Kybernetická a informační bezpečnost – pro dodavatele

Co je informační a kybernetická bezpečnost?

Informační bezpečnost je ochrana všech informací – ať už jsou v počítači, na papíře nebo v hlavě – před ztrátou, zneužitím, únikem či poškozením.

Zjednodušeně informační bezpečnost znamená:

- že informace se dostanou jen k těm, kdo k nim mají mít přístup,
- že informace zůstávají přesné, úplné a nezměněné,
- že jsou informace k dispozici, když je potřebujeme.

Součástí informační bezpečnosti je **kybernetická bezpečnost** – ochrana všech digitálních zařízení v kybernetickém prostoru, zjednodušeně všeho, co je „připojeno k síti“, tzn. např. počítačů, serverů, mobilních telefonů, aplikací a systémů v nich před útoky, zneužitím či poškozením.

Z pohledu kybernetické bezpečnosti je **nejzranitelnějším článkem v každé firmě zaměstnanec**, který otevře infikovaný soubor nebo klikne na škodlivý odkaz. Proto je důležité:

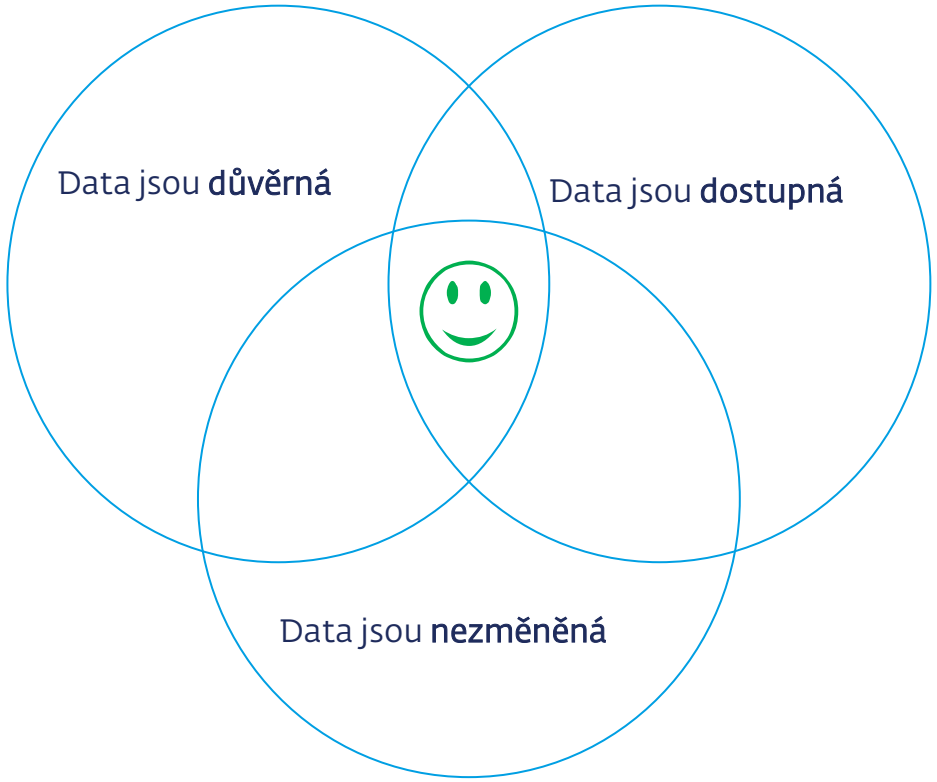
- mít přehled o aktuálních hrozbách,
- být obezřetní a vždy jakoukoli podezřelou aktivitu hlásit.

ČD jako poskytovatel regulované služby dle ZoKB č. 264/2025 Sb.

