Kybernetické útoky na rôzne priemyselné odvetvia sa podľa Global Risk Report 2018 radia do prvej päťky svetových hrozieb! Jeden zo známych kybernetických útokov bol práve malvér Stuxnet. Tomu sa na začiatku 21. storočia podarilo dostať do iránskych priemyselných riadiacich systémov na obohacovanie uránu a narušiť tak kompletnú infraštruktúru. Ako je možné, že také dôležité odvetvie nie je na zabezpečenie svojej kritickej infraštruktúry pripravené?

VYPADLA VÁM RIADIACA JEDNOTKA? NEMUSÍ TO BYŤ SYSTÉMOVÁ CHYBA!

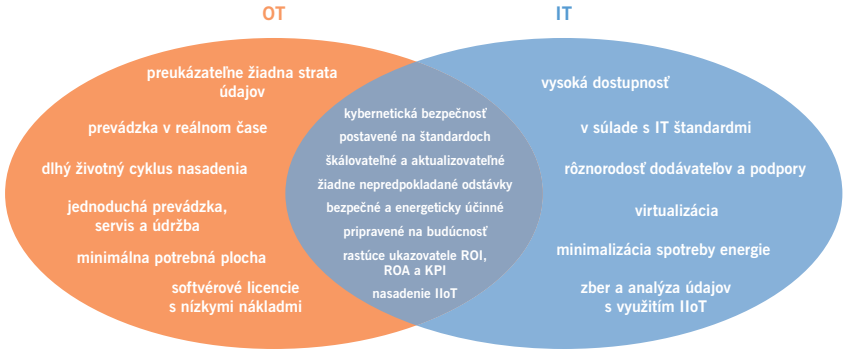
Internet vecí v priemysle? Hrozba kybernetických útokov?

Priemyselný internet vecí (IoT) či Priemysel 4.0. Tieto témy často rezonujú v najnovších trendoch. Ich cieľom je zredukovať náklady, zvýšiť efektivitu a produktivitu či rýchlejšie vyhovieť zákazníckym potrebám. Hoci prinášajú mnoho výhod, myslia spoločnosti aj na zabezpečenie týchto systémov?

„Prednedávnom som absolvoval školenie o zabezpečení kritickej infraštruktúry v priemyselných podnikoch. Zarážajúce pre mňa bolo, keď som sa dozvedel, že až 80 % priemyselných podnikov nemá prehľad o komunikácii zariadení v ich OT (Operation Technology) sieti, čo výrazne uľahčuje šírenie malvéru a znásobuje ničivé následky jeho pôsobenia. Prvým krokom k lepšej kybernetickej bezpečnosti je lepšia viditeľnosť infraštruktúry OT," vysvetľuje Pavol Gramblička, Presales Consultant distribútora IT produktov s pridanou hodnotou Veracomp Slovakia.

Ako obmedziť riziká kybernetických útokov v priemyselnom odvetví?

Alfou a omegou je spojenie IT oddelenia s OT oddelením. Ďalším z nevyhnutných krokov je investovanie do nových technológií. Tie dopomôžu k zvýšeniu viditeľnosti v sieti a odolnosti systémových počítačov proti kybernetickým útokom.



Zdroj: Craig Resnick, ARC Advisoru Group, publikované so súhlasom

Obr. 2 Zosúladenie OT/IT priorít s cieľom zlepšenia kybernetickej bezpečnosti

Prečo spojiť IT a OT?

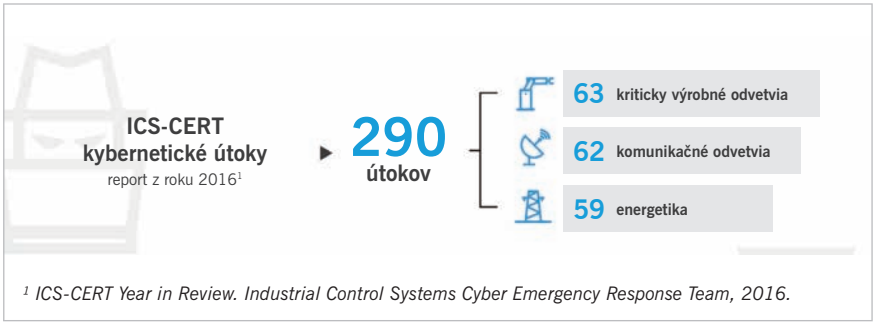
Systémy, ktoré využívajú, sú si blízke a čoraz viac spájajú. Keď spoja sily, existuje možnosť zníženia kybernetického rizika či nákladov na jeho odstránenie.

Prečo investovať do novej technológie v OT?

Pretože zvyšuje spoľahlivosť, kybernetickú bezpečnosť aj produktivitu zamestnancov a tímovú prácu – a je to oveľa jednoduchšie, ako by ste mohli očakávať, čo prináša takmer okamžitú návratnosť investícií.

Riešenia na zabezpečenie priemyselných systémov a systémov SCADA

Švajčiarsky výrobca NOZOMI NETWORKS je jedným z lídrov v oblasti kybernetickej bezpečnosti priemyselných systémov a systémov SCADA. Poskytuje inovatívnu technológiu na monitorovanie a hodnotenie priemyselných riadiacich systémov, a to na fyzickom zariadení alebo vo virtuálnom prostredí. To sa pasívne pripojí do priemyselnej siete bez narušenia prevádzky. Sleduje celú prevádzku v rámci riadiacich a procesných sietí, analyzuje ju na všetkých úrovniach vrstiev v súlade s modelom OSI. Využíva techniky umelej inteligencie a strojového učenia na vytvorenie podrobných profilov správania pre každé zariadenie podľa stavu, aby sa rýchlo zistili kritické hodnoty.



[1] *ICS-CERT Year in Review. Industrial Control Systems Cyber Emergency Response Team, 2016.*

Obr. 1

-tog-