

Biometrie pod palbou hackerů: Útoky na industriální sítě lámou rekordy

23.5.2025 - | PROTEXT

Hrozby podle odvětví

Biometrický sektor byl terčem útoků více než kterákoli jiná vertikální odvětví (škodlivé objekty byly zablokovány na 28,1 % počítačů ICS), následovala automatizace budov (25 %), energetická zařízení (22,8 %), stavební zařízení (22,4 %), inženýrská zařízení (21,7 %), ropná a plynárenská zařízení (17,8 %) a výroba (17,6 %).

Hlavní zdroje hrozeb

Kybernetické hrozby v oblasti operačních technologií (OT) zůstávaly na začátku roku 2025 různorodé, přičemž hlavním zdrojem kybernetických rizik pro počítače OT byly stále hrozby šířící se přes internet (tyto hrozby byly blokovány na 10,11 % počítačů ICS), následované e-mailovými klienty (2,81 %) a vyměnitelnými médii (0,52 %).

Kategorie škodlivých objektů

Nejrozšířenějšími kategoriemi blokováných škodlivých objektů byly škodlivé skripty, phishingové stránky a také zdroje ze seznamu zakázaných nebezpečných webových stránek.

„V prvním čtvrtletí roku 2025 se podíl počítačů ICS napadených malwarem šířeným přes internet poprvé od začátku roku 2023 zvýšil. Internet tak zůstává primárním zdrojem hrozeb pro počítače ICS. Hlavní kategorie hrozeb z internetu jsou známé nebezpečné internetové zdroje, škodlivé skripty a phishingové stránky. Škodlivé skripty a phishingové stránky jsou hlavní kategorií malwaru používaného k počáteční infekci počítačů ICS – fungují jako přenašeči další fáze malwaru, jako je spyware, kryptominery a ransomware. Nárůst internetových útoků na ICS zdůrazňuje kritickou potřebu pokročilé detekce hrozeb pro boj se sofistikovanými malwarovými kampaněmi,“ komentoval Jevgenij Gončarov, vedoucí oddělení Kaspersky ICS CERT.

Aby byly počítače OT chráněny před různými hrozbami, odborníci společnosti Kaspersky doporučují:

[1] Servery pro dohledové řízení a sběr dat (SCADA), (historizační) servery pro ukládání dat, datové brány (OPC), stacionární pracovní stanice inženýrů a operátorů, mobilní pracovní stanice inženýrů a operátorů, rozhraní člověk-stroj (HMI), počítače pro správu sítí operačních technologií (OT), počítače pro vývoj softwaru průmyslových řídicích systémů (ICS).

Kompletní zpráva o hrozbách pro ICS za 1. čtvrtletí 2025 je k dispozici zde.

<https://www.ceskenoviny.cz/tiskove/zpravy/biometrie-pod-palbou-hackeru-utoky-na-industrialni-site-lamou-rekordy/2677268>