- Dne 1.11.2025 vešel v účinnost zákon o kybernetické bezpečnosti č. 264/2025 Sb., který zohledňuje požadavky evropské směrnice NIS2 a stanovuje režimy nižších a vyšších povinností pro poskytovatele regulované služby.
- ČD obdržely rozhodnutí o registraci od NÚKIB jako poskytovatele regulované služby v režimu vyšších povinností a musí se řídit požadavky vyhlášky č. 409/2025 Sb.

- Z tohoto důvodu je nutné, aby všichni zaměstnanci dodavatele podílející se na předmětu plnění souvisejícím s regulovanou službou, byli prokazatelně seznámeni s bezpečnostními požadavky ČD a tyto požadavky dodržovali a postupovali v souladu s nimi.

CIA triáda bezpečnosti informací



Důvěrnost (confidentiality) – znamená, že data smí vidět jen ti, kdo k nim mají oprávnění.
Ochrana: šifrování, řízení přístupů, hesla, vícefaktorové ověřování, atd.

Integrita (integrity) – znamená, že data musí být přesná, úplná a nezměněná bez oprávnění.
Ochrana: auditní záznamy změn, digitální podpisy a certifikáty, atd.

Dostupnost (availability) – znamená, že data a systémy musí být přístupné, když je potřebujeme.
Ochrana: redundance, zálohování, atd.

Dodavatel jako součást bezpečnosti regulované služby

- **Dodavatel** není pouze externím partnerem, **je přímou součástí poskytování regulované služby**, protože jeho činnost může ovlivnit kybernetickou bezpečnost.
- Nedodržení bezpečnostních pravidel a standardů může mít dopad na:
  - Dostupnost služby (výpadky, nedostupnost systémů)
  - Integritu (poškození nebo změna dat)
  - Důvěrnost (únik citlivých informací)

Odpovědností dodavatele je zejména:

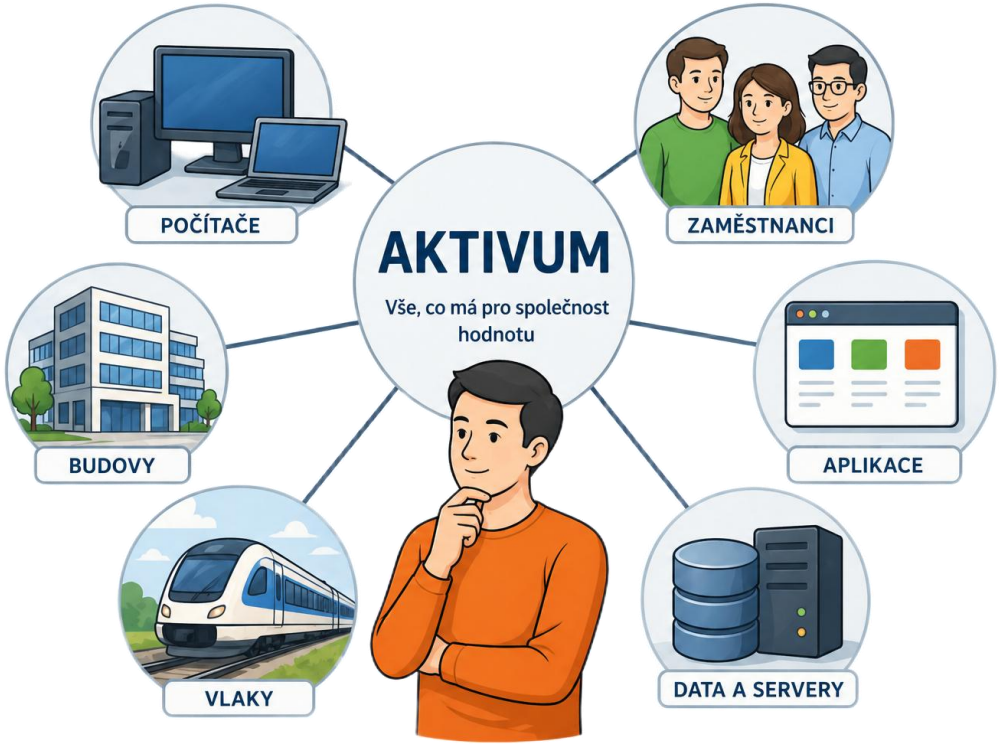
- Dodržovat smluvní a bezpečnostní požadavky ČD
- Řídit se stanovenými bezpečnostními politikami, pravidly a procesy ČD
- Aktivně přispívat k ochraně systémů a dat ČD
- Neprodleně hlásit kybernetické bezpečnostní incidenty

