Ďakujeme za možnosť využiť tento dokument spracovaný expertnou skupinou Safety & Security rakúskej národnej platformy Industrie 4.0 vydaného v júli 2019.

Cyber-Security Leitfaden für Produktionsbetriebe

Sprievodca kyber-bezpečnosťou pre výrobné podniky

Ochrana pred IT-útokmi – viac bezpečnej pridanej hodnoty

Obsah

Table of Contents

Predslov

Vážené čitateľky a čitatelia!
Milí členovia Platformy Industrie 4.0!

Rozsiahla digitalizácia, ktorá medzičasom obsiahla takmer všetky oblasti našej spoločnosti, závratným tempom zmenila pravidlá hry v hospodárstve ale tiež niektoré mechanizmy nášho spolužitia. Digitálne komunikačné systémy silne ovplyvňujú náš každodenný život. Proces digitalizácie a digitálnej transformácie naberá novú dynamiku sieťovým prepojením mnohých fyzických objektov do internetu vecí (IoT – Internet of Things).
Táto dynamika sa týka aj našich výrobných podnikov a podnikateľov. Nasadenie počítačov a softvéru vo všetkých strojových zariadeniach, globálne zosieťovanie našich informačných systémov a dôležitá úloha, ktorú majú dáta pre naše obchodné modely a procesy – to všetko budú rozhodujúce prvky našej konkurencieschopnej obchodnej stratégie. Táto zmena smerujúca k Industry 4.0, hnaná digitalizáciou, stavia každého z nás pred nové výzvy.

Digitalizácia našich výrobných zariadení prináša so sebou popri zvýšení produktivity, zlepšení kvality, zjednodušení procesov a prínosov pre zákazníkov aj veľký problém: zvýšené bezpečnostné riziko pre naše systémy a pre generované dáta. Zákaznícke údaje, patenty, pracovné postupy sa stávajú zaujímavými cieľmi útokov zo strany konkurencie. Zraniteľné systémy a kritická infraštruktúra môžu byť potenciálne cieľom teroristických útokov, prípadne sa celé podniky môžu stať cieľom pre organizovaný zločin. Digitalizáciou a globálnym prepojením rastú na jednej strane príležitosti pre obchodný úspech, avšak aj scenáre ohrozenia naberajú na vážnosti a môžu sa potenciálne stať otázkou prežitia jednotlivých firiem.
Popri konštatovaní nových možných ohrození sprevádzajúcich digitalizáciu sa však musíme zoznámiť aj s novými možnosťami zvýšenia našej kompetencie a použitia vhodných technických opatrení pre zabezpečenie konkurenčnej výhody našich firiem. Ochrana súkromných dát, bezpečné a vysoko spoľahlivé výrobky a bezpečná výroba budú v globálnej konkurencii v konečnom dôsledku dôležitým príspevkom k vytvoreniu USPs (unique selling propositions – jedinečných predajných argumentov). Preto musí byť bezpečnosť pevne zakotvená v produktovej a výrobnej stratégii každého rakúskeho výrobcu. Kyber-security technológie „Made in Austria“ sú vedúce na trhu, sú k dispozícii od inovatívnych rakúskych dodávateľov a umožňujú aby sa rakúske inovatívne priemyselné výrobky úspešne predávali na globálnom trhu aj v digitálnej ére.
Táto brožúra vám poskytne prehľad o aktuálnych scenároch ohrozenia a prvý návod, ako môžete nakoniec dospieť k bezpečnému digitálnemu systému, tak, aby ste aj v budúcnosti obstáli na globálnom trhu. Berúc do úvahy tento cieľ, ponúkame čitateľovi zrozumiteľným spôsobom popis a vysvetlenie rozšírených druhov útokov, ako sú DDoS, ransomware a metód infiltrácie škodlivého softvéru, ohrození pri servisných prístupoch cez internet a tiež možného nebezpečenstva zo strany vlastného personálu podniku. Na záver dopĺňame prehľad známych útokov na rakúske firmy v roku 2018 a prvý checklist pre kontrolu kyber-bezpečnosti. Poskytujeme takto prvú pomoc pre ľubovoľnú priemyselnú firmu.
Na záver pokladám za potrebné konštatovať, že sa žiadna firma nesmie pokladať za príliš malú a z globálneho pohľadu za príliš nevýznamnú na to, aby sa nemohla z pohľadu kyber-kriminálneho prostredia stať predsa len zaujímavou. Kyber-kriminalite ako aj obchodnej

a priemyselnej špionáži s ich vysoko vyspelými metódami útokov sa dá čeliť len efektívnymi ochrannými opatreniami.

DI Dr. Wilfried Enzenhofer, MBA

1. Úvod

V tejto brožúre ponúkame v podobe jednoduchých príkladov a zhrnutí prvý prehľad o problematike kyber-bezpečnosti v oblasti výroby. Cieľom predložených príkladov a scenárov, ktoré napospol vychádzajú z ozajstných prípadov z praxe, je ukázať, aký význam môže mať nedostatočné povedomie o tejto problematike pre výrobný podnik. Najnovšie štatistiky ukazujú, že Rakúsko patrí medzi 5 najčastejších cieľov kyber-útokov v celosvetovom meradle [1.1]. Popisy scenárov ohrozenia ako aj prvých náznakov návrhov na riešenie majú čitateľovi ponúknuť pomoc pri plánovaní a implementácii ďalších konkrétnych krokov.

V časti 2 diskutujeme základnú problematiku škodlivého softvéru v kontexte IT-systémov a výrobných riadiacich systémov. V časti 3 sa pozrieme na to, akú rolu v oblasti IT-bezpečnosti podniku má človek ako používateľ, resp. ako pracovník. V časti 4 vysvetlíme hrozbu DDoS-útokov a v časti 5 sa zaoberáme mimoriadnou hrozbou spôsobenou zle zabezpečených servisných prístupov k výrobným zariadeniam. Časť 6 sa zaoberá novými výzvami pre bezpečnosť dát a IT pri cloudových riešeniach a v časti 7 diskutujeme problematiku narušení ochrany dát v dôsledku bezpečnostných dier. Napokon v časti 8 predstavujeme novú službu pre rakúske malé a stredné firmy: horúcu linku pre oblasť kyber-bezpečnosti, ktorú zriadila Rakúska obchodná komora, ktorá disponuje prehľadom o uskutočnených útokoch na rakúske firmy v roku 2018. Na záver ponúkame prehľad najdôležitejších pojmov z tejto oblasti a ich vysvetlenie, ako aj prvú verziu checklistu kyber-bezpečnosti ako prvú pomoc pre zainteresovaných čitateľov.

ZDRUŽENIE INDUSTRIE 4.0 – PLATFORMA PRE INTELIGENTNÚ VÝROBU

Združenie „Industrie 4.0 Österreich“ bolo založené v roku 2015 ako iniciatíva spolkového ministerstva dopravy, inovácií a technológií ako aj zamestnávateľských a zamestnaneckých zväzov. Títo členovia vypracúvajú spoločne s členmi z hospodárskej sféry, vedy a záujmových združení v expertných skupinách stratégie udržateľnú a úspešnú realizáciu digitálnej transformácie na Priemysel 4.0. Cieľom združenia je digitalizáciou čo najlepšie implementovať technický vývoj a inovácie tak, aby to bolo spoločensky únosné pre firmy, zamestnancov a celú rakúsku spoločnosť. Združenie Industrie 4.0 Österreich v tomto procese zohráva dôležitú úlohu pri národnej a medzinárodnej koordinácii, hľadaní vhodných stratégií a sprístupňovaní informácií.

EXPERTNÁ SKUPINA OCHRANA A BEZPEČNOSŤ

Pre úspešné zavedenie priemyslu 4.0 a komplexného zosieťovania dodávateľských reťazcov je neodmysliteľné spoľahlivé, vysoko dostupné a trvalo bezpečné využitie globálne zosieťovaných strojov a zariadení a inovatívnych dátových technológií. Manipulácia, neoprávnený prístup k senzitívnym informáciam a cielené, vysoko špecializované kyber-útoky predstavujú niektoré z ohrození. Tieto a ďalšie ohrozenia spôsobujú, že udržanie bezpečnosti IT systémov a riadiacich systémov ako aj zabezpečenej funkčnosti , spoľahlivosti a právnej bezpečnosti systémov sa stávajú jednou z ústredných výziev pre spoločnosť a národné hospodárstvo. Zriadením expertnej skupiny Ochrana a bezpečnosť sleduje Platforma Industrie 4.0 Österreich zvýšenie povedomia, dôležitosti a významu témy bezpečnosť pre Industry 4.0, prepojenie relevantných hráčov v Rakúsku a chce tak

dosiahnuť, aby sa z ochrany a bezpečnosti stala rakúska konkurenčná výhoda. Zástupcovia univerzít a iných výskumných pracovísk, politiky a správy, firiem a záujmových združení pritom fungujú ako centrálne riadiace grémium a určujú ťažiská práce a obsahové zameranie aktivít Platformy Industrie 4.0 v oblasti „Ochrana a bezpečnosť“.

2. INFILTRÁCIA ŠKODLIVÉHO SOFTVÉRU CEZ INTERNET A INTRANET V OBLASTI VÝROBY

2.1 PRIEMYSEL 4.0 – IT a OT

Aby firmy úspešne zvládli prechod na Industry 4.0, musia už od počiatočného systémového návrhu zahrnúť aj príslušné bezpečnostné aspekty. Výrobné podniky sa spravidla vyznačujú dvomi osobitnými typmi systémov: informačnými technológiami (IT) pre bežné obchodné procesy (office-IT) a počítačovými technológiami pre riadenie výrobných zariadení (z angličtiny „OT – operational technologies). Táto osobitosť výrobných podnikov so sebou nesie špecifické nároky na systémový návrh a prevádzkové procesy.

