INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOST (IKB)

Školení dodavatelů

PRAVIDLA CYBEX

Útvar Informační a kybernetická bezpečnost

INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOST

PROČ SE JÍ ZABÝVÁME?

Zpoždění při spouštění íránské jaderné elektrárny – virus Stuxnet

- Útok z roku 2010, který měl oddálit či zastavit spuštění elektrárny. Cíleno na závod pro obohacování uranu.
- Virus zničil několik stovek centrifug tím že změnil frekvenci jejich otáček. Nejprve je roztočil nad povolenou hranici a poté jejich otáčky naopak snížil na velmi pomalé.
- Stuxnet je natolik kvalitní a modulární systém, že je možné jej u průmyslových systémů využít pro téměř libovolnou podobnou činnost.

Masivní výpadek dodávky elektrického proudu na Ukrajině

- V roce 2015 bylo až 700 000 lidí bez proudu na několik hodin.
- Nejednalo o náhodný výpadek, ale koordinovanou součinnost skupiny hackerů.
- Pomocí trojského koně BlackEnergy pronikli do jednotlivých komponent distribučních sítí.
- Kromě funkcí destruktivního malwaru (odstranění systémových souborů, které znemožní spustit systém) se tato varianta speciálně zaměřila na sabotáže v průmyslových systémech.
- Jedná se o první jasně potvrzený útok na rozvodnou elektrickou síť v tomto rozsahu.

INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOST

PRINCIPY ŘÍZENÍ IKB

Informační a kybernetická bezpečnosti:

- **je odpovědnostní každého externího spolupracovníka** s přístupem k informacím společnosti Skupiny ČEZ.
- je definována interní řídící dokumentací v procesu A05 (součástí systému řízení SKČ)

Informační a kybernetická bezpečnost je systém opatření (technických, organizačních, personálních, aj.) pro zajištění atributů informačních aktiv:

- **Důvěrnost** – Informace jsou přístupné nebo sděleny pouze těm, kteří jsou k tomu oprávněni.
- **Dostupnost** – Informace je pro oprávněné uživatele přístupná v okamžiku její potřeby.
- **Integrita** – Informace je správná a úplná.

INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOST

NEED-TO-KNOW

Každý externí spolupracovník má přístup a užívá:

- **Pouze taková informační aktiva Skupiny ČEZ**, které nezbytně potřebuje k řádnému výkonu svých pracovních povinností. Zpřístupnění informací nad tento rámec zvyšuje rizika jejich úniku, zneužití a neoprávněné modifikace.

- **Pouze takové prostředky a zdroje Skupiny ČEZ**, které nezbytně potřebuje k řádnému výkonu své práce. Zpřístupnění prostředků a zdrojů nad tento rámec zvyšuje rizika jejich zneužití, poškození či nedostatečné kapacity pro uživatele SKČ, kteří je k výkonu své práce potřebují.

INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOST

CO ZNAMENÁ IKB PRO MĚ?

Jako externí spolupracovník nesu odpovědnost za to, jak se chovám k informacím a souvisejícím informačním aktivům společnosti Skupiny ČEZ, k nimž získám přístup.

- **Bezpečné zacházení s informacemi** v souladu s principy ochrany klasifikace informací
- **Dodržování bezpečnostních zásad** při užívání služeb a ICT/ICS techniky
- **Udržování povědomí o hrozbách a rizicích** spojených se zpracováním informací a ICT/ICS technikou
- **Dodržování zásad stanovených řídící dokumentací**, pracovními či metodickými postupy a pokyny odpovědných zaměstnanců
- **Udržovat v naprosté tajnosti přidělené autentizační informace** (ID, hesla, karty…)

Nedodržení zásad nebo porušení **informační a kybernetické bezpečnosti může být posuzováno jako porušení pracovních povinnosti** s vyvozením příslušných důsledků, včetně ukončení smluvního vztahu.

INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOST

ZÁKLADNÍ PRAVIDLA VYUŽÍVÁNÍ ICT TECHNIKY

Základní pravidla

Uživatelé by se měli snažit minimalizovat možnost zavlečení škodlivých programů do systémů společnosti.

