ÚJV Řež, a. s. – Školení dodavatelů
Pravidla CYBEX

1.1.2024, Informační a kybernetická bezpečnost (IKB)

Skupina ÚJV
LIDÉ | INOVACE | TECHNOLOGIE

PROČ SE ZABÝVÁME IKB?

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.

PROČ SE ZABÝVÁME IKB?

Aktuální stav na https://www.privacyaffairs.com/dark-web-price-index-2021/

PRINCIPY ŘÍZENÍ IKB

Informační a kybernetická bezpečnost:

- je odpovědnostní každého externího spolupracovníka s přístupem k informacím společnosti Skupiny ÚJV.
- je definována interní řídící dokumentací v procesu MP 13 (součástí systému řízení ÚJV)

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.

CO ZNAMENÁ IKB PRO MĚ?

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

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.

BEZPEČNOSTNÍ UDÁLOST A INCIDENT

Bezpečnostní událostí nazýváme takový stav systému, služby nebo sítě který ukazuje na možné porušení bezpečnostní politiky. Označováno je také jako **Neshoda** nebo **Skoronehoda**
Může se jednat o:

- Selhání bezpečnostních opatření
- Situace, která dříve nenastala a může 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.

Uživatel je povinen hlásit jakýkoli nestandardní stav, který by mohl vést k bezpečnostní události! Pro hlášení využívá dostupné komunikační kanály Helpdesku nebo přímo svému vedoucímu pracovníkovi

POJMY – SCADA, ICS, OT

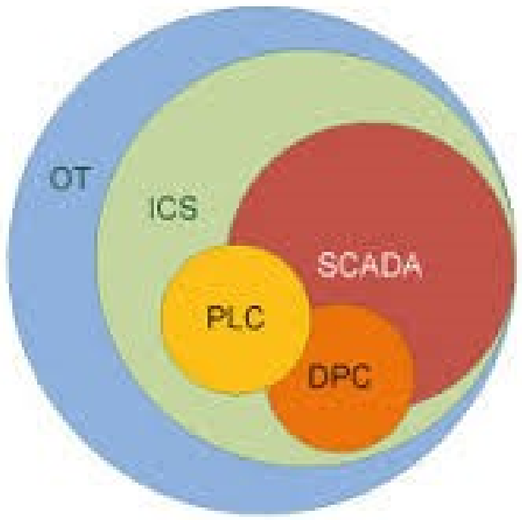
OT (Operational Technology) – je hardware a software, který monitoruje a ovládá fyzická zařízení, procesy a události ve společnosti.

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 vvužívá isou:

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



BEZPEČNOSTNÍ KLASIFIKACE ICT / ICS

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

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 dle IEC 61226 respektive 1E 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**.

BEZPEČNOSTNÍ KLASIFIKACE ICT / ICS

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 **systémy dohledu v reálném čase pro velín**, případně neklasifikovaný systém jaderných zařízení nebo elektráren a vybraných systémů ICT včetně systémů klasických elektráren.
C **NÍZKÁ**	• Systém zpracovávající **veřejně nepřístupná data a informace**, tvoří **know-how společnosti** Skupiny ÚJV nebo 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!

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.

Informační systém základní služby (ISZS) - informační systém, na jehož fungování je závislé **poskytování základní služby (PZS)**

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)

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 technologických celků jako jsou např. i 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.

PRÁCE NA PRVCÍCH KII /ISZS

- **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
- **Bezpečně zacházím s informacemi** v souladu s principy ochrany klasifikace informací

BEZPEČNOSTNÍ POŽADAVKY NA DODAVATELE

Prosazování bezpečnostních požadavků na dodavatele probíhá v rámci procesu přezkumu smluv zejména útvarem nákup a právním oddělením a dle Standardu SKČ_ST_0027 resp. dle harmonizovaných příloh směrnice UJV SM_1400_061_Informační_bezpečnost:

- Příloha A - Bezpečnostní požadavky pro dodávky standardních systémů a technologií
- Příloha G - Seznam požadavků na dodavatele a poskytovatele služeb pro smlouvy na údržbu
- Příloha J - Bezpečnostní požadavky na konzultační a poradenskou činnost

Odkazem nebo začleněním textu příloh jsou do nových i stávajících smluv prosazovány bezpečnostní požadavky na dodavatele

Rozlišení o správné příloze je v kompetenci žadatele nákupního požadavku a správce smlouvy resp. garanta aktiva

Školení dodavatelů

- Příloha I - CYBEX – školení dodavatelů (harmonizovaná s VP I SKČ_ST_0027) – Pravidla CYBEX
- V rámci vstupního a opakovaného školení (pro zaměstnance i vedoucí pracovníky) dle plánu rozvoje bezpečnostního povědomí ÚJV Řež, a. s.

