ČISTÁ
ENERGIE
ZÍTŘKA

Výzvy a specifika řešení IKB v prostředí jaderné elektrárny

Ing. Dušan Mareček / ČEZ, a.s.

SCADA konference ČB 2024 – 18. 4. 2024

ÚVOD - MOTTO

KYBERNETICKÝ PROSTOR PŘINESL LIDSTVU ŘADU NOVÝCH MOŽNOSTÍ, OTEVŘEL NOVÉ OBLASTI PODNIKÁNÍ, MĚNÍ NÁM PRACOVNÍ I SOUKROMÝ ŽIVOT. MĚJME VŠAK NA PAMĚTI, ŽE TENTO NOVÝ PROSTOR NENÍ ANONYMNÍ, NENÍ ZADARMO A ROZHODNĚ NENÍ BEZPEČNÝ.

OCHRANU SKUPINY ČEZ V KYBERPROSTORU STAVÍME NA TŘECH PILÍŘÍCH:

SYSTÉMU ŘÍZENÍ, TECHNOLOGIÍCH A LIDECH

POKUD MÁME SPOLEČNĚ USPĚT, CHCE TO ODPOVĚDNOST A ZDRAVÝ ROZUM!

OSNOVA

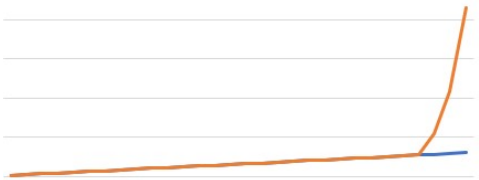
- **PROČ?**
- **LEGISLATIVA (VNĚJŠÍ, VNITŘNÍ)** – regulace
- **ŘÍDÍCÍ DOKUMENTACE** - máme pro své systémy správnou dokumentaci?
- **ORGANIZACE IKB V ČEZ – ZABEZPEČENÍ (FO A IKB)** - máme personál pro správu a udržování bezpečnosti ICS?
- **PRINCIPY, PRAVIDLA, POLITIKY** – jak na to
- **AKTIVA (EVIDENCE, ŘÍZENÍ RIZIK)** – specifika JE (Divize, legacy systémy). Víme, co je v provozu nainstalované?
- **DODAVATELÉ** – bez nich to nejde (údržba, ND,..)
- **VZDĚLÁVÁNÍ** – učit se, učit se, učit se,..
- **BEZPEČNOSTNÍ UDÁLOSTI** – šetření, testování. Je zabezpečená správa incidentů a reakce na incidenty?
- **JAK TO VŠE MUSÍME CHRÁNIT (FO, SJK, ŽDP) SPECIFIKA (STP, ZP, ŽDP)** – Chrání opatření zabezpečení IT naše systémy, nebo vytvářejí více problémů?
- **KONTROLA A HODNOCENÍ IKB** – děláme to dobře?

INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOST V OT
NENÍ OTÁZKOU JESTLI, ALE KDY?

- 1982 – Plynovod, Sibiř (Rusko) malware v OT systémech.
- 2003 – Slammer (Internet).
- 2010 – Stuxnet (Írán).
- 2011 – Flame (Írán, Rusko, Rakousko, Maďarsko).
- 2012 – Shamoon (Vyřazeno 30 000 PC Saudi Aramco).
- 2014 – Dragonfly – Energetic Bear (Vznik ruské skupiny zaměřené na ICS).
- 2015 – BlackEnergy (Ukrajina – útok na rozvodnou síť).
- 2016 – Industroyer (Ukrajina – polovina Kyjeva a pětina bez elektřiny).
- 2017 – Trisis/Triton (Saúdská Arábie – vypnutí bezpečnostních systémů).
- 2018 – Grey Energy útok na energetický průmysl (Ukrajina)
- 2019 – Nuclear Power Corporation of India Limited (Kudankulam infikované PC) malware.
- 2019 – Korea Hydro & Nuclear Power
- 2019 – Natanzu (Írán)
- 2020 – SolarWinds (Vektor útoku na 300 000 zákazníků firmy 18 000 institucí) malware.

INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOST V OT
NENÍ OTÁZKOU JESTLI, ALE KDY?

- 2020 – Fakultní nemocnice Brno (CZ - ransomware).
- 2020 – Nemocnice Benešov (CZ - ransomware).
- 2021 – Colonial Pipeline, oblast 11 500 000 obyvatel, 65% pump mimo provoz ransomware.
- 2021 – Metsamor NPP (Arménie - data leak).
- 2021 – Iranian Railways (Írán - nefunkční systém řízení jízdních řádů a vydávání jízdenek) nefunkční benzínové pumpy.
- 2022 – Ředitelství silnic a dálnic (CZ - ransomware)
- 2022 – opakovaně vyřazené sítě mobilních operátorů (CZ - DoS)
- 2022 – ÚJV Řež (CZ – ransomware / data leak).
- 2022 – Europarlament (EU - DoS)
- 2022 – řetězec obchodů Makro (CZ - ransomware)
- 2022 – Guardian Media Group (GB - ransomare)
- 2023 – Royal Mail Group (GB - ransomware)
- 2023 – Sodexo Pass Česká republika (CZ)
- 2024 – Kdo bude další?…



INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOST V OT
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.