Doposiaľ sa ciele informačnej bezpečnosti v oblastiach informačných technológií (IT) a riadiacich/výrobných technológií (OT), akými sú napr. systémy priemyselnej automatizácie definovali a realizovali oddelene a s rôznymi prioritami. Príčinou toho je, že z vlastností IT a OT systémov sa vyvodzovala rozdielna potreba bezpečnosti. Tak sa napr. pri OT kládol dôraz hlavne na dostupnosť a spoľahlivosť. U klasických biznis-IT systémov mala spravidla prednosť dôvernosť a integrita dát. OT-Systémy sú často založené na proprietálnych technológiach a často sa spoliehali len na princíp „security through obscurity“ (bezpečnosť založená na nezrozumiteľnosti pre útočníka). Preto sa ich striktné oddelenie od internetu pokladalo za nevyhnutné minimum opatrení, ktoré sa realizovali [2.1]. Koncepty Industry 4.0 však predpokladajú vzájomné prepojenie týchto svetov o.i. na základe vytvorenia internetu vecí (IoT) a tak čoraz viac zanikajú hranice medzi IT a OT a na internet sa pripájajú priemyselné riadiace systémy, ktoré sú inherentne nezabezpečené. Vzniká tak technické prepojenie podnikovej siete s výrobnou sieťou. V dôsledku toho sú výrobné systémy čoraz viac terčom kyber-útokov. Tieto môžu prichádzať z internetu alebo tiež z (nevýrobnej) podnikovej siete, čiže z intranetu. Tento trend k situácii väčšieho ohrozenia sa dá vypozorovať z rastúcich ročných počtov bezpečnostných incidentov, nahlásených úradom. Tak napr. v r.2010 sa v USA riešilo len 39 bezpečnostných incidentov v kritických infraštruktúrnych podnikoch, kým v r.2016 ich bolo už 290 [2.2, 2.3].

Môžeme zhrnúť, že oblasť OT sa od oblasti IT líši v troch dôležitých aspektoch:

› Safety verzus Security: Pod „safety“ tu rozumieme prevádzkovú bezpečnosť systémov, t.j. zamedzenie škôd spôsobených ľuďom a veciam. Prevádzková bezpečnosť má vo výrobe najvyššiu prioritu, keďže chybná obsluha alebo chyba funkčnosti zariadenia môžu ohroziť ľudský život alebo spôsobiť vysokú vecnú škodu. „Security“ označuje zabezpečenie pred nedovoleným prístupom k technickým systémom s kriminálnym úmyslom, čo bol doposiaľ pojem udomácnený v oblasti office-IT. Postupujúcim vzájomným prerastaním office-IT s výrobným-IT dostáva aj kyber-bezpečnosť vo výrobe stále väčší význam, pretože aj výrobné zariadenia a ich riadiace systémy sa čoraz častejšie stávajú terčom útokov.

› Zavedenie opatrení na zvýšenie kyber-bezpečnosti vo výrobnom prostredí je sťažené tým, že v oblastiach výrobného IT a office IT sa sledujú rôzne ciele. Kým vo výrobnom IT je najvyššou prioritou nepretržitá dostupnosť, sú v office-IT krátke výpadky, resp. odstávky ešte

akceptovateľné. Zato v office-IT nesmie byť kompromitovaná dôvernosť , kým vo výrobe je dôvernosť menej podstatná.

Chýbajúce povedomie o kyber-bezpečnosti vo výrobnom IT (čiže v OT): Kým aplikácia bezpečnostných opatrení v oblasti informačných technológií (IT) je už roky bežnou praxou, takéto opatrenia nie sú ešte v oblasti výroby (OT) samozrejmé. Doposiaľ tu neexistovala nutnosť osobitných bezpečnostných opatrení, keďže výrobné zariadenia buď neboli digitalizované alebo neboli pripojené na internet. To spôsobuje, že ani potrebné povedomie nie je u zodpovedných osôb príliš vyvinuté. Napr. sa v priemyselnom prostredí z praktických dôvodov, resp. pohodlia často používajú štandardné heslá, ktoré dokážu veľmi ľahko uhádnuť alebo prelomiť aj neskúsení kyber-zločinci.

Okrem toho si treba uvedomiť, že existujú jednoduché a verejne dostupné nástroje, pomocou ktorých je možné identifikovať zariadenia s bezpečnostnými dierami. Napr. vyhľadávač Shodan (www.shodan.io) nájde zariadenia, ktoré sú prístupné z internetu – ako napr. wifi routre, chladiace boxy, kamery, riadenia tepelnej techniky ale aj kompletné výrobné riadiace systémy, tieto zariadenia sú nájdené a overí sa, či sú vôbec chránené alebo stačí použiť jednoduché heslá alebo majú len veľmi jednoduché bezpečnostné nastavenia, napr. sú použité bežné heslá. Niekto, kto má kriminálne úmysly potom už ľahko získa do týchto systémov prístup.
Často sa tiež podceňuje to, že externí poskytovatelia služieb alebo dodávatelia môžu predstavovať bezpečnostné riziko a zanedbávajú sa potrebné bezpečnostné opatrenia. Taktiež treba myslieť na to, že cudzí pracovníci v podniku majú jednoduchý prístup k výrobným zariadeniam a k podnikovej sieti a tým môžu (zámerne alebo bez zámeru) infikovať zariadenia alebo informačné systémy škodlivým softvérom (viď. časť 3).
Pozn.prekladateľa: v ďalšom texte používam okrem pojmu „škodlivý softvér“ aj pojem „malvér“ rovnakého významu.

› Zastaralá architektúra: mnohé firmy majú ešte stále jednoúrovňovú s tým pádom ľahko ohroziteľnú sieťovú architektúru, v ktorej sa škodlivý softvér ľahko šíri. Mnohé výrobné systémy sú priamo pripojené na internet, často jednoducho z pohodlnosti a nevedomosti.

2.2 Ochranné a nápravné opatrenia

Priemyselné riadiace systémy je možné ochrániť pred infikovaním malvérom, pristupujúcim z internetu alebo intranetu pomocou nasledovných bezpečnostných opatrení:

1. Treba dbať na vhodnú segmentáciu siete, aby sa dosiahla bezpečnostná architektúra v zmysle defense-in-depth, t.j. redundancia bezpečnostných mechanizmov. Tým budú OT-komponenty primerane oddelené od podnikovej siete a prestanú byť ľahko dosiahnuteľné z internetu. Celá výrobná sieť je rozdelená na zóny podľa služieb a potreby ich ochrany. Zóny tvoria automatizované bunky, vybavené technickými prostriedkami ochrany, napr. firewall-mi [2.4]. Tak sa dosiahne, že aj rozhrania medzi zónami budú dôsledne kontrolované a tým sa zabezpečí prehľad o tokoch dát medzi segmentmi siete. Popri nasadzovaní firewall-ov na oddelenie zón možno využiť aj špeciálne zariadenia (tzv. dátové diódy) ak treba garantovať prechod dát len v jednom smere. Segmentovanie siete na logické úrovne je možné navrhnúť podľa

dávno známeho Purdue modelu [2.5]. Vychádzajúc z neho je sieť rozdelená na zóny a prechody medzi zónami v zmysle normy IEC 62443-3-2.

2. Plocha útoku, t.j. rozsah možností vniknutia do systému cez jeho zraniteľné miesta, musí byť čo najmenšia. Jej redukcia sa dá dosiahnúť napr. aj tak, že sa deaktivujú nevyužívané funkcie systémov. Ďalej je treba odstrániť predinštalované používateľské kontá, ktoré sú spravidla vybavené štandardnými heslami. Ďalej by sa mal implementovať dobre premyslený systém oprávnení, aby sa prístup používateľov obmedzil len na služby, ktoré nevyhnutne potrebujú.
3. Známe slabiny (zraniteľnosti) IT systémov treba odstraňovať priebežnou aktualizáciou softvéru. Nové verzie však treba pred nasadením otestovať v testovacom prostredí, aby sa vylúčilo zavedenie nových chýb.
4. Napokon, OT systémy by mali byť dôsledne sledované monitorovacími systémami, aby sa bezpečnostné incidenty zavčasu zachytili a v prípade potreby boli zapojené zodpovedné osoby a tak sa zavčasu zamedzilo potenciálnym útokom.

2.3 Príklad škodlivého softvéru

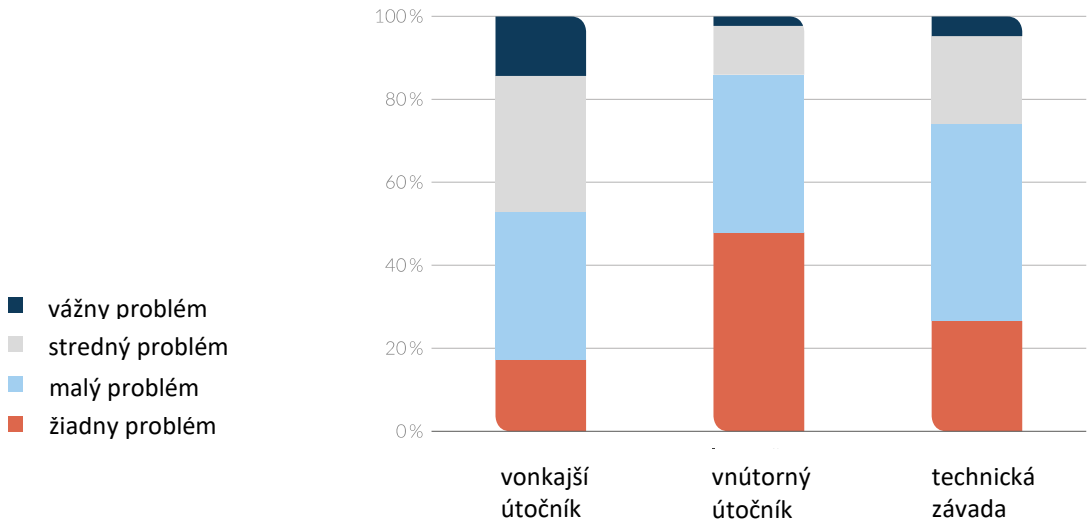
Od roku 2011 je na internete malvér BlackEnergy2 [2.6]. Využíva určité zraniteľnosti používateľských rozhraní (HMI – Human Machine Interface) systémov vo výrobných zariadeniach, ktoré sú priamo pripojené na internet. Cez takéto diaľkové prístupy, ktoré sa často zriaďujú kvôli diaľkovej údržbe/diagnostike sa môžu aj potenciálni útočníci dostať k riadiacemu systému výrobného zariadenia. Touto problematikou sa budeme detailne zaoberať ešte v časti 5. Cez tento malvér sa dá cielene manipulovať s riadiacimi systémami.

