno Strumento di Rilevamento Attivo** Utilizzare uno strumento di rilevamento attivo per identificare le risorse connesse alla rete aziendale. Configurarlo per l'esecuzione quotidiana o più frequente.	Dispositivi	Rilevare		●	●
	1.4	**Utilizzare i log del Protocollo Dinamico di Configurazione Host (DHCP)** Utilizzare i log su tutti i server DHCP o altri strumenti di gestione degli indirizzi IP (Internet Protocol) per aggiornare l'inventario delle risorse aziendali. Rivedere ed utilizzare i registri per aggiornare l'inventario delle risorse settimanalmente o più frequentemente.	Dispositivi	Identificare		●	●
	1.5	**Utilizzare uno Strumento di Rilevazione Passiva** Utilizzare uno strumento di rilevazione passiva per identificare le risorse connesse alla rete aziendale. Rivedere e utilizzare le scansioni per aggiornare l'inventario delle risorse almeno una volta alla settimana o più frequentemente.	Dispositivi	Rilevare			●
02		**Inventario e Controllo delle Risorse Software** Gestire attivamente (inventariare, tracciare e correggere) tutto il software (sistemi operativi e applicazioni) sulla rete in modo che solo il software autorizzato possa essere installato ed eseguito e che il software non autorizzato e non gestito venga trovato impedendone l'installazione o l'esecuzione.					
	2.1	**Stabilire e Mantenere un Inventario Software** Stabilire e mantenere un inventario dettagliato di tutto il software con licenza installato sulle risorse aziendali. L'inventario del software deve documentare il titolo, l'editore, la data di installazione/utilizzo iniziale e la sua finalità; se opportuno, includere URL, app store, versione(i), distribuzione e data di disattivazione. Rivedere e aggiornare l'inventario del software semestralmente o più frequentemente.	Applicazioni	Identificare	●	●	●
	2.2	**Accertare il Supporto del Software Autorizzato** Assicurare che solo il software attualmente supportato sia individuato come autorizzato nell'inventario software delle risorse aziendali. Se il software non è supportato, ma è necessario per gli scopi aziendali, documentare un'eccezione che riporti la mitigazione dei controlli l'accettabilità del rischio residuo. Qualsiasi software non supportato privo di documentazione di eccezione, deve essere indicato come non autorizzato. Rivedere l'elenco del software per verificarne il supporto almeno mensilmente o più frequentemente.	Applicazioni	Identificare	●	●	●

CONTROLLI	SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
	2.3	**Trattare il Software non Autorizzato** Assicurare che il software non autorizzato venga rimosso dalle risorse aziendali o riceva un'eccezione documentata. Rivedere mensilmente o più frequentemente.	Applicazioni	Rispondere	●	●	●
	2.4	**Utilizzare Strumenti Automatici per l'Inventario del Software** Utilizzare strumenti di inventario del software, quando possibile, in tutta l'azienda per automatizzare l'individuazione e la documentazione del software installato.	Applicazioni	Rilevare		●	●
	2.5	**Elenco del Software Consentito** Utilizzare i controlli tecnici, come l'elenco delle applicazioni autorizzate, per garantire che solo il software consentito possa essere accessibile o eseguibile Aggiornare semestralmente o più frequentemente.	Applicazioni	Proteggere		●	●
	2.6	**Elenco delle Librerie Consentite** Utilizzare controlli tecnici per garantire che solo le specifiche librerie software autorizzate, come file .dll, .ocx, .so, ecc., possano essere caricate in un processo di sistema. Impedire il caricamento delle librerie non autorizzate in un processo di sistema. Rivalutare semestralmente o più frequentemente.	Applicazioni	Proteggere		●	●
	2.7	**Elenco degli Script Consentiti** Utilizzare controlli tecnici, come le firme digitali e controllo di versione, per garantire che solo gli script autorizzati, come file .ps1, .py, ecc., possano essere eseguiti. Impedire l'esecuzione di script non autorizzati. Rivalutare semestralmente o più frequentemente.	Applicazioni	Proteggere			●
03		**Protezione dei Dati** Sviluppare processi e controlli tecnici per identificare, classificare, elaborare in sicurezza, conservare ed eliminare i dati.					
	3.1	**Stabilire e Mantenere una Procedura di Gestione dei Dati** Stabilire e mantenere una procedura di gestione dei dati. Considerarne la sensibilità, il proprietario, la gestione, i limiti di conservazione e i requisiti di rimozione, in base agli standard aziendali di riservatezza e conservazione. Rivedere e aggiornare la documentazione ogni anno o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.	Dati	Identificare	●	●	●
	3.2	**Stabilire e Mantenere un Inventario dei Dati** Stabilire e mantenere un inventario dei dati, basato sulla procedura di gestione aziendale dei dati. Inventariare come minimo i dati sensibili. Rivedere e aggiornare l'inventario almeno una volta all'anno, dando priorità a quest'ultimi.	Dati	Identificare	●	●	●
	3.3	**Configurare le Liste di Controllo degli Accessi** Configurare le liste di controllo degli accessi ai dati in base alle esigenze di conoscenza di un utente. Utilizzare queste liste, note anche come permessi di accesso, a file system locali e remoti, database e applicazioni	Dati	Proteggere	●	●	●
	3.4	**Determinare la Conservazione dei Dati** Conservare i dati secondo la procedura aziendale di gestione dei dati. La conservazione dei dati deve includere tempi minimi e massimi.	Dati	Proteggere	●	●	●
	3.5	**Rimozione Sicura dei Dati** Eliminare i dati in modo sicuro secondo la procedura aziendale di gestione dei dati Assicurare che il processo ed il metodo di eliminazione siano commisurati alla loro sensibilità.	Dati	Proteggere	●	●	●
	3.6	**Crittografare i Dati sui Dispositivi degli Utenti Finali** Crittografare i dati sui dispositivi degli utenti finali contenenti dati sensibili. Le implementazioni possono includere ad esempio: Windows BitLocker®, Apple FileVault®, Linux® dm-crypt.	Dispositivi	Proteggere	●	●	●
	3.7	**Stabilire e Mantenere un Sistema di Classificazione dei Dati** Stabilire e mantenere uno schema generale di classificazione dei dati aziendali. Le aziende possono utilizzare etichette, come "Sensibile", "Riservato" e "Pubblico" per classificare i propri dati in base a tali elementi. Rivedere e aggiornare lo schema di classificazione annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.	Dati	Identificare		●	●

