SICUREZZA IN RETE

Migliori prassi per la sicurezza di hardware e software in rete

EL.MO. SPA

SICUREZZA IN RETE

La sicurezza informatica è un aspetto essenziale per la protezione di dati di aziende e società e richiede competenze sempre più specifiche in considerazione della maggiore frequenza delle minacce informatiche e del loro crescente livello di sofisticazione. In termini di sicurezza informatica, le aziende presentano livelli diversi di vulnerabilità; il primo passo da fare, quindi, in un'ottica proattiva, è la realizzazione di un'analisi dei rischi che permetta l'attuazione di una strategia vincente per la protezione dei dati e la prevenzione degli attacchi informatici. L'analisi dovrà prendere in considerazione, accanto alle potenziali minacce, anche l'ammontare dei danni che le stesse potrebbero causare e i costi relativi che le aziende dovrebbero sostenere per ripristinare l'intera rete o il sistema.

La creazione e la manutenzione di reti sicure richiede considerevoli sforzi e grandi investimenti in termini di strumenti all'avanguardia, pianificazione di efficaci strategie difensive e divulgazione di informazioni agli utenti circa l'importanza vitale che le reti rivestono per l'attività di ogni giorno. La sicurezza delle reti informatiche prevede l'utilizzo di strumenti appropriati (filtri, firewall, sistemi di codificazione dati, ecc.), interventi di manutenzione regolari e la protezione di tutti i dispositivi connessi alla rete stessa.

Le reti informatiche con difese avanzate e la cui efficienza è garantita da regolari interventi garantiscono un livello di sicurezza maggiore. Al contrario, una rete protetta in modo non adeguato diventa allettante per gli hacker che saranno in grado di rubare facilmente dati o altro materiale o, più semplicemente, potranno immettere nel sistema malware, virus o altre minacce informatiche. L'impatto e i costi di queste azioni dannose non posso essere adeguatamente stimati ma non devono essere sottostimati, né per le reti, né per tutti i sistemi che utilizzano queste reti per la loro attività quotidiana.

È quindi necessario che i clienti prendano tutte le necessarie precauzioni per mettere in sicurezza le loro reti e, di conseguenza, i loro sistemi e pretendano la stessa propensione alla sicurezza da parte degli installatori partner che realizzeranno i loro sistemi con tutti i dispositivi e gli strumenti che ne fanno parte.

In considerazione della vulnerabilità e della dimensione globale delle reti attuali, **un fallimento del sistema di sicurezza dovuto alla non implementazione di adeguate precauzioni, o alla sottovalutazione delle stesse, non può essere imputato al fornitore del sistema stesso.**

Seguono informazioni più dettagliate su come aumentare le protezione e la resilienza di reti e dispositivi in rete.

MANTENERSI INFORMATI

La lettura di questa guida sicuramente può dare una buona visione dell'universo della sicurezza informatica.

Tuttavia, come per tutto quanto riguarda l'informatica, minacce e contromisure sono in costante evoluzione: è consigliabile, quindi, utilizzare internet per documentarsi regolarmente sulle nuove minacce, sulle più recenti contromisure e anche per approfondire la conoscenza degli argomenti trattati in questa guida.

Una maggiore conoscenza consente, infatti, di farsi un'idea migliore delle minacce informatiche, di valutare la sicurezza del sistema e di fare un'adeguata analisi dei rischi per definire l'opportunità di aggiornare le procedure di sicurezza.

I **termini in grassetto** nel testo rappresentano concetti complessi che è utile approfondire. Usate un motore di ricerca o Wikipedia per acquisire maggiori informazioni.

GESTIONE DELLE PASSWORD

È necessario prevenire l'accesso da parte di utenti non autorizzati a un sistema di sicurezza, costoro potrebbero infetti disabilitarne alcune parti, modificarne le impostazioni o utilizzarne le informazioni per scopi diversi dai quali sono stati conservati.

Contemporaneamente, però, lo stesso sistema deve anche poter garantire l'accesso agli utenti autorizzati affinché svolgano le funzioni previste e questo, normalmente, avviene tramite l'utilizzo di una password.

In questa sezione saranno fornite indicazioni sulla creazione di password complesse e difficili da indovinare e sulla corretta gestione delle stesse.

Utilizzo di password complesse

Se la password non è complessa e quindi è facile da indovinare, è come se non fosse stata impostata.

