PRIEMYSELNÉ PODNIKY NIE SÚ NA KYBERNETICKÉ ÚTOKY PRIPRAVENÉ. ANI TECHNICKY, ANI ORGANIZAČNE

Digitalizácia stavia priemyselné podniky pred nové výzvy. Popri zvýšení produktivity, zlepšení kvality, zjednodušení procesov a prínosov pre zákazníkov otvára aj veľký problém: zvýšenie bezpečnostného rizika pre podnikové systémy a generované dáta. Úroveň kybernetickej bezpečnosti sa v digitálnom podniku stáva jednou z kľúčových otázok budúcich úspechov a konkurencieschopnosti firiem. Napriek tomu je bezpečnosť výrobných systémov v podnikoch stále na okraji záujmu, firmy jej nevenujú dostatočnú pozornosť. Hnacím motorom bezpečnostných opatrení sú samotné incidenty.

Diskusia Združenia inteligentného priemyslu – Industry4UM otvorila niekoľko aktuálnych problémov priemyselných podnikov, ktoré majú spoločného menovateľa – nedostatočnú pripravenosť na kybernetické útoky. Podniky sú pre kybernetických útočníkov ľahkými cieľmi, pretože väčšina z nich nemá zavedenú stratégiu kybernetickej bezpečnosti. Ohrozené nezvládnutím atakov sú primárne malé a stredné podniky, pretože nedokážu mať tak profesionálne pokryté bezpečnostné služby a kybernetickú bezpečnosť jednoducho podceňujú. Pritom môžu byť hrozbou aj pre svojich odberateľov, pretože vzájomné komunikačné väzby sa môžu ľahko stať kanálom, cez ktorý sa kybernetický útok vykoná.

Digitalizácia transformuje priemyselné podniky a stáva sa rozhodujúcim nástrojom ich budúcej konkurencieschopnosti. Súčasne však otvára prístupy pre kybernetické incidenty. Ich zvládnutie či nezvládnutie sa tak môže stať otázkou budúceho prežitia. „Čoraz viac platí, že ochrana súkromných dát, bezpečné a spoľahlivé výrobky a chránená výroba môžu byť v globálnej konkurencii v konečnom dôsledku faktorom, ktorý rozhodne o budúcnosti podnikov. Preto musí byť kybernetická bezpečnosť pevne zakotvená v produktovej a výrobnej stratégii každého výrobcu," konštatuje Martin Morháč, prezident Združenia inteligentného priemyslu – Industry4UM.

Výrobné prevádzky sú čoraz častejšie ohrozované atakmi preťažujúcimi výrobné systémy, destabilizované infiltráciou škodlivého softvéru či ohrozované cez internetové servisné prístupy. Nie sú dostatočne pripravené ani na útoky a nebezpečenstvá hroziace zo strany zamestnancov podniku. Možné škody pre firmu siahajú od rozsiahlych hospodárskych strát spôsobených výpadkom služieb, výroby a predaja či poškodenia imidžu až po nespokojnosť a stratu zákazníkov. Postoj, ktorý najčastejšie majú, je prekvapivý, konštatovanie, že im sa to nemôže stať, že nie sú dostatočne zaujímaví a veľkí, nie je na mieste. „Dnes sa žiadna firma nesmie pokladať za príliš malú a z globálneho pohľadu za príliš nevýznamnú na to, aby sa nemohla stať zaujímavou pre kyberkriminálne prostredie," upozorňuje Peter Prónay, spolupracovník Industry4UM.

Pozor na OT

Výrobcovia sa vo fáze digitalizácie systémov a zariadení dostávajú do ohrozenia z dôvodu konektivity IT a OT (operational technologies) systémov. Neuvedomujú si, že z vlastností IT pre bežné firemné procesy a OT systémov vo výrobách sa vyvodzuje rozdielna potreba bezpečnosti. Uniká im fakt, že koncepty Industry 4.0 prepájajú tieto svety. Vzniká technické prepojenie podnikovej siete s výrobnou sieťou. A tak sa na internet pripájajú priemyselné riadiace systémy, ktoré sú inherentne nezabezpečené. V dôsledku toho sa výrobné systémy stávajú ohroziteľnými a ľahkým terčom kybernetických útokov.

Kým aplikácia bezpečnostných opatrení v IT oblasti je už roky bežnou praxou, opatrenia v oblasti OT nie sú zďaleka samozrejmé. „Keďže výrobné zariadenia dosiaľ neboli digitalizované alebo pripojené na internet, nebol dôvod na osobitné bezpečnostné opatrenia. Tento fakt spôsobuje, že ani potrebné povedomie nie je u zodpovedných osôb príliš vyvinuté a tak chýbajú stratégie kybernetickej bezpečnosti pre výrobnú časť podniku," hodnotí situáciu M. Morháč. Bežnou praxou je, že firmy majú ešte stále jednoúrovňovú, ľahko ohroziteľnú sieťovú architektúru, v ktorej sa škodlivý softvér ľahko šíri, alebo sú priamo pripojené na internet.