Co znamená informační a kybernetická bezpečnost pro dodavatele

- Jako externí spolupracovník **zodpovídá dodavatel za bezpečnost informací** souvisejících s aktivy společnosti ČD, ke kterým získá přístup, **a je povinen:**
  - postupovat v souladu s platnými a účinnými právními předpisy, zejména pak v souladu s požadavky vyplývajícími pro ČD, jakožto povinnou osobu **v režimu vyšších povinností ze zákona č. 264/2025 Sb., o kybernetické bezpečnosti** a souvisejících předpisů;
  - plnit své řešení/dodávku/správu tak, aby **respektovalo požadavky na bezpečnost ČD, zabránilo kybernetickým bezpečnostním incidentům a krizovým situacím** a **odpovídat za dodávku a implementaci** řešení v požadované kvalitě **i z pohledu bezpečnosti;**
  - zajistit adekvátní dodržování těchto bezpečnostních pravidel rovněž svými **subdodavateli.**
- Nedodržení zásad nebo porušení informační a kybernetické bezpečnosti může být posuzováno jako porušení povinností dodavatele ujednaných ve smlouvě.

Co je aktivum v kybernetické bezpečnosti

- Aktivum je **cokoli, co má pro společnost hodnotu** a je nutné zajistit jeho dostupnost, důvěrnost a integritu.
- Může jít o hmotné či nehmotné, technologické, informační, lidské nebo smluvní prvky, které mohou být ohroženy bezpečnostními incidenty a jejichž kompromitace může mít negativní dopady na obchodní činnost společnosti či reputaci.
- Správné řízení aktiv je základním stavebním kamenem pro ochranu regulované služby proti kybernetickým hrozbám a zajištění kontinuity obchodních činností ČD v případě incidentu.



Obrázek: vlastní tvorba pomocí online nástroje ChatGPT

Základní bezpečnostní zásady – přístupová oprávnění

1. Každý zaměstnanec dodavatele podílející se na plnění smlouvy **musí mít veden jedinečný uživatelský účet s přiřazenými specifickými rolemi pro určené systémy**, a to:
   - **v rámci své IT infrastruktury**
   - **i v rámci IT infrastruktury ČD.**
2. Zaměstnanci dodavatele jsou povinni v IT infrastruktuře ČD **využívat uživatelská oprávnění jen po dobu nezbytně nutnou** pro vykonání činnosti související výhradně s plněním smlouvy.
3. Zaměstnanci dodavatele **musí používat silná a originální hesla** a své přihlašovací údaje adekvátně chránit a **s nikým je nesdílet**.
4. Pokud je to možné, používají zaměstnanci dodavatele **pro ověření přihlášení vícefaktorovou autentizaci**.
5. Zaměstnanci dodavatele **nesmí používat jakékoli sdílené účty**.
6. Při opuštění pracovní stanice musí zaměstnanci dodavatele **uzamknout své zařízení**.
7. V případě **ztráty nebo při podezření na únik přihlašovacích údajů k IT infrastruktuře ČD hlásí** zaměstnanec dodavatele tuto **událost okamžitě** kontaktním osobám ČD.