CONTROLLI	SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
	3.8	**Documentare il Flusso dei Dati** Documentare il flusso dei dati. La documentazione include i flussi di dati dei fornitori di servizi e dovrebbe essere basata sulla procedura gestionale dei dati aziendali Rivedere e aggiornare la documentazione ogni anno o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.	Dati	Identificare		●	●
	3.9	**Crittografare i Dati sui Media Rimovibili** Crittografare i dati sui media rimovibili.	Dati	Proteggere		●	●
	3.10	**Crittografare i Dati Sensibili in Transito** Crittografare i dati in transito. Esempi di implementazione includono: Transport Layer Security (TLS) e Open Secure Shell (OpenSSH).	Dati	Proteggere		●	●
	3.11	**Crittografare i Dati Sensibili a Riposo** Crittografare i dati sensibili a riposo su server, applicazioni e database. La crittografia a livello di archiviazione, nota anche come crittografia lato server, soddisfa i requisiti minimi di questa Salvaguardia. Ulteriori metodi di crittografia possono includere quella a livello di applicazione, nota anche come crittografia lato client, in cui l'accesso ai dispositivi di archiviazione non permette l'accesso ai dati in chiaro	Dati	Proteggere		●	●
	3.12	**Segmentare Elaborazione ed Archiviazione dei Dati secondo la Sensibilità** Segmentare elaborazione ed archiviazione dei dati in base alla sensibilità. Non elaborare dati sensibili utilizzando risorse aziendali predisposte per livelli inferiori di sensibilità.	Rete	Proteggere		●	●
	3.13	**Adottare una Soluzione per la Prevenzione della Perdita dei Dati** Implementare uno strumento automatizzato, di prevenzione della perdita di dati (DLP) basato su host, per identificare tutti i dati sensibili archiviati, elaborati o trasmessi attraverso le risorse aziendali, compresi quelli in locale o presso un fornitore di servizi remoto, aggiornando l'inventario dei dati sensibili.	Dati	Proteggere			●
	3.14	**Mantenere un Log di Accesso ai Dati Sensibili** Mantenere un log che registri l'accesso ai dati sensibili, inclusa la loro modifica e l'eliminazione.	Dati	Rilevare			●
04		**Configurazione Sicura delle Risorse Aziendali e del Software** Stabilire e mantenere la configurazione sicura delle risorse aziendali (dispositivi dell'utente finale, inclusi portatili e mobili, dispositivi di rete, dispositivi non informatici / IoT, server) e software (sistemi operativi e applicazioni).					
	4.1	**Stabilire e Mantenere una Procedura di Configurazione Sicura** Stabilire e mantenere una procedura di configurazione sicura per le risorse aziendali (dispositivi dell'utente finale inclusi portatili e mobili, dispositivi non informatici / IoT) e per il software (sistemi operativi ed applicazioni). Rivedere e aggiornare la documentazione annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.	Applicazioni	Proteggere	●	●	●
	4.2	**Stabilire e Mantenere una Procedura di Configurazione Sicura per l'Infrastruttura di Rete** Stabilire e mantenere una procedura di configurazione sicura per i dispositivi di rete. Rivedere e aggiornare la documentazione annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.	Rete	Proteggere	●	●	●
	4.3	**Configurare il Blocco Automatico della Sessione sulle Risorse Aziendali** Configurare il blocco automatico della sessione sulle risorse aziendali dopo un periodo di inattività definito. Per i sistemi operativi generici, il periodo non deve superare i 15 minuti. Per i dispositivi mobili dell'utente finale, il periodo non deve superare i 2 minuti.	Utenti	Proteggere	●	●	●
	4.4	**Implementare e Gestire un Firewall sui Server** Implementare e gestire un firewall sui server, quando supportato. Esempi di implementazione includono un firewall virtuale, un firewall del sistema operativo o un agent firewall di terze parti.	Dispositivi	Proteggere	●	●	●

CONTROLLI	SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
	4.5	**Implementare e Gestire un Firewall sui Dispositivi dell'Utente Finale** Implementare e gestire un firewall basato su host o uno strumento di filtraggio delle porte sui dispositivi degli utenti finali, con una regola predefinita di negazione che elimina tutto il traffico ad eccezione di porte e servizi esplicitamente consentiti.	Dispositivi	Proteggere	●	●	●
	4.6	**Gestire in modo Sicuro Risorse e Software Aziendali** Gestire in modo sicuro risorse e software aziendali. Esempi di implementazione includono la gestione della configurazione tramite il controllo di versione dell'infrastruttura tramite codice e l'accesso alle interfacce amministrative utilizzando protocolli di rete sicuri, come Secure Shell (SSH) e Protocollo di trasferimento Ipertestuale Sicuro (HTTPS). Non utilizzare protocolli di gestione non sicuri, come Telnet (Teletype Network) e HTTP, a meno che non siano essenziali dal punto di vista operativo.	Rete	Proteggere	●	●	●
	4.7	**Gestire gli Account Predefiniti di Risorse e Software Aziendali** Gestire gli account predefiniti di risorse e software aziendali, come root, amministratore e altri account preconfigurati rilasciati dal fornitore. Esempi di implementazione includono: disabilitare o rendere inutilizzabili gli account predefiniti.	Utenti	Proteggere	●	●	●
	4.8	**Disinstallare o Disabilitare Servizi e Software non Necessari sulle Risorse Aziendali** Disinstallare o disabilitare servizi e software non necessari sulle risorse aziendali, come un servizio di condivisione file inutilizzato, un modulo di applicazione Web o una funzione di servizio.	Dispositivi	Proteggere		●	●
	4.9	**Configurare Server DNS Sicuri sulle Risorse Aziendali** Configurare server DNS sicuri sulle risorse aziendali. Esempi di implementazione includono: configurazione delle risorse affinché utilizzino server DNS controllati dall'azienda o accesso a server DNS esterni affidabili.	Dispositivi	Proteggere		●	●
	4.10	**Abilitare il Blocco Automatico sui Dispositivi Portatili dell'Utente Finale** Abilitare il blocco automatico del dispositivo portatile dell'utente finale dopo una soglia stabilita di tentativi di autenticazione non riusciti, ove supportato. Per i laptop, non consentire più di 20 tentativi di autenticazione falliti; per tablet e smartphone, non più di 10. Esempi di implementazione includono: Microsoft® InTune Device Lock e Apple® Configuration Profile maxFailedAttempts.	Dispositivi	Rispondere		●	●
	4.11	**Abilitare la Cancellazione da Remoto sui Dispositivi Portatili dell'Utente Finale** Cancellare da remoto i dati aziendali dai dispositivi portatili di proprietà dell'utente finale quando è necessario, ad esempio dispositivi smarriti o rubati, o quando una persona lascia l'azienda.	Dispositivi	Proteggere		●	●
	4.12	**Separare gli Spazi di Lavoro Aziendali sui Dispositivi Portatili dell'Utente Finale** Assicurare che gli spazi di lavoro aziendali sui dispositivi mobili degli utenti finali siano separati, ove supportato. Esempi di implementazione includono: l'utilizzo di Apple® Configuration Profile, Android™ Work Profile per separare applicazioni e dati aziendali da quelli personali.	Dispositivi	Proteggere			●
05		**Gestione degli Account** Utilizzare procedure e strumenti per assegnare e gestire l'autorizzazione delle credenziali a risorse e software aziendali, per gli account utente, inclusi quelli amministrativi e di servizio.					
	5.1	**Stabilire e Mantenere un Inventario degli Account** Stabilire e mantenere un inventario di tutti gli account aziendali. L'inventario deve includere account utenti e amministrativi. L'inventario, dovrebbe contenere almeno il nome della persona, il nome utente, le date di inizio/fine e l'area lavorativa. Assicurare che tutti gli account attivi siano autorizzati, con una pianificazione almeno trimestrale o più frequentemente.	Utenti	Identificare	●	●	●
	5.2	**Utilizzare Password Univoche** Utilizzare password univoche per tutte le risorse aziendali. L'implementazione delle "best practice" prevede, come minimo, una password di 8 caratteri per gli account che utilizzano l'autenticazione multi fattore e una password di 14 caratteri per gli account che non la prevedono.	Utenti	Proteggere	●	●	●