Uživatelům není dovoleno:

- Instalovat na svěřených zařízeních jiné než schválené programové vybavení.
- Modifikovat nastavení webového prohlížeče a jiných programů.
- Vypínat antivirovou ochranu na svěřených zařízeních.
- Zasahovat do běhu antivirových programů a jiné instalované ochrany.
- Využívat jiné než schválené způsoby komunikace.
- Nenechávat IT zařízení bez dozoru například v zamčeném automobilu na parkovišti atp.

INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOST

BEZPEČNOSTNÍ UDÁLOST A INCIDENT

Bezpečnostní událostí nazýváme takový stav systému, služby nebo sítě který ukazuje na možné porušení bezpečnostní politiky.

V sytému SNAP označováno jako **Neshoda**

Muže se jednat o:

- Selhání bezpečnostních opatření
- Situace, která dříve nenastala a muže být z pohledu bezpečnosti informací důležitá(provozní událost)

Bezpečnostní událost může být příčinou vzniku **bezpečnostního incidentu**

Bezpečnostním incidentem se stává jedna nebo více nežádoucích či neočekávaných bezpečnostních událostí, u kterých existuje vysoká pravděpodobnost kompromitace činnosti organizace a ohrožení bezpečnosti informací.

V sytému SNAP označováno jako **Událost**

Může se jednat o:

- Narušení důvěrnosti informací
- Narušení integrity informací
- Snížení dostupnosti informací

Uživatel je povinen hlásit svému nadřízenému, zadáním do ServiceDesku, SNAPu nebo EZOPu jakýkoli nestandardní stav, který by mohl vést k bezpečnostní události či bezpečnostnímu incidentu!

INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOST

POJMY – SCADA, ICS, OT

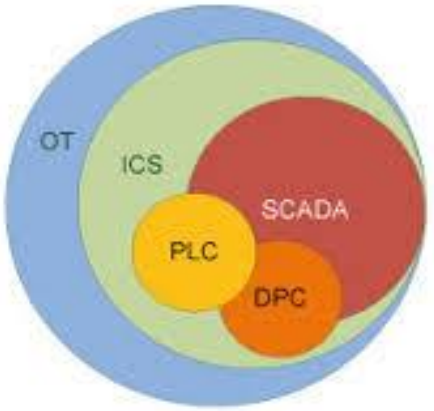
OT (Operational Technology) – je hardware a software, který monitoruje a ovládá fyzická zařízení, procesy a události ve společnosti.

ICS (Industrial Control System) – zahrnuje několik typů průmyslových a řídicích informačních systémů a souvisejícího přístrojového vybavení používané v průmyslové výrobě, včetně:

- dispečerského řízení a sběru dat (SCADA) systémů
- distribuovaných řídicích systémů (DCS)
- menších kontrolních systémů, jako programovatelné logické celky (PLC).

SCADA systém pro centrální dohled a řízení průmyslových a technických celků, který zahrnuje procesy a technologie. Příkladem oblastí, kde se SCADA využívá jsou:

- protipožární systémy,
- řízení distribuční sítě (elektřina, voda, plyn),
- sledování spotřeby el. energie,
- strojní výroba,
- dopravních sítě a řízení dopravní signalizace.



INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOST

BEZPEČNOSTNÍ KLASIFIKACE ICT / ICS SYSTÉMŮ

Ohodnocení dat (bezpečnostní klasifikace) probíhá dle stanovené metodiky, každý atribut (dostupnost, důvěrnost a integrita) může nabývat pěti úrovní: A+ (kritická) = fialová, A (vysoká) = červená, B (střední) = žlutá, C (nízká) = zelená, D (velmi nízká) = světle modrá