Zlý úmysel si cestu nájde

Ak sa menšie podniky považujú za nezaujímavé na kybernetické útoky, nemôžu sa viac mýliť. Každý podnik je z tohto hľadiska zaujímavý. Z rôznych dôvodov a motivácií. Najrozšírenejšími atakmi na komunikačnú infraštruktúru podniku sú útoky preťažujúce siete (DoS, DDoS), ktoré zariadenia paralyzujú zahltením. Na neželaný vstup do podnikov stačia aj na internet pripojené set-top-boxy alebo dohľadové kamery. Časté sú ohrozenia vyplývajúce z diaľkovej údržby, špecifické hrozby prinášajú umiestnenia systémov a komponentov v cloudoch. Aby neboli naplnené, musí byť výrobná sieť striktne oddelená tak, aby sa cez autentifikáciu výrobkov nedalo na ňu zvonku dostať. Pri využívaní externých služieb počas výroby sa musí dbať na to, aby zaručená dostupnosť tejto služby bola zosúladená s požiadavkami výroby. V každom prípade sa dôsledné oddelenie od internetu pokladá za nevyhnutné minimum opatrení. Dôležité je, aby preventívne opatrenia boli v súlade vo všetkých oddeleniach.

Za najslabší článok v bezpečnostnom reťazci označujú experti človeka. Pri svojej každodennej práci s podnikovými IT systémami alebo výrobnými zariadeniami sa stáva častou príčinou bezpečnostných incidentov. Nepozorné otvorenie prílohy mailu, ktorá obsahuje škodlivý vírus, mobil pripojený na USB port, hrubá neznalosť technických rizík pri práci, to všetko môže byť spúšťačom kybernetického útoku. Dôsledky aj drobných chýb môžu mať na podnik osudový dosah. „Preto zohráva náležité povedomie, vzdelávanie a školenie personálu zamerané na ochranu dát v podnikoch kľúčovú rolu. Pre jednotlivé pracovné oblasti treba nastaviť a uskutočniť špecifické školenia a periodicky preverovať ich účinnosť," odporúča Peter Prónay.

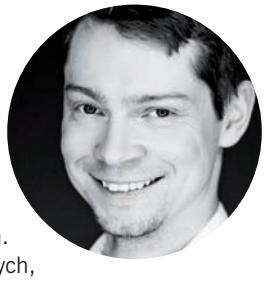
Technológia nestačí

Kyberkriminalite sa dá čeliť len strategickým prístupom a efektívnymi ochrannými opatreniami. Preto jednou z dôležitých ciest, ako tomu zabrániť, je posilnenie manažmentu rizík. Budovanie bezpečnostnej stratégie musí byť koordinované a vedené naprieč jednotlivými oddeleniami, pretože rôzni pracovníci majú rôznu východiskovú kvalifikáciu, vzdelanie a znalosti. Riziká číhajúce na výrobcov nie sú len technické, v strojoch, ovládacích prvkoch alebo softvéri, ale aj organizačné, postavené na zamestnancoch, postupoch a procesoch. Samotná technológia nie je riešením, mala by byť súčasťou komplexnej stratégie bezpečnosti podniku. Pre podniky má zmysel robiť si bezpečnostné audity, penetračné testy. Vynúti si to síce prácu navyše, ale každá skúsenosť prinesie ďalšie impulzy na zlepšenie.

Problémom signalizujúcim komplikácie aj v budúcnosti je nedostatok IT odborníkov a absolútny nedostatok špecialistov na kybernetickú bezpečnosť. V Európskej únii dnes v tejto oblasti chýba viac ako 20-tisíc špecialistov. Vo vyspelých krajinách je podpora kybernetickej bezpečnosti súčasťou celoštátnych programov. Štát by podľa odborníkov mal podporovať bezpečnosť najmä malých a stredných podnikov. Slovenský priemysel je postavený na subdodávateľských sieťach a jeho úspech závisí aj od nich. „Digitalizácia napreduje a miera zabezpečenia výroby by tomu mala byť priamo úmerná. Pomôže aj vzdelávanie k danej téme. Mala by byť súčasťou všetkých učebných osnov. Musíme preložiť edukáciu praxou a infiltrovať ju do podnikov, lebo tam žijeme realitu doby," zhrnul Igor Šuba.

Ako vnímate aktuálnu situáciu v oblasti kybernetickej bezpečnosti priemyselných podnikov?

