a nedávný Triton, který je zacílený na konkrétní bezpečnostní systém SIS (*Safety Instrumented System*) – a seznam se neustále rozrůstá. Útoky Stuxnetu a BlackEnergy ukázaly, že stačí jeden napadený USB disk nebo jeden cílený phishingový e-mail a dobře připravení útočníci mohou překonat *air gap* a proniknout do izolované sítě.

Vedle malwaru a cílených útoků čelí průmyslové organizace dalším hrozbám a rizikům, které cílí na osoby, procesy a technologická zařízení – a podceňování těchto rizik může mít závažné následky.

Problém lidského faktoru v kyberbezpečnosti je součástí širšího, komplikovanějšího kontextu. Narůstající složitost průmyslových infrastruktur vyžaduje pokročilejší ochranu a dovednosti. Naproti tomu společnosti trápí nedostatek odborníků, kteří by zvládali nové hrozby, a potýkají se s nízkým povědomím mezi zaměstnanci.

„Každý zaměstnanec – od obchodního oddělení po výrobu – hraje v kyberbezpečnosti svou roli, a proto jsou školení a zvyšování povědomí nesmírně důležité. Zpráva společnosti Kaspersky *Stav kybernetické bezpečnosti v průmyslu 2019* a související výzkum ukázaly, že lidský faktor často ohrožuje průmyslové procesy: chyby zaměstnanců nebo neúmyslné činy stály za 52 % incidentů s negativním dopadem na provozní zařízení a sítě průmyslového řídicího systému (OT, ICS) v minulém roce," uvádí Miroslav Kořen, generální ředitel firmy Kaspersky pro východní Evropu. Dodává: „I když jsme zaznamenali trend, že se společnosti snaží zlepšit ochranu průmyslových sítí, jsem pevně přesvědčen, že jí lze dosáhnout jen tehdy, když budou řešit rizika spojená s nedostatkem kvalifikovaného personálu a s chybami zaměstnanců. Použití komplexního několikavrstvového přístupu, který kombinuje technickou ochranu s pravidelným školením specialistů na IT bezpečnost a správců průmyslových sítí, zaručí ochranu sítě před hrozbami a aktuálnost dovedností."

Podle průzkumu společnosti Kaspersky se kyberbezpečnost OT a ICS stává hlavní prioritou průmyslových společností, což potvrdila většina (87 %) respondentů. Aby ale dosáhli potřebné úrovně ochrany, musí investovat do speciálních opatření a mít ve svých řadách vysoce kvalifikované odborníky, kteří zajistí jejich efektivní fungování. Ačkoliv to uvedly jako prioritu, jen něco více než polovina (57 %) společností vyhradila na průmyslovou kyberbezpečnost prostředky z rozpočtu.

Vedle rozpočtových omezení zde zůstává i problém s odborností personálu. Společnosti nejen že čelí nedostatku odborníků na kyberbezpečnost s příslušnými dovednostmi potřebnými k řízení ochrany průmyslových sítí, ale mají i obavy, že správci jejich sítí OT a ICS si nejsou dostatečně vědomi chování, které může způsobit narušení kyberbezpečnosti. Tyto problémy představují dvě z hlavních obav, které se vztahují k řízení kyberbezpečnosti, a do značné míry vysvětlují, proč chyby zaměstnanců způsobují polovinu incidentů týkajících se systémů ICS – jako jsou např. napadení malwarem nebo cílené útoky.

Ke snížení kybernetických rizik hrozících průmyslovým systémům doporučují bezpečnostní odborníci z Kaspersky tato opatření:

- vyhodnoťte bezpečnost s cílem identifikovat a odstranit bezpečnostní mezery,
- vyžádejte si externí informace: informace od renomovaných dodavatelů pomáhají organizacím předvídat budoucí útoky na průmyslovou infrastrukturu společnosti,
- pravidelně školte svůj personál,
- poskytněte ochranu uvnitř a vně vnější hranice – náležitá bezpečnostní strategie musí věnovat značné zdroje na odhalení útoku a reakci na něj, tj. na zablokování útoku předtím, než se dostane ke kriticky důležitým objektům,
- zvažte pokročilé metody ochrany: scénář výchozího odmítnutí (*Default Deny*) pro systémy SCADA, pravidelné prověrky integrity u kontrolorů a specializovaný monitoring sítě – díky tomu zvýšíte celkovou bezpečnost společnosti a snížíte šance na úspěšné narušení, a to i přesto, že nebude možné opravit či odstranit některá zranitelná místa.

(Kaspersky)

Evropská komise uvedla do provozu systém varovné výstrahy

Členové Evropské komise a zaměstnanci jejího ředitelství budou brzy dostávat do svých mobilních telefonů lokalizované výstražné zprávy. A to díky aplikaci, která upozorní na možné nebezpečí v podobě požáru v budově, podezřelého zavazadla či hrozícího útoku. Nový výstražný systém EUWARN byl spuštěn 11. září 2019 v Bruselu za přítomnosti komisaře Günthera Oettingera, prezidenta Fraunhoferova institutu prof. Dr. Reimunda Neugebauera a výkonného ředitele společnosti Turm solutions GmbH Ortwina Neuschwandera. Systém EUWARN vyvinul Ústav pro otevřené komunikační systémy Fraunhoferova institutu na základě podnětu společnosti Turm solutions. Je založen na systému KATWARN, což je systém výstrahy veřejnosti, který již několik let úspěšně funguje v Německu a Rakousku.

„Bezpečnost našich zaměstnanců a návštěvníků je mou nejvyšší prioritou. Teroristické útoky v Bruselu byly výjimečnou událostí, avšak jeden incident nám již ukázal, jak zranitelní jsme. Aplikace EUWARN je novým interním výstražným systémem, který nám dovoluje spojit se s našimi pracovníky v Bruselu a Lucemburku. Další místa budou následovat. Systém je navržen tak, aby umožnil ostatním institucím EU jej v budoucnosti rovněž využívat," uvedl Oettinger. Ředitelství Evropské komise pro bezpečnost vydává varovná hlášení v němčině, angličtině a francouzštině. Na rozdíl od varovných oznámení pro veřejnost se tyto zprávy týkají výhradně prostor budov Evropské komise a budou prozatím zasílány pouze jejím zaměstnancům. Soustava bude později napojena na systém výstrahy veřejnosti KATWARN, který je vybaven bezplatnou aplikací, která je (podle situace v konkrétní zemi) již dostupná nebo je ve fázi testů před zpřístupněním. „Všichni návštěvníci prostor sídla Evropské komise pak budou dostávat upozornění a oznámení prostřednictvím systému KATWARN," doplnil Neuschwander.

Systém KATWARN

Systém KATWARN je využíván německými autoritami v oblasti bezpečnosti. Vydává výstrahy v podobně zpráv SMS již od roku 2011 a od roku 2012 je k dispozici také jako aplikace do chytrých telefonů. To, co činí systém KATWARN unikátním, je přesnost jeho lokalizační funkce. Systém zasílá výstrahu pouze do míst či budov, ve kterých příslušné nebezpečí hrozí. V roce 2017 byl v Rakousku spuštěn systém KATWARN/Austria, který je se soustavou v Německu propojen. Fraunhoferův institut bude v zastoupení společnosti Turm solutions systém KATWARN nadále aktualizovat, např. rozšířením výstrah prostřednictvím veřejných reklamních ploch, digitální signalizace v prostředcích veřejné dopravy i palubních počítačů osobních automobilů a také v rámci adaptace systému na standard bezdrátové komunikace 5G. Společnost Turm solutions dodává systém KATWARN na evropský i mimoevropský trh.

(jh)