Agilita versus stabilita: bezpečné řízení provozní techniky v budoucnosti

Po deseti letech, kdy se společnosti po celém světě snaží vylepšit své fungování s pomocí digitální transformace, může znít slovo digitalizace poněkud oposlouchaně. Digitální transformace ale poskytuje flexibilitu, lepší odezvu na měnící se poptávku a ekonomické podmínky, schopnost softwarových aplikací optimalizovat a modernizovat technologické i obchodní procesy a poskytnout nové způsoby, jak pracovat [1]. Horizonty digitalizace se rozšiřují, a proto je třeba s tímto tématem dále pracovat. V současné době jsou navíc zřejmé změny, které digitalizace v podobě průmyslu 4.0 vnese do oblasti provozní techniky (OT).

Sbližování tradičních informačních systémů (IT – *Information Technology*) a provozní techniky (OT – *Operational Technology*) bude pokračovat, a tak může dojít k neshodám mezi profesionály z obou oblastí. S přechodem k digitalizaci si odborníci na IT vyvinuli postup myšlení, který upřednostňuje dosažení agility hledáním nových způsobů ochrany a využití dat [2]. Pro oblast provozní techniky jsou ale zásadními faktory dostupnost, nepřetržitý provoz a spolehlivost – pro kritické procesy mohou i krátké výpadky mít nákladné (a někdy i nebezpečné) následky. Hlavním úkolem tak bude nalezení shody mezi agilitou a spolehlivostí.

Nalézt takovou shodu je určitě možné, ale je to jako když se konstruuje letadlo. Zatímco se na první pohled zdá, že pro letectví budou nejdůležitější stabilita a spolehlivost, inženýři již delší dobu zkoumají situace, kde může být výhodou přesný opak. Stabilnější letadlo sice může znamenat bezpečnější letadlo, avšak také letadlo, se kterým se hůře manipuluje – a to je hlavně pro některá letadla, jako třeba vojenská, skutečný problém.

Kybernetické útoky ve fyzickém prostředí

S tím, jak průmysl 4.0 sbližuje IT a OT, bude zapotřebí, aby profesionálové z obou oborů hledali nové cesty, jak si lépe rozumět a tak porozumět celému systému a zajistit vše potřebné pro oba světy – agilitu i stabilitu. Informační systémy i systémy řízení provozní techniky mají jednu společnou věc, a to jsou data.

Jednou z nejpalčivějších otázek provozní techniky pro budoucnost je její zabezpečení. Na pozadí propojování IT a OT stojí snaha uchopit provozní techniku prostřednictvím dat, jak se to dělá v mnoha jiných oblastech. Tím se do oblasti provozní techniky dostávají výhody softwarových řešení – rychlost, agilita a vzdálená kontrola.

Znamená to ale také, že do světa provozní techniky pronikají rizika spojená se softwarem. Je důležité si uvědomit, že každá přednost většinou má své vedlejší účinky, a všichni si proto musí být vědomi toho, že digitalizace s sebou nese nová a větší rizika. Jestliže se uživatelé nebudou dostatečně zabývat zabezpečením řídicích systémů, jsou kybernetické útoky na výrobní linky, infrastrukturu nebo elektrické a distribuční sítě nevyhnutelné.

Existuje několik reálných příkladů kybernetických útoků na provozní systémy. V roce 2013 byl cílem americký řetězec obchodů Target[1)]. Napadení provedené prostřednictvím vzdáleného přístupu k systému HVAC upozornilo na nebezpečí kybernetické bezpečnosti v dodavatelských řetězcích. Letos to bylo několika útoků na provozní systémy v továrnách a vodárenských společnostech (např. Oldsmar v USA[2)]). Další útoky (např. ransomwarové) vedly k uzavření důležitého ropovodu firmy Colonial Pipeline a následujícímu nedostatku pohonných hmot na celém východním pobřeží USA[3)].