Audit dodavatelů

- Dle Přílohy A mají společnosti Skupiny ÚJV právo na audit IKB u dodavatele, zajištění je v odpovědnosti Garanta aktiva, IKB spolupracuje

HESLA

„Hesla využíváme od počátku věků (počítačů)“

Základní pravidla:

- Držet hesla (případně PIN) v tajnosti a měnit je 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 stejné heslo pro různé služby

Nikdy a nikomu nesdělujte své heslo

SLOŽITOST HESLA

- Čím delší nebo komplexnější heslo, tím bezpečnější před odhalením hrubou silou
- Sílu hesla je možné otestovat na https://howsecureismypassword.net (doporučujeme nezadávat vaše konkrétní heslo)
- Jednoduchou změnou lze dosáhnout vyšší bezpečnosti

mojepivo	**5 vteřin**
mojePivo	**42 minut**
moje5Pivo	**4 dny**
moje5Pivo@	**6 let**

JAK DLOUHO TRVÁ ODHALENÍ HESLA

Složitost hesla je dána:

- Množstvím znaků
- Použitím čísel
- Použitím speciálních znaků

Jak dlouho trvá odhalení?		Počet znaků							
		8	9	10	11	12	13	14	15
Komplexita hesla	a-z	sekundy	minuty	hodiny	dny	měsíce	roky	desítky let	tisíce let
	A-z	minuty	hodiny	měsíce	roky	stovky let	tisíce let	tisíce let	tisíce let
	A-z, 0-9	hodiny	dny	měsíce	desítky let	tisíce let	tisíce let	tisíce let	tisíce let
	A-z, 0-9, @?*	hodiny	měsíce	roky	stovky let	tisíce let	tisíce let	tisíce let	tisíce let

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 zašifrováním souborů v PC/NB
- 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.

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 kontrola odesílatele a kontrola odkazů
- 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
- Ověřujte si jestli osoba se kterou komunikujete je skutečně ta za kterou se vydává

E-MAIL – ZÁKLADNÍ INFORMACE

E-mail je v dnešní době nejpoužívanější prostředek pro komunikaci

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 označujte v Outlooku.
- 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.

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**

VÝMĚNA DAT VE SPOLEČNOST I MIMO NI

Na výměnu dat v rámci firmy můžeme využít tyto komunikační kanály:

- SharePoint, OneDrive nebo Teams
- Sdílený diskový prostor (disk J:, W:)
- Email

Na výměnu dat mimo společnost můžeme využít tyto komunikační kanály:

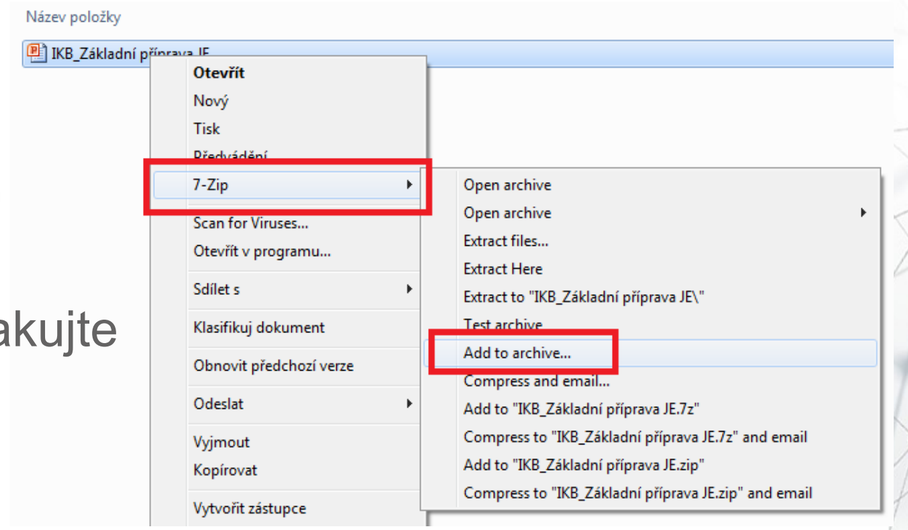
- Externí přístup na sdílený diskový prostor J:, W: na adrese https://ujvcloud.ujv.cz/login K úložišti nelze přistupovat anonymně a je potřeba pro externistu požádat o přidělení účtu prostřednictvím Helpdesku.
- Externí Teams, SharePoint nebo DMS, který lze na vyžádání zřídit prostřednictvím
- Email (klasifikace důvěrnosti veřejné a interní) a Šifrovaný email (klasifikace důvěrnosti chráněné)
- Datová schránka (pro oficiální komunikaci se státní správou a regulátory)