Pri šikovne vykonanom kyber-útoku na výrobné zariadenie sa dá aj zamaskovať útočníkova manipulácia a to tak, že na displejoch obsluhy sa zobrazujú normálne prevádzkové stavy a personál si nedovolenú manipuláciu nevšimne.

Hoci útoky pomocou BlackEnergy2 boli zamerané na špionáž [2.7], môže mať infekcia týmto malvérom (škodlivým softvérom) aj závažné negatívne dopady na funkčnosť celých výrobných systémov. Závažné dôsledky útoku malvérom BlackEnergy3 (nástupca BlackEnergy2) na priemyselné riadiace systémy sa ukázali v roku 2015. Útočníci sa pomocou tohoto malvéru dostali do podnikovej siete ukrajinského dodávateľa energie a odtiaľ do jeho výrobnej siete [2.7]. Dôsledkom bol výpadok dodávky energie pre viac než 225 tisíc domácností na Ukrajine po dobu 6 hodín. Je to dôkaz, že kyber-útokmi sa dajú reálne spôsobiť veľkoplošné výpadky zásobovania elektrinou (cyber-blackouts). Takémuto nebezpečenstvu sú vystavení nielen dodávatelia elektriny ale aj výrobné firmy.

3. Pracovníci ako rizikový faktor

Obr. 3.1: Incidenty v obl. kyber-bezpečnosti v rakúskych firmách, odhadnutý podiel príčin, 2018



Pri svojej každodennej práci s podnikovými IT-systémami alebo výrobnými zariadeniami zastávajú zamestnanci firiem dôležitú úlohu pri bezpečnom zaobchádzaní s dôležitými informáciami a systémami. Pritom vykonávajú úkony vedome, ale často aj bez toho aby si uvedomovali dôsledky svojho konania a oboje môže byť príčinou bezpečnostných incidentov. Nepozorné otvorenie prílohy mailu ktorá obsahuje škodlivý vírus, neautorizované posunutie informácie ďalej počas telefonátu alebo jednoducho neznalosť technických rizík pri práci, to všetko môže byť spúšťač kyber-útoku. Dôsledkom môže byť strata informácií, ktoré bolo treba chrániť, finančná strata alebo poškodenie reputácie firmy. Preto patria k rozhodujúcim predpokladom zvýšenia bezpečnosti v technickej infraštruktúre firiem aj vytvorenie povedomia o dôležitosti bezpečnosti u zamestnancov, ich školenie a vôbec ich senzibilizácia voči tejto téme.

Každoročná správa spolkovej vlády Rakúska o kyber-bezpečnosti v rakúskych firmách uvádza popri technických príčinách a vonkajších útokoch aj prehrešky vlastných zamestnancov ako ich častú príčinu – viď. obrázok 3.1. Zo správy nie je zrejmé, v akom pomere ide o aktívnu sabotáž alebo krádež informácií resp. nevedomé konanie či nedbanlivosť.

3.1 Príklady útokov

Nasledujúci text obsahuje štyri príklady kyber-útokov, pri ktorých je rozhodujúcou príčinou chybné konanie ľudí.

CEO fraud

Útočník sa vydáva za vysokého manažéra firmy (napr. konateľa alebo finančného riaditeľa) a žiada o urýchlený finančný prevod z firmy na falošný účet. Pritom často zdôrazňuje, že záležitosť je dôverná. Spravidla tak koná falošným e-mailom na pracovníka učtárne [3.2].
V januári 2016 zverejnili média informáciu o prípade firmy v Hornom Rakúsku, ktorú takto neznámy útočník pripravil o dvojcifernú sumu v miliónoch Eur [3.3]. Nasledovali personálne opatrenia, boli prepustení zodpovední manažéri. Takéto prípady môžu viesť aj k internému vymáhaniu spôsobenej škody pre nedodržanie interných postupov.

Škodlivý a šifrujúci softvér zaslaný cez phishingový email

Veľmi sa rozmnožili útoky cez malvér skrytý v prílohách emailov. Zamestnanec bezmyšlienkovite otvorí nenápadný mail. „Obľúbenou“ metódou bolo a zostáva infikovať počítače mailovými správami o údajne nevydarenom doručení zásielky cez DHL. Otvorenie prílohy mailu, ktorý obsahuje správu o tom, že „Vaša DHL zásielka nemohla byť doručená, viac informácií nájdete v prílohe ...“ vedie k tomu, že „pribalený“ počítačový vírus sa nainštaluje na danom počítači, rozšíri sa po firemnej sieti, zbiera informácie a prípadne zašifruje súbory a následne je firma vydieraná jeho pôvodcami. Ak takýto malvér neodchytia a nezlikvidujú technické protiopatrenia (firewally, antivírový skener), môže to mať závažné dôsledky. Celosvetový útok vírusom *WannaCry* spôsobil v posledných rokoch vážne škody vo firmách.
V jednom hoteli v južnom Rakúsku [3.4] sa tento vírus rozšíril, zašifroval dáta vo všetkých počítačoch a dokonca zamkol elektronické zámky všetkých hotelových izieb, takže sa hostia nemohli dostať s čipovými kartami do izieb. Napadnutá firma zaplatila vydieračom výpalné aby sa znovu dostala k svojim systémom.
Riaditeľ hotela sa k tomu takto vyjadril [3.4]: „Mali sme plne obsadený hotel so 180 hosťami, nemali sme inú možnosť, ani polícia ani poisťovňa vám v takejto situácii nepomôžu. Prvý útok v lete nás stál niekoľko tisíc Eur. Od poisťovne sme doposiaľ nedostali žiadne peniaze, keďže páchateľa sa nepodarilo určiť.“

Vnesenie malvéru zamestnancami

Podľa analýzy BSI (nemecký Spolkový úrad pre bezpečnosť IT) sú druhým najčastejším typom útokov na firmy tie, ktoré sú založené na infiltrácii malvéru (vírusov, trójskych koní). Ešte častejšie sú útoky založené na sociálnom inžinieringu, napr. pomocou phishingových emailov. Infiltrácia malvéru nastáva často pri použití prenosných médií, napr. USB kľúčov. T.j. útok nastane zvnútra firmy. Ukážkovým príkladom bol útok na iránske nukleárne zariadenia malvérom Stuxnet. Bol vyvinutý špeciálny malvér orientovaný na zariadenia, ktoré mali byť napadnuté a dostal sa do systému cez špeciálne upravené USB-kľúče. To, že v takej situácii vôbec nemusí ísť o zlý úmysel zamestnanca, ktorý svojím konaním nakoniec (aspoň čiastočne) paralyzuje priemyselný podnik, ukazuje nasledujúci príklad:

Zamestnanec pracujúci vo výrobe v istej high-tech firme v Rakúsku počas nočnej smeny očakával telefonát svojej manželky, ktorá bola krátko po svojom prvom pôrode. Jeho mobilný telefón bol takmer vybitý a nemal so sebou nabíjačku. Pripojil teda telefón na USB-port riadiaceho počítača výrobného zariadenia. O necelú hodinu došlo náhle k odstávke obrábacieho centra. Malvér, ktorý sa nachádzal na jeho telefóne dokázal cez USB port

infikovať riadiaci počítač a ešte využil aj hotspot-funkciu mobilu na to, aby komunikoval s určitým malvérom na internete. Pracovník nevedel, že USB-port sa dá ľahko zneužiť. Po incidente firma rýchlo reagovala a investovala do bezpečnostného konceptu, ktorý aj implementovala. Bol špecificky zameraný na zvýšenie bezpečnosti vo výrobe [3.6].

Útoky založené na sociálnom inžinierstve

Nasledujúci príklad názorne ukazuje typický kyber-útok využívajúci metódy sociálneho inžinierstva.

Traja študenti technickej odbornej školy si pre svoju seminárnu prácu „Zriaďovanie a bezpečnosť výrobných sietí" vybrali ako cieľ neďalekú továreň na výrobu keksov. Keďže bezpečnostné pravidlá továrne z pochopiteľných dôvodov neboli zverejnené a študentom neboli poskytnuté ani na ich žiadosť, rozhodli sa študenti rešeršovať inými metódami. S využitím svojich notebookov a smartfónov sa pokúsili napadnúť cez internet, avšak bez úspechu. Potom sa pokúsili dostať k interným informáciam firmy. Jeden z nich zašiel do budovy riaditeľstva firmy a poprosil, aby mohol zájsť na toaletu. Cestou na toaletu si všimol, že v jednej z presklených zasadačiek sú na flipcharte napísané prístupové dáta k firemnej WIFI sieti. Tieto si odfotografoval smartfónom. Z najbližšej lavičky pri pozemku firmy sa traja laickí hackeri (ich schopnosti ďaleko zaostávali za schopnosťami skutočných hackerov) dokázali dostať až do výrobnej siete firmy. Pomocou verejne dostupných softvérových nástrojov spustili skenovanie siete. Pritom sa rôznymi metódami zisťuje, aké zariadenia sú na sieti. Čoho si študenti neboli vedomí, je fakt, že štruktúra a požiadavky na výrobné (OT) siete sa značne líšia od sietí v oblasti office-IT. Jeden z kritických faktorov vo výrobe je komunikácia zariadení v reálnom čase. Skenovanie siete, ktoré spustili študenti, sieť natoľko zaťažilo, že došlo k výpadku celého výrobného zariadenia firmy.

