Cybersecurity reference guide

Manuale per l'utente

Cybersecurity reference guide

Sommario

Cybersecurity reference guide

Introduzione

Introduzione

Il fine di questa guida è mettere a disposizione una base comune e fungere da riferimento per i materiali relativi alla cybersecurity prodotti da Axis. Sono descrizioni, modelli e strutture semplificati basati su conferenze NIST, SANS, ISO e RSA, nonché materiali di diverse organizzazioni all'interno della comunità di cybersecurity.

Link ad altri materiali di Axis:

- *axis.com/about-axis/cybersecurity*
- *help.axis.com/cybersecurity-qna*
- *axis.com/support/cybersecurity/resources*
- *help.axis.com/axis-security-development-model*
- *axis.com/support/cybersecurity/vulnerability-management*

Definizione di cybersecurity

Basato parzialmente sulla definizione di NIST:

La cybersecurity è la tutela di sistemi e servizi su computer dalle minacce informatiche. Le pratiche di cybersecurity annoverano processi di prevenzione dei danni e di ripristino di computer, sistemi e servizi di comunicazione elettronici, comunicazioni cablate ed elettroniche e informazioni memorizzate per assicurare disponibilità, integrità, sicurezza, autenticità, riservatezza e il non ripudio.

Tipi di organizzazione

Organizzazioni diverse hanno risorse, esposizione e cyber maturity diverse. Quando si segue la prassi raccomandata, *i CIS Controls (precedentemente conosciuti come Critical Security Controls)* definiscono tre profili organizzativi.

- **Gruppo di implementazione SANS 1 (IG1)**

  Nella maggioranza dei casi, un'impresa IG1 è generalmente di piccole o medie dimensioni con competenze IT e di cybersecurity limitate da dedicare alla tutela delle risorse e del personale IT.

- **Gruppo di implementazione SANS 2 (IG2)**

  Un'impresa IG2 ha alle sue dipendenze individui responsabili della gestione e della tutela dell'infrastruttura IT. Queste imprese generalmente supportano molteplici reparti con diversi profili di rischio sulla base alle funzioni e alle mission di ruolo. Piccole unità di imprese possono avere oneri di conformità normativa.

- **Gruppo di implementazione SANS 3 (IG3)**

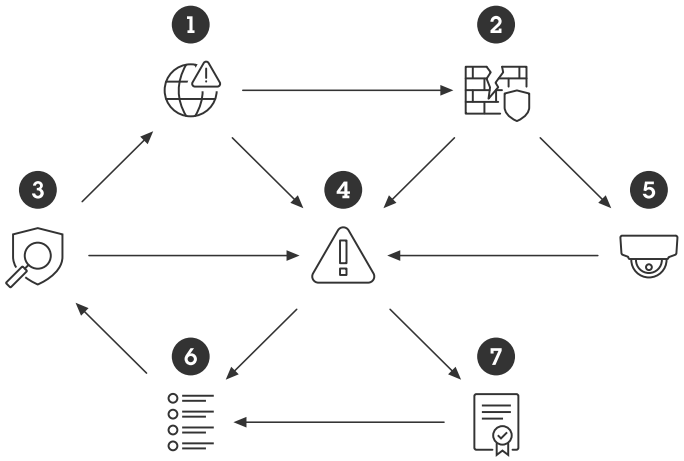
  Un'impresa IG3 si avvale solitamente di esperti di sicurezza che sono specializzati nei vari aspetti della cybersecurity (ad esempio gestione dei rischi, test di penetrazione, sicurezza applicazioni). Le risorse e i dati IG3 contengono informazioni sensibili o funzioni soggette a supervisione normativa e di conformità.

Terminologia

Terminologia

Terminologia

La mappa terminologia illustra le relazioni di specifici termini chiave di cybersecurity menzionati in questo documento.



