Nouzová komunikace pro výtahy

Standardy kybernetické bezpečnosti od 2N

2N.com

Kybernetická bezpečnost

Toto téma již dávno nerezonuje pouze mezi IT specialisty, kteří mají na starosti síťovou infrastrukturu! Stačí jedno slabé místo v jakémkoliv „chytrém“ produktu a celý systém může být ohrožen. Pokud chcete, aby byla vaše budova zabezpečena, musíte věnovat pozornost všem zařízením, i těm pro nouzovou komunikaci ve výtazích!

Jakýkoliv útok na výtahový systém může představovat vážné ohrožení bezpečnosti v budově. Při fyzickém napadení hrozí, že se do budovy dostanou neoprávněné osoby či dokonce zločinci, kybernetické útoky zase mají za následek narušení klíčových aktivit a procesů ve firmě, ohrožení pověsti společnosti a pokuty v řádech milionů korun.

Jaké kroky tedy můžete podniknout, abyste neohrozili každodenní provoz budovy – a tedy ani lidi uvnitř?

2N: váš spolehlivý partner

Normy a certifikace

Certifikace ISO 27001, kterou společnost 2N získala v roce 2021, je důkazem, že nejen s citlivými daty nakládáme systematicky a bezpečně. Tato certifikace nám nastavuje procesy, jak se bránit potenciálním bezpečnostním hrozbám, a je zároveň ideální odpovědí na rostoucí potřeby zákazníků v oblasti bezpečnosti i na legislativní požadavky, jako je GDPR.

Kvalita našich produktů je pro nás i naše zákazníky klíčová, proto je navrhujeme, vyvíjíme a testujeme podle:

- Norem pro bezpečnost systémů pro průmyslovou automatizaci a řízení **IEC 62443-4-1 a 62443-4-2**
- Technických pravidel pro provozní bezpečnost **TRBS 1115**
- Vybraných principů specifikace **„Secure by Design“**
- **Bezpečnostního rámce ASDM** naší mateřské společnosti Axis
- Našich interních procesů a poznatků

Implementované bezpečnostní principy pro jednotlivé skupiny produktů

Nabízíme řešení pro analogové, digitální a IP technologie. Navíc, pro všechny tyto produkty jsme implementovali řadu principů pro zajištění bezpečnosti – jak fyzické, tak kybernetické.

1. Produkty založené na Linux OS

Produkty společnosti 2N určené pro nouzovou komunikaci ve výtazích přes IP

2N® LiftGate | 2N® EasyGate IP | 2N® LiftIP 2.0

- Zabezpečené spouštění (Secure boot) na bázi operačního systému Quectel
- Zabezpečené klíče SSL: délka je minimálně 256 bitů, stejně jako u HTTPS a dalších zabezpečených protokolů
- Náš vlastní protokol „Tribble Tunnel“ zaručuje zabezpečenou HTTPS komunikaci mezi 2N produkty pro nouzovou komunikaci a portálem 2N® Elevator Center. Celý komunikační kanál je šifrován pomocí TLS protokolu a využívá certifikáty vydané cloudem.
- Nové verze firmwaru jsou dodávány v digitálně podepsaných a zašifrovaných balíčcích, čímž je zajištěna kontrola a ochrana proti podvržení neautorizovaného firmwaru.
- Inteligentní systém správy hesel zabraňuje slovníkovým útokům. Správce je po prvním přihlášení nucen změnit výchozí heslo na silnější.
- Znemožněte hackerům získat přihlašovací údaje ze zálohy konfigurace zařízení pomocí šifrovaného ukládání hesel: jsou ukryta ve webové konfiguraci.
- Možnost nastavení uživatelských oprávnění – např. přístup pro běžného uživatele s oprávněním pouze pro čtení.
- Protokol SIPS šifruje obsah SIP zpráv, což zabraňuje zneužití dat (man-in-the-middle útok apod.) a krádeži identity.