Čo sa stalo? Viaceré senzory neboli kvôli spomaleniu siete schopné v reálnom čase odovzdať namerané dáta riadiacemu systému. Riadiaci systém vyhodnotil situáciu ako kritickú pre pracovníkov, pracujúcich na zariadení a zariadenie odstavil. Úplne prekvapený vedúci výroby sa pokúsil nájsť problém a odstrániť a nakoniec chcel zariadenie znovu spustiť, čo sa však nedalo, pretože ešte stále bežalo skenovanie siete, ktoré spustili študenti. Keď ich skenovanie nakoniec dobehlo, bolo už pre výrobcu keksov neskoro. Bolo nutné časti výrobného zariadenia úplne rozobrať a vyčistiť, pretože cesto už stvrdlo vo vstrekovacích tryskách. Celková škoda predstavovala zhruba 500 tis. Eur.

Pôvodcov škody – troch študentov – sa nakoniec po veľkom úsilí a vynaložených nákladoch podarilo vypátrať [3.7].

3.2 Ochranné opatrenia a protiopatrenia

Tvorba povedomia a školenie zamestnancov

Aby sa vylúčili prípady ako horeuvedené, treba si v každej firme zodpovedať nasledujúce otázky:

1. Sú si všetci zamestnanci vedomí reálnych rizík a scenárov ohrozenia?
2. Aký dopad by mal výpadok výroby trvajúci 1 hodinu/1 deň/1 týždeň?
3. Aké ochranné opatrenia sú už vo výrobe / dielňach / montáži realizované? Čo treba ešte urobiť alebo zlepšiť?
4. Čo treba robiť v prípade krízy a kto v tej situácii zodpovedá za ktoré úlohy?

Používanie bezpečných hesiel

Už aj jednoduché opatrenia dokážu zvýšiť bezpečnosť. Jedným z prvých sú pravidlá tvorby a používania hesiel v rôznych aplikáciach. Jedno zo základných pravidiel je nepoužiť rovnakú kombináciu mailovej adresy a hesla v rôznych aplikáciach. Na webovej stránke https://haveibeenpwned.com/ sa dá zistiť, aké prístupové dáta ako mailové adresy alebo heslá už boli prelomené a prípadne sa s nimi obchoduje v darknete.

4. Útoky typu DoS a DDoS

Útok typu denial-of-service (útok DoS) je pokus vyradiť IT- a komunikačnú infraštruktúru podniku jej preťažením. Pri takomto útoku sa komunikačné systémy ako napr. webové stránky, technické zariadenia alebo servre, ktoré majú aktívne pripojenie na internet stanú preťaženými. To sa dosiahne posielaním veľkého množstva dátových paketov alebo dotazov na komunikačné zariadenie cez internetové pripojenie. Zahltením informáciami nemôže zariadenie vykonávať svoju skutočnú funkciu. Takto spôsobený výpadok funkčnosti môže podľa intenzity a trvania útoku trvať minúty, hodiny ale aj dni.
Pokiaľ útočník používa pri útoku tzv. botnet, t.j. veľký počet infikovaných počítačov v internete, ktoré súčasne generujú tento príval dát, hovorím o útoku typu distributed-denial-of-service (DDoS). Všetky zúčastnené počítače posielajú v tom istom okamihu na určitú IP-adresu dátový paket alebo dopyt a tak spôsobujú preťaženie cieľového systému. Ak sú nejaké systémy pripojené na internet útočníkom vyzvané posielať odozvu na adresu, ktorá je cieľom útoku, nazýva sa takýto útok distributed-reflected-denial-of-service (DRDoS).

Napadnuté systémy, ktoré nie sú vybavené mechanizmami obrany proti DDoS-útokom nedokážu spracovať (alebo preniesť) takéto množstvo dát a vedie to k zrúteniu bežnej komunikácie. Napadnuté servery alebo webstránky sú vtedy cez internet nedosiahnuteľné alebo len dosiahnuteľné vo veľmi obmedzenej miere.

Čím viac počítačov je v botnete použitých, tým väčšie množstvo dát sa generuje a tým masívnejší je útok. V minulosti boli takto napádané hlavne sieťové zariadenia ako routre, firewally alebo servery. V poslednej dobe rastie význam útokov na aplikačný softvér.
S rastúcim významom internetu vecí (IoT) sa na DDoS útoky zneužívajú aj zariadenia, ktoré na prvý pohľad vyzerajú úplne neškodne, ako napr. na internet pripojené set-top-boxy, dohľadové kamery alebo senzory v smart-domoch. Tieto zariadenia sú často dodávané so štandardnými heslami a ich firmware sa zriedka aktualizuje. To z nich robí atraktívne ciele pre zaradenie do botnetov. Tak sa všeobecný trend k IoT významne podieľa na potenciálnej hrozbe DDoS útokov.

4.1 Motivácia DDoS útokov

Motívom pre uskutočnenie DDoS útoku býva spravidla spôsobenie maximálnej možnej hospodárskej škody napadnutému. Príčinou útoku býva kriminálny úmysel, ako napr. následné vydieranie výpalného ako podmienka ukončenia útoku, prípadne aj sabotážny úmysel konkurenta, sklamaného zákazníka alebo konanie politicky motivovaných aktivistov. DDoS útoky sú aj zásadným nebezpečenstvom pre kritickú infraštruktúru krajiny, ako je napr. elektrická distribučná sieť, elektrárne, verejná doprava, letiská a zariadenia inštitúcií a ako také tvoria možný scenár ohrozenia pre udržanie národnej bezpečnosti.

4.2 Možné škody

Možné škody pre firmu siahajú od rozsiahlych hospodárskych strát z titulu výpadkov služieb, výroby a predaja a poškodenia imidžu na trhu až po nespokojnosť a stratu zákazníkov.
V oblasti národnej bezpečnosti môže dosiahnuť škoda celoštátne účinky, napr. nemožnosťou udržania verejnej dopravy.

4.3 Ochranné opatrenia a protiopatrenia

Tri dôležité opatrenia sú účinné pre ochranu pred DDoS-útokmi:

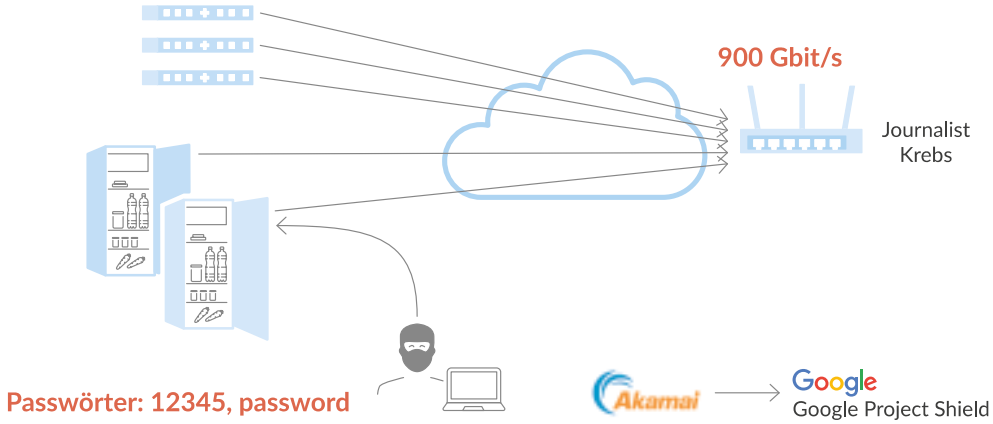
- Nasadenie špeciálnych zariadení na sledovanie dátového toku. T.j. špeciálnych senzorov, ktoré dokážu rozoznať útok, sú umiestnené na správnych miestach siete a sú prepojené s moderným systémom typu Security Information and Event Management System (SIEM). To umožní útok zavčasu odhaliť.
- Nasadenie špeciálnych sieťových zariadení na vstupe firemnej siete so sieťovou infraštruktúrou na pozadí, ktorá dokáže v prípade útoku odfiltrovať škodlivé dáta z internetu, tieto presmerovať a tak zneškodniť (tzv. scrubbing center).
- Firma má s poskytovateľom internetovej konektivity odsúhlasený núdzový proces, ktorým dokáže poskytovateľ v prípade potreby rýchlo presmerovať internetové pripojenie na iné spojenie. Samozrejme musí ísť o poskytovateľa, ktorého infraštruktúra to umožňuje.

4.4 Príklady DDoS útokov

V roku 2016 bol DDoS útoku vystavený rakúsky sieťový operátor A1 [4.1]: A1 bol od soboty 30.1. opakovane obeťou tzv. DDoS útokov. Pri tomto útoku je sieťová infraštruktúra preťažená enormným množstvom paketov, ktoré sú odosielané cez veľký počet krajín s cieľom sťažiť prístup do internetu. Dôsledkom bolo odstavenie alebo značné spomalenie služby mobilného internetu. Postihnutí boli všetci zákazníci služieb A1, bob, yesss! a Georg, pristupujúci do internetu cez siete 2G, 3G a 4G zo smartfónov, tabletov alebo cez rádiové modemy.

Ďalší, veľmi silný DDoS útok sa uskutočnil v r. 2016 pomocou tzv. Mirai IoT botnetu [5.2]. Útok mal za cieľ žurnalistu zaoberajúceho sa bezpečnosťou, ktorému bola zablokovaná online služba. Pri tomto útoku došlo k zneužitiu niekoľkých desiatok tisícov nechránených IoT zariadení na internete na generovanie toku dát s celkovou sieťovou záťažou 900 Gb/s. Bolo nutné zapojiť globálneho prevádzkovateľa akým je Google aby sa podarilo tento tok útočných dát eliminovať. Len Google disponuje takými výkonnými globálnymi sieťami, ktoré umožňujú presmerovať také veľké množstvo dát do iných sietí. Scenár útoku Mirai IoT DDoS je naznačený na obr. 4.1.

Obr. 4.1 Mirai IoT botnet



5. Ohrozenie vyplývajúce z diaľkovej údržby

Pod diaľkovou údržbou rozumieme prístup zo vzdialeného miesta cez internet do IT systému alebo riadiaceho systému priemyselného zariadenia za účelom údržby. Strojové zariadenia je možné na diaľku patchovať, upgradovať, riadiť alebo administrovať. Tak sa eliminuje nutnosť toho, aby špičkový odborník musel pricestovať do výrobného závodu. Priamo zo svojho pracoviska dokáže pohodlne vykonať potrebné zmeny, dokonca aj keď sa zariadenie nachádza na inom kontinente. Rozhrania určené na vykonávanie diaľkovej údržby odpadávajú často veľmi drahé cesty technikov, pričom je možné rýchlo odstrániť poruchy a servisné činnosti sú omnoho lacnejšie.