- **(1) Minacce** utilizzano le **(2) vulnerabilità** esponendo le **(5) risorse** e aumentando i **(4) rischi**
- **(4) Rischi** influenzano la **(7) policy** e indicano i **(6) requisiti**
- **(6) Requisiti** sono indirizzati nei **(3) controlli di sicurezza** che affrontano costantemente **(1) minacce** mitigando al tempo stesso i **(4) rischi**

Rischio

La cybersecurity è incentrata sulla gestione dei rischi nel corso del tempo. I rischi non possono mai essere eliminati, solo attenuati. Talvolta le persone confondono i termini: rischio, risorsa, minaccia, vulnerabilità o impatto negativo

RFC 4949 Internet Security Glossary definisce il rischio come una previsione di perdita espressa come la probabilità che una particolare minaccia sfrutti una determinata vulnerabilità con un particolare risultato dannoso.

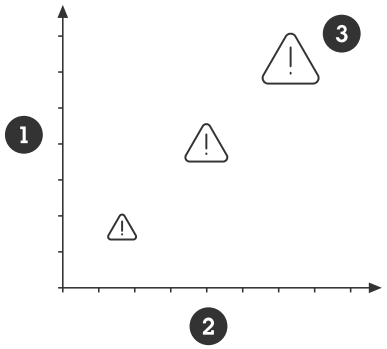
Una definizione abbreviata comunemente usata è **rischio = probabilità x impatto**

Questa formula è usata per dare la priorità ai rischi. La definizione RFC comprende il termine "particolare" per minacce, vulnerabilità e risultati dannosi. Ogni minaccia va osservata singolarmente, partendo da quella caratterizzata dalla maggiore plausibilità e dall'impatto negativo più elevato.

Una difficoltà in merito alla discussione del rischio è rappresentata dal fattore di probabilità. Le cose possono succedere o no. La probabilità che un avversario sfrutti una vulnerabilità è frequentemente stabilita dalla facilità con cui la vulnerabilità è sfruttata (esposizione) e dal potenziale vantaggio che l'avversario può traerne sfruttandola.

Si possono tracciare rischi con queste due dimensioni: usare come un asse la probabilità che un rischio si verifichi e come l'altro asse l'impatto del rischio, nel caso si verifichi. Questo fornisce una visione chiara del potenziale impatto e della priorità da dare a ciascun rischio.

Terminologia



1 ***Probabilità*** *dal basso all'alto*
2 ***Impatto negativo*** *dal basso all'alto*
3 ***Livelli di rischio*** *dal basso all'alto*

Valore attacco = vantaggio attacco – costo attacco

Aggiungere protezione incrementerà il costo dell'attacco e ridurrà perciò le probabilità. Il costo dell'attacco è correlato a quanto tempo, risorse, abilità e sofisticazione servono perché l'attacco riesca. Anche il rischio di essere scoperti o conseguenze negative di altro tipo fa parte del prezzo dell'attacco.

La valutazione dei rischi, il processo per analizzare i rischi nel ciberspazio, è identica alla protezione fisica. Le domande su cui riflettere sono le seguenti:

1. Cosa si desidera proteggere?
2. Da cosa lo si desidera proteggere?
3. Che probabilità di impatto negativo ci sono?
4. Quanto sono gravi le conseguenze di un eventuale fallimento?
5. Quali strategie andrebbero implementate per la riduzione dei rischi?

Implementare qualsiasi misura di protezione o controllo di sicurezza comporta un certo tipo di costo. Le risorse finanziarie di tutte le organizzazioni sono limitate. Se non si conoscono i rischi, è complicato stimare il budget per la propria sicurezza. Si dovranno sempre accettare i rischi, ma deve trattarsi di una decisione intenzionale basata sui rischi.

Eseguire la stima del potenziale impatto negativo su ogni tipo di risorsa è difficile e complesso. In vari casi, le stime sono soggettive e l'analisi degli impatti è spesso una sottostima. Usare il modello di impatto ISO 27000 e i tipi di designazione (ad es. limitato, serio, grave o catastrofico) può contribuire ad ottenere una rapida panoramica che permette l'assegnazione di priorità. Mette a disposizione un modo facile per stabilire un valore più rigoroso basando la stima su quanto tempo servirebbe per riprendersi da un impatto negativo, ad esempio:

- **Limitato** = da ore a giorni
- **Serio** = da giorni a settimane
- **Grave** = da settimane a mesi
- **Catastrofico** = da mesi a anni, se mai sarà possibile