Základní bezpečnostní zásady – přístup do interních systémů ČD

1. Zaměstnanci dodavatele **přistupují pouze k systémům a informacím ČD, které přímo souvisí s plněním smlouvy a byly takto specifikovány v NDA. Je zakázáno přistupovat k jakýmkoli jiným interním systémům a informacím ČD.**
2. **Z externí sítě přistupují** zaměstnanci dodavatele k systémům a infrastruktuře ČD **výhradně přes zabezpečené a schválené připojení přes VPN.**
3. **Při využití externího zařízení musí mít toto zařízení aplikovány bezpečnostní záplaty a nainstalovanou, spuštěnou a aktualizovanou antivirovou ochranu.**
4. Je **zakázáno** provádět jakékoli **neoprávněné změny konfigurací interních systémů ČD či obcházet bezpečnostní kontroly.**
5. Je **zakázáno** provádět jakékoli **instalace software na svěřeném zařízení bez schválení ČD.**

Jak si vytvořit originální a silné heslo?

- Minimální délka by měla být alespoň **12 znaků**.
- Použijte malá a velká písmena, číslice a speciální znak.
- Vyhýbejte se použití písmen s háčky nebo čárkami.
- Místo slov **použijte frázi nebo celou větu**, kterou si snadno zapamatujete.
- **Nepoužívejte hesla spojovaná s vaší osobou** jako je vaše jméno, datum narození, jména vašich rodinných příslušníků nebo mazlíčků, apod.
- **Nepoužívejte komplikované znaky, které se špatně pamatují.**
- Nepoužívejte ani informace, které máte veřejně dostupné na sociálních sítích.
- Některá písmena můžou být nahrazeny čísly, symboly či speciálními znaky (např. a=@, E=3, v=w, o=0).

Příklady možných silných hesel

- KazdyDenVypiju2Kavy& 1Caj
- HodinkyUkazuji16&TakJduDomu!
- VRybnickuPlavalo5KapruA2Kachny!
- NaOblozeJsou2Letadla.
- Ranov6SiDamK@fe!
- Ranov6SiDamK@fe!FB

- Pro různé služby a účty můžete používat heslo, k němuž jednoduše přidáte znaky odpovídající dané službě nebo účtu např. e-mail, Facebook.
- **Tam, kde je to možné, používejte vícefaktorové ověření.**

Základní pravidla pro manipulaci s heslem

- Hesla uchovávejte v tajnosti a nikdy je nikomu nesdělujte (kolegovi, nadřízenému, ani pracovníkům IT služby).Při podezření na vyzrazení hesla ho ihned změňte a událost nahlaste.
- Vždy, když ukončujete práci v aplikaci nebo v prostředí Internetu, se nezapomeňte odhlásit z účtu, který právě používáte.
- Vždy změňte výchozí heslo po prvním přihlášení. Změna i zadání hesla by měla být prováděna tak, aby heslo nemohlo být odečteno, například pohledem přes rameno.
- Nelepte si poblíž počítače hesla napsaná na papír.
- Neukládejte hesla do prohlížečů a nepoznamenávejte si je poblíž počítače.
- Nepoužívejte stejná hesla pro různé služby.

Jaká jsou nevhodná hesla a co je tedy špatně?

1. **Často jsou používána nevhodná hesla složená z běžně používaných slov.** Útočníci mají vytvořený seznam těchto hesel tzv. hesel ze slovníku.

Zadejte heslo:	vlacek

Zadejte heslo:	nevim

Nejčastěji používaná hesla v ČR v roce 2025

1) Heslo1234
2) admin
3) 123456
4) qwert1234
5) Automaty123
6) 123456789
7) Pokus123
8) 12345678
9) qwert123
10) michal

2. Často používáme nevhodná hesla spojovaná s naší osobou (mohou být snadno uhodnutelná).

- Jméno (uživatele, potomka, manžela, zvířátka).
- Data a místa (narození, svatba, škola).
- Předměty z blízkého okolí (lampička, pendolino).
- Spojení s naším životním stylem (kniha, emoce, seriál, superhrdina).
- Po sobě jdoucí nebo opakující se znaky

(například AAA, abcefgh, 1234567).