Z těchto příkladů je zřejmé, že světy IT a OT jsou úzce provázané, ač si to třeba inženýři v jednotlivých oblastech zatím neuvědomují. A jak se tyto dvě oblasti budou nadále přibližovat, možnost takových útoků bude narůstat. A proto je třeba nová vize kybernetické bezpečnosti, která bude fungovat ve virtuálním i reálném světě a pokryje potřebu jak stability, tak i agility.

Lidé, procesy, technologie

Pro technické problémy se vždy hledá nejdříve technické řešení. K dispozici jsou již známé zabezpečovací nástroje a systémy, jako firewally a bezpečnostní monitorovací systémy pro provozní techniku. Technika však sama nestačí. Nabízí jen nástroje, které ale musí být správně implementovány a užívány odborníky, kteří rozumějí provozní technice i kybernetické bezpečnosti.

A to je důvod, proč by kybernetická bezpečnost provozní techniky neměla záviset pouze na technice samé. Využití technických prostředků, které vyřeší problémy v oblasti provozní techniky, bude postupné a týmy, které byly dříve samostatné, budou muset daleko více spolupracovat.

V *prvním kroku* tedy půjde o lidi. Bude zapotřebí specifické vyškolení různých skupin zaměstnanců, aby se dosáhlo společného porozumění, zavedl se jazyk, který bude všem srozumitelný, a nastavila se metodika založená na fungujících příkladech. Poté bude možná diskuse o nových hrozbách a řešeních.

Druhým krokem bude nutnost zjistit, jaké změny procesu budou třeba. Systémy řízení, monitorování a kontroly budou pravděpodobně v IT a OT velmi rozdílné – budou shromažďovat různá data, využívat jiné metriky a sledovat jiné plány. Ze zkušeností je známo, že reakce na kybernetický útok musí být soudržná, aby byla efektivní, a to vyžaduje společné plánování. A je třeba, aby postup zahrnoval také partnery a dodavatele: unifikované přihlašovací postupy, standardy pro přístup a další organizační pravidla.

A zde přichází na řadu *třetí krok*. Je důležité provést audit celé struktury a všech zařízení, rozumět tomu, co vše bude do sítě společnosti zahrnuto, a ověřit, že skutečná situace odpovídá očekáváním. S jasnou představou o budoucí architektuře pak lze implementovat vhodné metody autorizace uživatelů a zabezpečení perimetru systému. Zařízení by také měla být pořizována od dodavatelů, kteří re-

Poznámky redakce:

1) V roce 2013 útočníci s využitím slabin v zabezpečení přístupu v systému řetězce obchodů Target získali přístup k databázi zákaznických služeb, nainstalovali do systému malware a získali jména, telefonní čísla, e-mailové adresy, čísla platebních karet, ověřovací kódy kreditních karet a další citlivé údaje. Spolu s dopadem na 41 milionů zákaznických platebních karet se porušení dotklo kontaktních informací více než 60 milionů zákazníků řetězce Target.

2) K útoku na vodárenskou společnost města Oldsmar došlo 5. února 2021. V tomto případě útočníci provedli změny v systému řídícím úpravu vody a výrazně zvýšili koncentraci hydroxidu sodného v pitné vodě. Vyšetřovací zpráva FBI konstatuje: „Útočníci pravděpodobně získali přístup k systému tak, že využili slabiny kybernetické bezpečnosti, včetně špatné správy hesel, a zastaralého operačního systému Windows 7 ke kompromitaci softwaru používaného ke vzdálené správě systému řídícího úpravu vody. Útočníci také pravděpodobně použili software pro sdílení plochy TeamViewer, aby získali neoprávněný přístup do systému.“ Na incidentu je nebezpečné to, že šlo o útok na relativně malou společnost, které mají na profesionální zabezpečení proti kybernetickým útokům často omezený rozpočet.

