7 OSVĚDČENÝCH POSTUPŮ PRO CYBERSECURITY

2N
An Axis company

AKTUALIZUJTE SOFTWARE

Pokud chcete zmírnit možná rizika kybernetické bezpečnosti, používejte zařízení s nejnovější verzí firmwaru. Ve chvíli, kdy výrobce zjistí potenciální chybu, opraví ji v příštím vydání softwaru. **Instalace aktualizací zajistí, že budete používat bezpečnostní záplaty pro všechny nově objevené zranitelnosti systému.**

2N
An Axis company

POUŽÍVEJTE SILNÁ HESLA

To nejmenší, co můžete jako uživatel udělat, je **vytvořit dostatečně silné heslo, které nebude snadné hacknout.** Ideální heslo by mělo obsahovat alespoň šest znaků. Mělo by kombinovat čísla, písmena a symboly. Nepoužívejte snadno uhodnutelná hesla, jako je datum narozenin nebo název vašeho rodného města. I když se vám podaří vytvořit silné heslo, ještě nemáte vyhráno. **Vyhněte se sdílení svých údajů s ostatními uživateli. Heslo také čas od času změňte.**

2N
An Axis company

RŮZNÉ ÚČTY PRO RŮZNÉ ROLE

Je důležité mít **více účtů s různými oprávněními.** Omezte práva uživatelů pouze na provádění těch změn, které se týkají jejich konkrétních pracovních úkolů. I zde platí, že byste své heslo neměli sdílet s nikým jiným. Snížíte tak možnost šíření vašich přihlašovacích údajů v rámci celé společnosti.

2N
An Axis company

OMEZTE VYSTAVENÍ INTERNETU

Chcete-li se vyhnout malwaru, **použijte router s podporou funkce firewall,** který blokuje podezřelý přenos dřív, než se dostane do sítě. Samozřejmě je nemyslitelné úplně se odpojit od internetu. O to víc je důležité být opatrný a **chránit síť silným heslem.** Hackeři neustále prohledávají internet ve snaze najít zařízení vystavena internetu. Pokud chcete vědět, jaká zařízení jsou viditelná, podívejte se na www.shodan.io. Čím více zařízení odstraníte z přímého vystavení internetu, tím větší riziko snížíte. Nezapomeňte také vždy **povolit pouze ty funkce produktů, které nezbytně potřebujete.**

2N
An Axis company

ZABEZPEČTE SÍŤ

a) **Vytvořte nezávislou síť** určenou výhradně pro zařízení, která obsahují citlivé informace. A pokud budete používat separátní switche pro různé sítě, fyzicky znemožníte útočníkovi se do sítě dostat.

b) Používejte **virtuální LAN (VLAN).** VLAN je izolovanou sítí v datovém centru a každá síť je samostatnou broadcastovou doménou.

c) Velmi užitečné je také zabezpečení sítě pomocí protokolu **IEEE 802.1X.** Tento protokol zabraňuje neoprávněným zařízením v přístupu k místní síti.

d) Ujistěte se, že výrobci zařízení nebo softwaru, které používáte, implementují **protokoly, jako jsou HTTPS, TLS, SIPS nebo SRTP,** povolené ve výchozím nastavení. Zabráníte tak „Man in the middle“ kybernetického útoku.

2N
An Axis company

VYBERTE SPRÁVNÉHO POSKYTOVATELE VZDÁLENÉ SPRÁVY

Spravovat všechna místa instalace z jednoho účtu je velmi pohodlné. Bez ohledu na to, kde se instalace nachází, k nim můžete přistupovat vzdáleně, z pohodlí vaší kanceláře. S ohledem na všechna nebezpečí vystavení zařízení internetu popsaná výše se to může zdát jako nebezpečné. Proto si vyberte poskytovatele vzdálené správy, jehož služba je založena na **zabezpečeném cloudu.** V tomto případě již nemusíte řešit router s podporou funkce firewall nebo tunelling. **Cloudová služba sama nastaví šifrovanou komunikaci.**

2N
An Axis company

ZABEZPEČTE EKOSYSTÉM IOT

Vytvořte **samostatnou síť pouze pro zařízení IoT,** zvolte **silné heslo routeru** pro ochranu sítě, nikdy **neinstalujte žádnou novou elektroniku bez ověření výrobce, nepovolujte na zařízení zbytečné funkce** a **pravidelně aktualizujte firmware a software.**

2N
An Axis company