Risorse

Mentre la protezione fisica si concentra sul proteggere persone e oggetti fisici, la protezione di cybersecurity si concentra sul proteggere risorse informatiche e dati. Esistono tre aree principali:

- **Confidentiality (Riservatezza)**: diffusione di informazioni o risorse

Terminologia

- **Integrity (Integrità)**: distruzione o alterazione di informazioni o risorse
- **Availability (Disponibilità)**: accessibilità a informazioni e risorse

Questi ambito sono definiti anche come la triade CIA. La tecnologia operativa (OT) dà spesso la priorità all'usabilità, mentre chi lavora con la tecnologia dell'informazione (IT) dà spesso la priorità alla sicurezza. Individuare il giusto equilibrio tra riservatezza, integrità e disponibilità è spesso complicato.

È necessario che le risorse siano classificate per determinare livelli di protezione adeguati. Non tutti i dati e le risorse informatiche sono uguali in termini di impatto negativo. Sono spesso classificati come segue:

- **Pubblico**: la risorsa è destinata un consumatore pubblico. Oppure l'impatto negativo è limitato in caso di divulgazione al pubblico.
- **Privato**: si tratta di risorse privilegiata per un gruppo specifico/selezionato. Generalmente, l'impatto negativo è limitato ad un'organizzazione specifica, ad esempio un'azienda o una famiglia.
- **Riservato**: si tratta di una risorsa privilegiata destinata ad individui selezionati all'interno di un'organizzazione.

I video dal vivo in un sistema video si possono classificare come pubblici, con riferimento sia al pubblico in generale sia a quello interno di un'organizzazione. Tuttavia, nella gran parte dei casi, i video dal vivo sono classificati come privati, cioè sono accessibili solo a una specifica unità organizzativa. Invece i video registrati, nella maggior parte dei casi, sono classificati come riservati perché potrebbero contenere scene potenzialmente molto sensibili. Anche le credenziali e le configurazioni sono dati che da classificare come riservati.

Minacce

Si può definire come minaccia qualsiasi cosa abbia la potenzialità di compromettere o danneggiare beni o risorse. Generalmente, le persone tendono ad associare le minacce informatiche ad hacker malintenzionati e malware. In realtà, gli effetti negativi sono spesso causati da incidenti, uso improprio involontario o guasti hardware.

Gli attacchi non arrivano dal nulla. Esiste sempre qualche motivazione per compromettere un sistema e le sue risorse. Gli attacchi si possono classificare come opportunistici o mirati. Nella cybersecurity, i malintenzionati sono anche chiamati "avversari" che potrebbero avere cattive intenzioni.

La maggior parte degli attacchi al giorno d'oggi sono opportunistici: attacchi che avvengono solo perché si presenta un'opportunità. In vari casi, un aggressore opportunistico esterno non sa nemmeno chi è la vittima. Questi aggressori usano vettori di attacco a basso costo, ad esempio phishing e probing. In tali casi, non sono abbastanza determinati ad impiegare tempo e risorse in un attacco fallito; passano in fretta al prossimo tentativo. Applicare un livello di protezione standard attenuerà la gran parte dei rischi relativi ad attacchi opportunistici. È più difficile tutelarsi dagli attacchi mirati, da quei malintenzionati che prendono di mira un sistema specifico con un obiettivo specifico. Gli attacchi mirati si servono degli stessi vettori di attacco a basso costo di quelli opportunistici. Tuttavia, se gli attacchi iniziali non riescono, sono più determinati e sono disposti a spendere tempo e risorse per usare metodi più sofisticati per conseguire i propri obiettivi. Per loro, la priorità è il valore della posta in gioco.

Avversari frequenti (threat actor)

- **Intimo**: gente che potrebbe voler scavare nella tua vita personale
- **Dipendenti**: o gente che può aver eseguito lecitamente l'accesso al sistema, accidentalmente o per uso improprio intenzionale
- **Burloni**: persone che si divertono a interferire con i sistemi informatici
- **Hacktivist**: persone che vogliono attaccare le organizzazioni per motivi politici o ideologici.
- **Cyber criminali**: persone che vogliono guadagnare soldi attraverso truffe o la vendita di informazioni preziose
- **Concorrenti industriali**: entità alle quali interessa ottenere un vantaggio economico per le proprie società o organizzazioni
- **Cyber terroristi**: persone o entità che implementano un attacco pensato per causare allarme o panico, spesso per motivi ideologici o politici
- **Stati-nazione**: agenti di servizi di intelligence stranieri che agiscono per ottenere vantaggi economici e politici o per causare danni a sistemi di informazione critici

