

Siemens a RICAIP Testbed Praha představují novou službu pro testování kyberbezpečnosti ve výrobě

Datum 5.10.2026
Subjekt Siemens
Region Tschechische Republik
Kategorie IT und Kommunikation, IT-Industrie, Sicherheit

Otestovat si odolnost výrobních linek proti kybernetickým hrozbám nanečisto a v bezpečném prostředí. To firmám umožní nová služba, kterou spouští RICAIP Testbed Praha při CIIRC ČVUT ve spolupráci se společností Siemens. Podniky si tak mohou v praxi ověřit, jak jejich infrastruktura zareaguje na útok zvenčí, pokus o neoprávněný vzdálený přístup nebo připojení infikovaného zařízení. Průmyslové podniky ji budou moci využívat od podzimu 2026. Služba se aktuálně představuje na Mezinárodním strojírenském veletrhu v Brně.

„Čím více systémů spolu ve výrobě komunikuje, tím větší význam získává jejich zabezpečení. Kybernetický útok dnes nemusí mít jen klasický scénář s požadavkem na výkupné za zašifrovaná data. Může dojít například k zahlcení sítě a zastavení jejího provozu, což vede k okamžitému výpadku výroby. Bezpečnost proto nelze řešit až ve chvíli, kdy je výrobní systém hotový. Musí se stát součástí jeho návrhu,“ vysvětluje Miroslav Kuric, manažer týmu obchodních specialistů společnosti Siemens.

Bezpečný prostor pro rizikové scénáře

Jádrem nového testovacího prostředí je SINEC Security Monitor od společnosti Siemens. Tento nástroj nepřetržitě a zcela pasivně analyzuje síťový provoz, takže nenarušuje komunikaci strojů. Automaticky identifikuje zařízení a vyhledává odchylky signalizující bezpečnostní incident. V Testbedu si tak firmy mohou vytvořit běžný provoz, nasimulovat rizikovou situaci a sledovat, zda ji bezpečnostní architektura dokáže včas detekovat a zastavit.

Služba je určena širokému spektru podniků – od těch, které s návrhem zabezpečení teprve začínají, až po firmy, jež potřebují otestovat odolnost již hotového řešení před jeho nasazením do reálného provozu.

Výroba není IT oddělení

Potřeba podobného testování vychází ze specifické povahy výrobního prostředí (OT – Operational Technology). Zatímco zabezpečení firemních IT systémů je dnes pro většinu firem samozřejmostí, v průmyslových provozech je situace podstatně složitější. Průmyslové technologie mají dlouhou životnost, vznikaly v různých obdobích a jejich propojování přináší nová rizika. Případné narušení navíc nemá jen digitální, ale především fyzický dopad na stroje a kvalitu produkce.

„Kybernetická bezpečnost už není jen otázkou IT. Naší velkou výhodou je, že v Testbedu máme zařízení, která se běžně používají v průmyslu – řídicí systémy, roboty nebo senzory propojené do funkčních celků. Lze na nich simulovat situace, ke kterým může ve skutečnosti dojít,“ uvádí Pavel Burget, ředitel RICAIP Testbedu Praha při CIIRC ČVUT.

Know-how z reálných továren

Spolupráce se společností Siemens přináší do projektu know-how ověřené v praxi. Siemens aplikuje bezpečnostní řešení ve vlastních výrobních závodech, takže testovací scénáře vycházejí z reálných průmyslových potřeb, nikoliv z teoretických úvah.

Zavedení kybernetické bezpečnosti do výroby navíc nemusí být finančně nedostupné ani pro menší firmy. Díky podpůrným programům zajišťovaným ve spolupráci s EDIH CTU, AI-MATTERS/TEF nebo nově Czech AI Factory mohou malé a střední podniky získat na tyto služby finanční podporu.

<https://www.siemenspress.cz/siemens-a-ricaip-testbed-praha-predstavuji-novou-sluzbu-pro-testovani-kyberbezpecnosti-ve-vyrobe>