Malwarový útok na jadernou elektrárnu Kudankulam (KKNPP) v indickém státě Tamilnádu

- Vyšetřování indického ministerstva pro atomovou energii odhalilo, že uživatel připojil osobní počítač infikovaný malwarem k IT síti elektrárny.
- Podle NPCIL jsou provozní sítě (OT) v Kudankulamu – ty, které řídí reaktory elektrárny o výkonu 1 000 megawattů – zcela odděleny od administrativních (IT) systémů. Bylo však odcizeno velké množství dat z administrativní sítě KKNPP.
- Organizace ani země, která za útoky stojí, nebyla určena.

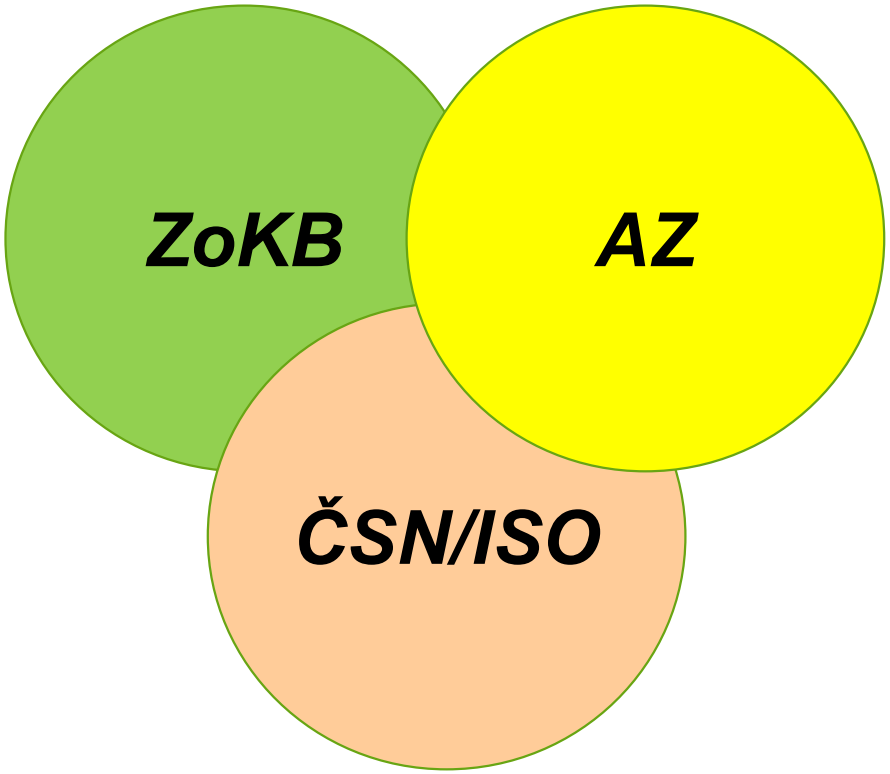
Útok na společnost Korea Hydro & Nuclear Power, která zajišťuje až 30 % dodávek energie v zemi.

- Došlo k úniku dat, která ovšem podle vyjádření společnosti nepatřila mezi klíčová. Informace však mohou být cenné při plánování dalšího útoku.

Útok na největší íránské zařízení na obohacování uranu v Natanzu

- Předpokládá se, že byl proveden Izraelem – útok způsobil výpadek napájení.

ZÁSADNÍ LEGISLATIVA A NORMY PRO IKB V JE



LEGISLATIVA V OBLASTI KYBERNETICKÉ BEZPEČNOSTI V JE

- ISO/IEC 27000:2018 – Information technology – Security techniques - Information security management systems
- ISO/IEC 27001:2022 – ISMS Information security, cybersecurity and privacy protection – ISMS Requirements
- ISO/IEC 27002:2022 – Information security, cybersecurity and privacy protection - Information security controls
- ISO/IEC 27005:2022 – Information security, cybersecurity and privacy protection - Guidance on managing information security risks

- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a změně souvisejících zákonů (ZKB)
- Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti).

- Zákon č. 263/2016 Sb., atomový zákon, § 163 povinnosti držitele povolení v oblasti zabezpečení jaderného zařízení a jaderného materiálu
- Vyhláška č. 361/2016 Sb., o zabezpečení jaderného zařízení a jaderného materiálu, §19 Zabezpečení počítačových systémů, §28 odst. 3e3, - plán zajištění počítačového zabezpečení(Tvorba PZPZ)

