Domande e risposte sulla sicurezza informatica

Manuale per l'utente

Domande e risposte sulla sicurezza informatica

In caso tu cerchi altre domande e risposte, visita il *database delle domande frequenti* di Axis.

Domande e risposte sulla sicurezza informatica

Domande generali

Domande generali

Cos'è la cybersecurity?

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.

La cybersecurity consiste nel gestire i rischi durante un periodo di tempo prolungato. I rischi non possono mai essere eliminati, solo attenuati.

In linea di massima, cosa implica la gestione della cybersecurity?

La cybersecurity riguarda i dispositivi, le persone, le tecnologie e i processi continui.

Comporta dunque l'**identificazione** e la valutazione di vari aspetti dell'organizzazione, tra cui la redazione di un inventario di dispositivi, sistemi, software e firmware, la definizione di obiettivi critici, la documentazione di procedure e politiche di sicurezza; l'applicazione di una strategia di gestione dei rischi e l'esecuzione continua di valutazioni dei rischi relativamente alle tue risorse.

Comporta l'implementazione di controlli di sicurezza e misure di **protezione** di dati, dispositivi, sistemi e strutture che hai riconosciuto come prioritari contro attacchi informatici.

Inoltre, comporta lo sviluppo e l'implementazione di attività che permettono il **rilevamento** di attacchi cyber affinché tu possa attuare azioni rapide. Ciò potrebbe, ad esempio, comportare un sistema SIEM (Security Information and Event Management) o un sistema SOAR (Security Orchestration, Automation and Response) che gestisca i dati dai dispositivi di rete e dal software di gestione, che aggreghi dati relativi a comportamenti anomali o potenziali cyber attacchi e analizzi tali dati per mettere a disposizione avvisi in tempo reale. I dispositivi Axis supportano i registri SYS e Remote SYS che sono la fonte principale di dati per il tuo sistema SIEM o SOAR.

La gestione della cybersecurity comporta anche sviluppare ed implementare procedure per **reagire** a un incidente di cybersecurity una volta rilevato. Devi tenere in considerazione le normative locali e le politiche interne, nonché i requisiti per la pubblicazione di incidenti di cybersecurity. Axis mette a disposizione una *Guida forense AXIS OS* che permette di comprendere se un dispositivo Axis è stato compromesso nel corso di un attacco alla cybersecurity.

Anche sviluppare e implementare attività per mantenere piani di resilienza e **recupero** o ripristino di qualsiasi capacità o servizio che sia stato compromesso per via di un incidente di cybersecurity sarà importante. *AXIS Device Manager*, ad esempio, rende facile ripristinare i dispositivi Axis supportando punti di ripristino, che sono "istantanee" salvate della configurazione di sistema in un punto temporale. In assenza di un punto di ripristino rilevante, lo strumento può darti una mano a riportare tutti i dispositivi ai loro stati predefiniti e ad inviare i modelli di configurazione salvati attraverso la rete.

Cosa sono i rischi di cybersecurity?

A costituire un rischio di cybersecurity (in base alla definizione di RFC 4949 Internet Security Glossary) *è una previsione di perdita espressa come la probabilità che una particolare minaccia sfrutti una determinata vulnerabilità con un particolare risultato dannoso.*

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.

Per ottenere informazioni su come si valutano i rischi e si assegna loro la priorità, consulta la *Guida di riferimento alla cybersecurity*.

Cosa sono le minacce?

Si può definire come minaccia qualsiasi cosa abbia la potenzialità di compromettere o danneggiare i tuoi beni o le tue 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 si possono classificare come opportunistici o mirati. La maggior parte degli attacchi al giorno d'oggi sono opportunistici: attacchi che avvengono solo perché si

Domande generali

presenta un'opportunità. Questi attacchi usano vettori di attacco a basso costo, ad esempio phishing e probing. Applicare un livello di protezione standard attenuerà la gran parte dei rischi relativi ad attacchi opportunistici.

È più difficile tutelarsi dai 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.

Quali sono le minacce più diffuse e come si possono affrontare?

