Kybernetická bezpečnost průmyslových podniků – čeká nás „průmyslová katastrofa"?

Dnes nikoho nepřekvapí, když se v médiích dočteme, že se cílem kybernetického útoku stala nějaká finanční instituce, kde si útočníci úspěšným útokem neoprávněně přisvojili finanční prostředky.

Motivace útočníků je v těchto případech jednoduchá. Podle statistik více než 70 % všech kybernetických útoků má v pozadí takovýto finanční motiv. Není divu, tento vysoce rostoucí byznys kybernetické kriminality již dnes celosvětově představuje více než 210 miliard dolarů.

Jinou otázkou je situace v oblasti kybernetických útoků na průmyslové podniky. I v této oblasti se objevují nepříjemné zprávy. Z nedávné minulosti je možno jmenovat například německou ocelárnu, olejářskou firmu Aramco či útok na energetickou soustavu na Ukrajině.

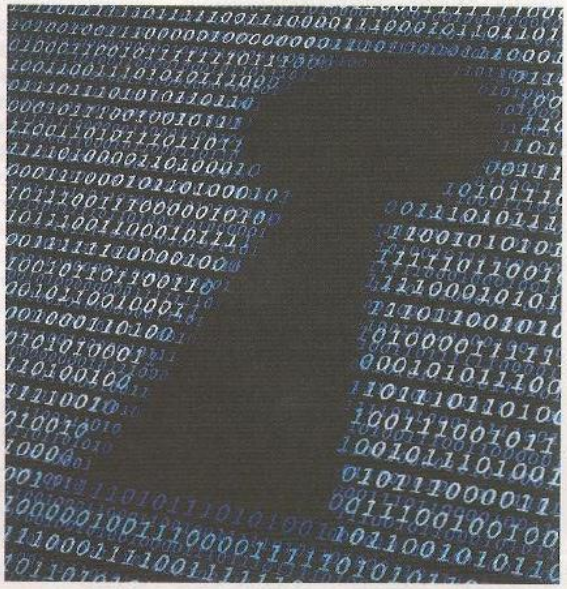
Motivace útočníků jsou v těchto případech jiné než ve finančním sektoru. Jsou spojeny v tom lepším případě se zájmem získat citlivé informace o výrobních postupech, patentech (Cyber Espionage), kdy podle celosvětových statistik právě tyto motivace stojí za více než devíti procenty všech kybernetických útoků. V této souvislosti je navíc potřeba si uvědomit, že toto procento může být ve skutečnosti daleko vyšší, neboť mnohdy firmy ani nezjistí, že byly napadeny a že si někdo takříkajíc „vypůjčil" jejich průmyslová tajemství.

Horším případem je jiná forma konkurenčního boje, kdy je veden kybernetický útok přímo na prostředí průmyslových řídicích systémů (tzv. ICS systémy). Dopady těchto útoků jsou viditelné na výrobních systémech. Jsou spojené se změnou výrobních receptur a tím i s porušením kvality výrobků, případně poškozením nebo úplným odstavením výrobní kapacity. Nejhorší je však situace u těch průmyslových podniků, kde případné dopady kybernetických útoků na výrobní systémy znamenají přímo následné dopady na společnost – ekologickou katastrofu, ztráty na životech či celospolečenský chaos. Za útoky tohoto typu již mohou stát jiné státy, vlády a jejich armády. Tato forma napadení je typickým příkladem zneužití kybernetického prostoru jako bojového nástroje. Motivace tohoto typu stojí zhruba za pěti procenty všech kybernetických útoků.

Bohužel lze očekávat, že množství útoků spojených s konkurenčním soubojem a se zneužitím kybernetického prostoru jako bojového nástroje se bude v nejbližší budoucnosti dramaticky zvyšovat. Dnešní relativně malé zastoupení těchto útoků je dáno faktem, že svět průmyslových systémů byl donedávna velmi uzavřený a pro hackerskou komunitu poměrně nedostupný. To se však mění tím, jak se kybernetičtí útočníci profesionalizují. Zároveň se zranitelnosti těchto systémů dostávají do obecného povědomí a objevuje se stále více relativně snadno dostupných scénářů útoků na průmyslová zařízení. To povede v nejbližší době ke zvyšování počtu útoků s razantními dopady na potenciální oběti.

Podívejme se, kde leží rizika spojená s napadením průmyslových řídicích systémů.