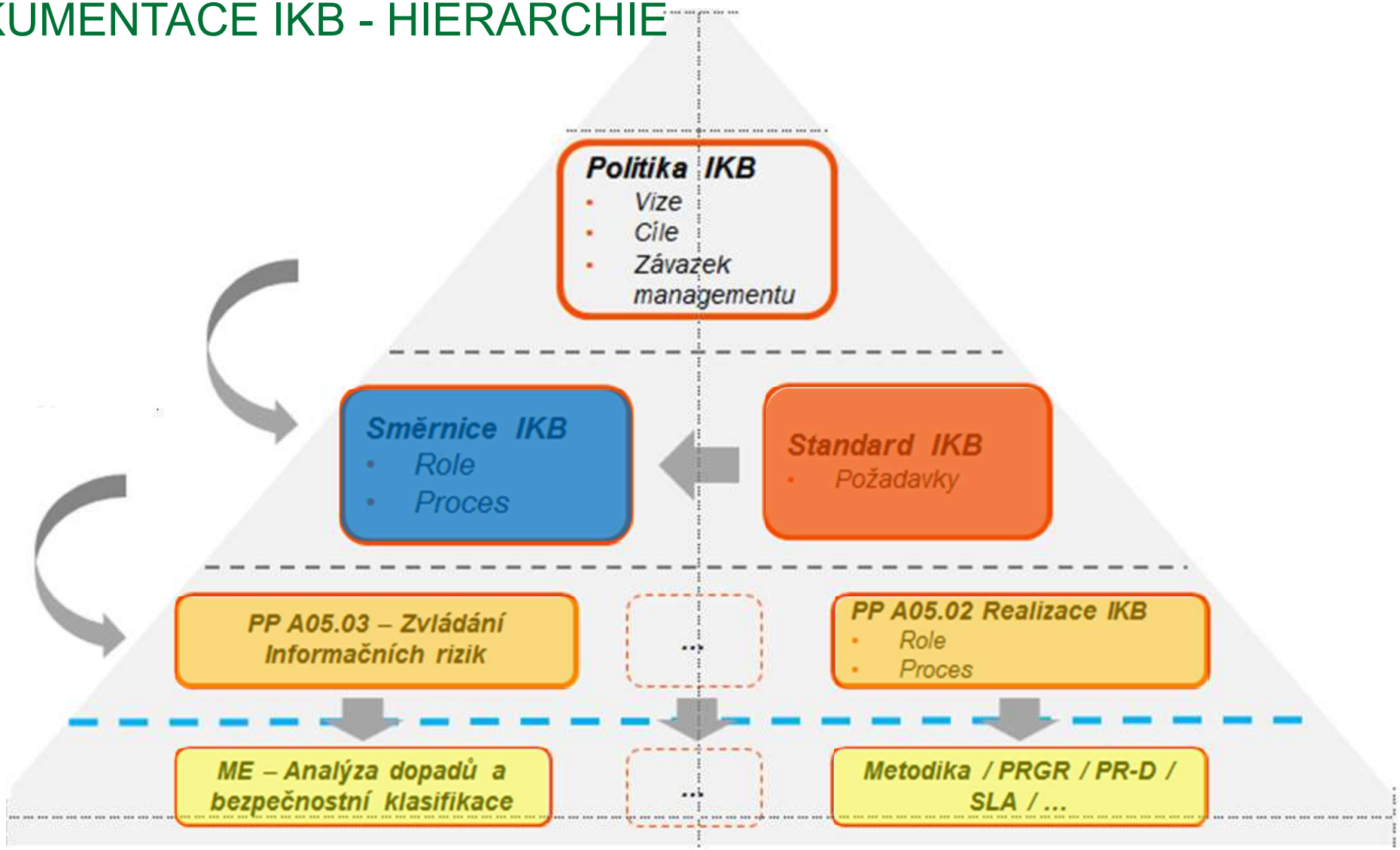
- Standard – Standard Informační a kybernetické bezpečnosti
- Směrnice – Směrnice Informační a kybernetické bezpečnosti
- Postup - Řízení inf. rizik a řízení kontinuity činností infomačních aktiv ve SKČ
- Postup - Realizace informační a kybernetické bezpečnosti v ČEZ, a. s. DJE
- Metodika – Uživatelský manuál IKB
- Metodika - Bezpečnost technologických řídicích a informačních systémů ETE
- Metodika - Bezpečnost technologického řídícího a informačního systému

- Návod IAEA NSS No.17 Computer Security at Nuclear Facilities
- NRC RG 5.71 Cyber Security Programs for Nuclear Facilities

- EPRI 1019187 Technical Guideline for Cyber Security Requirements and Life Cycle Implementation Guidelines for Nuclear Plant Digital Systems

DOKUMENTACE IKB - HIERARCHIE

Program - Systém řízení informační a kybernetické bezpečnosti
(popisuje celý systém řízení bezpečnosti informací – rozsah ISMS)