Bezpečnostní klasifikaci daného systému najdete v systému ADS

Klasifikační třída	Charakteristika systému ICT
A+ KRITICKÁ	• Systém zpracovávající data a informace **vyžadující nadstandardní míru ochrany**. • Systém důležitý pro **bezpečnost osob a spolehlivého chodu jaderných zařízení**. (spouštěcí a ochranné systémy) • Systémy **kategorie A případně B (EDU – dle IEC 61226), respektive 1E (ETE – dle IEEE 603).**
A VYSOKÁ	• Systém zpracovávající **důvěrná data a informace** (např. **strategické obchodní tajemství, citlivé osobní údaje, biometrické údaje** apod.). • Systém související se zajištěním **bezpečnosti osob, chodu společnosti, logického, technologického nebo technického celku.** • Jedná se zejména o systém související s **řízením provozu**, **řízením přístupu, systémy MaR pro manipulaci a skladování paliva, systémy požární ochrany nebo infrastruktura hlasové a datové komunikace.**

INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOST

BEZPEČNOSTNÍ KLASIFIKACE ICT / ICS SYSTÉMŮ

B **STŘEDNÍ**	• Systém zpracovávající data a informace a vyžadující ochranu stanovenou právními předpisy nebo smluvními ujednáními (např. **obchodní tajemství, osobní údaje** apod.). • Systém plnící zejména **informační, monitorovací a diagnostické funkce bez přímého vlivu na technickou bezpečnost a provozuschopnost**, případě **řízení méně významných technologických celků nebo menších technologických částí**. • Jedná se např. o **systém demineralizace** nebo **systémy dohledu v reálném čase pro velín**, případně neklasifikovaný systém jaderných elektráren a vybraný systém ICT klasických elektráren.
C **NÍZKÁ**	• Systém zpracovávající **veřejně nepřístupná data a informace**, tvoří **know-how společnosti** Skupiny ČEZ. • **Systém neprovozního charakteru**, zajišťující **automatické kancelářské činnosti**. • **Monitorovací a diagnostické funkce bez přímého vlivu na technickou bezpečnost a provozuschopnost** • Jedná se např. o **systém pro správu pracovních povolení a příkazů,** pro **podporu inženýringu a údržby** nebo pro **řízení dokumentace a konfigurace**.

Při práci na systémech ICT/ICS je nutné brát v potaz uvedenou klasifikaci a dodržovat požadované postupy!

INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOST

ZÁKON O KYBERNETICKÉ BEZPEČNOSTI (ZKB)

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti – upravuje práva a povinnosti osob a společností a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti.

Kritická informační infrastruktura (KII) – obdoba kritické infrastruktury, jak ji specifikuje nařízení vlády a krizový zákon, do které je vložen pojem „informační“ a týká se informačních a komunikačních systémů.

Primární aktivum – informace nebo služba, kterou zpracovává nebo poskytuje určený informační systém (informace zobrazené a archivované v TŘIS)

Podpůrné aktivum – **technické aktivum, zaměstnanci a dodavatelé** podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního systému (veškerá dokumentace TŘIS včetně popisu algoritmů, IP adres apod., aplikační SW, dále pak veškeré technické prostředky TŘIS a to včetně servisních notebooků)

Technické aktivum – technické vybavení, komunikační prostředky a programové vybavení informačního systému (veškerý HW SKŘ – systém kontroly a řízení)

INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOST
KRITICKÁ INFORMAČNÍ INFRASTRUKTURA (KII)

- **Definována dle zákona č. 181/2014 Sb. (Zákon o kybernetické bezpečnosti)**

- Prvky jejichž narušení funkce by mělo **závažný dopad** např. **na bezpečnost státu**, **zabezpečení základních životních potřeb obyvatelstva**, **zdraví osob** nebo **ekonomiku státu**.

- **V praxi se jedná o informační a komunikační systémy, příp. ICS/SCADA systémy, které jsou zásadní pro bezpečné fungování provozu elektrárny**

- **Každý prvek KII má určen svého garanta aktiva**. Obsazení role garant aktiv, **odpovědnosti a** jejich **pravomoci jsou definovány ve směrnici** informační a kybernetické bezpečnosti SKČ_SM_0057.

INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOST

PRÁCE NA PRVCÍCH KII

- ✓ Jsem si vědom, že pracuji na zařízení s nejvyšší bezpečnostní klasifikací
- ✓ Informační a kybernetické bezpečnosti věnuji zvýšenou pozornost
- ✓ Dodržuji striktně řídicí dokumentaci a pracovní postupy
- ✓ Hlásím bezpečností události a incidenty příslušnými komunikačními kanály

INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOST

HESLA

Základní pravidla:

- **Držet hesla v tajnosti** a změnit hesla v případě jakéhokoliv náznaku možného kompromitování
- **Měnit hesla v pravidelném intervalu** a vyhýbat se opakovanému použití nebo opakování původních hesel
- **Nezaznamenávat si hesla na papír** či do souborů
- **Nepoužívat** všude **stejná hesla**

Jak vytvořit silné heslo?

Vyjděte ze snadno zapamatovatelného slova. Třeba váš oblíbený film – např. **Pelíšky**

Vynechte samohlásky – **Plšk**

Dál písmeno „š“ nahraďte příslušnou číslicí na klávesnici – **Pl3k**

Přidejte speciální znak – **Pl3k@**

A doplňte oblíbené číslo – **Pl3K@413**

Rychlost prolomení hesla – jednoduchou změnou lze docílit vyšší bezpečnosti

telefon - 13 minut **telefoN** - 1den **telefoN7** - 3 dny **telefoN7369** - 100let

INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOST

MALWARE – PŘEHLED A RANSOMWARE

Malware (zkratka pro škodlivý software) je typ softwaru, který má za úkol zajistit útočníkovi tajný přístup k vašemu zařízení.

Pod souhrnné označení malware se zahrnují: **ransomware, počítačové viry, trojské koně, spyware** (špehovací software) nebo **adware** (reklamní software)

Malware pro šíření využívá různé techniky. Nejčastěji je to phishing a sociální inženýrství

Ransomware – aktuálně nejčastější hrozba

- zabraňuje přístupu k infikovanému počítači
- zpravidla vyžaduje zaplacení výkupného (anglicky ransom)
- šifruje soubory na pevném disku (dokumenty, fotky atd.) nebo jen zamkne systém a výhrůžnou zprávou se snaží donutit uživatele k zaplacení.

Co dělat pokud zjistím, že můj počítač byl infikován:

Nikdy neplaťte!! Pravděpodobnost, že vaše data budou obnovena je minimální a svoji platbou podporujete nové útoky tohoto typu.

INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOST

MALWARE – SOCIÁLNÍ INŽENÝRSTVÍ A PHISHING

Sociální inženýrství

„Nejslabším článkem každého bezpečnostního řešení je člověk.“

Způsob manipulace lidí za účelem provedení určité činnosti nebo získání určité informace. **Techniky** sociálního inženýrství **spoléhají** na **zvědavost, chamtivost, strach nebo lidskou závist**.

Nejčastější technikou sociálního inženýrství je **Phishing.**
Používá se hlavně v emailové komunikaci pro získání citlivých údajů (hesla, čísla platebních karet, aj.)
Phishingové zprávy vypadají jako zprávy od důvěryhodných organizací (kolega, banka, PayPal).

Ochrana před phishingem:

- Základním pravidlem je obezřetnost
- Nikomu nesdělujte vaše hesla a citlivé informace – po telefonu, osobně nebo emailem
- Kontrolujte správnost URL adresy navštěvovaných stránek (např. v chybném písmeně v URL adrese nebo v odlišné doméně (.com namísto .cz)
- Dodržovat pravidla bezpečné práce s emailem

INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOST

E-MAIL – ZÁKLADNÍ INFORMACE

E-mail je v dnešní době nejpoužívanější prostředek pro komunikaci v rámci společnosti.

Pro co největší bezpečnost e-mailu doporučujeme dodržovat následující zásady:

- Neotevírat nevyžádané, neznámé a potenciálně nebezpečné přílohy.
- Nezneužívat elektronickou poštu pro zasílání nevyžádaných zpráv v rámci společnosti i vně.
- Nepoužívat emailovou schránku pro registraci na různá diskuzní fóra či webové služby, pokud toto přímo nesouvisí s jejich pracovní náplní.
- Nereagovat na nevyžádanou poštu (spam). Nevyžádanou poštu zašlete jako přílohu na *spam@cez.cz.*
- Nerozesílat hromadné či řetězové maily.
- Nezasílat emailem citlivé či jinak důvěrné informace, pokud je to nutné využijte šifrování emailu.