- **Individui**: una persona o un gruppo specifico che agisce individualmente, le cui motivazioni possono differire da quelle sopra elencate. Può essere un giornalista investigativo, un hacker white hat o simile. Gli hacker white hat (cioè hacker etici) possono essere una minaccia se si dà la priorità a nascondere i difetti piuttosto che a correggerli.

Vulnerabilità

Ogni sistema presenta vulnerabilità. Le vulnerabilità mettono a disposizione degli avversari l'opportunità di attaccare o ottenere accesso a un sistema. Possono essere il risultato di difetti, esposizione, funzionalità o errori umani. I malintenzionati potrebbero cercare di sfruttare qualsiasi vulnerabilità nota, combinandone frequentemente una o più. La maggior parte delle violazioni è il risultato di errori umani, sistemi configurati male o non sottoposti adeguatamente a manutenzione, spesso per mancanza di politiche adeguate, responsabilità indefinite e scarsa consapevolezza a livello organizzativo.

Vulnerabilità software

Un'API (interfaccia per la programmazione di applicazioni) di dispositivo e un servizio software possono presentare difetti o funzionalità sfruttabili in un attacco. Nessun fornitore potrà mai garantire prodotti privi di difetti. Se i difetti sono conosciuti, è possibile attenuare i rischi tramite misure di controllo della sicurezza di compensazione. D'altra parte, se un aggressore scopre un nuovo difetto sconosciuto, il rischio di exploit zero-day riusciti è più elevato perché la vittima non ha avuto tempo per tutelare il sistema.

Il Common Vulnerability Scoring System (CVSS) è una maniera per classificare la gravità di una vulnerabilità del software. Una formula che esamina la facilità di un exploit e qual è l'impatto negativo. Il punteggio è un valore tra 0 e 10. 10 rappresenta la maggiore gravità. Troverai spesso un numero CVSS in rapporti Common Vulnerabilities and Exposures (CVE) pubblicati.

Axis usa il CVSS come una delle misure per stabilire quanto sia critica una vulnerabilità identificata nel software/dispositivo

Criterio

È importante stabilire politiche e processi di sistema chiari in modo da raggiungere un'adeguata riduzione dei rischi a lungo termine. Un approccio consigliato consiste nel lavorare secondo un framework di protezione informatico ben definito, quale ISO 27001, NIST o simili. Anche se questa attività può risultare gravosa per le società di piccole dimensioni, avere una documentazione del processo e una politica seppur minima è molto meglio di niente.

Controlli di sicurezza

I controlli di sicurezza sono misure di sicurezza o contromisure utilizzate per evitare, rilevare, neutralizzare o minimizzare i rischi per la sicurezza di proprietà fisiche, informazioni, sistemi informatici o altre risorse. I processi per implementare i controlli di sicurezza sono chiamati frequentemente "hardening" (protezione).

I controlli di sicurezza di compensazione rappresentano misure di sicurezza alternative che utilizzabili quando non risulta possibile l'applicazione del controllo di sicurezza preferito o quando c'è la possibilità che il controllo preferito non sia disponibile o sia eccessivamente costoso.

I controlli di sicurezza si devono monitorare e aggiornare di continuo man mano che minacce, valori, vulnerabilità ed esposizione cambiano nel tempo. Perciò si devono definire e seguire criteri e processi.

SANS Institute ha pubblicato una *lista di controlli CIS*, un set di migliori prassi di cybersecurity prioritarie. Per illustrare la varietà dei controlli di sicurezza, eccone l'elenco completo.