POVINNOSTI VYCHÁZEJÍCÍ Z LEGISLATIVY
DLE ZKB

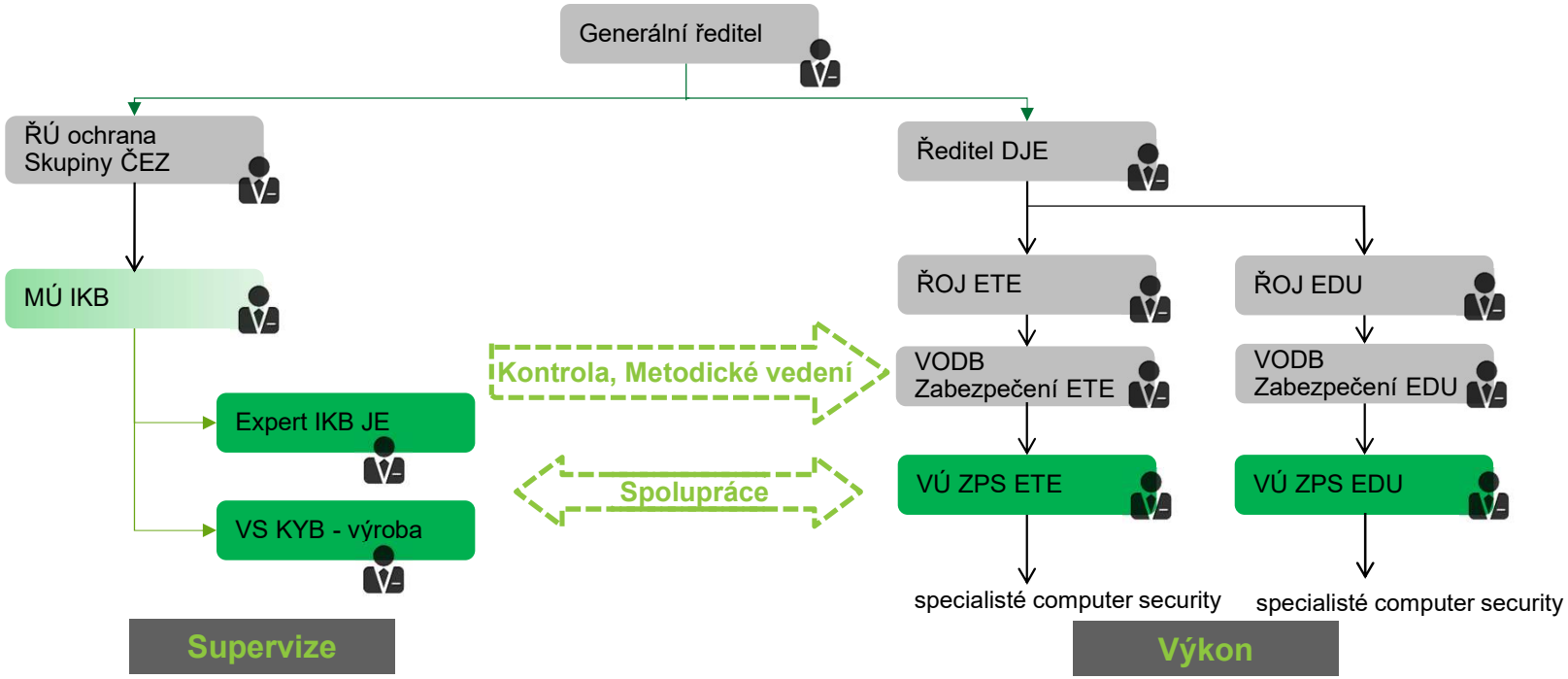
Organizační opatření

- Systém řízení bezpečnosti informací
- Řízení rizik
- Bezpečnostní politika
- Organizační bezpečnost
- Stanovení bezpečnostních požadavků pro dodavatele
- Řízení aktiv
- Bezpečnost lidských zdrojů
- Řízení provozu a komunikací
- Řízení přístupu a bezpečné chování uživatelů
- Akvizice, vývoj a údržba
- Zvládání kybernetických bezpečnostních událostí a incidentů
- Řízení kontinuity činností
- Kontrola a audit

Technická opatření

- Fyzická bezpečnost
- Nástroj pro ochranu integrity komunikačních sítí
- Nástroj pro ověřování identity uživatelů
- Nástroj pro řízení přístupových oprávnění
- Nástroj pro ochranu před škodlivým kódem
- Nástroj pro zaznamenávání činností KII a VIS, jejich uživatelů a administrátorů
- Nástroj pro detekci kybernetických bezpečnostních událostí
- Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí
- Aplikační bezpečnost
- Kryptografické prostředky
- Nástroj pro zajišťování úrovně dostupnosti
- Bezpečnost průmyslových a řídicích systémů

ORGANIZACE BEZPEČNOSTI
INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOST V DJE



ŘÚ – ředitel útvaru MÚ – manažer útvaru ŘOJ – ředitel organizační jednotky VODB – vedoucí odboru VÚ – vedoucí útvaru
ZPS – zabezpečení počítačových systémů VS – vedoucí skupiny KYB – kybernetická bezpečnost

INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOST PRINCIPY ŘÍZENÍ IKB

Informační a kybernetická bezpečnost:

- je **odpovědnostní každého pracovníka** 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.

ZÁKLADNÍ INFORMACE Z OBLASTI IKB PRO ZAMĚSTNANCE

Každý pracovník nese odpovědnost za to, jak se chová k informacím a souvisejícím informačním aktivům společnosti Skupiny ČEZ, k nimž získá přístup.

- **Bezpečné zacházení s informacemi** (klasifikace informací)
- **Dodržování bezpečnostních zásad** při užívání služeb a ICT/ICS techniky
- **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.

UPLATNĚNÍ RESTRIKČNÍCH A SANKČNÍCH OPATŘENÍ V JE

Restrikční a sankční opatření (omezení činností a pokuty) jsou součástí spravedlivé kultury, uplatňované v jaderném průmyslu, kdy za neúmyslné chyby netrestáme a uplatňujeme politiku netrestání (blame free culture), ale za zjevné a úmyslné porušení pravidel udělujeme sankce a omezujeme činnosti.