Evitare l'utilizzo di:

- password di default, accessibili a tutti nella documentazione tecnica;
- password brevi, deboli di fronte ad attacchi basati sulla **ricerca esaustiva**;
- una o più parole contenute in un dizionario, esposte agli **attacchi a dizionario**;
- parole contenute in un dizionario, sostituendo caratteri con altri simili (es. P455W0RD);
- sequenze comuni di caratteri (es. *123*, oppure *asd*);
- dati personali di facile reperibilità (es. data di nascita, nomi di familiari, ecc.).

Per essere considerata complessa una password deve contenere almeno 8 caratteri scelti con criterio casuale che includano lettere maiuscole e minuscole, numeri e simboli.

Utilizzo di password uniche

Spesso accade che la stessa password venga utilizzata per diversi servizi. È invece corretto impostare una password diversa per ogni servizio utilizzato, malgrado l'impegno di doverne imparare molte.

Infatti, se un hacker riuscisse a trovare la password per un servizio (es. con il **phishing** o in seguito alla violazione di un database contenente password, **data breach**) quasi sicuramente tenterebbe di risalire all'identità dell'utente per provare ad accedere ai suoi servizi utilizzando la stessa password.

Per gli stessi motivi, è sconsigliabile utilizzare la stessa password per più dispositivi connessi alla medesima rete. Infatti, se qualche malintenzionato trovasse la password per uno di questi (es. telecamera) i danni sarebbero limitati a quel dispositivo specifico in quanto non riuscirebbe ad accedere agli altri.

Protezione delle password

Non confidare la password a nessuno. Nel caso in cui fosse necessario l'accesso di altri al vostro sistema, fate in modo che abbiano una password personale o digitatela voi stessi di nascosto.

Più persone sono a conoscenza di una password, maggiore è il rischio che una di esse se la lasci sfuggire.

In sistemi in cui nome utente e password sono usati per tener traccia di quale utente ha modificato le impostazioni, confidare i dati di accesso significa poter essere ritenuto responsabile di azioni altrui.

Modificare spesso le password

Se un malintenzionato apprende una password e la usa per spiare il sistema mantenendo un basso profilo (**snooping**), cambiare la password impedirà l'accesso dell'intruso una volta che la sua password e quella corrente non coincideranno più.

Dover scegliere spesso nuove password potrebbe spingere all'utilizzo di password deboli o già utilizzate in precedenza: se si cede a questa tentazione, cambiare password spesso diventa controproducente.

Disabilitare il login automatico

Nel caso in cui un sistema di sicurezza risieda su un computer utilizzato da diversi utenti, verificare che il login automatico sia disabilitato per prevenire potenziali accessi indesiderati al sistema o alla rete.

Valutare l'utilizzo di un password manager

La necessità di utilizzare molte password diverse e complesse richiede uno sforzo (**password fatigue**) che spesso porta a scegliere di usare password più deboli o già usate per altri servizi, aumentando così la vulnerabilità della rete e del sistema.

Una possibile soluzione è l'utilizzo di un password manager, uno strumento contenente l'elenco protetto di tutte le password in uso. Pur essendo vero che questo strumento semplifica la gestione di un numero elevato di password, la sottrazione della password principale comporterà la sottrazione di tutte.

Diffondere la cultura della sicurezza dei dati

Assicurarsi che le persone che impostano e utilizzano le password siano a conoscenza di quanto riportato nei paragrafi precedenti.

Creazione di un account amministratore di backup

Nel caso in cui un hacker riesca ad accedere al vostro sistema, potrebbe tentare di cambiare la password per impedirvene l' accesso. Se il sistema lo consente, create un account amministratore di backup da utilizzare per accedere al sistema e modificare le password dell'account hackerato in modo da riguadagnarne il controllo in caso di accesso indesiderato.

SETUP DEL SISTEMA

Accertarsi che lo storico fornisca informazioni utili

Impostare correttamente data e ora, in modo che lo storico fornisca sempre informazioni corrette.

Sincronizzate data e ora del dispositivo con un server NTP (Network Time Protocol) pubblico o privato.

Ridurre la superficie di attacco

A una maggior complessità del sistema corrisponde una più ampia **superficie di attacco**, cioè il numero di punti della rete o del sistema attaccabili dall'esterno.

Installare i dispositivi su reti separate

Creare reti separate per i vari dispositivi di sicurezza (telecamere, DVR, NVR, ecc.) e per gli altri dispositivi collegati in rete (PC, telefoni VoIP, ecc.), in modo l'accesso indesiderato a una rete non influisca sull'altra.