CONTROLLI	SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
	5.3	**Disabilitare gli Account Dormienti** Cancellare o disabilitare tutti gli account dormienti dopo un periodo di 45 giorni di inattività, quando supportato.	Utenti	Rispondere	●	●	●
	5.4	**Limitare i Privilegi Amministrativi agli Account dell'Amministratore** Limitare i privilegi amministrativi agli account di amministratore riservati alle risorse aziendali. Effettuare attività informatiche generali, navigazione in Internet, posta elettronica ed uso delle suite di produttività, da un account utente non privilegiato.	Utenti	Proteggere	●	●	●
	5.5	**Stabilire e Mantenere un Inventario degli Account di Servizio** Stabilire e mantenere un inventario degli account di servizio. L'inventario, deve contenere almeno il referente dell'area lavorativa, data di revisione e scopo. Eseguire revisioni degli account di servizio per verificare che tutti quelli attivi siano autorizzati, con una pianificazione ricorrente almeno trimestrale o più frequentemente.	Utenti	Identificare		●	●
	5.6	**Centralizzare la Gestione degli Account** Centralizzare la gestione degli account con un servizio di directory o identità.	Utenti	Proteggere		●	●
06		**Gestione del Controllo degli Accessi** Utilizzare processi e strumenti per creare, assegnare, gestire e revocare credenziali di accesso e privilegi per gli account utenti, amministratori, di servizio per le risorse e i software aziendali.					
	6.1	**Stabilire una Procedura di Concessione degli Accessi** Stabilire e seguire una procedura, preferibilmente automatizzata, per concedere l'accesso alle risorse aziendali in caso di nuova assunzione, attribuzione di diritti o cambio di ruolo di un utente.	Utenti	Proteggere	●	●	●
	6.2	**Stabilire una Procedura di Revoca degli Accessi** Stabilire e seguire una procedura, preferibilmente automatizzata, per revocare l'accesso alle risorse aziendali, disabilitando gli account immediatamente dopo la cessazione, la revoca dei diritti o il cambio di ruolo di un utente. La disattivazione degli account, piuttosto che la loro eliminazione, potrebbe essere necessaria per consentire gli audit di tracciamento.	Utenti	Proteggere	●	●	●
	6.3	**Richiedere MFA per le Applicazioni Esposte Esternamente** Richiedere che tutte le applicazioni aziendali o di terze parti esposte esternamente applichino l'autenticazione multi fattore, ove supportata. Il suo utilizzo tramite un servizio di directory o un provider SSO è un'implementazione	Utenti	Proteggere	●	●	●
	6.4	**Richiedere MFA per l'Accesso di Rete Remoto** Richiedere l'autenticazione multi fattore per l'accesso di rete da remoto	Utenti	Proteggere	●	●	●
	6.5	**Richiedere MFA per l'Accesso Amministrativo** Richiedere l'autenticazione multi fattore per l'accesso di tutti gli account amministrativi, se supportata, per tutte le risorse aziendali, sia gestite in locale sia utilizzando un fornitore esterno	Utenti	Proteggere	●	●	●
	6.6	**Stabilire e Mantenere un Inventario dei Sistemi di Autenticazione ed Autorizzazione** Stabilire e mantenere un inventario dei sistemi di autenticazione ed autorizzazione aziendali, inclusi quelli ospitati in locale o presso un fornitore di servizi remoto. Rivedere e aggiornare l'inventario, come minimo, annualmente o più frequentemente.	Utenti	Identificare		●	●
	6.7	**Centralizzare il Controllo degli Accessi** Centralizzare il controllo degli accessi per tutte le risorse aziendali tramite un servizio di directory o un provider SSO, se supportato.	Utenti	Proteggere		●	●
	6.8	**Definire e Mantenere un Controllo degli Accessi Basato sui Ruoli** Definire e mantenere il controllo degli accessi basato sui ruoli, determinando e documentando i diritti di accesso necessari per ciascun ruolo aziendale per consentire lo svolgimento dei compiti assegnati. Esegui le revisioni del controllo degli accessi delle risorse aziendali per assicurare che tutti i privilegi siano autorizzati, secondo una pianificazione almeno annuale o più frequentemente.	Dati	Proteggere			●

CONTROLLI	SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3

07 Gestione Continua delle Vulnerabilità

Sviluppare un piano per valutare e monitorare costantemente le vulnerabilità su tutte le risorse aziendali all'interno dell'infrastruttura, al fine di rimediare e ridurre al minimo la finestra di opportunità per gli aggressori. Monitorare le fonti di informazione del settore pubblico e privato per conoscere le più recenti minacce e vulnerabilità.

7.1	**Stabilire e Mantenere una Procedura di Gestione delle Vulnerabilità.**	Applicazioni	Proteggere	●	●	●
	Stabilire e mantenere una procedura di gestione delle vulnerabilità documentata. Rivedere ed aggiornare la documentazione annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.					
7.2	**Stabilire e Mantenere una Procedura di Correzione**	Applicazioni	Rispondere	●	●	●
	Stabilire e mantenere una strategia di correzione documentata basata sul rischio nell'ambito di una procedura di correzione, rivedendola mensilmente o più frequentemente.					
7.3	**Gestire l'Aggiornamento Automatico del Sistema Operativo**	Applicazioni	Proteggere	●	●	●
	Eseguire gli aggiornamenti del sistema operativo delle risorse aziendali per mezzo di un sistema automatizzato, mensilmente o più frequentemente.					
7.4	**Gestire l'Aggiornamento Automatico delle Applicazioni**	Applicazioni	Proteggere	●	●	●
	Eseguire gli aggiornamenti delle applicazioni delle risorse aziendali per mezzo di un sistema automatizzato di installazione delle patch, mensilmente o più frequentemente.					
7.5	**Eseguire Scansioni di Vulnerabilità delle Risorse Aziendali Interne**	Applicazioni	Identificare		●	●
	Eseguire scansioni automatizzate delle vulnerabilità delle risorse aziendali interne, trimestralmente o più frequentemente. Effettuare scansioni sia autenticate che non, utilizzando uno strumento di scansione delle vulnerabilità compatibile SCAP.					
7.6	**Eseguire Scansioni di Vulnerabilità delle Risorse Aziendali Esposte Esternamente**	Applicazioni	Identificare		●	●
	Eseguire scansioni automatizzate delle vulnerabilità delle risorse aziendali esposte esternamente utilizzando uno strumento conforme SCAP, mensilmente o più frequentemente.					
7.7	**Correggere le Vulnerabilità Rilevate**	Applicazioni	Rispondere		●	●
	Correggere le vulnerabilità rilevate nel software per mezzo di strumenti e procedure, mensilmente o più frequentemente, secondo la procedura di correzione.					

08 Gestione dei Log di Controllo

Raccogliere, avvisare, esaminare e conservare i log di controllo degli eventi che potrebbero aiutare a rilevare, comprendere o rimediare in seguito ad un attacco.

8.1	**Stabilire e Mantenere una Procedura di Gestione dei Log di Controllo**	Rete	Proteggere	●	●	●
	Stabilire e mantenere una procedura di gestione dei log di controllo che soddisfi i requisiti di registrazione. Come minimo, salvare i log delle risorse aziendali, per la loro revisione e conservazione. Rivedere e aggiornare la documentazione ogni anno o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.					
8.2	**Raccogliere i Log di Controllo**	Rete	Rilevare	●	●	●
	Raccogliere i log di controllo. Assicurare che la procedura aziendale di gestione dei log sia attivata su tutti i dispostivi aziendali .					
8.3	**Assicurare un Spazio Adeguato per l'Archiviazione dei Log**	Rete	Proteggere	●	●	●
	Assicurare che le destinazioni di archiviazione dei log mantengano uno spazio adeguato per adattarsi al processo aziendale di gestione dei log di controllo.					
8.4	**Standardizzare la Sincronizzazione dell'Orario**	Rete	Proteggere		●	●
	Standardizzare la sincronizzazione dell'orario. Configurare almeno due sorgenti orarie sulle risorse aziendali, se supportato.					