Uplatňování Restrikční a sankční opatření je řízené řídící dokumentací a z ní vycházejí následné sankce v oblasti IKB:

Za porušení pracovních povinností je považováno:	Sankční opatření
Nedodržení interních předpisů ČEZ, a. s., pro práci s výpočetní technikou z pohledu informační a kybernetické bezpečnosti	**5000 Kč**
Neoprávněná manipulace s výpočetní technikou dle interních předpisů ČEZ z pohledu informační a kybernetické bezpečnosti, jak je popsáno v ČEZ_PChD_0001;	**20 000 Kč**
Neoprávněná manipulace s daty a informacemi ČEZ, a. s., (schéma o infrastruktuře, popis algoritmů, databáze signálů, dokumentace o popisu řídicích systémů apod.) z pohledu informační a kybernetické bezpečnosti;	**20 000 Kč**
Způsobení bezpečnostního incidentu dle řídicí dokumentace ČEZ, a. s., nebo způsobení bezpečnostního incidentu (dle definice vyhlášky č. 82/2018 Sb., v platném znění) majícího za následek nutnost provádění nápravných činností a opatření.	**50 000 Kč**

SYSTÉMOVÉ BEZPEČNOSTNÍ POLITIKY
SÍŤOVÁ ARCHITEKTURA

- Definice bezpečnostních zón.
- Definice pravidel pro přenos informací do jiné bezpečnostní zóny:
  - Bezpečnostní systémy jsou důsledně izolované, komunikace do nižší bezpečnostní zóny musí být technicky omezena na jednosměrnou směrem ven, např. pomocí datových diod, DHG apod.
  - Systémy s vlivem na bezpečnost jsou důsledně oddělené, komunikace směrem do nižší bezpečnostní zóny je jednosměrná, přístupy dovnitř jsou přísně kontrolovány, pokud existují. Řízení na úrovni FW, datových diod, DHG apod.
  - Nižší technologické bezpečnostní zóny jsou přísně oddělené zejména od korporátní sítě a Internetu, využívá se DMZ. Komunikace řízena na úrovni FW.

SYSTÉMOVÉ BEZPEČNOSTNÍ POLITIKY
PŘENOSNÁ MÉDIA

Pravidla pro používání přenosných médií:

- Používat se smí pouze **evidovaná** přenosná média a zařízení.
- Přenosná média evidována k Technologickým řídícím informačním systémům (dále jen TŘIS) se **nesmí připojovat k internetu.**
- Je zakázáno používat přenosná media, pro jiný systém, než na který jsou evidována.
- Evidovaná média dodavatelů je nutné před připojením do TŘIS **prověřit** na škodlivý kód.
- Přenosná média připojovat do TŘIS pouze na k tomu **určeném a v provozní dokumentaci popsaném místě.**
- V případě ztráty přenosného média musí být informován správce TŘIS ke kterému je přenosné zařízení evidováno.
- Je zakázáno měnit přidělené jméno i jakýkoliv jiný evidovaný parametr přenosného média.
- Připojovaná zařízení musí splňovat systémovou bezpečnostní politiku SKČ.
- Používat personifikované autentizační údaje, nevyužívat admin účet pro běžnou práci (výjimkou na personifikované účty je stálá směna).
- Zpracovávaná data a informace společností SKČ na zařízení se musí chránit v souladu s jejich bezpečnostní klasifikací.
- Pokud tyto zásady z historických důvodů nejsou dodrženy, je třeba je aplikovat v rámci změnových řízení.
- Evidence médií, likvidace paměťových zařízení a médií, přeprava, manipulace, popis procesu v řídící dokumentaci.

PRIMÁRNÍ A PODPŮRNÁ AKTIVA KII

Na základě výše uvedených požadavků určil Národní úřad pro kybernetickou a informační bezpečnost pro ČEZ, a. s., v divizi Jaderná energetika pro organizační jednotky EDU a ETE opatřením obecné povahy (OOP), číslo jednací 2947/2019-NÚKIB-E/350 ze dne 4. 11. 2019, tři prvky kritické informační infrastruktury (KII). Jejich popis je uveden viz Tabulka 1. OOP nabylo účinnosti dne 19. 11. 2019.

Název prvku KII v OOP	Popis
KII ČEZ EDU 01 KII ČEZ ETE 01	Jedná se o informační a komunikační systém, který slouží k řízení a regulaci procesu výroby tepelné a elektrické energie v rámci jaderné elektrárny Dukovany.
KII ČEZ EDU 02 KII ČEZ ETE 02	Jedná se o informační a komunikační systém slouží k zajištění jaderné bezpečnosti jaderné elektrárny Dukovany.
KII ČEZ EDU 03 KII ČEZ ETE 03	Jedná se o Technický systém fyzické ochrany (TSFO) nezbytný k řízení fyzické ochrany jaderné elektrárny Dukovany.

Práce na 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.
- Dodržovat pravidla a podmínky dle provozního předpisu.

ORGANIZACE BEZPEČNOSTI
INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOST V DJE

Implementace informační a kybernetické bezpečnosti ve změnových řízeních u projektů na elektrárně. Požadavky z oblasti informační bezpečnosti v záměrech projektu v oblastech (Architektura, Ochrana do hloubky, Hardening, Ochrana proti malware, Bezpečnost komunikací, Řízení přístupu, Zálohování (systémů, funkcí, dat, redundance, diversita), bezpečnostní monitoring - správa logů , provozní diagnostika)

Ověřování IKB

Bezpečnostní klasifikace, kontroly shody, interní audity - v rámci těchto kontrol je ověřována míra plnění požadavků informační a kybernetické bezpečnosti stanovená v řídící dokumentaci informační a kybernetické bezpečnosti

- je realizovaná formou interview s garantem aktiva na elektrárně
- závěry/ nálezy jsou využity:
  - ke stanovení bezpečnostní klasifikace daného aktiva (systému)
  - slouží jako vstup do analýzy rizik
  - návrhu nápravných opatření pro minimalizaci rizik zjištěných v procesu ověřování IKB