- Comando CIS #1: Inventario e controllo delle risorse aziendali
- Comando CIS #2: Inventario e controllo delle risorse software
- Comando CIS #3: Protezione dati
- Comando CIS #4: Configurazione sicura delle risorse e del software aziendali
- Comando CIS #5: Gestione account
- Comando CIS #6: Gestione del controllo degli accessi

Terminologia

- Comando CIS #7: Gestione continua delle vulnerabilità
- Comando CIS #8: Gestione registro di controllo
- Comando CIS #9: Protezioni per e-mail e browser Web
- Comando CIS #10: Difese da malware
- Comando CIS #11: Recupero dati
- Comando CIS #12: Gestione dell'infrastruttura di rete
- Comando CIS #13: Monitoraggio e difesa rete
- Comando CIS #14: Consapevolezza in materia di sicurezza e formazione per le competenze
- Comando CIS #15: Gestione provider di servizi
- Comando CIS #16: Sicurezza software applicazione
- Comando CIS #17: Gestione reazione agli incidenti
- Comando CIS #18: Test di penetrazione

La *Guida alla protezione AXIS OS* si basa su CIS.

Misure di tutela contro le minacce comuni

Comprendendo e contrastando le minacce comuni, si possono ridurre la maggioranza dei rischi.

Uso improprio intenzionale o accidentale del sistema

Trovare un equilibrio tra l'usabilità e la sicurezza di un sistema è complicato. Molti sistemi sono rafforzati dal punto di vista della comodità, non della sicurezza. Ciò mette a disposizione occasioni per l'uso improprio intenzionale o accidentale. Le persone autorizzate ad accedere a un sistema sono la minaccia più diffusa in qualsiasi sistema.

Esempi di minacce diffuse:

- Individui che potrebbero accedere a servizi (come video dal vivo o registrati) senza esserne autorizzati
- Individui che commettono errori
- Individui che potrebbero tentare di rimediare a un problema e causare una riduzione delle prestazioni del sistema
- Individui che sono scontenti potrebbero causare danni intenzionali al sistema
- Individui vulnerabili al social engineering
- Individui che rubano
- Individui che perdono o mettono al posto sbagliato componenti critici (tessere di accesso, telefoni, laptop, documentazione, ecc.)
- Individui i cui computer possono essere compromessi e infettare involontariamente un sistema con malware

Le misure di tutela diffuse consigliate sono:

- Processo e politica definiti per gli account degli utenti
- Schema di autenticazione degli accessi adeguato
- Strumenti per la gestione degli account utente e dei privilegi nel tempo
- Riduzione dell'esposizione
- Formazione nell'ambito della cybersecurity

Come Axis aiuta nel contrasto di questa minaccia:

- La *Guida alla protezione AXIS OS* descrive controlli di sicurezza comuni per le minacce comuni a un dispositivo
- La *Guida alla protezione di AXIS Camera Station* descrive controlli di sicurezza comuni per i sistemi video
- *AXIS Device Manager* e *AXIS Device Manager Extend* aiutano nella gestione di controlli di sicurezza comuni

Manomissione fisica e sabotaggio

La tutela fisica dei sistemi IT è molto importante sotto l'aspetto della cybersecurity.

Esempi di minacce diffuse:

- Le attrezzature fisicamente esposte possono essere soggette a manomissioni
- Le attrezzature fisicamente esposte possono essere rubate
- I cavi fisicamente esposti potrebbero essere sconnessi, reindirizzati o tagliati

Misure di tutela diffuse consigliate:

- Posizionamento dell'attrezzatura di rete (ad es. server e switch) in aree bloccate
- Montaggio delle telecamere affinché siano difficili da raggiungere
- Uso di alloggiamento protettivo in caso di esposizione fisica
- Protezione dei cavi in pareti o canaline

Come Axis aiuta nel contrasto di questa minaccia:

- Scheda di memoria crittografata affinché non sia possibile riprodurre video se un utente non autorizzato riesce ad espellere la scheda di memoria
- Rilevamento di manomissione della vista della telecamera
- Rilevamento apertura alloggiamento

Sfruttamento delle vulnerabilità note del software

Tutti i prodotti basati su software hanno vulnerabilità che potrebbero essere sfruttate. Si possono categorizzare come note e sconosciute. Tutte le vulnerabilità sconosciute finiranno per essere note; non è che una questione di tempo. La gran parte delle vulnerabilità presenta un basso rischio, il che vuol dire che sono molto difficili da sfruttare o che il relativo impatto negativo è limitato. Occasionalmente, sono scoperte vulnerabilità che potrebbero essere sfruttabili e causare un impatto negativo significativo. MITRE ospita un ampio database di CVE (Common Vulnerabilities and Exposures) per aiutare le altre persone ad attenuare i rischi.