2. Proprietární systémy

Produkty společnosti 2N určené pro tradiční analogovou i digitální nouzovou komunikaci

2N® Lift1 2N® Lift8

- Tyto produkty disponují naším vlastním proprietárním systémem (firmwarem), který nelze snadno napadnout ani zneužít.
- Bezpečné aktualizace chráněné speciálním algoritmem kontrolního součtu – nelze podvrhnout škodlivý firmware
- Proprietární konstrukce pro fyzické zabezpečení produktů

3. Aplikace

- Naše aplikace pro operační systémy Windows a Android umožňují konfiguraci systému na místě, konfiguraci na dálku, aktualizaci i sledování alarmových a kontrolních volání.
- Patří mezi ně 2N Call Center Communicator a Server, 2N Control Panel, 2N® Lift1 a 2N® Lift8 Service Tools.
- Instalační balíčky všech aplikací jsou chráněny bezpečnými algoritmy založenými na klíčích 2N a vestavěných bezpečnostních mechanismech systému Windows 10 (a vyšších).

4. 2N® Elevator Center

Hosting

Tato cloudová platforma je hostována na platformě Amazon Web Services (AWS). Abychom našim zákazníkům poskytli co nejvyšší zabezpečení, řídí se náš Systém Řízení Bezpečnosti Informací nejlepšími bezpečnostními postupy AWS.

Zabezpečení

2N® Elevator Center je moderní cloudové řešení, které nabízí řadu bezpečnostních výhod:

- Nepřetržité monitorování výkonnosti a možného narušení
- Okamžité nasazení nejnovějších bezpečnostních aktualizací jak na straně AWS, tak i na straně 2N
- Náš vlastní protokol pro udržování trvalého a zabezpečeného spojení mezi 2N® Elevator Center cloudem a produkty 2N Lift (moderní a bezpečný protokol založený na TLS)

Šifrovaná komunikace

Cloudová platforma poskytuje služby, které vyžadují několik komunikačních rozhraní mezi součástmi 2N® Elevator Center cloudu a 2N výtahovými zařízeními. Všechna uvedená rozhraní zajišťují zabezpečenou komunikaci prostřednictvím protokolu HTTPS/TLS:

- Synchronizace cloudu – všechna data v cloudu jsou bezpečně uložena na šifrovaných discích a přenášena prostřednictvím vlastního protokolu založeného na TLS.
- Vzdálená konfigurace – uživatel může bezpečně získat vzdálený přístup k webovému rozhraní každého výtahového zařízení prostřednictvím krátkodobého spojení sestaveného na vyžádání.
- Poskytování/obnovování certifikátů – certifikáty zařízení jsou vydávány s platností na 3 měsíce, s automatickým obnovením 1 měsíc před vypršením platnosti a s podporou manuálního odebrání v případě potřeby.
- Aktualizační server – 2N zařízení lze bezpečně aktualizovat na nové, digitálně podepsané verze FW z našeho aktualizačního serveru 2N.
- Bezpečnostní kódy a předběžné ověřování – připojení zařízení ke cloudu je možné pouze prostřednictvím bezpečnostního kódu/předběžného ověřování.

Díky uplatnění těchto a mnoha dalších zásad v procesu vývoje **splňují 2N produkty pro nouzovou komunikaci ve výtazích ta nejpřísnější bezpečnostní kritéria** pro ochranu osobních údajů, zabezpečení produktů a síťové infrastruktury.

Základní kroky, které můžete učinit již dnes, abyste zvýšili zabezpečení svého systému

Snažte se, aby vaše interní procesy a vámi instalovaná zařízení byly ve shodě se základními bezpečnostními normami (ISO 27001, IEC 62443-4-1, IEC 62443-4-2, TRBS 1115)

Ujistěte se, že systém pro nouzovou komunikaci pro výtahy **využívá šifrovanou komunikaci** (protokoly jako HTTPS, SIPS, TLS by měly být povoleny ve výchozím nastavení)

Vytvořte si několik účtů s různými oprávněními (zajistěte, aby uživatelé mohli provádět pouze změny související s jejich konkrétními úkoly)

Pravidelně aktualizujte software, abyste potlačili možné kybernetické hrozby.

Chcete-li se vyhnout hrozbám sociálního inženýrství, proškolte své zaměstnance. Lidská pochybení představují nejzranitelnější součást jakéhokoli systému.

2N TELEKOMUNIKACE a.s.
Praha , Česká republika | +420 261 301 500 | sales@2n.com

2N.com