CONTROLLI	SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
	8.5	**Raccogliere i Log di Controllo Dettagliati** Configurare il logging dettagliato per le risorse aziendali che contengono dati sensibili. Includere l'origine dell'evento, data, nome utente, marca temporale, indirizzo di origine e di destinazione, ed altri elementi utili che potrebbero aiutare in una indagine forense.	Rete	Rilevare		●	●
	8.6	**Raccogliere i Log di Controllo del DNS** Raccogliere i log di controllo delle query DNS sulle risorse aziendali, ove appropriato e supportato..	Rete	Rilevare		●	●
	8.7	**Raccogliere i Log di Controllo delle Richieste URL** Raccogliere i log di controllo delle richieste URL, ove appropriato e supportato.	Rete	Rilevare		●	●
	8.8	**Raccogliere i Log di Controllo dai Command-Line** Raccogliere i log di controllo delle interfacce command-line. Esempi di implementazione includono la raccolta dei log di PowerShell®, BASH™, e terminali di amministrazione remota.	Dispositivi	Rilevare		●	●
	8.9	**Centralizzare i Log di Controllo** Centralizzare, per quanto possibile, raccolta e conservazione dei log di controllo delle risorse aziendali.	Rete	Rilevare		●	●
	8.10	**Conservare i Log di Controllo** Conservare i log di controllo delle risorse aziendali per un minimo di 90 giorni.	Rete	Proteggere		●	●
	8.11	**Effettuare le Revisioni dei Log di Controllo** Effettuare le revisioni dei log di controllo per rilevare anomalie o eventi inconsueti che potrebbero indicare una potenziale minaccia. Attuare i controlli su base settimanale o più frequentemente.	Rete	Rilevare		●	●
	8.12	**Raccogliere i Log dei Fornitori di Servizi** Raccogliere i log dei fornitori di servizi, se supportati. Esempi di implementazione includono la raccolta di eventi di autenticazione e autorizzazione, eventi di creazione ed eliminazione di dati ed eventi di gestione degli utenti.	Dati	Rilevare			●
09		**Protezione della Posta elettronica e del Browser Web** Migliorare le protezioni ed il rilevamento delle minacce provenienti dalle e-mail e da vettori web, che danno l'opportunità agli aggressori di manipolare il comportamento umano sfruttandone il diretto coinvolgimento.					
	9.1	**Assicurare l'Utilizzo di Client E-mail e di Browser Pienamente Supportati** Assicurare che venga permessa l'esecuzione solo di client di posta elettronica e di browser pienamente supportati ed aggiornati alla versione più recente rilasciata dal fornitore.	Applicazioni	Proteggere	●	●	●
	9.2	**Utilizzare Servizi di Filtro DNS** Utilizzare i servizi di filtro DNS su tutte le risorse aziendali per bloccare l'accesso ai domini riconosciuti come pericolosi.	Rete	Proteggere	●	●	●
	9.3	**Mantenere ed Applicare i Filtri URL di Rete** Applicare ed aggiornare i filtri URL di rete per limitare la connessione di una risorsa aziendale a siti Web potenzialmente dannosi o non approvati. Esempi di implementazione includono i filtri basati sulla categoria, i filtri basati sulla reputazione o tramite l'uso di elenchi di blocco. Applicare i filtri su tutte le risorse aziendali.	Rete	Proteggere		●	●
	9.4	**Limitare le Estensioni di Browser e Client E-Mail non Necessarie o non Autorizzate** Limitare, disinstallando o disattivando dal browser o dal client di posta elettronica, qualsiasi estensione, plug-in e applicazione add-on, non autorizzata o non necessaria.	Applicazioni	Proteggere		●	●
	9.5	**Implementare DMARC** Per ridurre la possibilità di e-mail contraffatte o modificate da domini validi, implementare le policy e le verifiche DMARC, iniziando con l'implementazione del Sender Policy Framework (SPF) e degli standard di Chiave Identificativa Dominio Mail (DKIM).	Rete	Proteggere		●	●

CONTROLLI	SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
	9.6	**Bloccare i Tipi di File non Necessari** Bloccare i tipi di file non necessari in ingresso sul gateway di posta elettronica aziendale.	Rete	Proteggere		●	●
	9.7	**Installare e Mantenere le Protezioni Anti-Malware del Server di Posta** Installare e mantenere le protezioni anti-malware del server di posta, esempio scansione degli allegati e/o sandboxing.	Rete	Proteggere			●
10		**Difesa dal Malware** Prevenire o controllare installazione, diffusione ed esecuzione di applicazioni, codici o script dannosi sulle risorse aziendali.					
	10.1	**Distribuire e Mantenere il Software Anti-Malware** Distribuire e mantenere il software anti-malware su tutte le risorse aziendali.	Dispositivi	Proteggere	●	●	●
	10.2	**Configurare gli Aggiornamenti Automatici delle Firme Anti-Malware** Configurare gli aggiornamenti automatici dei file delle firme anti-malware su tutte le risorse aziendali.	Dispositivi	Proteggere	●	●	●
	10.3	**Disabilitare Esecuzione e Riproduzione Automatica per i Supporti Rimovibili** Disabilitare l'esecuzione e la riproduzione automatica per i supporti rimovibili.	Dispositivi	Proteggere	●	●	●
	10.4	**Configurare la Scansione Automatica dei Supporti Rimovibili** Configurare il software anti-malware per la scansione automatica dei supporti rimovibili.	Dispositivi	Rilevare		●	●
	10.5	**Abilitare le Funzioni Anti-Exploit** Abilitare le funzioni anti-exploit sui software e sui dispositivi aziendali, se possibile, come ad esempio Microsoft® Prevenzione di Esecuzione in area Dati (DEP), Windows® Defender Exploit Guard (WDEG), Apple® Protezione di Integrità del Sistema (SIP), Gatekeeper™.	Dispositivi	Proteggere		●	●
	10.6	**Gestire Centralmente il Software Anti-Malware** Gestire in modo centralizzato il software anti-malware.	Dispositivi	Proteggere		●	●
	10.7	**Utilizzare un Software Anti-Malware Basato sul Comportamento** Utilizzare un software anti-malware basato sul comportamento.	Dispositivi	Rilevare		●	●
11		**Recupero dei Dati** Stabilire e mantenere sufficienti procedure di ripristino dei dati per riportare le risorse aziendali in funzione ad uno stato attendibile di pre-incidente.					
	11.1	**Stabilire e Mantenere una Procedura di Recupero dei Dati** Stabilire e mantenere una procedura di recupero dei dati. Definire l'ambito delle attività di ripristino dei dati, la priorità del ripristino e la sicurezza dei dati di backup. Rivedere e aggiornare la documentazione annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.	Dati	Recuperare	●	●	●
	11.2	**Eseguire Backup Automatizzati** Eseguire backup automatizzati delle risorse aziendali in funzione. Eseguire il backup settimanalmente o più frequentemente, in base alla sensibilità dei dati.	Dati	Recuperare	●	●	●
	11.3	**Proteggere i Dati di Ripristino** Proteggere i dati di ripristino con controlli equivalenti ai dati originali. Applicare la crittografia necessaria o separare i dati in funzione dei requisiti.	Dati	Proteggere	●	●	●
	11.4	**Stabilire e Mantenere una Istanza Isolata dei Dati di Ripristino** Stabilire e mantenere un'istanza isolata dei dati di ripristino. Le implementazioni di esempio includono il controllo della versione delle destinazioni di backup tramite sistemi o servizi offline, cloud e off-site.	Dati	Recuperare	●	●	●
	11.5	**Recupero Dati di Prova** Testare il ripristino del backup trimestralmente, o con maggiore frequenza, per un campione di risorse aziendali in funzione.	Dati	Recuperare		●	●

CONTROLLI	SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3

12 Gestione dell'Infrastruttura di Rete

Stabilire, implementare e gestire attivamente (tracciando, segnalando, correggendo) i dispositivi di rete, al fine di impedire agli aggressori di sfruttarne servizi e punti di accesso vulnerabili.