Tomáš Zaťko,
Citadelo,
Asociácia kybernetickej bezpečnosti



„Podniky začína ich bezpečnosť zaujímať, až keď dôjde k výpadku. Často si hovoria:, Prečo by sme my mali byť zaujímavým cieľom?' Doba sa mení, zločin sa profesionalizuje a bezpečnostné incidenty sa množia, čo má, samozrejme, obrovský ekonomický dosah. Dnes sú firmy z rôznych príčin v rôznych, zväčša nedostatočných úrovniach pripravenosti. Treba si povedať, že to nie je hanba, že sú v tomto stave, má to svoje dôvody. Treba si to priznať, vytvoriť plán nápravných opatrení a implementovať vhodné riešenia. Top manažmenty si musia uvedomiť, že napriek priorizácii biznisových cieľov, ak bude firma disfunkčná, biznis ciele nenaplnia. Stáva sa, že priorita bezpečnostných opatrení sa zvýši, až keď pocítia, že sa bezpečnosť nerobí dostatočne."

Peter Prónay,
Industry4UM

„Kým ľudia v klasickom IT svete, v administratívnej budove, už počuli veľa o vírusoch a vo svojom PC či notebooku majú spravidla antivírusový program zabezpečený heslami, pre výrobných pracovníkov je kybernetická bezpečnosť tabula rasa. Je to to posledné, čo by ich trápilo. Často sa bezpečnosť vo výrobe rieši systémom security trough obscurity. Podniky tvrdia, že stačí, aby bola odpojená sieť a tým činom o nich nikto nevie. Táto éra sa končí. Úplne oddelená sieť od výroby sa stáva minulosťou, pretože to už čoskoro z podstaty charakteru výroby reálne nebude možné."

David Dvořák,
Soitron

„Už desať rokov sa vo firmách stretávame s dogmami a predsudkami. Najčastejším je: Prečo by sa to malo týkať práve nás? Pre viac ako 80 % podnikov bezpečnosť výrobných systémov dokonca nie je ani témou. Je to alarmujúce, pretože takýchto útokov bude čoraz viac. To, čo vidíme, a to, čo je v štatistikách, je len známe číslo, ale je tu drvivá väčšina incidentov, o ktorých nevieme, že sa stali. Priemerný čas od ataku dovtedy, kým sa to zistí, je 211 dní! Dnes je teda množstvo podnikov, ktoré o incidente nevedia. Firmy nevedia, čo sa im odohráva v infraštruktúre. Problémom priemyslu je monitoring, vizibilita. Podniky incidenty schovávajú, niektoré však zverejnia svoju skúsenosť aj kvôli tomu, aby si ostatné firmy zobrali príklad."

Igor Šuba,
Matador Group

„Pre nás v automotive sú kybernetické útoky tvrdou realitou, sme dlhé roky pod ich tlakom. Dôvodom je fakt, že automotive je ťahúňom ekonomiky, je v ňom potenciál, komerčná sila. Výroba je dlhodobo oddelená od ERP systémov. Keďže automotive funguje v subdodávateľských schémach, musíme mať zabezpečené nielen vlastné procesy, ale musíme zaistiť bezpečnosť aj za svojich dodávateľov. Zákazníka nezaujíma, že my máme v dodávateľskom reťazci firmy, ktoré bezpečnosť vôbec neriešia. Ako bezpečnosť uchopiť? Pre všetky firmy by malo platiť, že riešením je kompromis medzi dosiahnuteľnými zdrojmi, ktoré vieme obhájiť, a tým, koľko možných útokov budú schopné eliminovať."

Martin Morháč,
Industry4UM

„Podniky sa boria s veľkým deficitom kvalifikovaných IT špecialistov, o odborníkoch na IT bezpečnosť ani nehovoriac. Je chybou, že táto problematika nie je zahrnutá v učebných predmetoch a školský systém nepripravuje špecialistov pre oblasť kybernetickej bezpečnosti. Zodpovednosť za edukáciu a prípravu zamestnancov ostáva zatiaľ na firmách samotných. Som rád, že sa začína skloňovať otázka formovania expertnej skupiny zloženej z výrobných firiem, dodávateľov technológií a IT bezpečnostných expertov, ktorá sa bude snažiť o vypracovanie zrozumiteľných odporúčaní pre stredné a malé výrobné firmy v oblasti IT a OT bezpečnosti a ktorá bude analyzovať požiadavky relevantných noriem a legislatívy pre oblasť bezpečnosti dát. Súčasne by formulovala relevantný odborný profil absolventov stredných odborných škôl na pozície špecialistov na IT bezpečnosť a diskutovala o nich so školami."

www.industry4um.sk