JAK ZAŠIFROVAT SOUBOR

Nejjednodušší cestou k zašifrování souboru je vytvoření archivu s heslem .

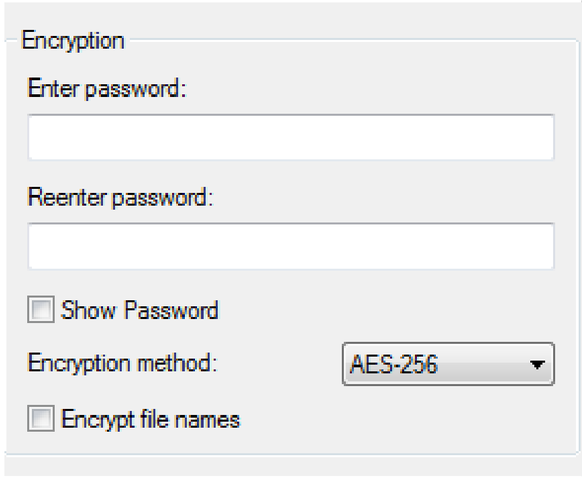
Postup k vytvoření archivu s heslem:

- Vyberte daný soubor či složku
- V menu (pravé tlačítko) zvolte 7-Zip ->Add to archive…
- V části Encryption zadejte heslo a heslo zopakujte
- Encryption metod zvolte: AES 256



Správné heslo by mělo obsahovat:

- Délka ideálně 20 znaků
- Malá i velká písmena
- Speciální znak a číslo
- Pro vytvoření silného hesla je možné využít online generátor např. https://passwordsgenerator.net/



Heslo nikdy nezasílejte společně se šifrovaným souborem. Pokud soubor posíláte emailem heslo zašlete například pomocí SMS