12.1	**Assicurare l'Aggiornamento dell'Infrastruttura di Rete**	Rete	Proteggere	●	●	●
	Assicurare che l'infrastruttura di rete sia sempre aggiornata. Esempi di implementazione includono l'esecuzione dell'ultima versione stabile del software e / o l'utilizzo delle potenzialità NaaS (network-as-a-service) attualmente disponibili. Rivedere le versioni del software mensilmente o più frequentemente per verificarne il supporto					
12.2	**Stabilire e Mantenere una Architettura di Rete Sicura**	Rete	Proteggere		●	●
	Stabilire e mantenere un'architettura di rete sicura. Un'architettura di rete sicura deve prevedere almeno la segmentazione, i privilegi minimi e la disponibilità.					
12.3	**Gestione Sicura dell'Infrastruttura di Rete**	Rete	Proteggere		●	●
	Gestire in sicurezza l'infrastruttura di rete. Esempi di implementazione includono il controllo di versione dell'infrastruttura tramite codice e l'uso di protocolli di rete sicuri, come SSH e HTTPS.					
12.4	**Stabilire e Mantenere il / i Diagramma / i dell'Architettura**	Rete	Identificare		●	●
	Stabilire e mantenere i diagrammi dell'architettura e / o altra documentazione del sistema di rete. Rivedere e aggiornare la documentazione ogni anno o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.					
12.5	**Centralizzare Autenticazione, Autorizzazione e Auditing di Rete**	Rete	Proteggere		●	●
	Centralizzare AAA di rete.					
12.6	**Utilizzare Protocolli Sicuri di Gestione e Comunicazione della Rete**	Rete	Proteggere		●	●
	Utilizzare protocolli sicuri di gestione e comunicazione della rete (esempio 802.1X, Protocollo di Accesso Wi-Fi 2–WPA2 versione Enterprise o superiore)					
12.7	**Assicurare l'Utilizzo di VPN per i Dispositivi Remoti e Connessione AAA all'Infrastruttura Aziendale**	Dispositivi	Proteggere		●	●
	Richiedere agli utenti l'autenticazione alla VPN aziendale e ai servizi di autenticazione prima dell'accesso alle risorse aziendali dai dispositivi degli utenti finali.					
12.8	**Stabilire e Mantenere Risorse Informatiche Dedicate per tutto il Lavoro Amministrativo**	Dispositivi	Proteggere			●
	Stabilire e mantenere risorse informatiche dedicate, fisicamente o logicamente separate, per tutte le attività amministrative o che richiedano l'accesso amministrativo. Le risorse informatiche dovrebbero essere segmentate dalla rete primaria dell'azienda e non avere accesso a Internet.					

13 Monitoraggio e Difesa della Rete

Adottare processi e strumenti per stabilire e mantenere un monitoraggio completo della rete e una difesa contro le minacce alla sicurezza dell'infrastruttura di rete aziendale e agli utenti.

13.1	**Centralizzare gli Avvisi degli Eventi di Sicurezza**	Rete	Rilevare		●	●
	Centralizzare gli avvisi degli eventi di sicurezza delle risorse aziendali per la correlazione ed analisi dei log. L'implementazione delle best practice prevede l'uso di un SIEM, che includa gli avvisi di correlazione degli eventi definiti dal fornitore. Anche una piattaforma di analisi dei log configurata con avvisi di sicurezza correlati e rilevanti soddisfa questa salvaguardia.					
13.2	**Adottare una Soluzione di Rilevamento Intrusioni Basata su Host**	Dispositivi	Rilevare		●	●
	Adottare una soluzione di rilevamento delle Intrusioni basata su host sulle risorse aziendali, ove appropriato e/o supportato					
13.3	**Adottare una Soluzione di Rilevamento Intrusioni Basata sulla Rete**	Rete	Rilevare		●	●
	Adottare una soluzione di rilevamento delle intrusioni basata sulla rete sulle risorse aziendali, ove appropriato. Esempi di implementazione includono l'utilizzo di un Sistema di Rete per il Rilevamento delle Intrusioni (NIDS) o un servizio fornito in cloud equivalente (CSP)					

CONTROLLI	SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
	13.4	**Filtrare il Traffico tra i Segmenti di Rete** Filtrare il traffico tra i segmenti di rete ove appropriato	Rete	Proteggere		●	●
	13.5	**Gestire il Controllo degli Accessi per le Risorse Remote** Gestire il controllo degli accessi per le risorse che si connettono da remoto alle dotazioni aziendali. Determinare il numero di accessi in base a: software anti-malware aggiornato installato, conformità della configurazione sicura relativamente al processo definito dall'azienda, verifica di aggiornamento del sistema operativo e delle applicazioni.	Dispositivi	Proteggere		●	●
	13.6	**Salvare i Log del Flusso di Traffico di Rete** Salvare i log del flusso di traffico di rete e / o il traffico di rete per esaminare e inviare avvisi dai dispositivi di rete.	Rete	Rilevare		●	●
	13.7	**Adottare una Soluzione di Prevenzione delle Intrusioni Basata su Host** Adottare una soluzione di prevenzione delle intrusioni basata su host sulle risorse aziendali, ove appropriato e / o supportato. Esempi di implementazione includono l'uso di un client Endpoint di Rilevamento e Risposta (EDR) o di un agent IPS basato su host.	Dispositivi	Proteggere			●
	13.8	**Adottare una Soluzione di Prevenzione delle Intrusioni Basata sulla Rete** Adottare una soluzione di prevenzione delle intrusioni di rete, ove appropriato. Esempi di implementazione includono l'uso di un sistema di prevenzione delle intrusioni di rete (NIPS) o di un servizio CSP equivalente.	Rete	Proteggere			●
	13.9	**Implementare il Controllo degli Accessi a Livello di Porta** Adottare il controllo degli accessi a livello di porta che utilizzi 802.1x o protocolli di controllo di accesso alla rete simili, come i certificati, includendo l'autenticazione dell'utente e / o del dispositivo.	Dispositivi	Proteggere			●
	13.10	**Eseguire il Filtraggio a Livello di Applicazione** Eseguire il filtraggio a livello di applicazione. Esempi di implementazione includono un proxy di filtraggio, un firewall a livello di applicazione o un gateway.	Rete	Proteggere			●
	13.11	**Perfezionare le Soglie di Avviso degli Eventi di Sicurezza** Ottimizzare le soglie di avviso degli eventi di sicurezza mensilmente o più.	Rete	Rilevare			●
14		**Sensibilizzazione e Formazione sulle Competenze di Sicurezza** Stabilire e mantenere un programma di sensibilizzazione alla sicurezza per istruire il personale affinché sia consapevole ed adeguatamente preparato per ridurre i rischi di sicurezza informatica aziendali.					
	14.1	**Stabilire e Mantenere un Programma di Sensibilizzazione alla Sicurezza** Stabilire e mantenere un programma di sensibilizzazione alla sicurezza. Lo scopo è quello di istruire il personale su come interagire con le risorse e i dati aziendali in modo sicuro. Effettuare la formazione al momento dell'assunzione e, come minimo, annualmente. Rivedere e aggiornare i contenuti annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.	N/A	Proteggere	●	●	●
	14.2	**Formare il Personale nel Riconoscimento degli Attacchi Social Engineering** Formare il personale nel riconoscimento degli attacchi social engineering, come il phishing, pre-texting e tailgating.	N/A	Proteggere	●	●	●
	14.3	**Formare il Personale sulle Migliori Tecniche di Autenticazione** Formare il personale sulle migliori tecniche di autenticazione. Alcuni esempi includono MFA, composizione delle password e gestione delle credenziali.	N/A	Proteggere	●	●	●
	14.4	**Formare il Personale sulle Migliori Tecniche di Gestione dei Dati** Formare il personale su come identificare, salvare trasferire, archiviare e cancellare in modo appropriato i dati sensibili. È compresa la formazione del personale sulla disattivazione dello schermo quando viene lasciata la postazione, sulla cancellazione di lavagne fisiche o virtuali a fine riunione, sull'archiviazione sicura di dati e risorse	N/A	Proteggere	●	●	●
	14.5	**Formare il Personale sulle Cause di Esposizione Involontaria di Dati** Formare il personale sulle cause di esposizione involontaria di dati. Alcuni esempi includono l'errato trasferimento di dati sensibili, la perdita di un dispositivo portatile dell'utente finale o la pubblicazione di dati non dovuta.	N/A	Proteggere	●	●	●