Nel caso in cui non fosse richiesto l'accesso al sistema di sicurezza dall'esterno, è bene utilizzare una rete privata non connessa a Internet.

Connettere le telecamere a porte PoE

Connettere le telecamere alle porte PoE dei registratori e non alla rete generale: questo renderà il sistema più sicuro perché è impossibile accedere direttamente alle porte PoE dall'esterno.

Applicare il Principio del Privilegio Minimo

Ogni account dovrebbe avere accesso solo a dati e risorse necessari per lo svolgimento delle funzioni previste. In questo modo, un hacker che ottenesse l'accesso a un account avrebbe accesso solo a quei dati e a quelle risorse, contenendo così i danni potenziali dell'attacco.

In base al medesimo principio, non autorizzare gli utenti per l'accesso dell'account amministratore.

Disabilitare tutte le funzioni non necessarie all'operatività

Disabilitare una funzione mette fuori dalla portata degli hacker alcuni punti vulnerabili del sistema o della rete. Verificare l'abilitazione di funzioni e servizi necessari e la disattivazione degli altri.

La disattivazione di un servizio, inoltre, lo rende indisponibile per eventuali hacker che riuscissero ad attaccare una singola telecamera ma non l'intero sistema.

- Disattivare la funzione audio se non richiesta.
- Disattivare la funzione Multicast utilizzata per inviare un video a più dispositivi.
- Disattivare il protocollo **SNMP** che consente di controllare dispositivi da un'applicazione centrale. Non disattivarlo in caso di tracciamento o test dei dispositivi. Se è necessario usarlo, scegliere SNMP v3.
- In caso si usi il port forwarding manuale, disabilitare la funzione **UPnP** (port forwarding automatico).
- Disabilitare il protocollo IPv6 se la rete non utilizza **indirizzi IPv6**, in modo da prevenire accessi non autorizzati.

Limitare il port forwarding

Il Port Forwarding è una funzione che consente di indirizzare porte di comunicazione specifiche per dispositivi su rete IP (es. PC, DVR, telecamere). Nei sistemi di videosorveglianza, viene utilizzata per permettere agli utenti di visualizzare e controllare dispositivi TVCC da remoto.

Trasmettere al dispositivo, ma solo i numeri delle porte TCP effettivamente necessari. Non utilizzare un'area DMZ per gli indirizzi IP dei dispositivi. Nel caso in cui una serie di dispositivi (es. telecamera) sia connessa ad un'unica macchina (es. NVR, DVR), trasmettere solo il numero di porta del singolo dispositivo. Utilizzare un **firewall** per prevenire l'accesso a tutte le porte non utilizzate.

Modificare le porte di default

Le porte TCP sono utilizzate per comunicare e per visualizzare dati video da remoto.

I dati che viaggiano su rete sono consegnati correttamente grazie ad un indirizzo (che identifica il dispositivo singolo) e ad un numero di porta (che designa un servizio del dispositivo). Ad esempio, il browser Internet del vostro PC legge i dati inviati alle porte TCP numero 80 (HTTP) e 443 (HTTPS).

Eventuali malintenzionati possono più facilmente monitorare e intercettare i dati nel sistema se sono a conoscenza della/e porta/e utilizzata/e.

I vari servizi possono essere resi operativi su porte differenti (es. http://xxx.xxx.xxx.xxx:30231 è operativo sulla porta 30231 invece che sulla porta 80) in modo da rendere possibile la trasmissione di streaming video anche su altre porte senza compromettere il corretto funzionamento del sistema.

L'invio di dati a una porta con numero diverso da quello di default riduce sensibilmente il rischio che malintenzionati siano in grado di individuarla, quindi è buona misura modificare il numero di default delle porte TCP e HTTP utilizzate. Impostare numeri di porta compresi nel range 1025÷65535.

La procedura di modifica del numero delle porte può variare in base al prodotto in uso: leggere attentamente e seguire le istruzioni fornite nella documentazione tecnica del singolo prodotto. Per l'accesso ad alcuni dispositivi, sarà necessario l'utilizzo dei dati forniti sull'etichetta del prodotto.

Impostare un filtro IP

Un filtro IP garantisce l'accesso al sistema solo a dispositivi con indirizzi IP specifici.

Abilitare questo filtro, se disponibile, per assicurare l'accesso ai soli dispositivi con indirizzi IP conosciuti.