ŘÍZENÍ RIZIK V DJE

Analýza rizik

- Definovaná NO
- Záznam do SNAP
- Implementační plán

Kontrola shody s ISO 27001, 27002, ZoKB

- Definovaná NO
- Záznam do Teams

ŘÍZENÍ RIZIK V RÁMCI CHANGE MANAGEMENTU

- Nákupní požadavek – již v nákupním košíku identifikace dopadů na IKB (zejména prvky KII, soulad s požadavky IKB - VP A, G, H a J ke Standardu)
- Významné změny a významní dodavatelé
- Řízení změn: Tipom – SW nástroj
  - Posouzení záměru projektu, návrh bezpečnostních požadavků architektem IKB
  - Posouzení návrhu architektury, posouzení dokumentace (Analýza rizik, dotazník IKB)
  - Testování změn z pohledu bezpečnosti, naplnění bezpečnostních požadavků, kontrola shody, hardening, zranitelnosti,
    - [vývojové a testovací prostředí oddělené], bezpečnost testovacích dat, předávání dodavateli, přístupy dodavatele po dobu realizace změny
    - Řízený přenos změn do produkčního prostředí.
    - Bezpečnost testovacích dat – předávání dodavateli
- Kontroly dodavatelů z pohledu IKB
- Hodnocení dodavatelů

BEZPEČNOSTNÍ POŽADAVKY NA DODAVATELE

Spolupráce s centrálním nákupem – prosazení bezpečnostních požadavků na dodavatele dle Standardu:

- VP H - Bezpečnostní požadavky pro dodávky kritické informační infrastruktury
- VP A - Bezpečnostní požadavky pro dodávky standardních systémů a technologií
- VP G - Seznam požadavků na dodavatele a poskytovatele služeb pro smlouvy na údržbu
- VP J - Bezpečnostní požadavky na konzultační a poradenskou činnost

VP součástí smlouvy s dodavatelem

Školení dodavatelů

- VP I (Standardu) – Pravidla CYBEX
- V rámci vstupního a opakovaného školení (pro zaměstnance i vedoucí pracovníky), stránky pro dodavatele, řídící dokumentace –Pravidla chování dodavatele JE

Audit dodavatelů

- Dle VP A a H má ČEZ právo na audit IKB u dodavatele, zajištění je v odpovědnosti Garanta aktiva, IKB spolupracuje

BEZPEČNOSTNÍ POŽADAVKY NA DODAVATELE - KONTROLA

V rámci řízení rizik dodavatelů dochází v průběhu roku k:

- Kontrola dodavatelů při výkonu činností na EDU / ETE dle nastavených parametrů v řídící dokumentaci
- Posouzení plnění požadavků IKB v průběhu prací i po převzetí díla
- Audit dodavatelů – zabývající se plněním požadavků IKB (ČSN ISO/IEC 27001) v rámci firemního prostředí
- Analýza rizik dodavatelů – která je součástí Auditu, zaměřuje se na konkrétní body dle „Dotazník k hodnocení rizik s dopady do Informační a kybernetické bezpečnosti“ odpovídající požadavkům ČSN ISO/IEC 27001
- Účast IKB na jednotném systému hodnocení dodavatelů (JSHD) – přizvaní experti za oblast IKB

BEZPEČNOST LIDSKÝCH ZDROJŮ
VZDĚLÁVÁNÍ UŽIVATELŮ

Vzdělávání zaměstnanců

1. E-learning IKB - 1. úroveň – plošně na všechny zaměstnance Koncernu ČEZ
2. E-learning IKB - 2. úroveň – na zaměstnance pracující s prvky KII
3. Expertní školení IKB – pro administrátory TŘIS (včetně KII prvků), techniky, osoby zastávající bezpečnostní role (včetně IKB), garanty aktiva
4. Expertní školení IKB – pro zaměstnance útvarů IKB (Kybernetický polygon -KYPO MU Brno,..)

Vzdělávání dodavatelů

DJE:

- Školení IKB v rámci školicích dní – vstupní, periodické, pro vedoucí pracovníky
- Dodatečné školení IKB pro Vedoucí práce a přípraváře
- Materiály dodány IKB
- Zajišťuje Centrum Přípravy personálu (CPP) Brno(školící dny) a zaměstnanci IKB (školení pro vedoucí práce a přípraváře)

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**
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 svému nadřízenému jakýkoli nestandardní stav, který by mohl vést k bezpečnostní události! Využijte nástroj který vaše společnost na hlášení využívá (např. SNAP/ServiceDesku atp.

ZVLÁDÁNÍ BEZPEČNOSTNÍCH INCIDENTŮ

Dokumentace:

- Zajištění procesu Security Incident Management
- Security Incident Management
- Zajištění procesu Security Incident Management v DJE

Popisuje zvládání kybernetických bezpečnostních událostí a incidentů (KBU/KBI) a reakce na reaktivní a ochranná opatření.
Na elektrárně se systematicky sledují události v provozu (analýza chování provozního personálu, dostupnost funkcí bezpečnostních, řídících a informačních systémů), které mají potenciál KBU nebo KBI z nástrojů jako jsou provozní deníky, SNAP, SD. Jsou navržena nápravná opatření pro eliminaci budoucího výskytu. Zaznamenané události /incidenty evidovány v měsíční zprávě o stavu elektrárny.
Kdokoliv (nejen provozní personál) je oprávněn zaznamenat neshodu do SD, SNAPa kybernetická bezpečnost se tím bude zabývat.