CONTROLLI	SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
	14.6	**Formare il Personale sul Riconoscimento e Segnalazione degli Incidenti di Sicurezza** Formare il personale affinché riconosca un potenziale incidente e possa segnalarlo	N/A	Proteggere	●	●	●
	14.7	**Formare il Personale su Identificazione e Segnalazione di Mancati Aggiornamenti dei Dispositivi Aziendali** Formare il personale per capire come verificare e segnalare un mancato aggiornamento automatizzato di uno strumento o procedura. Parte di questa formazione dovrebbe prevedere la modalità di segnalazione al personale IT di qualsiasi malfunzionamento di strumenti o procedure automatizzati.	N/A	Proteggere	●	●	●
	14.8	**Formare il Personale sui Pericoli di Connessione e Trasmissione di Dati Aziendali su Reti non Sicure** Formare il personale sui pericoli della connessione e della trasmissione di dati su reti non sicure per le attività aziendali. Se l'azienda dispone di lavoratori remoti, la formazione deve includere le indicazioni per garantire che tutti gli utenti configurino in modo sicuro la propria infrastruttura di rete domestica.	N/A	Proteggere	●	●	●
	14.9	**Effettuare una Formazione Specifica sulla Competenze e per la Sensibilizzazione sulla Sicurezza** Effettuare una formazione specifica sulle competenze e per la sensibilizzazione sulla sicurezza. Esempi di implementazione includono corsi di amministrazione sicura dei sistemi per il personale IT (OWASP® Top 10 sulla consapevolezza e prevenzione delle vulnerabilità per sviluppatori di applicazioni Web e formazione avanzata sulla sensibilizzazione social engineering per ruoli di alto profilo).	N/A	Proteggere		●	●
15		**Gestione dei Service Provider** Sviluppare una procedura per valutare i Service Provider che detengono dati sensibili o sono responsabili delle piattaforme o dei processi IT aziendali più importanti, per assicurarsi che proteggano tali piattaforme ed i dati in modo appropriato.					
	15.1	**Stabilire e Mantenere un Inventario dei Service Providers** Stabilire e mantenere un inventario dei service providers. L'inventario deve riportare tutti i service providers conosciuti, compresa la classificazione e il contatto aziendale designato. Rivedere ed aggiornare l'inventario annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.	N/A	Identificare	●	●	●
	15.2	**Stabilire e Mantenere un Criterio di Gestione del Service Provider** Stabilire e mantenere un criterio di gestione del service provider. Garantire che i criteri includano la classificazione, l'inventario, la valutazione, il monitoraggio e la disattivazione dei service provider. Rivedere ed aggiornare i criteri annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.	N/A	Identificare		●	●
	15.3	**Classificare i Service Providers** Classificare i service provider. La classificazione può includere una o più caratteristiche, come la sensibilità dei dati, volume dei dati, requisiti di disponibilità, normative applicabili, rischio intrinseco e rischio mitigato. Rivedere ed aggiornare la classificazione annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero influire su questa Salvaguardia.	N/A	Identificare		●	●
	15.4	**Garantire che i Contratti dei Service Provider Includano Requisiti di Sicurezza** Garantire che i contratti dei service provider includano i requisiti di sicurezza. Esempi di requisiti possono includere: requisiti minimi del programma di sicurezza, notifica e risposta di incidenti di sicurezza e / o violazione dei dati, requisiti di crittografia dei dati e procedure di dismissione dei dati. Questi requisiti di sicurezza devono essere coerenti con la politica di gestione del service provider aziendale. Rivedere i contratti del service provider annualmente per garantire la presenza di tali requisiti.	N/A	Proteggere		●	●
	15.5	**Valutare i Service Provider** Valutare i service provider aziendali in coerenza con i relativi criteri di gestione. La valutazione può variare in base alle classificazioni e può includere la revisione di rapporti di valutazione standardizzati, come il Servizio di Controllo Organizzazione 2 (SOC 2) e l'Attestato di Conformità (AoC) del Settore delle Carte di Pagamento (PCI), questionari personalizzati o altre adeguate e rigorose procedure. Rivalutare i fornitori di servizi annualmente o in occasione nuovo contratto o di suo di rinnovo.	N/A	Identificare			●