Nasledujúci príklad vysvetľuje výhody a riziká diaľkového servisného prístupu k výrobnému zariadeniu:

Výrobný šéf stredne veľkej rakúskej továrne pracuje so zariadeniami, ktoré majú rozhranie pre diaľkový servis, prístupné z internetu. To umožňuje, aby jeho zariadenia mohli byť efektívne a lacno servisované. Pred niekoľkými mesiacmi bol takto jednoducho a rýchlo odstránený problém jedného zo zariadení. Špecialista dodávateľa zariadenia sa cez internet prihlásil do zariadenia a rýchlo odstránil príčinu chybového hlásenia. Nebol tak potrebný drahý zásah na mieste, ako tomu bývalo v minulosti. Výrobný šéf však nevedel, že takéto rozhranie diaľkovej údržby musí byť primerane zabezpečené. Kriminálnikovi sa podarilo cez toto rozhranie dostať do riadiaceho systému zariadenia a zmeniť nastavené parametre. Stroj sa prepol na vyššie otáčky a začal sa prehrievať až sa napokon úplne pokazil. Výroba niekoľko dní stála, finančná škoda bola značná.

To, čo možno znie ako fikcia sa medzičasom stalo bežnou realitou a musí byť brané do úvahy ako reálna hrozba pri realizácii projektov Industry 4.0. Podľa názoru špičkových expertov je škodlivý prístup cez rozhrania diaľkového servisu jedným z top 10 rizík v oblasti priemyselných riadiacich systémov [5.1, 5.2]. Útoky cez rozhrania diaľkového servisu sú o to nebezpečnejšie, že spravidla zostanú nepovšimnuté a dajú sa len ťažko odsledovať.

5.1 Ochranné opatrenia a protiopatrenia

Aby boli vylúčené takéto incidenty, treba si v každej firme zodpovedať nasledujúce otázky:

1. Aké fyzické rozhrania a aké WIFI rozhrania v podniku existujú a ako sú zabezpečené?
2. Akým spôsobom je realizované oddelenie firemných IT systémov od výrobnej siete (OT)?
3. Existujú vo firme jasne komunikované bezpečnostné smernice a ako sa realizujú, aj v oblasti prístupu externých osôb?

Ako sme vyššie uviedli, môže rozhranie diaľkového servisu pre firmu znamenať značné riziko. Pomocou rôznych organizačných a technických opatrení môžu byť systémy zabezpečené a riziká do značnej miery minimalizované:

Organizačné opatrenia

- Školenie personálu o možných ohrozeniach vyplývajúcich z konceptov Industry 4.0
- Definovanie bezpečných procesov diaľkovej diagnostiky a údržby
- Nahradenie štandardných hesiel, resp. hesiel predinštalovaných výrobcami zariadení
- Dokumentovanie a protokolovanie všetkých prístupov do systémov za účelov spätného overenia
- Kontrola resp. audit externými audítormi

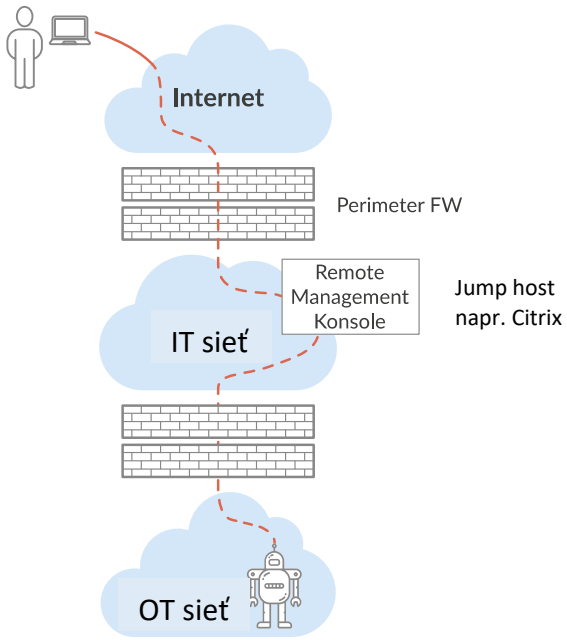
Technické opatrenia

- Zabezpečiť jednoznačnú identifikáciu servisných pracovníkov
- Zaviesť bezpečné postupy pre jednoznačnú identifikáciu servisných pracovníkov, t.j. okrem bežného prihlásenia pracovníka údržby zaviesť ešte špeciálnu identifikáciu
- Implementovať segmentovanie a oddelenie sietí v IT aj OT infraštruktúre aby sa zamedzilo šíreniu malvéru [viď. obr. 5.1]. Užitočný návod poskytuje model architektúry Purdue.
- Zabezpečiť prenosy dát šifrovaním
- Otvoriť porty komunikačných zariadení len v definovaných časoch
- Umožniť prístup na výrobné systémy len cez osobitne zabezpečené siete (tzv. DMZ – demilitarizované zóny)
- Kontrolovať počítače servisných technikov na prítomnosť malvéru

Takéto organizačné a technické opatrenia sú definované aj v príslušných normách, napr. ISO/IEC 27001, IEC 62443, NIST SP 800.

Keďže dosiahnutie komplexnej ochrany môže byť dosť náročné, je užitočné oprieť sa o osvedčené skúsenosti (best practices) iných firiem.

Obr. 5.1: Príklad segmentovania siete



6. Cloudová bezpečnosť – ohrozenie extranetu a cloudových komponentov

Priemyselné firmy v súčasnosti využívajú pre svoje výrobné systémy (Industrial Control Systems (ICS)), ako aj pre iné systémy (napr. IoT zariadenia) extranet a komponenty umiestnené v cloudoch. A to napr. na podporné služby, na diaľkovú údržbu, na inštalovanie softvérových updatov a patchov ako aj na prenájom výpočtovej kapacity v podobe virtualizačných služieb.
Tieto cloudové služby sú spravidla prevádzkované externými poskytovateľmi IT služieb (infrastructure-as-a-service alebo software-as-a-service). Cloudové služby a riešenia šetria firmám náklady tým, že sa nemusia samy starať o prevádzku príslušnej techniky a tiež nemusia vo firmách budovať príslušné IT know-how.
Využívanie komponentov v extranete, resp. cloudoch prináša však špecifické bezpečnostné hrozby, ktorých si musia byť vedomí externí poskytovatelia IT služieb ale aj samotné priemyselné firmy. V ďalšom popíšeme na príkladoch dve také hrozby a tiež, ktorými protiopatreniami im môžu firmy čeliť.

6.1 Závislosť výroby na službe poskytovanej z extranetu, resp. cloudu

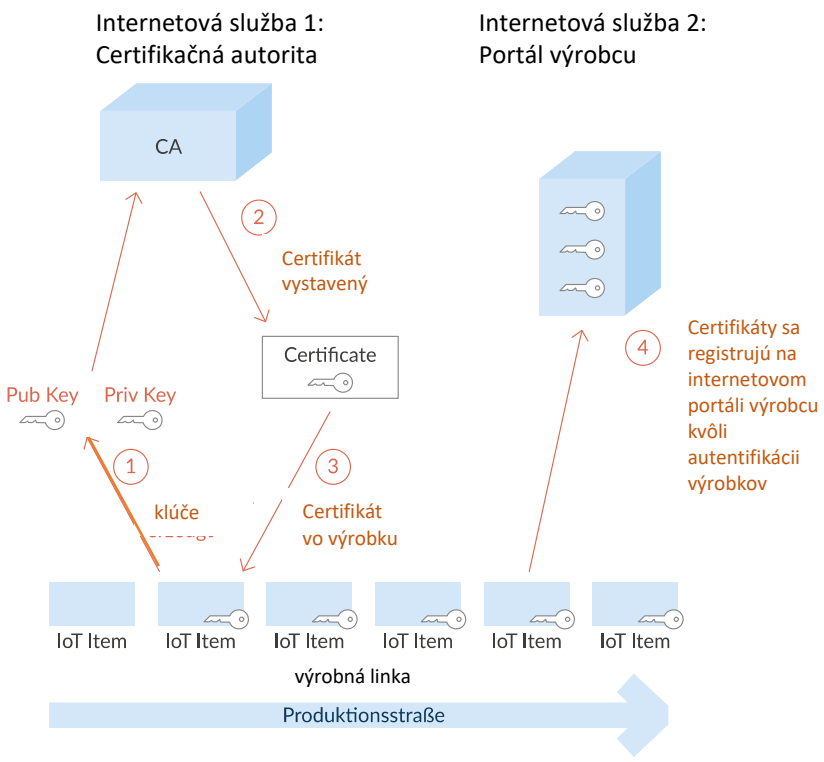
Výrobné zariadenia, ktoré komunikujú s internetovou službou výrobcu, musia byť za normálnych okolností v tejto službe registrované. Tým môže vzniknúť závislosť výroby od dostupnosti tejto internetovej služby.
Typický príklad využitia cloudových služieb vo výrobných procesoch a z toho prameniaca problematika IT-bezpečnosti nasleduje:

V našom scenári vyrába výrobca inteligentné zariadenia, ktoré počas svojej prevádzky v zákazníkovej sieti komunikujú s internetovou službou výrobcu, aby poskytovali zákazníkovi plnohodnotnú službu/zážitok *(príkladom môže byť napr. inteligentná osobná váha).*
V určitom výrobnom kroku dostane každý výrobok pridelený jednoznačný identifikátor, napr. certifikát zariadenia na základe jeho konfigurácie. Pomocou tejto jednoznačnej identifikácie sa neskôr výrobky prihlásia do internetovej služby a jednoznačne sa voči nej autentifikujú. Pridelenie tejto identifikácie (certifikátu) takisto zabezpečuje príslušná internetová služba. Výrobky obsahujú modul, je to počítač so sieťovým rozhraním. Keď sa počas výroby do tohoto počítača nahrá firmware, program vygeneruje kľúčový pár a spojí sa so službou, generujúcou certifikáty (CA – certifikačnou autoritou). CA beží u externého poskytovateľa na internete. Znamená to, že výrobky musia pristupovať k službe, ktorá je na internete už počas výrobného procesu. Akonáhle výrobok dostal svoj certifikát a uložil si ho, je tento výrobný krok ukončený. Každopádne však musí výrobok počkať na pridelenie certifikátu. Znamená to, že dosiahnuteľnosť a doba odozvy služby CA je priamo relevantná pre efektívnosť výroby. Výpadok prístupu k CA alebo strata jej odozvy znamená odstávku výroby.
V ďalšom kroku výrobný systém vyčíta certifikát z výrobku a zaregistruje výrobok v internetovej evidencii výrobcu. Výrobca si zvolil tento prístup aby dopyty zákazníkov boli relevantné len ak ide o reálne vyrobený a dodaný výrobok.
Výrobný systém sa teda autentifikuje na registračnom rozhraní internetovej služby výrobcu a získa oprávnenie registrovať nové zariadenia. Čiže dostupnosť tohoto registračného rozhrania je takisto relevantná pre výrobu.