WIFI

V prostorách Skupiny ÚJV využíváme několik WI-FI sítí. Každá sít má jiné využití

UJV_Interni

- Síť určená pro firemní zařízení

UJV_GUEST

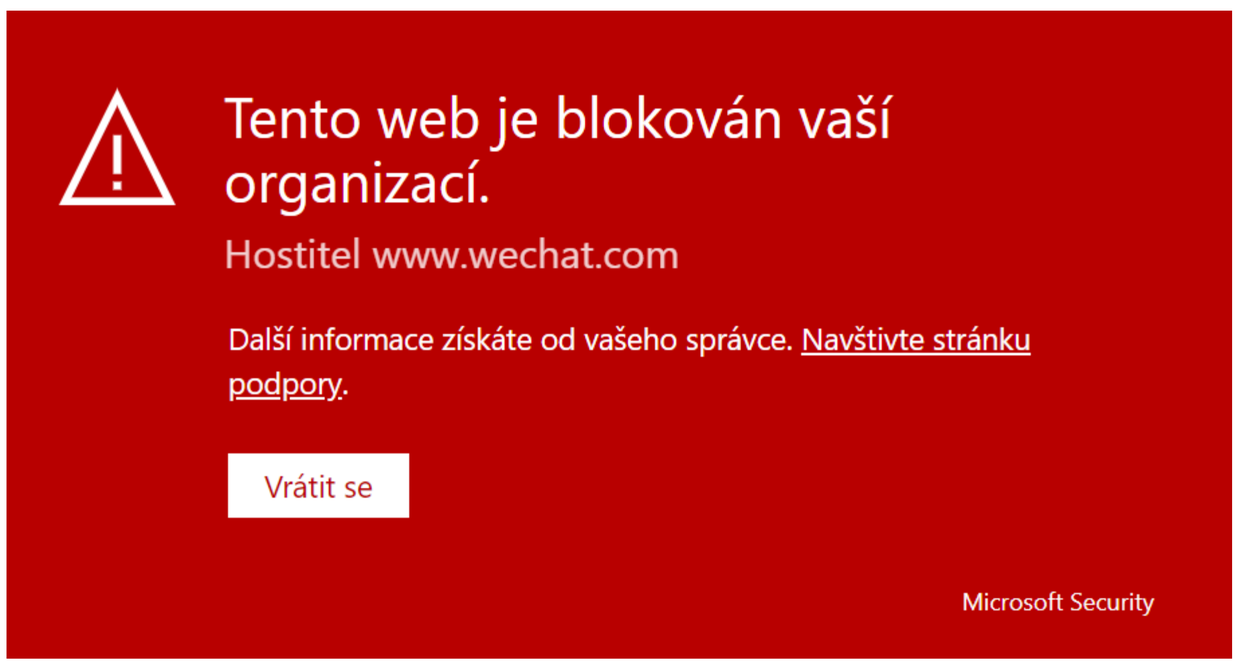
- Síť určená pro soukromá zařízení nebo zařízení dodavatelů. Zabezpečení vyžaduje zadat přihlašovací údaje které získáte zadáním požadavku v Helpdesku

CEZ_OPEN

- Otevřená WIFI určená návštěvám nebo externistům v prostorách Skupiny ČEZ
- Maximální rychlost 512 Kbps a časový limit relace 8 hod.
- Přihlášení přes webový portál

BLOKOVÁNÍ INTERNETU A MONITORING SÍTĚ

- **Přístup na nebezpečné stránky je z firemních počítačů blokován.**
- **Z důvodu ochrany naší sítě jsou informace o přístupu na tyto stránky zaznamenávány.**
- **Nejčastěji se jedná o stránky s rizikovým obsahem, s tématikou hazardu, pornografie či warezu**



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:

- Sdílený diskový prostor (disk J:)
- Zabezpečený diskový prostor (disk S:)
- Sharepoint,
- na šifrované USB disky (je možné požádat o ně prostřednictvím Helpdesku)

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, OneDrive, Google disk).

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 Helpdesku.
- **Administrátorská oprávnění používejte pouze k předepsaným účelům a na předepsaných typech účtů.** 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 (J:, S:), Sharepoint či šifrované USB disky. Nikdy ne na soukromý email, na soukromé USB disky či webová uložiště.

SOUVISEJÍCÍ DOKUMENTY

- Tato prezentace je harmonizovaná s volnou přílohou VP I řídícího dokumentu SKČ_ST_0027 Standard informační a kybernetické bezpečnosti Skupiny ČEZ
- Autor: Jakub Svěrek
- Datum zpracování: 16.6 2023
- Prezentace je výstupem plánu rozvoje bezpečnostního povědomí ÚJV Řež, a. s. dle přílohy směrnice 2UJ_SM__1400_017_r05__Rozvoj_zamestnancu_a_rizeni_znalosti - 2UJ_SM_1400_017_r05_07_Plán_rozvoje_bezpečnostního_povědomí_harmonizovaný se SKČ ME 0017 VP A PRBP

SKUPINA ÚJV

Portfolio služeb mateřské společnosti ÚJV Řež synergicky doplňují 100% vlastněné dceřiné společnosti, spojené do Skupiny ÚJV.

Skupinu ÚJV tvoří:

ÚJV Řež (www.ujv.cz)

Centrum Výzkumu Řež (www.cvrez.cz)

Výzkumný a zkušební ústav Plzeň (www.vzuplzen.cz)

ŠKODA PRAHA (www.skodapraha.cz)

RADIOMEDIC (www.radiomedic.cz)

Skupina ÚJV
LIDÉ | INOVACE | TECHNOLOGIE

ÚJV Řež, a. s.
Hlavní 130, Řež
250 68 Husinec, Czech Republic

e-mail: sales@ujv.cz
www.ujv.cz

Skupina ÚJV
LIDÉ | INOVACE | TECHNOLOGIE