CONTROLLI	SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
	15.6	**Controllare i Service Providers** Controllare i service provider aziendali in coerenza con i relativi criteri di gestione. Il monitoraggio può includere una rivalutazione periodica della conformità, il monitoraggio delle note di rilascio e il monitoraggio del dark web.	Dati	Rilevare			●
	15.7	**Disattivazione Sicura dei Service Providers** Disattivazione sicura dei service providers. Esempi di considerazioni includono la disattivazione degli account utente e di servizio, l'interruzione dei flussi di dati e la rimozione sicura dei dati aziendali dai sistemi.	Dati	Proteggere			●
16		**Sicurezza degli Applicativi** Gestire la sicurezza del ciclo di vita del software sviluppato in proprio, ospitato o acquistato per prevenire, rilevare e rimediare ai punti deboli di sicurezza prima che possano impattare sull'azienda.					
	16.1	**Stabilire e Mantenere una Procedura di Sviluppo Sicuro delle Applicazioni** Stabilire e mantenere una procedura di sviluppo sicuro delle applicazioni. In questo procedimento si considerino elementi quali: standard di progettazione di applicazioni sicure, pratiche di codifica sicura, formazione per gli sviluppatori, gestione delle vulnerabilità, sicurezza del codice di terze parti e procedure di test di sicurezza delle applicazioni. Rivedere e aggiornare la documentazione annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero avere un impatto su questa Salvaguardia.	Applicazioni	Proteggere		●	●
	16.2	**Stabilire e Mantenere una Procedura di Accettazione e Risoluzione delle Vulnerabilità** Stabilire e mantenere una procedura di accettazione e risoluzione delle segnalazioni di vulnerabilità del software, inclusa quella dedicata per la segnalazione da parte di entità esterne. Il procedimento deve includere elementi quali: un criterio di gestione delle vulnerabilità che identifichi il processo di segnalazione, il responsabile della gestione delle segnalazioni di vulnerabilità e un sistema per la presa in carico, l'assegnazione, la risoluzione e la relativa verifica. Come parte del processo, utilizzare un sistema di rilevamento delle vulnerabilità che includa livelli di gravità e metriche per misurarne i tempi di identificazione, analisi e correzione. Rivedere e aggiornare la documentazione annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero avere un impatto su questa salvaguardia. Gli sviluppatori di applicazioni di terze parti devono rendere pubblici questi criteri al fine di soddisfare le aspettative delle parti interessate	Applicazioni	Proteggere		●	●
	16.3	**Eseguire l'Analisi della Causa Principale sulle Vulnerabilità della Sicurezza** Eseguire l'analisi della causa principale sulle vulnerabilità della sicurezza. Quando si esaminano le vulnerabilità, l'analisi della causa principale è il lavoro di valutazione dell'origine sottostante che crea il punto debole nel codice permettendo ai team di sviluppo di andare oltre la semplice correzione dei singoli problemi quando si presentano.	Applicazioni	Proteggere		●	●
	16.4	**Stabilire e Gestire un Inventario di Componenti Software di Terze Parti** Stabilire e gestire un inventario aggiornato dei componenti di terze parti utilizzati nello sviluppo, spesso indicato come "distinta del materiale", nonché dei componenti previsti per un uso futuro. Questo inventario deve includere i rischi che ogni componente di terzi potrebbe comportare. Valutare l'elenco almeno mensilmente per identificare eventuali modifiche o aggiornamenti a questi componenti e verificarne il corrente supporto.	Applicazioni	Proteggere		●	●
	16.5	**Utilizzare Componenti Software di Terze Parti Aggiornati** Utilizzare componenti software di terze parti aggiornati e affidabili. Quando possibile, scegliere framework e librerie consolidati e comprovati che forniscano una sicurezza adeguata. Acquisire questi componenti da fonti attendibili o valutare le vulnerabilità del software prima dell'uso.	Applicazioni	Proteggere		●	●
	16.6	**Stabilire e Mantenere un Sistema di Valutazione della Gravità e una Procedura per le Vulnerabilità delle Applicazioni** Stabilire e mantenere un sistema di valutazione della gravità e una procedura per le vulnerabilità delle applicazioni che faciliti la priorità dell'ordine in cui vengono scoperte e risolte. Questo processo include la definizione di un livello minimo di accettabilità di sicurezza per il rilascio di codice o applicazioni. I livelli di gravità offrono un modo sistematico di valutazione delle vulnerabilità che migliorano la gestione del rischio e aiutano a garantire che i bug più gravi vengano corretti per primi. Rivedere e aggiornare il sistema e la procedura annualmente.	Applicazioni	Proteggere		●	●

CONTROLLI	SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3
	16.7	**Utilizzare Modelli di Hardening Standard per la Configurazione dell'Infrastruttura Applicativa** Utilizzare modelli di hardening standard di tipo industriale per la configurazione dei componenti dell'infrastruttura applicativa. Ciò include i relativi server, i database, i server web e si applica ai contenitori cloud, ai componenti Platform as a Service (PaaS) e ai componenti SaaS. Non consentire al software sviluppato internamente di indebolire l'hardening della configurazione.	Applicazioni	Proteggere		●	●
	16.8	**Separare i Sistemi in Produzione e da quelli non in Produzione** Mantenere ambienti separati tra i sistemi in produzione e quelli non in produzione	Applicazioni	Proteggere		●	●
	16.9	**Formare gli Sviluppatori sui Concetti di Sicurezza delle Applicazioni e sulla Codifica Sicura** Garantire che tutto il personale di sviluppo software riceva formazione sulla scrittura di codice sicuro per il proprio ambiente di sviluppo e le proprie responsabilità. La formazione può includere principi generali di sicurezza e pratiche standard di sicurezza delle applicazioni. Predisporre la formazione almeno annualmente e progettandola in modo da promuovere la sicurezza all'interno del team di sviluppo e favorire la cultura della sicurezza tra gli sviluppatori.	Applicazioni	Proteggere		●	●
	16.10	**Applicare Principi di Progettazione Sicura nelle Architetture Applicative** Applicare principi di progettazione sicura nelle architetture applicative. I principi di progettazione sicura includono il concetto di privilegio minimo e l'applicazione della mediazione per validare ogni operazione eseguita dall'utente, applicando il concetto di "non fidarsi mai dell'input dell'utente". Gli esempi includono la garanzia che il controllo degli errori espliciti venga eseguito e documentato per tutti gli input, inclusi dimensioni, tipi di dati, intervalli o formati accettabili. Progettazione sicura significa anche ridurre al minimo la superficie di attacco dell'infrastruttura dell'applicazione, disattivando porte e servizi non protetti, rimuovendo programmi e file non necessari e rinominando o rimuovendo gli account predefiniti..	Applicazioni	Proteggere		●	●
	16.11	**Utilizzare Moduli o Servizi Controllati per i Componenti di Sicurezza delle Applicazioni** Utilizzare moduli o servizi controllati per i componenti di sicurezza delle applicazioni, come la gestione delle identità, la crittografia, il controllo e il logging. L'utilizzo delle funzionalità della piattaforma nelle funzioni di sicurezza più importanti ridurrà il carico di lavoro degli sviluppatori e ridurrà al minimo la probabilità di errori di progettazione o implementazione. I sistemi operativi moderni forniscono meccanismi efficaci per l'identificazione, l'autenticazione e l'autorizzazione e li rendono disponibili per le applicazioni. Utilizzare solo algoritmi di crittografia standardizzati, attualmente accettati e ampiamente controllati. I sistemi operativi forniscono anche meccanismi per creare e mantenere i log di controllo	Applicazioni	Proteggere		●	●
	16.12	**Implementare Controlli di Sicurezza a Livello di Codice** Applicare strumenti di analisi statica e dinamica nel ciclo di vita dell'applicazione per verificare che vengano seguite pratiche di codifica sicura.	Applicazioni	Proteggere			●
	16.13	**Effettuare Test di Penetrazione sull'Applicazione** Effettuare test di penetrazione sulle applicazioni. Per le applicazioni critiche, i test di penetrazione autenticati sono più adatti per trovare vulnerabilità rispetto alla scansione del codice e ai test di sicurezza automatizzati. Il test di penetrazione si basa sull'abilità del tester di manipolare un'applicazione come utente autenticato e non autenticato.	Applicazioni	Proteggere			●
	16.14	**Effettuare la Modellazione delle Minacce** Effettuare la modellazione delle minacce. Consiste nell'identificazione e risoluzione dei difetti di progettazione della sicurezza delle applicazioni all'interno di un progetto, prima della creazione del codice. Viene realizzata attraverso personale appositamente addestrato che valuta la progettazione dell'applicazione misurando i rischi per la sicurezza per ogni punto di ingresso e livello di accesso. L'obiettivo è mappare l'applicazione, l'architettura e l'infrastruttura in modo strutturato per comprenderne i punti deboli.	Applicazioni	Proteggere			●

CONTROLLI	SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3

17 Gestione e Risposta agli Incidenti

Stabilire un programma per sviluppare e mantenere una capacità di risposta agli incidenti (ad esempio criteri, piani, procedure, ruoli definiti, formazione e comunicazioni) per prepararsi a rilevare e rispondere rapidamente ad un attacco.