Misure di tutela diffuse consigliate:

- Un processo continuo di patch aiuta nella riduzione al minimo del numero di vulnerabilità note in un sistema.
- La riduzione al minimo dell'esposizione della rete per rendere più difficile individuare e sfruttare vulnerabilità note.
- La collaborazione con subfornitori fidati che lavorino in base a politiche e processi che riducono al minimo le falle, che hanno processi per mettere a disposizione patch e sono trasparenti sulle vulnerabilità critiche rilevate.

In che modo Axis fornisce il suo aiuto:

- *Axis Security Development Model* è un framework che definisce i processi e gli strumenti che Axis usa per la riduzione del rischio di rilascio di prodotti contenenti vulnerabilità software.
- *I criteri di gestione delle vulnerabilità di Axis* comportano l'identificazione, la correzione e la divulgazione delle vulnerabilità che i i clienti devono conoscere per intraprendere le azioni appropriate. Dall'aprile 2021, Axis è stata approvata come Common Vulnerabilities and Exposures (CVE) Numbering Authority (CNA) per i prodotti Axis, il che ci permette di adattare i processi ai processi standard di settore di MITRE Corporation. Questo, ci aiuta a sua volta a sostenere meglio i nostri clienti.
- *Le guide Axis sulla protezione avanzata*, come *Guida alla protezione AXIS OS*, forniscono consigli su come si riduce l'esposizione e si aggiungono controlli di compensazione ai fini della riduzione del rischio di sfruttamento di falle nel software.
- Le versioni firmware LTS (supporto a lungo termine) permettono ai clienti di eseguire patch sul sistema operativo dei dispositivi Axis riducendo al minimo i rischi di problemi di incompatibilità con video management system di terze parti.

Attacco alla catena di fornitura

Un attacco alla catena di fornitura è un attacco informatico che tenta di arrecare danno ad un'organizzazione prendendo di mira gli elementi meno sicuri nella catena di fornitura. Si usa principalmente quando altri vettori di attacco (ad esempio, social engineering, phishing e probing dell'interfaccia) falliscono per via di livelli elevati di protezione del sistema. L'attacco viene realizzato compromettendo software/firmware/prodotti e inducendo l'amministratore ad installarli nel sistema. È possibile che un prodotto venga compromesso nel corso della spedizione al proprietario del sistema. Per eseguire con successo un attacco alla catena di fornitura sono necessari competenze, tempo e risorse.

Le misure di tutela diffuse consigliate sono:

Misure di tutela contro le minacce comuni

- Una politica che stabilisca che si devono installare unicamente software di fonti attendibili e verificate.
- La verifica dell'integrità software paragonando il checksum del software (digest) con il checksum del fornitore prima di eseguire l'installazione.
- Il controllo della confezione o del prodotto alla consegna per verificare che non siano stati manomissioni.

Come Axis aiuta nel contrasto di questa minaccia:

- il software Axis è pubblicato con un checksum, permettendo agli amministratori di convalidare l'integrità del software prima di installarlo.
- Il firmware firmato in un dispositivo Axis garantisce che AXIS OS sia di proprietà di Axis e garantisce che anche qualsiasi nuovo firmware da scaricare e installare nel dispositivo sia firmato da Axis.
- L'avvio sicuro su un dispositivo Axis permette al dispositivo di verificare che il firmware sia dotato di una firma Axis. Se il firmware non è autorizzato o ha subito alterazioni, il processo di avvio si interrompe.
- L'ID dispositivo Axis conforme a IEEE 802.1AR è un certificato di fornitore Axis univoco del dispositivo che mette a disposizione del sistema una maniera per verificare che l'hardware nell'alloggiamento venga da Axis.
- La crittografia della scheda di memoria e la criptazione del file system impediscono l'estrazione dei dati memorizzati quando avviene il furto della scheda o del dispositivo.

Manuale per l'utente
Cybersecurity reference guide

Ver. M3.2
Data: Novembre 2023
Codice art. T10201166