3. **Hesla k různým aplikacím máme stejná.**
4. **Hesla nejsou měněna.**

Klasifikace a ochrana informací

- Informace ve společnosti ČD se dělí na **Veřejné, Interní, Interní – Citlivé a ČD Důvěrné**.
- Zaměstnanci dodavatele **musí při práci s informacemi ČD dodržovat tuto klasifikaci a informace, ke kterým získají přístup dle NDA, náležitě chránit.**
- Informace a data ČD nesmí být ukládána na soukromá zařízení nebo neautorizovaná cloudová úložiště.
- Citlivé informace mohou být přenášeny pouze schválenými zabezpečenými kanály.

Označení informací	Ochrana informace
Veřejné	Informace jsou veřejně přístupné nebo určené ke zveřejnění. Prozrazení nezpůsobuje žádné škody.
Interní	Informace **nejsou** veřejně přístupné a tvoří know-how ČD. Prozrazení způsobí menší obtíže.
Interní - Citlivé	Informace **nejsou** veřejně přístupné a jejich ochranu vyžadují právní předpisy, jiné předpisy či smluvní ujednání. Prozrazení má významný krátkodobý dopad na provozní činnost.
ČD - Důvěrné	Informace **nejsou** veřejně přístupné. Jedná se o nejcennější know-how ČD, které vyžaduje mimořádnou ochranu. Prozrazení má vážný dopad na dlouhodobé strategické cíle.

Klasifikace informací – PCI DSS

- ČD zpracovávají a přijímají platby platebními kartami, a proto jsou **povinné splňovat požadavky standardu PCI DSS** (= Payment Card Industry Data Security Standard, Standard zabezpečení dat v odvětví platebních karet).
- Z toho vyplývá, že musí chránit data držitelů karet a citlivé autentizační údaje svých zákazníků.

- To znamená, že ČD **nesmí ukládat plné číslo platební karty (PAN), jména držitelů karet, service code, datum ukončení platnosti, ani data z magnetického proužku či ekvivalentní data** obsažená v čipu nebo jinde po autorizaci transakce.

Pokud má zaměstnanec dodavatele podezření nebo zjistí, že se v systému, e-mailu, dokumentu nebo jiné komunikaci nachází číslo platební karty nebo jiné karetní údaje výše uvedené, nesmí tyto údaje za žádných okolností šířit jakoukoli formou dál a je povinen tuto skutečnost okamžitě nahlásit příslušným kontaktním osobám v ČD.

Sociální inženýrství jako nejběžnější typ útoku

SOCIÁLNÍ INŽENÝRSTVÍ je nejběžnější typ útoku, se kterým se můžeme v kybernetickém prostoru setkat.

Jde o manipulaci s lidmi za účelem získání citlivých informací nebo přístupu k informačním systémům.

Phishing – je technika sociálního inženýrství, kterou se útočník snaží získat přístup k důvěrným informacím, nejčastěji k přihlašovacím údajům.

Název pochází z angličtiny a můžeme ho přeložit jako „rybaření“. Technika totiž spočívá v tom, že útočník nahodí udici a čeká, která ryba se chytí. Útočník se také může zaměřit na konkrétní osobu či skupinu osob. V takovém případě mluvíme o **Spear-phishingu**, který je hůře rozpoznatelný a v současné době je jeho výskyt stále častější.

Smishing – je typ phishingu zasílaný přes SMS (případně zprávy na Messengeru, WhatsAppu a dalších aplikacích), který se často maskuje za oficiální sdělení známé instituce, například doručovací služby. Podobně jako u phishingu i zde je na oběť vyvíjen tlak za účelem kliknutí na odkaz a zadání citlivých údajů.

Jak se chránit před phishingem a smishingem?