17.1	**Designare il Personale Incaricato per la Gestione degli Incidenti**	N/A	Rispondere	●	●	●

Designare una persona chiave e almeno un sostituto che dirigerà la procedura di gestione degli incidenti. Il personale di gestione è responsabile del coordinamento e della documentazione delle attività di risposta e agli incidenti e relativo ripristino; ci si può avvalere di dipendenti interni, terzi o scegliendo una soluzione ibrida. Se si utilizza un fornitore di terze parti, designare almeno una persona interna all'azienda per supervisionarne il lavoro. Rivedere annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero avere un impatto su questa Salvaguardia.

17.2	**Stabilire e Mantenere le Informazioni di Contatto per la Segnalazione degli Incidenti di Sicurezza**	N/A	Rispondere	●	●	●

Stabilire e mantenere l'elenco delle figure che devono essere informate degli incidenti di sicurezza. I contatti possono includere personale interno, fornitori di terze parti, forze dell'ordine, compagnie di assicurazione informatica, agenzie governative, partner del Centro di Condivisione e Analisi delle Informazioni (ISAC) o altre parti interessate. Verificare i contatti annualmente per garantire che le informazioni siano aggiornate.

17.3	**Stabilire e Mantenere una Procedura Aziendale di Segnalazione degli Incidenti**	N/A	Rispondere	●	●	●

Stabilire e mantenere una procedura per il personale aziendale per segnalare gli incidenti di sicurezza. Sono inclusi i tempi di segnalazione, il personale di riferimento, il meccanismo di segnalazione e le informazioni minime da riportare. Assicurare che il procedimento sia disponibile pubblicamente per tutto il personale. Rivedere annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero avere un impatto su questa Salvaguardia.

17.4	**Stabilire e Mantenere una Procedura di Risposta agli Incidenti**	N/A	Rispondere		●	●

Stabilire e mantenere una procedura di risposta agli incidenti che preveda ruoli e responsabilità, requisiti di conformità e un piano di comunicazione. Rivedere annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero avere un impatto su questa Salvaguardia.

17.5	**Assegnare Ruoli Chiave e Responsabilità**	N/A	Rispondere		●	●

Assegnare ruoli chiave e responsabilità per la risposta agli incidenti, incluso il personale legale, IT, sicurezza delle informazioni, strutture, pubbliche relazioni, risorse umane, referenti di incidenti e analisti, se possibile. Rivedere annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero avere un impatto su questa Salvaguardia.

17.6	**Definire i Meccanismi di Comunicazione Durante la Risposta agli Incidenti**	N/A	Rispondere		●	●

Determinare quali modalità primarie e secondarie verranno utilizzati per comunicare e segnalare durante un incidente di sicurezza. I meccanismi possono includere telefonate, e-mail o lettere. Tenere presente che determinati meccanismi, come le e-mail, potrebbero non funzionare in seguito ad un incidente di sicurezza. Rivedere annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero avere un impatto su questa Salvaguardia.

17.7	**Condurre Esercizi di Routine in Risposta agli Incidenti**	N/A	Recuperare		●	●

Pianificare e condurre esercizi di routine e scenari in risposta agli incidenti per il personale chiave coinvolto nella procedura per prepararlo a fronteggiare l'eventualità in casi reali. Gli esercizi devono testare i canali di comunicazione, il processo decisionale e i flussi di lavoro. Effettuare test almeno su base annuale.

17.8	**Effettuare Revisioni Post-Incidente**	N/A	Recuperare		●	●

Effettuare revisioni post-incidente. Le revisioni post-incidente aiutano a prevenire il ripetersi di incidenti attraverso l'identificazione delle lezioni apprese e l'azione di follow-up.

17.9	**Stabilire e Mantenere i Livelli per gli Incidenti di Sicurezza**	N/A	Recuperare			●

Stabilire e mantenere i livelli per gli incidenti di sicurezza, inclusa, come minimo, la differenziazione tra un incidente e un evento. Gli esempi possono includere: attività anomale, vulnerabilità della sicurezza, debolezza della sicurezza, violazione dei dati, incidente di privacy, ecc. Rivedere annualmente o quando si verificano cambiamenti aziendali significativi che potrebbero avere un impatto su questa Salvaguardia.

CONTROLLI	SALVAGUARDIE	TITOLO/DESCRIZIONE	TIPO DI RISORSA	FUNZIONE DI SICUREZZA	IG1	IG2	IG3

18 Test di Penetrazione

Verificare l'efficacia e la resilienza delle risorse aziendali identificando e sfruttando i punti deboli nei controlli (persone, processi e tecnologia) e simulando obiettivi ed azioni di un utente malintenzionato.

18.1	**Stabilire e Mantenere un Programma di Test di Penetrazione**	N/A	Identificare		●	●

Stabilire e mantenere un programma di test di penetrazione adeguato alle dimensioni, alla complessità e alla maturità dell'azienda. Le caratteristiche del programma di test di penetrazione includono ambiti di rete, applicazioni Web, API (Interfaccia di Programmazione di un'Applicazione), servizi ospitati e controlli della sede fisica; frequenza, limitazioni (come orari accettabili e tipi di attacco esclusi), informazioni sul punto di contatto, azioni di rimedio (come i risultati verranno indirizzati internamente), requisiti retroattivi.

18.2	**Eseguire Periodicamente Test di Penetrazione Esterni**	Rete	Identificare		●	●

Eseguire periodicamente test di penetrazione esterni basati sui requisiti del programma, almeno annualmente. I test di penetrazione esterni devono includere l'ispezione dell'impresa e dell'ambiente per rilevare le informazioni soggette ad exploit. Questi test richiedono competenze ed esperienze specifiche e devono essere condotti da personale qualificato. I test possono avvenire in modalità "clear box" oppure "opaque box".

18.3	**Correggere Considerando i Risultati del Test di Penetrazione**	Rete	Proteggere		●	●

Rimediare in base ai risultati dei test di penetrazione considerando i criteri aziendali riferiti all'ambito di correzione ed ai livelli di priorità.

18.4	**Convalidare le Misure di Sicurezza**	Rete	Proteggere			●

Convalidare le misure di sicurezza dopo ogni test di penetrazione. Se si ritiene necessario, modificare i set di regole e le capacità di rilevamento delle tecniche utilizzate durante i test.

18.5	**Eseguire Periodicamente Test di Penetrazione Interni**	N/A	Identificare			●

Eseguire periodicamente i test di penetrazione interni basati sui requisiti del programma, almeno annualmente. I test possono avvenire in modalità "clear box" oppure "opaque box".

APPENDICE C

Note di Traduzione

La versione italiana dei Controlli CIS v.8 è stata realizzata conservando, per quanto possibile, il significato letterale, senza appesantire i paragrafi tradotti, alleggerendo la complessità e l'articolazione della lingua inglese. Le parti del documento che presentano un ordinamento alfabetico, vengono tradotte e conservate nella loro ordine originale. Alcuni termini tecnici della lingua inglese non hanno una versione italiana in quanto comunemente utilizzati; la tabella "Acronimi e Abbreviazioni" mantiene per miglior leggibilità sia il testo inglese, sia la traduzione italiana. Alcuni termini, soprattutto nei paragrafi più lunghi, vengono lievemente modificati, adottando quando opportuno e possibile, vari sinonimi, al fine di rendere la lettura più fluida e meno ripetitiva.

Contatti

giacomo.lunardon.125@posta.istruzione.it

CIS Center for Internet Security®

CIS Controls

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats.

Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices. To learn more, visit www.cisecurity.org or follow us on Twitter: @CISecurity.

cisecurity.org
info@cisecurity.org
518-266-3460
Center for Internet Security
@CISecurity
CenterforIntSec
TheCISecurity
cisecurity