Aby pri takýchto krokoch nevznikali bezpečnostné incidenty s negatívnym dopadom na výrobu, sú potrebné nasledujúce opatrenia:

- musí byť zaručená autenticita výrobného systému (čiže jej nastavenie musí byť chránené pred malvérom alebo neoprávnenou zmenou človekom), aby sa dali registrovať len pravé výrobky
- výrobná sieť musí byť striktne oddelená aby sa cez autentifikáciu výrobkov nedalo na ňu zvonku dostať
- pri využívaní externých služieb počas výroby (napríklad vyžiadanie certifikátu z CA) sa musí dbať na to, aby zaručená dostupnosť tejto služby bola zosúladená s požiadavkami výroby.

Obr. 6.1: Využitie cloudových služieb na autentifikáciu IoT zariadení



6.2 Nedostatočné oddelenie mandantov v cloudových platformách

Výrobné firmy môžu umiestniť časti IT-komponentov (hardvér, softvér) potrebných pre ich nevýrobné a (aj keď zriedkavejšie) výrobné procesy do cloudových platforiem poskytovateľov IT služieb. Poskytovateľ prevádzkuje v takom prípade systémy viacerých zákazníkov na spoločnej virtualizovanej technike cloudovej platformy.
Pokiaľ nie sú systémy zákazníkov (mandantov) v rámci cloudovej platformy dôsledne oddelené, sú možné presahy medzi sieťami, dátami a systémami rôznych mandantov. Príčiny môžu byť buď chyby v plánovaní alebo konfigurovaní na strane poskytovateľa cloudu, prípadne aj kritická slabina virtualizačnej technológie používanej poskytovateľom cloudovej platformy.
Takéto systémové nedostatky môžu byť využité na špionáž, napr. konkurentom, ktorý využíva služby toho istého IT poskytovateľa. Alebo môže vzniknúť možnosť, že externý útočník najprv napadne iného zákazníka IT poskytovateľa (napr. cez jeho online shop) a po úspešnom kompromitovaní prvého zákazníka cez slabinu cloudovej platformy zaútočí na svoj hlavný cieľ, ktorým sú IT systémy priemyselnej firmy.
Aby čelili tomuto nebezpečiu, musia poskytovatelia IT služieb dbať na to, aby boli ich cloudové platformy naplánované a prevádzkované robustným spôsobom, aby bolo oddelenie mandantov garantované. Technické komponenty použité na virtualizáciu platforiem musia byť udržované v aktualizovanom stave aby boli evt. kritické slabiny odstraňované updatmi. Pritom musí poskytovateľ dbať na to, aby jeho technické prostredie bolo vhodné pre vykonávanie údržby. Rovnako musí priemyselná firma dbať na to, aby jej IT-

poskytovateľ musí byť schopný v prípade výskytu kritických slabín svoje systémy zabezpečiť inštalovaním patchov. Zákazník a IT-poskytovateľ by mali mať vzájomne odsúhlasenú dohodu o prevádzke a patchovaní vrátane ustanovení o riešení núdzových situácií pri bezpečnostných incidentoch. Takáto dohoda je základom rýchlej reakcie na bezpečnostné hrozby v extranete a cloude.
Pre uspokojivé riešenie tejto problematiky je dôležité, aby výrobná firma dôverovala službám prevádzkovateľa cloudu – aby však tiež prevádzkovateľ predložil dôkaz svojej certifikácie alebo vykonaných auditov.

7. Porušenie ochrany dát kvôli bezpečnostné diery v IT

7.1 Ohlasovacia povinnosť ohrozenia ochrany dát

Nová legislatíva ochrany dát (rak. zákon o ochrane dát a vykonávacia vyhláška)[7.1] obsahuje povinnosť nahlasovať každý incident v tejto oblasti štátnemu úradu ochrany dát a podľa miery rizika pre postihnuté subjekty aj týmto subjektom. Medzi relevantné incidenty sa radia napr. aj strata nezašifrovaného USB kľúča s klientskými údajmi alebo preposlaný mail s osobnými údajmi na nesprávneho adresáta. Na čo sa však často nemyslí, je to, že relevantné dáta môžu byť ohrozené aj pri kyber-útoku, z čoho môže pre firmu vzniknúť masívny problém porušenia ochrany dát (data breach). Príkladmi sú prezradenie hesiel alebo aj informácií o zákazníkoch v dôsledku kyber-útoku.

Kým v minulosti sa o dátových incidentoch v mnohých prípadoch ani nevedelo alebo neboli zverejnené, hrozia v zmysle vykonávacej vyhlášky zákona o ochrane dát pri nenahlásení takýchto incidentov úradu vysoké pokuty.

Okrem možného poškodenia reputácie znamená bezpečnostný incident v oblasti ochrany dát aj okamžitú nutnosť vykonania nápravných činnosti v postihnutej firme. Musí odstrániť slabé miesta a postarať sa o minimalizáciu negatívnych dopadov – prostredníctvom technických a organizačných opatrení.

Podľa čl. 33 vyhlášky musí zodpovedná osoba úradu pri kompromitovaní dát o osobách poslať hlásenie a toto musí obsahovať aj „popis prijatých alebo navrhnutých opatrení na nápravu v ochrane osobných údajov a prípadne aj opatrení na zmiernenie dopadov slabých miest v ochrane“ [7.2].

7.2 Ochranné opatrenia a protiopatrenia

V kontexte interných firemných opatrení na ochranu dát sú dva postupy veľmi užitočné pre ochranu dát a súčasne pre zvýšenie kyber-bezpečnosti:

MANAŽMENT RIZÍK

Aj malé a stredné podniky sa musia čoraz viac venovať možným ohrozeniam svojich IT-systémov. Je pri tom potrebné jednotlivé systémy zhodnotiť, rozoznať možné zdroje ohrození a prijať technické a organizačné opatrenia. Tak to požaduje aj zákon o ochrane dát. Pritom treba koordinovať znalosti rôznych oddelení (IT, právne odd. alebo HR) aby sa dosiahol zosúladený pohľad na možné scenáre ohrozenia. Pretože pracovníci týchto oddelení majú rôznu východiskovú kvalifikáciu, vzdelanie a znalosti a spravidla používajú rôzne odborné pojmy. To sa musí zohľadniť vo formulácii a realizácii opatrení.

TVORBA POVEDOMIA A ŠKOLENIE PERSONÁLU V OBLASTI OCHRANY DÁT

Aj malé a stredné firmy musia senzibilizovať svoj personál voči novým technologicky podmieneným hrozbám. Dať pracovníkovi podpísať záväzok mlčanlivosti o senzitívnych informáciach je iba prvý krok (v Rakúsku to požaduje zákon). Je potrebné, evt. po dohode s odborovou organizáciou, pre jednotlivé pracovné oblasti nastaviť a uskutočniť špecifické školenia a periodicky preverovať ich účinnosť.

8. Horúca linka kyber-bezpečnosti 0800 888 133

Ako prvú pomoc a podporu pri kyber-incidentoch pre malé a stredné firmy zriadila Rakúska hospodárska komora (WKO) celoštátnu ponuku takejto služby. Malé a stredné firmy môžu pri problémoch s bezpečnosťou dát alebo systémov využiť túto službu po telefóne alebo cez web komory.

8.1 Bezpečnostná horúca linka

Webová stránka má adresu www.wko.at/cyber-security-hotline alebo aj WKO.at/cys alebo tiež www.cyber-security-hotline.at alebo http://cys.at alebo www.cys.at.

Telefonická hotline je nepretržite k dispozícii na horeuvedenom čísle. Call centrum vykonáva aj hodnotenie spokojnosti a úspešnosti u volajúcich obetí kyber-zločinov.
Napr. firma napadnutá trójskym koňom výpalného typu (ransomware), firma zavolá na pohotovostné číslo 0800 888 133 a dostane prvú pomoc v podobe základných odporúčaní. Ak to nestačí na okamžité riešenie problému, je poskytnutá on-line konzultácia s odborníkmi na IT-bezpečnosť. Za týmto účelom zostavila komora tím vysokošpecializovaných expertov na IT-bezpečnosť v rámci Odborného združenia WKO pre podnikové poradenstvo, účtovníctvo a IT (UBIT). Call centrum zriadi pri kontakte z napadnutej firmy tiket a tento postúpi expertnému tímu, projektovému tímu a servisným centrám v spolkových krajinách Rakúska. Experti sa pokúsia problém volajúcej firmy vyriešiť. Počiatočné konzultácie sú bezplatné. Obnova dát je firme spoplatnená.

Poznámka prekladateľa: Jedná sa o službu Hospodárskej komory pre jej členov. V Rakúsku je členstvo firiem vo WKO bežné.