1. Ověřujte si správnost adresy odesílatele e-mailu či zprávy jiným komunikačním kanálem, např. telefonicky.
2. **Neklikejte na podezřelé webové odkazy v e-mailu či zprávě** (skutečnou adresu, na kterou odkaz vede, můžete zobrazit po umístění kurzoru myši bez klikání na odkaz).
3. **Neotvírejte přílohy v podezřelých e-mailech, které jste neočekávali. Nepovolujte makra**.
4. **Neměňte heslo** prostřednictvím odkazu v podezřelém e-mailu, pokud jste k tomu vyzváni.
5. **Nesdělujte nikomu jakékoliv citlivé či osobní údaje**, jsou-li vyžadovány neoprávněně/nestandardně.

Nejčastější hrozby - Malware

Malware je jakýkoli škodlivý software, který po stažení do zařízení může např. sbírat data, vytvořit útočníkovi vzdálený přístup nebo zneužít zařízení k dalším rozsáhlejším útokům, rozšířit se do celé sítě a způsobit celou řadu škod. Může být i v souborech typu Excel, Word či Powerpoint, který obsahuje škodlivá makra, nebo v příloze podezřelého e-mailu.

Jak se před malwarem chránit

- Umožnit instalaci programového vybavení pouze v rozsahu platných licencí a používání dle licenčních podmínek;
- Znemožnit běžným uživatelům technicky i organizačně instalovat aplikace a programy na svoje zařízení;
- Mít nainstalovanou aktualizovanou antivirovou ochranu;
- Být obezřetní při otevírání neznámých příloh v e-mailu.

Jak lze poznat, že se něco děje?

- Neobvyklé chování systému;
- Zpomalení výkonu zařízení bez zjevného důvodu;
- Časté pády aplikací nebo samovolné restartování;
- Vysoké vytížení CPU/disku/sítě;
- Objevují se neznámé aplikace a procesy, které nebyly instalovány správcem;
- Vznik nových spustitelných souborů ve složkách uživatelů;
- Kompromitované účty uživatelů (opakované neúspěšné pokusy o přihlášení, přihlašování z neobvyklých geografických poloh, atd.);
- Chybějící nebo pozměněné logy.

Co dělat při podezření na malware?

- Neodkládat reakci a ihned informovat jak nadřízeného na straně dodavatele, tak kontaktní osoby ČD o situaci;
- Neprovádět vlastní zásahy.

Nejčastější hrozby - Ransomware

Ransomware je typ škodlivého kódu, který znepřístupní infikované zařízení nebo šifruje jeho obsah. Následně vyžaduje zaplacení výkupného (ransom) k opětovnému zpřístupnění zařízení či odšifrování dat. Zároveň může tento typ útoku pokračovat dalším vydíráním, které spočívá v odcizení citlivých dat a požadování výkupného za jejich nezveřejnění.

Jak dojde k nákaze ransomwarem?

- K útoku dochází např. prostřednictvím sociálního inženýrství, kdy si uživatel do zařízení stáhne škodlivý kód z odkazu v podvodných zprávách a e-mailech nebo např. použitím infikovaných USB.
- Typicky útočníci také zneužívají zranitelností v systémech a aplikacích.

Jak lze poznat, že se něco děje?

- Ransomware se obvykle šíří rychle a nepozorovaně, proto je potřeba sledovat indikátory kompromitace (IoC), jako je např.:
  - Náhlé šifrování souborů;
  - Nefunkční nebo nečitelná data;
  - Nemožnost otevřít běžně dostupné dokumenty; obrázky, databáze, atd.;
  - Celkové zpomalení PC a serverů;
  - Zvýšené využití CPU a disku;
  - Zablokování přístupu do zařízení nebo na obrazovku;
  - Zobrazení požadavku o zaplacení výkupného.

Co dělat při podezření na ransomware?

- Ihned izolovat zařízení od sítě, Wi-Fi, VPN, atd.;
- Neprovádět žádné vlastní zásahy a změny na zařízení (restart, mazání souborů, atd.);
- Ihned událost nahlásit nadřízenému a kontaktním osobám v ČD.