Předně, digitalizace postupně pronikla i do tohoto světa, a tak izolované jednoúčelové analogové systémy byly v posledních desetiletích postupně nahrazeny systémy digitálními, více či méně napojenými na podnikovou datovou síť. Dnes se používají tzv. PLC zařízení (programovatelné logické automaty, které ovládají na základě vloženého algoritmu akční prvky), která jsou úzce propojena s tzv. HMI systémy. Ty se používají pro vizualizaci a parametrizaci řídicích prvků tak, aby operátoři měli přehled, jak probíhá řízení klíčových fyzikálních veličin výrobního procesu v reálném čase. Svět těchto systémů je poměrně uzavřený a konzervativní. Systémy po několik let plní určitou konkrétní řídicí funkci a není žádoucí realizovat jakékoliv změny, které by mohly znamenat odstávky výroby a s tím spojené ekonomické ztráty. Řídicí systémy pracují na zastaralých platformách operačních systémů s neošetřenými zranitelnostmi. V infrastrukturách ICS systémů chybí jakékoliv bezpečnostní prvky, které často ani nelze aplikovat kvůli požadavkům na rychlost odezev řídicích systémů. Celková vzdělanost v oblasti kybernetické bezpečnosti je u personálu obsluhujícího tyto systémy na velmi nízké úrovni, zejména pak v porovnání s klasickým IT světem.



Cílem kybernetického útoku na ICS systémy bývá ovlivnění řídicího softwaru v PLC zařízeních, mající za následek neřízené odstavení výroby; to může být provázeno katastrofálními důsledky s přímým negativním dopadem na lidské životy nebo životní prostředí. Příkladem útoku tohoto typu bylo napadení energetické soustavy na Ukrajině, které způsobil virus s názvem BlackEnergy. Výsledkem útoku byl výpadek elektrické energie, tzv. blackout.

V jiných případech může být cílem „pouhá" modifikace softwaru v programovatelných PLC zařízeních, která znamená nežádoucí změny v parametrech či chování výrobní linky. Příkladem zneužití tohoto typu z minulosti je virus Stuxnet, který měnil otáčky centrifug a zapříčinil zničení jejich ložisek. Tento útok způsobil prodlení celého íránského jaderného programu.

S modifikací softwaru v PLC zařízeních bývá spojeno i napadení vizualizačních jednotek (tzv. HMI zařízení), které pak poskytují obsluhujícímu personálu irelevantní údaje o reálnému stavu regulovaných výrobních veličin. Tímto způsobem často dochází k maskování útoků na vlastní řídicí systémy.

Útočí se i na databázové systémy, které se používají v průmyslové regulaci pro ukládání informací o výrobních recepturách. V souvislosti s mnohdy dlouhou setrvačností výrobního procesu jde o velmi významné ekonomické ztráty nejen ve vztahu k vlastnímu výrobku, ale i ve vztahu ke ztrátě důvěry v produkční značku.

Nabízí se otázka, jakým způsobem zvýšit bezpečnost ICS systémů tak, aby bylo možno se vyrovnat s uvedenými trendy.

Přirozenou cestou je aplikace stejných principů, které se dnes používají v klasických IT systémech, se zohledněním určitých specifik průmyslových systémů.

Pokud se koncipuje nový řídicí systém, je nutno zakomponovat kybernetickou bezpečnost do vznikající architektury a provozních procesů.

V rámci již existujících řešení je vysoce účinným krokem provedení odborných bezpečnostních profylaxí, které s relativně minimálními náklady odstraní velké množství zranitelností (v technických a procesních částech celého systému). Logickým krokem je doplnění architektur průmyslových systémů o bezpečnostní technologie, které jsou důležité při prevenci a detekci kybernetických útoků. Klíčovou roli sehrává v bezpečnosti průmyslových systémů lidský faktor. Jeho schopnost odlišit provozní problém na řídicím systému od bezpečnostního je fundamentální pro rychlou identifikaci bezpečnostního incidentu a minimalizaci škod jím způsobených.

V rámci minimalizace škod jsou důležité nejenom potřebné technologické kompetence pracovníků, ale i funkční procesy obnovy systémů ze záloh, řízené odstavení a efektivní krizové rozhodování na odpovídajících úrovních organizace.

Závěrem si dovolím uvést ještě jednu skutečnost, která významně ovlivní dění v průmyslu v souvislosti s kybernetickou bezpečností: je to nástup Průmyslu 4.0 nebo také internet věcí (IoT). Tento trend je bohužel vodou na mlýn potenciálním útočníkům. Na druhou stranu je ale obrovskou příležitostí, aby se průmyslová kybernetická bezpečnost stala skloňovaným celospolečenským tématem.

Tomáš Přibyl,
generální ředitel CyberGym Europe, a.s.