L'abilitazione del filtro IP per gli utenti autorizzati è in grado di evitare che la telecamera risponda al traffico di rete di altri utenti. Verificare che tutti gli utenti autorizzati siano elencati nella *white list*.

Acquistare e utilizzare un certificato SSL per la rete TVCC

Alcune telecamere possono essere provviste di un certificato SSL che consente l'utilizzo del protocollo di comunicazione criptato HTTPS al posto del più comune HTTP non criptato. Il supporto di un protocollo criptato consente di installare una telecamera su una rete pubblica conservando un livello di sicurezza notevole.

Tuttavia, considerando che le impostazioni iniziali sono effettuate mentre è ancora in uso il protocollo HTTP, sarà necessario modificare la password di accesso alle telecamere dopo aver attivato il protocollo HTTPS.

Mettere sotto chiave i dispositivi

Per prevenire accessi fisici non autorizzati al sistema, installare i dispositivi all'interno di strutture protettive: armadi metallici, strutture rack, stanze che possano essere chiuse in sicurezza.

Nel caso di telecamere, puntare su modelli antivandalo e installarli seguendo le istruzioni in modo da proteggere anche i cavi: in questo modo è garantito un alto livello di protezione da atti di vandalismo, manomissione e sabotaggi fisici.

MANUTENZIONE DEL SISTEMA

Aggiornamento del firmware

Effettuare periodicamente gli update del firmware: le nuove versioni spesso riparano problemi o vulnerabilità esistenti, rendendo il sistema (o la rete) maggiormente resilienti nei confronti di nuove minacce.

Controllare lo storico di sistema

Gli storici di sistema (*log*) sono un utile strumento per verificare la presenza di accessi non autorizzati poiché mostrano gli indirizzi IP e le aree che hanno visitato.

Impostazioni di default

In caso di sistema compromesso da un attacco, l'hacker potrebbe avere già modificato alcune impostazioni all'insaputa di amministratore e utenti. Sarà quindi necessario ripristinare le impostazioni di default e riconfigurare i dispositivi per garantire nuovamente la sicurezza della rete o del sistema.

Alcuni attacchi potrebbero compromettere il sistema così a fondo da richiedere, invece, la spedizione del prodotto presso EL.MO. per la riparazione, il cambio di alcuni componenti o, nel caso peggiore, il rimpiazzo dell'intero dispositivo.

LISTA DI CONTROLLO

Quando si installa un dispositivo, seguire la lista per punti mostrata a pagina seguente.

TELECAMERE

Montaggio

- Fissare la telecamera nella posizione desiderata, seguendo il manuale d'istruzioni ☐
- Assicurarsi che la telecamera montata in esterno sia resistente alle intemperie (i cavi non portano acqua nel corpo della telecamera, i fori sono sigillati, ...) ☐
- Pulire la lente e altre superfici trasparenti ☐
- Se necessario, etichettare le telecamere ☐

Inquadratura e Impostazione dell'Immagine

- Mirare l'inquadratura della telecamera e regolare zoom e fuoco ☐
- Salvare un fermo immagine in piena luce (giorno) ☐
- Far approvare il risultato del fermo immagine al cliente ☐
- Salvare un fermo immagine in modalità notte ☐
- Far approvare il risultato del fermo immagine al cliente ☐
- Salvare un fermo immagine in condizioni di luce forte (se è presente una funzione WDR) ☐
- Far approvare il risultato del fermo immagine al cliente ☐

Impostazioni di Rete / di Sicurezza

- Trascrivere l'indirizzo MAC (MAC address) ☐
- Far assegnare l'indirizzo IP dall'IT manager e trascriverlo ☐
- Aggiornare il firmware all'ultima versione disponibile ☐
- Cambiare la password di default del profilo amministratore ☐
- Impostare un server NTP e configurare data e ora ☐
- Disabilitare i servizi inutilizzati e chiudere le porte non usate (FTP, telnet, SSH, UPnP, SNMP, ...) ☐
- Creare tutti gli utenti necessari ☐
- Configurare una *white list* per limitare l'accesso alla telecamera ai soli dispositivi autorizzati ☐