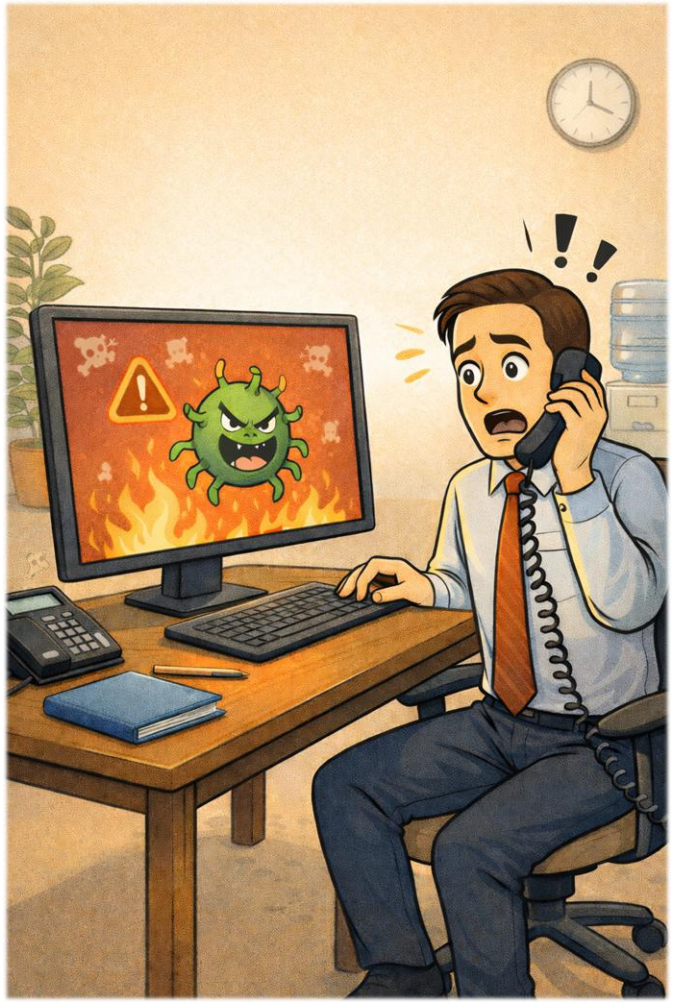
Hlášení kybernetických bezpečnostních událostí/incidentů

Kybernetická bezpečnostní událost je událost, která může vyústit v kybernetický bezpečnostní incident, který je narušením bezpečnosti informací v kybernetickém prostoru.

Příklady bezpečnostních událostí, případně incidentů:

- Umožnění neoprávněného přístupu k interním informacím;
- Otevření škodlivého souboru z e-mailu;
- Ztráta interních informací;
- Používání neschválených USB, cloudů či jiných úložišť pro citlivé informace;
- Přerušení dostupnosti služby na více než akceptovanou dobu;
- Spuštění virů, trojských koní a dalšího škodlivého software;
- Únik přihlašovacích údajů.

Všichni zaměstnanci dodavatele s přístupem k informacím ČD mají povinnost zjištěnou bezpečnostní událost neodkladně ohlásit nadřízenému a příslušným kontaktním osobám v ČD, zejména manažerovi kybernetické bezpečnosti ČD a odboru bezpečnosti.