3) K útoku na Colonial Pipeline Co. došlo 29. dubna 2021. Útočníci ze skupiny DarkSide měli situaci velmi snadnou: získali uživatelské jméno a heslo, která pravděpodobně unikla při některém z předchozích útoků v minulosti, a zjistili, že se jejich prostřednictvím dostanou do VPN, která má vzdálený přístup do firemní počítačové sítě. Firma pro zjednodušení používala pro přístup k různým systémům stejná uživatelská jména a hesla a při přihlašování nevyužívala multifaktorovou autentifikaci. O několik dní později začal ransomwarový útok a firma se rozhodla z bezpečnostních důvodů celý ropovod odstavit. Při pozdějším vyšetřování se naštěstí zjistilo, že v Colonial Pipeline Co. jsou systémy IT a OT důsledně oddělené a útočníkům se nepodařilo získat přístup k systémům řízení provozu ropovodu. Technická zařízení tedy nebyla poškozena a ropovod mohl být po ukončení útoku opět bezpečně spuštěn.

flektují bezpečnostní standardy specifické pro konkrétní oblast, jako je např. IEC 62443 *Bezpečnost pro systémy průmyslové automatizace a řízení*.

Agilitu a stabilitu budou různé organizace integrovat svým vlastním způsobem. Spojení, která tato integrace vytvoří, budou ale vždy vyžadovat kompletní informovanost o možném místě útoku. Budou-li tuto oblast uživatelé dobře řídit, může průmysl 4.0 nabídnout jak větší bezpečnost, tak také flexibilitu.

Literatura:

[1] Eaton [online]. *Kde inteligence řídí energii a internet věcí*. 2021. [2021-11-25]. Dostupné z: https://www.eaton.com/cz/cs-cz/company/news-insights/internet-of-things.html?source=-post:1427559821229090976

[2] Eaton [online]. *Díky nám spolehlivá připojení fungují*. 2021. [2021-11-25]. Dostupné z: https://www.eaton.com/cz/cs-cz/company/news-insights/what-matters/enabling-powerful-cybersecurity.html?source=post1427559821229090976

Eric Rueda, EMEA Business Development Manager, Eaton

krátké zprávy

Závod ABB v Brně rozšiřuje výrobu rozváděčů

Brněnský závod společnosti ABB bude po významném rozšíření výroby jako jediný v ABB dodávat oba hlavní druhy rozváděčů vysokého napětí, tedy vzduchem izolované i plynem izolované. Celkem 98 % výroby jde přitom na vývoz.

V rozšířeném závodě v Brně se budou plnit nové zakázky a současně tam bude převedena část výroby z Německa. Pro rozšíření výroby bude ABB potřebovat obsadit přibližně 100 pracovních míst. Část pokryje z vlastních kapacit, ale i tak bude nutné nabrat desítky nových zaměstnanců. Ti najdou uplatnění i v nově budovaném brněnském centru ABB pro vývoj a výzkum.

„Spokojenost s kvalitou naší výroby a zároveň schopnost pružně produkci inovovat sehrála roli v přesunu výrobních kapacit k nám," vysvětlil ředitel jednotky Rozváděčů vysokého napětí Václav Kovář a dodal: „O kvalitní práci našich brněnských techniků i obchodníků svědčí také setrvalý nárůst zakázek. Mezi nejnovější patří velká dodávka pro Chevron."

Zakázka pro firmu Chevron, nadnárodní společnost sídlící v USA, která se zabývá vyhledáváním ložisek, těžbou, dopravou a zpracováním ropy a zemního plynu a využitím geotermální energie, spočívá v dodání přístrojů a komponent kompletní elektrifikace v celkové hodnotě 120 milionů dolarů pro novou těžební plošinu zemního plynu. Jde o částečně podmořský a energeticky náročný projekt. Plyn je nutné pročistit a stlačit, aby mohl být dopraven potrubím o délce 135 km, což vyžaduje obrovské množství energie. Brněnský závod ABB se na projektu bude podílet právě dodávkou rozváděčů. Půjde o vzduchem izolované rozváděče vysokého napětí UniGear ZS1 a plynem izolované ZX.2.

(*ed*)