Configurazione

- Configurare la risoluzione ☐
- Configurare la frequenza dei fotogrammi (*framerate*) ☐
- Controllare che risoluzione e framerate del video registrato siano conformi alle specifiche del cliente ☐
- Configurare le impostazioni di compressione (inclusi quantizzazione, smart CODEC, etc.) ☐
- Configurare il WDR - *Wide Dynamic Range* (on/off, livelli, ...) ☐
- Configurare l'esposizione, (es. disattivare "otturatore lento", impostare l'otturatore a max 1/30s o più rapido a seconda delle necessità) ☐
- Configurare la potenza dell'illuminatore IR integrato e le impostazioni smart IR se presenti ☐
- Configurare le impostazioni di video motion detection, analitici e tamper ☐
- Configurare le privacy zone ☐
- Configurare i percorsi PTZ e le posizioni PTZ predefinite se utilizzate ☐
- Verificare i percorsi PTZ e le posizioni PTZ predefinite se utilizzate ☐
- Disabilitare o configurare l'audio ☐
- Configurare le scritte in sovrimpressione (nome della telecamera e data/ora) ☐
- Configurare le notifiche degli eventi (e-mail, testo, ...) ☐
- Scaricare e archiviare copia della configurazione della telecamera ☐

VMS/REGISTRATORI

Hardware/Sicurezza

- Trascrivere l'indirizzo MAC (MAC address) di ogni scheda di rete ☐
- Far assegnare gli indirizzi IP dall'IT manager e trascriverli ☐
- Aggiornare il sistema operativo (se non specificatamente sconsigliato nel manuale) ☐
- Creare una password sicura per il profilo amministratore ☐

- Creare tutti gli utenti necessari ☐
- Testare il gruppo di continuità (se previsto) e il suo tempo di scarica ☐

Impostazioni Generali

- Aggiornare il software e il firmware alla versione più recente ☐
- Cambiare la password di default del profilo amministratore ☐
- Creare profili utente personali ☐
- Impostare un server NTP e configurare data e ora ☐
- Configurare le periferiche di archiviazione (dischi fissi, NAS, SAN) ☐
- Configurare le quote d'archiviazione (massima durata di una registrazione) ☐
- Configurare la vita massima delle registrazioni secondo le indicazioni del garante alla privacy ☐
- Configurare la programmazione della registrazione (es. 24/7, 8-17, fuori orario, vacanze, ...) ☐

Postazioni PC

- Trascrivere l'indirizzo MAC (MAC address) di ogni postazione ☐
- Far assegnare gli indirizzi IP dall'IT manager e trascriverli ☐
- Aggiornare il sistema operativo (se non specificatamente sconsigliato nel manuale) ☐
- Creare una password sicura per il profilo amministratore ☐
- Creare tutti gli utenti necessari ☐
- Installare il client VMS e aggiornarlo all'ultima versione ☐
- Configurare le visuali delle telecamere come necessario ☐
- Configurare i percorsi di inquadratura PTZ e lo switching come necessario ☐
- Configurare le viste delle mappe ☐
- Configurare gli eventi e gli allarmi come necessario ☐
- Testare il gruppo di continuità (se previsto) e il suo tempo di scarica ☐

Rete

- Trascrivere l'indirizzo MAC (MAC address) di ogni dispositivo ☐
- Far assegnare gli indirizzi IP dall'IT manager e trascriverli ☐
- Aggiornare il firmware di switch, firewall o router all'ultima versione ☐
- Cambiare la password di default del profilo amministratore ☐
- Configurare le LAN virtuali (VLAN) come necessario ☐
- Configurare la funzione "qualità del servizio" (QoS) come necessario ☐
- Disabilitare le porte inutilizzate dello switch ☐
- Configurare il monitoraggio SNMP, se necessario ☐
- Configurare il filtraggio degli indirizzi MAC se necessario ☐
- Scaricare e archiviare copia della configurazione di ogni switch ☐
- Testare il gruppo di continuità (se previsto) e il suo tempo di scarica ☐

Cablaggio

- Etichettare tutti i cavi, i sezionatori, le prese a muro, ... ☐
- Assicurarsi che i cavi siano fissati ai supporti (ganci a J, travature, ...) ☐
- Nascondere i cavi dove possibile o necessario ☐
- Lasciare un tratto di cavo inutilizzato, inguainato e ordinatamente avvolto, a entrambi i capi del cavo ☐
- Testare tutte le terminazioni e documentare i risultati dei test ☐
- Se è necessaria una certificazione, testare tutti i cavi, documentando i risultati dei test ☐

EL.MO. SpA | Via Pontarola, 70 | 35011 Campodarsego (PD) - IT
Tel: +39.049.9203333 | Fax: +39.049.9200306
e-Mail: info@elmospa.com | www.elmospa.com