Uso improprio intenzionale o accidentale di un sistema

Le persone autorizzate ad accedere a un sistema sono fra le minacce più diffuse in qualsiasi sistema. È possibile che eseguano l'accesso a servizi a cui non sono autorizzati. Potrebbero rubare o causare danni intenzionali al sistema. Le persone possono anche commettere errori. Nel tentare di porvi rimedio, potrebbero inavvertitamente ridurre le prestazioni di sistema. Gli individui sono anche vulnerabili al social engineering; cioè tattiche che inducono utenti legittimi a divulgare informazioni sensibili. È possibile che gli individui perdano o spostino componenti critici (tessere di accesso, telefoni, laptop, documentazione, ecc.). I computer delle persone possono essere compromessi e infettare involontariamente un sistema con malware.

Le protezioni consigliate comprendono un processo e una politica definiti per gli account degli utenti, uno schema di autenticazione degli accessi sufficiente, strumenti per la gestione degli account e dei privilegi degli utenti nel tempo, riduzione dell'esposizione e formazione nell'ambito della cybersecurity.

Axis aiuta nel contrasto a questa minaccia con *guide alla protezione* e strumenti come *AXIS Device Manager* e *AXIS Device Manager Extend*.

Manomissione fisica e sabotaggio

Le apparecchiature esposte fisicamente possono essere soggette a manomissioni, furto, disconnessione, reindirizzamento o taglio.

Fra le protezioni consigliate sono inclusi il posizionamento dei dispositivi di rete (ad esempio server e switch) in aree chiuse a chiave, il montaggio delle telecamere affinché siano difficili da raggiungere, l'uso di alloggiamenti protetti quando sono fisicamente esposte e la protezione dei cavi nelle pareti o nelle canaline.

Axis aiuta a contrastare questa minaccia con *alloggiamenti protettivi* per dispositivi, viti anti-manomissione, telecamere capaci di crittografare le schede di memoria, rilevamento della manomissione della vista della telecamera e rilevamento dell'apertura di una custodia.

Sfruttamento delle vulnerabilità del software

Tutti i prodotti basati su software hanno vulnerabilità (note o sconosciute) che potrebbero essere sfruttate. 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, è possibile che siano scoperte vulnerabilità sfruttabili dall'impatto negativo significativo. MITRE ospita un ampio database di CVE (Common Vulnerabilities & Exposures) per aiutare gli altri ad attenuare i rischi.

Fra le protezioni consigliate sono inclusi l'esecuzione di un processo continuo di patch che permetta di ridurre al minimo il numero di vulnerabilità note in un sistema, la riduzione al minimo dell'esposizione della rete per rendere più difficile individuare e sfruttare le vulnerabilità note, e la collaborazione con subfornitori fidati che lavorino in base a politiche e processi che riducono al minimo i difetti e che mettono a disposizione patch e sono trasparenti sulle vulnerabilità critiche rilevate.

Axis affronta la minaccia con *Axis Security Development Model*, il cui fine è ridurre quanto più possibile le vulnerabilità del software Axis nonché con *Axis Vulnerability Management Policy*, che riconosce, risolve e annuncia vulnerabilità delle quali i clienti devono essere consapevoli per poter mettere in pratica misure adeguate. Da aprile 2021, *Axis è una Common Vulnerabilities and Exposures Numbering Authority* per i dispositivi Axis e ciò ci consente di adattare i nostri processi ai processi standard di settore di MITRE Corporation. Axis mette anche a disposizione *guide alla protezione* con consigli su come ridurre l'esposizione e aggiungere controlli per diminuire il rischio di sfruttamento delle vulnerabilità. Axis mette a disposizione degli utenti *due diverse tracce di software dei dispositivi* per mantenere aggiornato il sistema operativo di un dispositivo Axis:

1. La traccia attiva mette a disposizione aggiornamenti del software del dispositivo che supportano nuove caratteristiche e funzionalità, nonché correzioni di bug e patch di sicurezza.

2. La traccia di supporto a lungo termine (LTS) mette a disposizione aggiornamenti del software del dispositivo che supportano correzioni di bug e patch di sicurezza, riducendo al minimo i rischi di problemi di incompatibilità con sistemi di terzi.

Domande e risposte sulla sicurezza informatica

Domande generali

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. L'attacco viene realizzato compromettendo software/sistema operativo/dispositivi e inducendo l'amministratore ad installarli nel sistema. È possibile che un dispositivo venga compromesso nel corso della spedizione al proprietario del sistema.

