# Siemens dodá ve spolupráci s Palo Alto Networks ověřené řešení kybernetické bezpečnosti založené na umělé inteligenci pro průmyslovou 5G infrastrukturu

**5.3.2026 - | Siemens**

**Spojení privátní 5G infrastruktury a nepřetržitého monitoringu kybernetické bezpečnosti od společnosti Siemens s řešením kybernetické bezpečnosti využívajícím umělou inteligenci od Palo Alto Networks.**

- Speciálně vyvinuto pro výrobní technologie (OT), testováno v různých průmyslových prostředích
- Vyšši kybernetická bezpečnost pro průmyslové sítě 5G bez snížení výkonu, součást portfolia Siemens Xcelerato**r**

Společnost Siemens oznámila, že ve spolupráci s Palo Alto Networks vytvořila ověřené řešení kybernetické bezpečnosti pro privátní průmyslové sítě 5G. Spojuje privátní 5G infrastrukturu Siemens s firewallem nové generace (NGFW) společnosti Palo Alto Networks, který je speciálně optimalizován pro umělou inteligenci. Řešení prošlo rozsáhlými testy, aby byla ověřena jeho vysoká dostupnost, odolnost sítě a nepřerušovaný provoz. Výrobcům umožní splnit nejrůznější bezpečnostní požadavky v průmyslu při zachování vysokého výkonu, který je stále důležitější pro řízení výroby, jež stále více využívá umělou inteligenci.

„Závod na výrobu léčiv má jiné bezpečnostní požadavky než montážní linka na automobily," uvedl Michael Metzler, viceprezident pro horizontální řízení kybernetické bezpečnosti, Siemens Digital Industries. „Ověřené řešení společností Siemens a Palo Alto Networks řeší tyto specifické potřeby průmyslu prostřednictvím speciálně navržené architektury. Výrobci získají bezpečné 5G připojení přizpůsobené jejich provozu, aniž by došlo ke snížení výkonu."

„Palo Alto Networks a Siemens propojují nejen výrobní provozy, ale zároveň budují centrální nervový systém pro budoucnost průmyslu – budoucnost, která je inteligentní, autonomní a bezpečná již od samého počátku," řekl Dharminder Debisarun, výkonný ředitel pro kybernetickou bezpečnost, Palo Alto Networks.

### Ověřené řešení zajistí bezpečnost v průmyslových provozech

Výrobní systémy založené na datech vyžadují bezdrátové připojení nezbytné pro nejrůznější senzory a mobilní zařízení. Právě proto představují privátní sítě 5G zcela nepostradatelnou infrastrukturu. Případné kybernetické útoky mohou zároveň způsobit nákladné výpadky nebo ohrozit bezpečnost pracovníků. Předpisy, jako je například NIS2, navíc vyžadují zavedení bezpečnostní architektury s hloubkovou obranou, která bude splňovat normy IEC 62443. Standardizovaná řešení v oblasti IT bezpečnosti často vytvářejí problémy s výkonem nebo nedokážou řešit hrozby spojené s provozními technologiemi v průmyslových prostředích.

Spolupráce Siemensu a Palo Alto Networks nabízí řešení těchto problémů. Společnost Palo Alto Networks speciálně optimalizovala svou technologii NGFW pro privátní infrastrukturu 5G firmy

Siemens na základě rozsáhlého testování v různých prostředích. Tento ověřovací proces potvrdil, že řešení zajistí bezpečnost na průmyslové úrovni, aniž by ohrozilo nízkou latenci a vysoký výkon vyžadovaný u výrobních systémů v reálném čase – což je zásadní rozdíl oproti běžným přístupům k IT bezpečnosti.

**Tři bezpečnostní prvky**

Řešení spojuje tři prvky pro vylepšenou kybernetickou bezpečnost. Siemens speciálně testoval a ověřil řešení pro průmyslová prostředí ve své laboratoři Digital Connectivity Lab v německém Erlangenu:

- Privátní infrastruktura 5G společnosti Siemens nabízí lokální vyhrazenou bezdrátovou konektivitu pro mobilní a pohyblivá zařízení s integrovanými bezpečnostními funkcemi, která chrání základní síťovou infrastrukturu. Řešení zajišťuje datovou suverenitu a komunikaci s nízkou latencí nezávislou na mobilních operátorech.
- SINEC Security Monitor: Software společnosti Siemens pro pasivní, neinvazivní a nepřetržitý lokální monitoring bezpečnosti během výroby. Identifikuje komunikační anomálie, neautorizovaná zařízení nebo potenciální hrozby bez dopadu na výrobní provoz.
- Palo Alto Networks Firewall poskytuje zabezpečení vrstvy 7 a specializovanou analýzu protokolů provozních technologií (OT), která je specificky optimalizována pro průmyslová prostředí. Na rozdíl od obecných řešení IT bezpečnosti zajistí hloubkovou kontrolu paketů pro protokoly OT při zachování nízké latence požadované pro aplikace řízení v reálném čase – nyní také v bezdrátové komunikaci prostřednictvím privátních sítí 5G. Zahrnuje ochranu před malwarem, pokusy o vniknutí a exfiltraci dat bez snížení výkonu, k němuž dochází při použití běžných bezpečnostních nástrojů.

Tato ověřená architektura splňuje požadavky normy IEC 62443 na bezpečnost průmyslových automatizačních a řídicích systémů a zároveň zachovává výkonnostní charakteristiky nezbytné pro časově kritické výrobní aplikace. Řešení je nyní součástí portfolia Siemens Xcelerator.

https://www.siemenspress.cz/siemens-doda-ve-spolupraci-s-palo-alto-networks-overene-reseni-kybernetic-bezpecnosti-zalozene-na-umele-inteligenci-pro-prumyslovou-5g-infrastrukturu