Elektronický podpis a šifrování e-mailu

- Elektronický podpis je prostředek k tomu, jak v anonymním světě internetu ověřit totožnost odesílatele.
- Šifrování je jeden ze způsobů jak můžete výrazně zvýšit zabezpečení svého emailu. Je možné šifrovat celý email případně pouze zasílanou přílohu.
- Pro el. podpis a šifrování emailů je nutné mít vystavený certifikát.

INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOST

INTERNET

Pro správné a bezpečné fungování, byste měli dodržovat následující zásady:

- **Nenavštěvujte rizikové webové stránky** (pornografie, cracking, hacking, warez, drogy, násilí, …)
- **Nevyužívejte automatického ukládání hesel** – tyto hesla je poté snadné odhalit a zneužít
- **Neposílejte přes internet důvěrná data** – pokud je to nutné (např. platba kartou na internetu) tak jedině šifrovaně
- **Nesdělujte osobní informace** – zbytečně neprozrazujte informace, které nejsou potřebné (např. při registracích)
- **Pravidelně aktualizujte** – neodkládejte aktualizace Windows a dalších programů
- **Nevěřte každé informaci, kterou na Internetu získáte**

INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOST

ZÁLOHOVÁNÍ

Zálohování je nejlepší ochrana proti ransomware, lidské chybě (omylem smazaný soubor) či poškození IT techniky (poškození HDD). Není ovšem potřeba zálohovat veškeré soubory.

Co zálohovat:

- Zálohujte data, která jsou důležitá, opětovné vytvoření by vám zabralo neúměrné množství času nebo by nebylo vůbec možné.
- Data, jejichž ztráta či poškození by pro vás znamenala značné komplikace, ohrožení termínů úkolů či finanční sankce pro zaměstnavatele nebo pro vás osobně.

Kam zálohovat:

- ODP – Osobní diskový prostor (disk H:)
- SDP – Sdílený diskový prostor (disk U:)
- Sharepoint SKČ
- na šifrované USB disky (je možné požádat prostřednictvím SD)

Kam nezálohovat:

- na soukromý email (gmail, seznam aj.),
- na veřejná úložiště (uloz.to, letecká pošta a další),
- na soukromé USB disky,
- do webového uložiště (Dropbox, Google disk).

INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOST

BEZPEČNÉ CHOVÁNÍ V PRAXI

- **Dodržujte předepsanou politiku hesel**. Heslo nikomu nesdělujte. Nezasílejte je emailem a nepište si je na papírek u počítače.
- **Email používejte s rozumem**. Pokud nevíte, od koho e-mail je, nikdy nestahujte jeho přílohu a neklikejte na žádné odkazy. Elektronickou poštu může snadno zachytit útočník.
- **Nahlaste jakékoli podezřelé aktivity** prostřednictvím aplikace Servicedesk, SNAP či EZOP.
- **Administrátorská oprávnění používejte pouze k předepsaným účelům**. Nepoužívejte administrátorský účet k přístupu na internet.
- **Nikdy neukládejte citlivá data na cizí přenositelná média**.
- **Na Internetu nenavštěvujte rizikové webové stránky**, nevyužívejte automatického ukládání hesel, neposílejte důvěrná data ani nesdělujte osobní informace.
- **Zálohujte**. Firemní data na sítové disky (U: a H:), Sharepoint či šifrované USB disky. Nikdy ne na soukromý email, webová uložiště, či na soukromé USB disky.

INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOST

BEZPEČNÉ CHOVÁNÍ V PRAXI

Tato prezentace je volnou přílohou SKČ_ST_0027

Autor: Jindřich Šíp, Jakub Svěrek

Datum zpracování: 7.5 2019