Fra le protezioni raccomandate si annoverano una politica che preveda di installare esclusivamente software proveniente da fonti attendibili e verificate, la verifica dell'integrità del software confrontando il checksum (digest) del software con il checksum del fornitore prima dell'installazione, la verifica della presenza di eventuali segni di manomissione nei prodotti consegnati.

Axis contrasta questa minaccia in vari modi. Axis pubblica software dotato di un checksum per consentire agli amministratori di convalidarne l'integrità prima di installarlo. Quando si carica un nuovo sistema operativo per i dispositivi, i dispositivi Axis collegati in rete accettano solo il software del dispositivo firmato da Axis. L'*Avvio sicuro* sui dispositivi Axis connessi in rete assicura inoltre che sui dispositivi sia eseguito solo il sistema operativo Axis. Ogni dispositivo, inoltre, ha un ID dispositivo Axis univoco che consente al sistema di controllare che il dispositivo sia un dispositivo Axis originale. Dettagli su tali funzionalità di sicurezza informatica sono disponibili nel whitepaper *Axis Edge Vault* (pdf).

Per ulteriori dettagli in merito alle minacce, vedere la *Guida di riferimento alla sicurezza informatica*.

Cosa sono le vulnerabilità?

Le vulnerabilità mettono a disposizione degli avversari l'opportunità di attaccare o ottenere accesso a un sistema. Possono essere il risultato di difetti, 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 e non sottoposti adeguatamente a manutenzione, spesso per mancanza di politiche adeguate, responsabilità indefinite e scarsa consapevolezza a livello organizzativo.

Cosa sono le 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. D'altra parte, se un aggressore scopre un nuovo difetto sconosciuto, il rischio è più elevato perché la vittima non ha avuto tempo per tutelare il sistema.

Cos'è il Common Vulnerability Scoring System (CVSS)?

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 il numero CVSS in rapporti Common Vulnerability and Exposure (CVE) pubblicati.

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

Domande e risposte sulla sicurezza informatica

Domande specifiche per Axis

Domande specifiche per Axis

Di quali corsi di formazione e guide posso usufruire per capire meglio la cybersecurity e che posso fare per tutelare meglio i dispositivi e i servizi da incidenti informatici?

La pagina Web *Risorse* fornisce accesso a guide relative alla protezione (ad es. la *Guida alla protezione AXIS OS*, la *Guida alla protezione del sistema AXIS Camera Station* e la *Guida alla protezione degli switch di rete Axis*), a documenti sulle politiche e altro ancora. Axis mette inoltre a disposizione corsi di *e-learning* sulla sicurezza informatica.

Dove posso individuare il sistema operativo più recente per il mio dispositivo?

Andare al *software del dispositivo* e cercare il tuo dispositivo.

Come posso aggiornare in modo facile il sistema operativo sul mio dispositivo?

Per aggiornare il software del dispositivo, puoi usare un software per la gestione video Axis, ad esempio *AXIS Companion* o *AXIS Camera Station*, o strumenti come *AXIS Device Manager* e *AXIS Device Manager Extend*.

Nel caso di interruzioni nei servizi Axis, come posso esserne informato?

Visita *status.axis.com*.

Come posso essere informato sulla scoperta di una vulnerabilità?

Puoi iscriverti al *servizio di notifiche di sicurezza Axis*.

Com'è che Axis gestisce le vulnerabilità?

Vedi *Axis Vulnerability Management Policy*.

Com'è che Axis riduce al minimo le vulnerabilità dei software?

Leggi l'articolo *Rendere la cybersecurity parte integrante dello sviluppo software di Axis*.

In che modo Axis supporta la sicurezza informatica in tutto il ciclo di vita di un dispositivo?

Visitare *Un approccio del ciclo di vita alla sicurezza informatica*.

Quali sono le funzionalità di sicurezza informatica integrate nei dispositivi Axis?

Maggiori informazioni:

- *Axis Edge Vault*
- *AXIS OS*
- *Supportare la sicurezza informatica in tutto il ciclo di vita del dispositivo*

Domande e risposte sulla sicurezza informatica

Domande specifiche per Axis

Axis ha la certificazione ISO? A quali altre norme è conforme Axis?

Visita la pagina web *Conformità*.

In che modo Axis aiuta la mia azienda a rispettare NIS 2?

Vedere l'articolo su *NIS 2* (pdf).

Manuale per l'utente
Domande e risposte sulla sicurezza informatica

Ver. M4.2
Data: Luglio 2024
Codice art. T10189380