VYBAVENIE A PRIEBEH PODPORY

V callcentre pracuje školený personál, kompetentný pomôcť v núdzovej situácii. Pre riešenie nahlásených prípadov má callcentrum pripravené tieto podporné procesy:

1. Preverí sa, či je volajúca firma členom komory
2. Pokiaľ sa nejedná o núdzovú situáciu, volanie sa nerieši.
3. Poskytnutie najnutnejšieho návodu na riešenie (napr. riadené vypnutie servera).
4. Pokus identifikovať situáciu pomocou FAQ a checklistov pre akútny kyber-útok, vypracovaných expertnou skupinou pre IT-bezpečnosť WKO UBIT
5. Podľa geografickej polohy volajúcej firmy sú pridelení experti z neustále aktualizovaného zoznamu UBIT-ExpertsGroup-IT-Security.
6. Callcentrum informuje volajúceho, že ho bude (v čase od 8 do 18 hod.) volať IT expert a tiež, že poskytnutie podpory nad rámec informačného rozhovoru je odplatné, pričom sadzbu si určuje príslušný expert. Pridelený IT-expert podporu poskytne a uzavretie ticketu nahlási callcentru.
7. Prípady sú dokumentované v rámci ticketov.
8. Pripravuje sa aj to, že po získaní súhlasu od poškodenej firmy callcentrum WKO zašle potrebné hlásenie polícii a do CERT.at.

9. Napokon, callcentrum WKO vykonáva meranie spokojnosti a úspešnosti riešenia nahlásených incidentov.

Keďže Rakúsko je federálna krajina a aj WKO má štruktúru po spolkových krajinách je výkon týchto služieb v kompetencii organizácií WKO v spolkových krajinách. Bezpečnostní experti sú do tejto služby zaradení len ak majú absolvované veľmi kvalitné školenia a príslušné certifikáty v oblasti IT bezpečnosti a ochrany dát.

Poznámky prekladateľa: Dokument ďalej obsahuje zoznam koordinátorov/garantov tejto služby v jednotlivých spolkových krajinách Rakúska. Ďalej sú uvedené štátne inštitúcie, s ktorými hotline služba, resp. komora spolupracuje, medzi ktoré patrí Spolkové ministerstvo vnútra, Spolkový kriminálny úrad, CERT (Community Emergency Response Team) tímy. Dokument ďalej uvádza základné štatistiky o realizovaných podporách v rámci hotline organizácie:
Napr. v priebehu roku 2018 sa uskutočnilo 432 volaní na linku, z toho 303 bolo vyriešených priamo z callcentra a 129 bolo vo forme ticketov riešených bezpečnostnými expertmi v spolkových krajinách.

9. PRÍLOHY

› Regin je malvér, používaný službami ako NSA v USA alebo GCHQ v Británii na útoky proti počítačom s operačným systémom Microsoft Windows (https://en.wikipedia.org/wiki/Regin).

› Meltdown & Spectre sú osobitné druhy malvéru, využívajúce špecifické slabiny (vulnerabilities) moderných mikroprocesorov. Ba základe týchto slabín môžu byť dáta spracúvané procesorom vyčítané a zneužité. Keďže procesor je ústrednou súčiastkou počítača, sú tieto malvéry obzvlášť veľkou hrozbou.

9.1 Škodlivý softvér

Na jar 2019 už bolo zistených asi 900 miliónov rozličných škodlivých programov (vzoriek malvéru) [9.1]. 60 top firiem sveta pôsobiacich v oblasti IT bezpečnosti vytvorilo organizáciu AMTSO (Anti-Malware Testing Standards Organization) aby spoločne spracovávali a čelili tomuto enormne rastúcemu nebezpečenstvu (https://www.amtso.org/).

Nasleduje krátky popis niekoľkých dôležitých typov malvéru (vybratých ako príklady), ktoré už sú známe v celom svete:

- BlackEnergy (Black Energy 2 a Black Energy 3): Obvykle sa šíri v Microsoft Word a PowerPoint prílohách e-mailových správ. Aktivuje sa otvorením prílohy mailu. Malvér Black Energy bol pôvodne vyvinutý v r.2007 s cieľom realizovať útoky DDoS cez internetový protokol http a tak vyraďovať IT-systémy z prevádzky. V roku 2010 vznikla verzia ktorá útočila na IT-systémy (Black Energy 2) a v roku 2014 verzia Black Energy 3 s rozšírenými funkciami zapájať do útoku ďalšie softvérové komponenty (https://en.wikipedia.org/wiki/BlackEnergy).
- Mirai: Pomocou malvéru Mirai, ktorý bol odhalený v r.2016 je možné na diaľku ovládať zariadenia s operačným systémom Linux pripojené na internet a tak generovať veľké množstvá dát pre DDoS útoky (https://en.wikipedia.org/wiki/Mirai_(malware)).
- Stuxnet: Stuxnet je malvér odhalený v r.2010. Bol vytvorený na útoky na priemyselné riadiace systémy (SCADA) bežiace na Microsoft Windows a využíva viaceré slabiny (tzv. zero day exploits) (https://en.wikipedia.org/wiki/Stuxnet).
- WannaCry: Malvér napádajúci windows-počítače využívajúc slabiny (exploits) OS Windows. Malvér následne zašifruje dátové súbory a vydiera obete žiadosťou o výpalné (preto sa tento typ malvéru nazýva aj ransomware) (https://en.wikipedia.org/wiki/WannaCry_ ransomware_attack).
- EMOTET je účinný rámec pre útoky typu ransomware. Tieto útoky sú často zamerané na oblasť zdravotníctva. Využíva skutočnosť, že v zdravotníckej praxi sa často vyžaduje okamžité rozhodnutie, keďže ide často o ohrozenie ľudského života. Viď. tiež [9.2, 9.3].

9.2 Skratky

(Pozn.prekladateľa: ponechal som aj skratky z originálnej nemeckej verzie, ak by ju niekto chcel čítať)

AMTSO Anti-Malware Testing Standards Organization
BMI Bundesministerium für Inneres – Spolkové ministerstvo vnútra
BKA Bundeskriminalamt – Spolkový kriminálny úrad
BSI Bundesamt für Sicherheit in der Informationstechnik aus Deutschland - nemecký Spolkový úrad pre IT bezpečnosť
CA Certificate Authority
CEO Chief Executive Officer
CERT Computer Emergency Response Team
CIO Chief Information Officer
CSP Cyber Sicherheit Plattform
DoS Distributed-Denial-of-Service
DRDoS Distributed-Reflected-Denial-of-Service
FW Firewall
HMI Human-Machine-Interface
IACS Industrial Automation and Control Systems
ICS Industrial Control System
IEC International Electrotechnical Commission
IKT Informations- und Kommunikationstechnologien – Informačné a komunikačné technológie
IoC Indicator of Compromise TUSOM
IoT Internet of Things
ISO International Organization for Standardization
IT Information Technology
OT Operational Technology
SIEM Security Information und Event Management
System
STB Set-Top-Box
WKO Wirtschaftskammer Österreich WLAN Wireless Local Access Network

9.3 Glosár

- AMTSO: 60 top IT-bezpečnostných firiem na svete spoločne vytvorilo Anti-Malware Testing Standards Organization (AMTSO), aby bolo možné spoločne spracovávať a čeliť enormne rastúcej hrozbe pochádzajúcej zo škodlivého softvéru (https://www.amtso.org/).
- Botnet: Viacero (resp. Spravidla mnoho) infikovaných počítačov v internete, využitých útočníkom na kyber-útok.
- BSI: Spolkový úrad pre bezpečnosť v IT (www.bsi.bund.de). Štátna organizácia v Nemecku vydávajúca odporúčania a tiež štandardy pre oblasť bezpečnosti IT a informácií.

- CEO-Fraud: Útočník sa vydáva za príslušníka podniku, napr. Konateľa alebo finančného riaditeľa a žiada pracovníka ny prevod peňazí. Robí to napr. Falošným mailom na pracovníka účtarne.
- Computer Emergency Response Team (CERT): takéto tímy, reagujúce pomocou na núdzové stavy výpočtovej techniky existujú vo väčšine vyspelých krajín.
- Data breach: Bezpečnostný incident umožňujúci neautorizovaný prístup na dáta. bez potrebnej autorizácie.
- Datenpanne/Data leak: únik senzitívnych dát (často dát týkajúcich sa osobných údajov)
- Denial-of-Service-(DoS) útok: útočník z internetu spôsobí preťaženie zariadenia alebo komunikačného spojenia k službe
- Distributed-Denial-of-Service-(DDoS) útok: ak sa DoS útok uskutoční zapojením veľkého počtu infikovaných počítačov, hovoríme o DDoS útoku. Zapojené počítače posielajú v rovnakom okamihu dátový paket alebo dotaz na určitú IP-adresu a spôsobia tak preťaženie infraštruktúry
- Distributed-Reflected-Denial-of-Service-(DRDoS) Angriff: mnohé zariadenia na internete sú pri útoku požiadané o zaslanie odpovede na adresu, ktorá je cieľom útoku
- DMZ demilitarizovaná zóna: časť siete osobitne chránená technickými prostriedkami
- DSG: Datenschutzgesetz – zákon o ochrane dát
  DSGVO: Datenschutz-Grundverordnung - vykonávacia vyhláška zákona o ochrane dát
- Exploit: slabiny v technických systémoch, umožňujúce kyber-útoky. Vyhľadávanie týchto systémových slabín je predmetom činnosti kyber-zločincov ale aj tajných služieb
- Firewall (FW): bezpečnostné technické zariadenie
- Firmware: softvér, ktorý je súčasťou hardvéru technického zariadenia
- Forenzná činnosť: v tomto kontexte vyhľadávanie slabín v technických systémoch a softvéri, vyhľadávanie príznakov vykonaných útokov, prípadne aj pôvodcu útoku (attribution)
- ICS-CERT: CERT zameraný na priemyselné riadiace systémy (ICS)Indicators of Compromise (IoC): príznaky v systéme, ktoré indikujú ohrozenie systému (napr. vírusové signatúry, IP adresy, hash sumy, mená domén a URL, atď. - takéto data vyhľadávajú ICS (intrusion detection systémy alebo antivírové nástroje).
- Industrial Control Systems (ICS): priemyselné riadiace systémy (napr. PLC, SCADA, ...)
- Malware: škodlivý softvér, spravidla zameraný na preniknutie do IT-systému s cieľom spôsobenia škody
- Segmentovanie siete: rozdelenie firemnej siete na oblasti, ktoré sú buď oddelené od seba alebo je prepojenie spojenie s nutnosťou autorizácie – s cieľom zvýšenia bezpečnosti
- patch, patchovanie: updatovanie softvéru
- ransomware: škodlivý softvér, ktorý vlastníkovi dát, resp. IT systému znemožní ich / jeho využívanie, často s cieľom vyžadovať za uvoľnenie prístupu výpalné
- office-IT: IT systémy určené pre bežné (nevýrobné) firemné procesy
- operational-IT (OT): IT pre výrobu, resp. pre jednotlivé výrobné zariadenia
- phishing: pokusy dostať sa k osobným údajom používateľa internetu (alebo zariadenia) cez falošné webstránky, e-maily alebo sms-ky a tak ukratnúť jeho identitu