Co zaznamenávat?
Ztráty flash disků, otevřené dveře do místnosti SKŘ, neuzamčená pracovní plocha na pracovních stanicích, vložená média do neobsluhovaných stanic, připojená zařízení či média a instalovaný SW v rozporu s projektem, nepřítomnost obsluhy, zneužití oprávnění...

IDENTIFIKACE KBU/KBI V TECHNOLOGII
ZNAKY POTENCIÁLNÍCH KYBERNETICKÝCH ÚTOKŮ NA TS

- Identifikováno chování v SW prostředí, nebo technologie bez zjevného podnětu (ŘiS, operátor, servis).
  - Neovladatelné povely z periferií (myš, klávesnice, TrackBall).
  - Výzva, nebo neidentifikovatelný stav v SW prostředí bez zjevné příčiny.
  - Spouštění zařízení v technologii bez zjevné příčiny.

- Neidentifikovatelný HW, paměťové médium (PC, NB, USB, Router, Modem…) v technologickém systému.

- Anonym (zobrazení na monitoru, email, jiné oznámení bezpečnostního charakteru).

- Neovladatelné povely z periferií (myš, klávesnice).
- Samovolně se otvírají okna.
- Výzva, nebo neidentifikovatelný stav technologie bez zjevné příčiny.
- Změny stavu zařízení v technologii bez zjevné příčiny.
- Neidentifikovatelný HW, paměťové médium (PC, NB, USB, Router, Modem…) v TS.
- …a další nestandardní chování

Vždy v první řadě je povinnost oznámit hrozbu Směnovému Inženýrovi.

IDENTIFIKACE KBU/KBI V TECHNOLOGII
KYBERNETICKÁ BEZPEČNOSTNÍ UDÁLOSTI V DJE (2020)

Identifikováno připojené zařízení v technologii.
- Zjištěn diagnostický HW dodavatelské firmy.
- Připojen 4G modem k dodavatelské síti.
- V rozporu s pravidly IKB.

Identifikováno neznáme připojené zařízení na technologickém systému.
- Zjištěn diagnostický HW dodavatelské firmy.
- Bez vědomí systémového správce technologie.
- NB připojeno přes 4G modem k dodavatelské síti.
- V rozporu s pravidly IKB.

✓ **Jednalo se o potenciální bezpečnostní hrozby**
✓ **Postup dle řídící dokumentace a Zásahové instrukce**

POŽADAVEK LEGISLATIVY - FYZICKÁ OCHRANA JE

- Bezpečnostní zóny, kontroly vstupu, evidence klíčů, kontroly otevření dveří, kamery, místní provozní předpisy – pravidla chování v bezpečnostních zónách.
- Identifikační karta (vydání IK přes výdejnu – povolení, školení, bezúhonnost).
- Při vstupu do střeženého prostoru (STP) doplněno biometrickou kontrolou (ruka, prst).
- Na dalších turniketech doplněno o PIN.
- Na dveřních uzávěrech doplněno o

  přidělený klíč (např. objekty DGS, čerpací stanice,…).
- Zádržné mechanismy: Turniket, dveře.

FYZICKÁ OCHRANA
SJK – SYSTÉM JEDNOTNÉHO KLÍČE

- Evidence klíčů – viz řídící dokumentace - Zajišťování plnění bezpečnostních požadavků FO JZ a JM.

- **Systém jednotného klíče** (klíčové hospodářství) FO EDU, ETE zahrnuje evidenci, úschovu, ochranu a pohyb klíčů od vstupů do objektů a místností ve vymezených prostorech střežených prostředky TSFO. Jedná se o průchody přes bariéry FO, vstupy do objektů chráněných TSFO a kontrolované vstupy do vybraných objektů a místností důležitých z hlediska ochrany JZ a JM.
- Klíčové hospodářství zahrnuje pro výše uvedené objekty a vstupy v SJK, který se skládá ze dvou samostatných skupin klíčů určené pro místnosti s technologií TSFO a pro vybrané objekty a provozní technologické prostory.
- Systém završuje **„generální“ klíč**, který umožňuje **oprávněným osobám** přístup do všech objektů uzamčených zámky systému jednotného klíče.

Součástí klíčového hospodářství FO je i nakládání s klíči od prostorů nepodléhajících kontrole vstupu systémem TSFO a klíči od skříněk pro ukládání zavazadel.

FYZICKÁ OCHRANA
ŽIVOTNĚ DŮLEŽITÉ PROSTORY (ŽDP) - DEFINICE

Vyhláška SÚJB 361/2016 Sb. § 4

„vymezuje se životně důležitý prostor, pokud úmyslné poškození systémů a zařízení důležitých z hlediska jaderné bezpečnosti v tomto prostoru umístěných, může vést buď přímo či nepřímo k radiační havárii……

Zákon 263/2016 Sb. § 162

„za citlivou činnost se považuje vstup bez doprovodu do životně důležitého prostoru……

FYZICKÁ OCHRANA
ŽIVOTNĚ DŮLEŽITÉ PROSTORY (ŽDP) - REŽIMOVÁ OPATŘENÍ

Vyhláška SÚJB 361/2016 Sb. § 12 odst. (4)

„v ŽDP musí být zajištěna současně přítomnost alespoň 2 osob s oprávněním vstupu bez doprovodu……

„tyto 2 osoby musí mít srovnatelnou znalost technologie, která se v daném ŽDP nachází…….

