7 MIGLIORI PRATICHE PER LA CYBERSECURITY

2N
An Axis company

MANTENERE IL SOFTWARE AGGIORNATO

L’utilizzo di dispositivi con versioni firmware aggiornate è qualcosa di inevitabile quando si desidera ridurre al minimo i rischi per la cibersicurezza. Quando un fabbricante scopre un potenziale bug del software, lo risolve alla successiva versione del software. **L’installazione degli aggiornamenti del software consente all‘utente di sfruttare patch di sicurezza per tutte le vulnerabilità appena scoperte.**

2N
An Axis company

UTILIZZO DI PASSWORD FORTI

Il minimo che un utente possa fare è creare una **password complessa che non facile da violare.** La password ideale dovrebbe essere composta da almeno sei caratteri. Deve contenere numeri, lettere e simboli. Ovviamente non è una buona strategia usare password facili da indovinare, ad esempio la data del compleanno o il nome della propria città. Se riuscite dunque a creare una password forte, ben per voi. Ma è necessario **evitare di condividere le proprie credenziali** con altri utenti. Anche se si rispettano queste regole, è meglio **modificare la password** di tanto in tanto.

2N
An Axis company

ACCOUNT DIVERSI PER RUOLI DIVERSI

È importante avere **account multipli con privilegi diversi.** Un determinato utente avrà il limite di apportare solo quelle modifiche che sono correlate alle attività specifiche del suo lavoro. Inoltre, anche per questi tipi di account, è necessario ricordare di non condividere la propria password con nessuno. In questo modo si riduce al minimo la possibilità di diffondere credenziali in tutta l'azienda.

2N
An Axis company

ESPOSIZIONE LIMITATA A INTERNET

Per evitare il malware, utilizzare **firewall basati su router** che rifiutano il traffico sospetto prima che arrivi sulla rete. Ovviamente non è possibile pensare di disconnettersi completamente da Internet. Ma è importante prestare attenzione e **proteggere la rete con una password forte.** Chi realizza un attacco scansiona continuamente internet per individuare le macchine esposte. Per scoprire quali dispositivi utilizzati sono aperti alla rete, è possibile andare sul sito web www.shodan.io e verificare. Maggiore è il numero di dispositivi rimossi dall'esposizione diretta a internet, minori saranno i rischi. È necessario, inoltre, ricordare sempre di **abilitare solo le funzioni necessarie del prodotto.**

2N
An Axis company

PROTEZIONE DELLA RETE

a) **Creare una rete indipendente,** dedicata esclusivamente ai dispositivi contenenti informazioni sensibili. Rendere fisicamente impossibile l‘ingresso alla rete tramite interruttori separati.

b) Usare una **LAN virtuale (VLAN).** La VLAN contiene reti isolate all‘interno di un centro dati e ciascuna delle reti costituisce un dominio di trasmissione separato.

c) È molto utile anche assicurare la rete con un **protocollo IEEE 802.1X.** Esso impedisce ai dispositivi non autorizzati di accedere alla rete locale.

d) Assicurarsi che i fabbricanti dei dispositivi o dei software utilizzati implementino **protocolli quali HTTPS, TLS, SIPS o SRTP,** abilitati in modo predefinito. Si impedisce così anche il tipo di attacco cibernetico chiamato “man-in-the-middle”.

2N
An Axis company

SCEGLIERE IL FORNITORE GIUSTO PER LA GESTIONE IN REMOTO

È molto utile **gestire tutti i siti dell‘installazione da un singolo account.** A prescindere dalla posizione dei siti dell‘installazione, l‘utente potrà accedere ad essi in remoto dalla comodità del proprio ufficio. Questo potrebbe sembrare rischioso, considerando tutti i pericoli dell‘esposizione dei dispositivi a internet, come descritto sopra. È importante cercare un fornitore di gestione in remoto, il cui servizio sia basato su un cloud sicuro. In questo caso **non sarà più necessario fare affidamento su firewall basati su router o tunneling.** Il servizio basato su cloud **imposta da sé una comunicazione criptata.**

2N
An Axis company

PROTEZIONE DELL‘ECOSISTEMA IOT

Creare una **rete separata per i dispositivi IoT,** scegliere una **password forte per il router** per proteggere la rete, **non installare mai nuovi dispositivi elettronici senza controllarne il fabbricante,** non consentire alcuna funzione non controllata per i dispositivi e **aggiornare il firmware e il software** con regolarità.

2N
An Axis company