- scrubbing centre: spravidla centralizované „stanice čistenia dát“ určené na analýzu toku dát a odstraňovanie škodlivých dát z toku
- set-top-boxy: zariadenia na pripojenie TV prijímačov na internet umožňujúce interaktívne TV služby
- Shodan (www.shodan.io): softvérový vyhľadávač zariadení na sieti so slabinami (exploitmi)
- Side channels: nedomyslené funkcie softvéru resp. IT-systémov, kvôli ktorým vznikajú slabiny, resp. ktorých využitím sa dajú obísť ochranné mechanizmy
- SIEM-systémy: systémy Security Information and Event Management sa nasadzujú pre dohľad nad IT-systémami. Ich cieľom je upozorniť na pokusy o útok na softvérové aplikácie a hardvér.
- Social engineering – sociálne inžinierstvo: manipulovanie osobami s cieľom získať nepovolený prístup k dôverným informáciam alebo IT-systémom
- System vulnerabilities: slabiny softvéru a IT systémov, ktoré sa dajú využiť na ovplyvnenie systémov nedovoleným spôsobom (exploits)
- Trójsky kôň: malware, ktorý sa často vydáva za legitímny softvér
- WLAN: wireless local area network. Označenie pre wifi sieť, ktoré sa používa v nemecky hovoriacich krajinách
- Zero-day-exploits: bezpečnostné diery v technických systémoch umožňujúce kyber-útoky, ktoré nie sú známe výrobcovi a ani používateľom systémov. Pozná ich len útočník. Vyhľadávanie týchto systémových slabín je predmetom činnosti kyber-zločincov ale aj tajných služieb. Útok na zero-day-exploit sa spravidla uskutoční predtým, ako výrobca softvéru alebo IT-systému zverejní opravu slabiny.

10. Literatúra

Časť 1

[1.1] F-Secure Deutschland, Threat Landscape Report zum zweiten Halbjahr 2018: Anzahl der Attacken ist um das Vierfache gewachsen, https://blog.f-secure.com/de/ threat-landscape-report-h2-2018 (letzter Zugriff 1. August 2019).

Časť 2

[2.1] McLaughlin, Stephen, et al. „The cybersecurity landscape in industrial control systems.“ Proceedings of the IEEE 104.5 (2016): 1039-1057.
[2.2] ICS-CERT. Year in review 2012. Technical report, Department of Homeland Security, 2013
[2.3] ICS-CERT. Year in review 2016. Technical report, Department of Homeland Security, 2017
[2.4] ICS-CERT. Year in review 2015. Technical report, Department of Homeland Security, 2016
[2.5] Lee, Robert M. CRASHOVERRIDE: Analysis of the Threat to Electric Grid Operations. Technical Report, Dragos, Inc., 2017
[2.6] Obregon, Luciana. „Secure architecture for industrial control systems.“ SANS Institute InfoSec Reading Room (2015).
[2.7] Kobes, Pierre. Guideline Industrial Security: IEC 62443 is easy. VDE Verlag, 2017.

Časť 3

[3.1] Republik Österreich, Bericht Cyber Sicherheit 2018, https://www.bundeskanzleramt.gv.at/themen/cyber-sicher- heit-egovernment.html (letzter Zugriff: 4. Mai 2019)
[3.2] Republik Österreich, Bericht Cyber Sicherheit 2017, https://www.digitales.oesterreich.gv.at/documents/22124/30428/Bericht-Cyber-Sicherheit+2017/9e3aa25d-2bf0- 4c3c-841b-8c62f5dc8612 (letzter Zugriff: 4. Mai 2019). [3.3] Der Standard, Cyberbetrug: Bisher 86 Millionen erbeutet, 21.6.2017, https://tinyurl.com/derStandard21Ju- ni2017 (letzter Zugriff 4. Mai 2019)

[3.4] Kärnten ORF, Hotel zum vierten Mal von Hackern lahmgelegt, 22.1.2017, https://kaernten.orf.at/news/stories/2821290/ (letzter Zugriff 4. Mai 2019)
[3.5] BSI Analyse: das Bundesamt für Sicherheit in der In- formationstechnik (BSI) aus Deutschlanderstellt in regelmäßigen Abständen Analysen rund um das Thema Sicherheit (www.bsi.bund.de).

[3.6] Beispiel von Adrian Pinter, Siemens Aktiengesellschaft Österreich, 2019.

[3.7] Beispiel von Adrian Pinter, Siemens Aktiengesellschaft Österreich, 2019.

Časť 4

[4.1] A1 Homepage, Cyber-Angriff auf A1 Infrastruktur, 2.2.2016, https://newsroom.a1.net/news-cyber-an- griff-auf-a1-infrastruktur?id=59635&menueid=13054 (letzter Zugriff 4. Mai 2019)

[4.2] Josh Fruhlinger, The Mirai botnet explained: How teen scammers and CCTV cameras almost brought down the internet, CSO, 9. März 2018. https://www.csoonline.com/ article/3258748/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-in- ternet.html (letzter Zugriff 4. Mai 2019)

Časť 5

[5.1] Christina Fink, Erstellung eines Management-Models für Informationssicherheit im industriellen Internet, Master- arbeit, Fachhochschule Wiener Neustadt, 18.12.2017. [5.2] Bundesamt für Sicherheit in der Informationstechnik, Industrial Control System Security – Top 10 Bedrohungen und Gegenmaßnahmen 2019, BSI-CS 005, Version 1.30, 01.01.2019.

Časť 7

[7.1] WKO, EU-Datenschutz-Grundverordnung (DSGVO): Checkliste, https://www.wko.at/service/wirtschafts- recht-gewerberecht/EU-Datenschutz-Grundverord- nung:-Checkliste.html (letzter Zugriff 4. Mai 2019)

[7.2] Art. 33 Abs. 3 lit. d DSGVO

Časť 8

[8.1] Zertifizierung „Certified Data & IT Security, incite, Expert“ https://www.incite.at/de/zertifizierungen/certified-data-it-security-expert/

Časť 9

[9.1] AV-Test Sicherheitsreport, 2018/2019, https://www.av-test.org/fileadmin/pdf/security_report/ AV-TEST_Sicherheitsreport_2018-2019.pdf
[9.2] https://www.srf.ch/news/wirtschaft/bedrohliche-cy- ber-angriffe-wenn-der-operationssaal-stillsteht und

[9.3] https://www.heise.de/security/meldung/ BSI-warnt-vor-gezielten-Ransomware-Angriffen-auf-Unter- nehmen-4406590.html

11. Užitočné linky

- › CSP Cyber Sicherheit Plattform Österreich – https://www.digitales.oesterreich.gv.at/cyber-sicher- heit-plattform)

- › KSÖ Cyber Security – https://kuratorium-sicheres-oester- reich.at/allgemein/cyber-security/
- › KSÖ Cyber-Risikomatrix – https://kuratorium-sicheres-oesterreich.at/wp-content/uploads/2015/02/KSO_Cyber_Risikomatrix.pdf
- › Plattform Industrie 4.0, EG Security & Safety – https://plattformindustrie40.at/security-safety/
- › Österreichischer Verband für Elektrotechnik, Gesellschaft für Informations- u. Kommunikationstechnik, Cyber Security – https://www.ove.at/ove-gesellschaften/git/ aktivitaeten/cyber-security/
- › AIT Austrian Institute of Technology, Center for Digital Safety & Security – https://www.ait.ac.at/en/about-the- ait/center/center-for-digital-safety-security/
- › Seite zur Überprüfung, ob die eigene E-Mail-Adresse Teil von Daten-Leaks ist – https://haveibeenpwned.com/

AIT Austrian Institute of Technology:

› AIT Cyber Range – Trainings & Simulationsplattform: https://www.ait.ac.at/cyberrange/; https://cyberrange.at/

› AIT Safety & Security Co-Engineering: https://www.ait.ac.at/themen/dependable-systems- engineering/

› THREATGET – Cyber-Security-Management-System für den Fahrzeugsektor http://threatget.com/

› AECID – Intelligente Sicherheitstechnologie zur Anomalie- erkennung in Netzwerken, basierend auf Artificial Intelligence (AI): https://www.ait.ac.at/aecid/; https://aecid.ait.ac.at//

› AIT Cyber Security Lösungs- und Technologieportfolio: https://www.ait.ac.at/fileadmin//mc/digital_safety_security/downloads/Factsheet_-_CyberSecurity_de.pdf

› Big Data Analytics for Network Traffic Monitoring and Analysis: https://bigdama.ait.ac.at/

› AIT Technologien rund um die Quantenverschlüsselung: https://www.ait.ac.at/en/research-fields/physical-lay- er-security/optical-quantum-technologies

› 5G – Reliable and Secure Wireless Technology for Industry 4.0 and Automotive: https://www.ait.ac.at/themen/physical-layer-security/

› GraphSense – Cross-Ledger Cryptocurrency Analytics Platform https://graphsense.info/, https://www.ait.ac.at/graphsense/