Vyhláška SÚJB 361/2016 Sb. § 10 odst. (4)

„……může umožnit jiné fyzické osobě, ve výjimečných případech vstup do ŽDP s tím, že bude doprovázena osobou s oprávněním doprovodu…….

POŽADAVKY LEGISLATIVY – REPORTY A HODNOCENÍ STAVU

Stav a úroveň zabezpečení, změny a modernizace, které povedou ke zvyšování úrovně zabezpečení, popisuje **utajovaný** dokument „**Komplexní hodnocení zajištění zabezpečení v ČEZ, a.s. JE Dukovany/JE Temelín**“.

Dokument je zpracován na základě legislativních požadavků uvedených v § 22 vyhlášky SÚJB č. 162/2017 Sb., o požadavcích na hodnocení bezpečnosti podle atomového zákona a § 8 odst. 4 vyhlášky č. 21/2017 Sb., o zajišťování jaderné bezpečnosti jaderného zařízení.

HODNOCENÍ STAVU – AUDITY IKB

Interní audity – kontrola ISMS, legislativa, řídící postupy, procesy a dokumentace

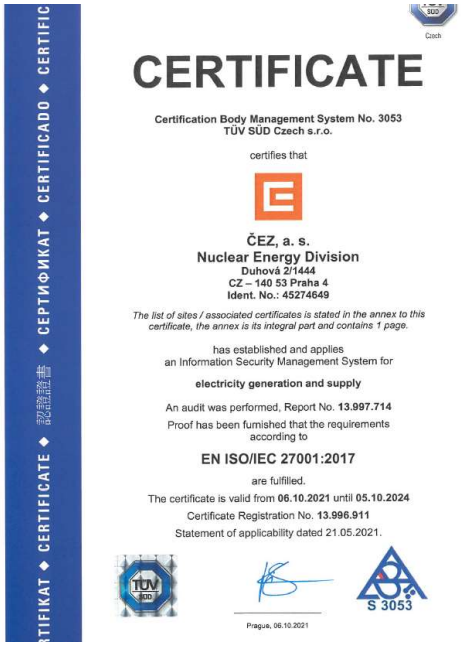
Mezinárodní agentura pro atomovou energii (IAEA - International Atomic Energy Agency) – mise OSART (Operational Safety Review Team)

SÚJB – kontrolní činnost

NUKIB – kontrolní činnost

Externí audity – **TÜV SÜD Czech** – certifikace ISO 27001 v roce 2021,

letos recertifikační audit



CERTIFICATE

Certification Body Management System No. 3053
TÜV SÜD Czech s.r.o.

certifies that

ČEZ, a. s.
Nuclear Energy Division
Duhová 2/1444
CZ – 140 53 Praha 4
Ident. No.: 45274649

The list of sites / associated certificates is stated in the annex to this certificate, the annex is its integral part and contains 1 page.

has established and applies
an Information Security Management System for

electricity generation and supply

An audit was performed, Report No. **13.997.714**
Proof has been furnished that the requirements according to

EN ISO/IEC 27001:2017

are fulfilled.

The certificate is valid from **06.10.2021** until **05.10.2024**
Certificate Registration No. **13.996.911**
Statement of applicability dated 21.05.2021.

Prague, 06.10.2021

S 3053

NA ZÁVĚR

Stíhačky F-35 čelí větším hrozbám kybernetických útoků než nepřátelských raket.

Zdroj: Zajímavé inženýrství ^

Odhaduje se, že do roku 2026 roční celosvětové náklady na počítačovou kriminalitu překročí 20 bilionů dolarů.

Zdroj: Cybersecurity Ventures ^

Svět bude mít letos 3.5 milionu neobsazených pracovních míst v oblasti kybernetické bezpečnosti.

Zdroj: Cybercrime Magazine ^

NA ZÁVĚR

Každý den došlo k 1.7 milionu útoků ransomwaru, což znamená celkem 620 milionů útoků ransomwaru v roce 2023.

Zdroj: Statista ^

Narušení sítě nebo dat je nejvyšší bezpečnostní narušení, které má dopad na odolnost a účty organizace. Tímto způsobem bylo postiženo 51.5 % podniků.

Zdroj: Cisco ^

Více než 90 % malwaru přichází prostřednictvím e-mailu.

Zdroj: CSO Online ^

NA ZÁVĚR

Počet malwarových e-mailů ve 3. čtvrtletí 2023 vzrostl na 52.5 milionu a představoval 217% nárůst ve srovnání se stejným obdobím předchozího roku (24.2 milionu).

Zdroj: Vadesecure ^

Téměř polovina všech kybernetických útoků míří na malé podniky.

Zdroj: Cybint Solution ^

83 % firem bylo v roce 2023 vystaveno phishingu.

Zdroj: Cybertalk ^

NA ZÁVĚR

Podle zprávy „State of the Phish“ společnosti Proofpoint existuje vážný nedostatek povědomí o kybernetické bezpečnosti a školení, které je třeba řešit.

Zdroj: Proofpoint ^

Jeden ze tří zaměstnanců pravděpodobně klikne na podezřelý odkaz nebo e-mail nebo vyhoví podvodnému požadavku.

Zdroj: KnowBe4 ^

ČISTÁ
ENERGIE
ZÍTŘKA

A teď nastává prostor…

… pro Vaše dotazy.