Obrázek: vlastní tvorba pomocí online nástroje ChatGPT

Bezpečnostní doporučení pro administrátory

Infrastruktura

- Členěte síť na menší celky (segmentace) a striktně oddělujte uživatelská práva napříč uživateli (segregace) s cílem oddělit citlivé informace a kritické služby typu autentizace uživatelů (např. Microsoft Active Directory) a vytvořit zóny s různou úrovní bezpečnostních omezení.
- Blokujte škodlivé IP adresy a domény na úrovni gateway (blacklisty) a nasaďte síťové systémy detekce/prevence průniku (IDS/IPS), používající signatury a heuristiky k identifikaci anomálního provozu v rámci sítě i překračujícího perimetr.
- Sledujte síťový provoz pomocí vybraných síťových prvků nebo rozmístěním dedikovaných síťových sond. Sledujte komunikaci mezi klienty a servery, komunikaci klientů do internetu, komunikaci mezi servery i provoz na perimetru sítě a identifikujte provozní a bezpečnostní problémy.
- Uchovávejte síťový provoz z/do kritických pracovních stanic a serverů a provoz překračující perimetr sítě pro případné forenzní zkoumání po průniku do sítě a systémů. Záznamy síťového provozu uchovávejte po dobu minimálně 18 měsíců plného záznamu datového provozu.
- Kontrolujte příchozí e-maily pomocí mechanismů Sender ID, SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) a DMARC (Domain-based Message Authentication, Reporting and Conformance) a blokujte podvržené zprávy. Tyto mechanismy nastavte i pro možnou kontrolu odchozích zpráv druhou stranou.

Bezpečnostní doporučení pro administrátory

Infrastruktura

- Používejte šifrované spojení mezi poštovními servery (TLS) pro zajištění důvěrnosti e-mailové komunikace, v ideálních případě použijte DANE (DNSbased Authentication of Named Entities). Kontrolu obsahu provádějte až poté, co je emailový provoz dešifrován.
- Provádějte automatizovanou dynamickou analýzu obsahu e-mailů a webů prováděnou v sandboxu – hledejte podezřelé chování podle síťového provozu, tvorby nových souborů, úpravy stávajících souborů nebo změn konfigurace.
- Povolte na firewallu pouze žádoucí služby a standardní provoz. V případě koncových stanic nezapomeňte také blokovat spojení z Vámi nekontrolované sítě.
- Kontrolujte používané klíče a certifikáty především pro SSH autentizaci, webové servery, vzdálenou plochu apod. Kde je to možné, použijte šifrovanou komunikaci.
- Zajistěte centralizované a časově synchronizované logování síťových událostí (povolených a blokovaných) s okamžitým automatickým vyhodnocováním a uložením po dobu minimálně 18 měsíců, více podle místních okolností a významu sítě.
- Aplikujte whitelisting webových domén pro všechny domény – pokud to dovoluje charakter práce uživatelů. Tento přístup je účinnější než blacklistovat malé procento škodlivých domén.

Bezpečnostní doporučení pro administrátory

Infrastruktura

- Volte jednoduché doménové názvy, aby byly jasně viditelné případné záměny písmen ve phishingových e-mailech.
- Nasaďte anti-DDoS technologie, které můžete po důkladné úvodní analýze řešit buď vlastními silami, nebo ve spolupráci s poskytovatelem internetového připojení. Anti DDoS ochranu nasaďte na kompletní IP rozsahy vaší organizace.
- Vypracujte disaster recovery plan (DRP) a mějte připravené správné a funkční emailové adresy a telefonní čísla na ostatní administrátory, nadřízené pracovníky a CERT/CSIRT týmy.

Bezpečnostní doporučení pro administrátory

Stanice a servery

- Udržujte aktuální operační systém pravidelnými aktualizacemi a v co nejkratší době aplikujte všechny vydané bezpečnostní záplaty.
- Udržujte aktuální software a pravidelně kontrolujte verze instalovaného softwaru. U neaktuálního softwaru proveďte v rámci možností update. Zastaralé mohou být i verze použitých doplňků či modulů nebo firmware zařízení.
- Nepoužívejte nepodporované produkty, používejte pouze produkty (software i operační systémy), pro které jsou dostupné bezpečnostní záplaty.
- Ověřujte identitu aplikací a souborů a povolte jen ty důvěryhodné včetně skriptů a DLL knihoven. V prostředí Windows použijte Device Guard, AppLocker, popřípadě Zásady omezení softwaru (SRP).
- Provádějte hardening konfigurace uživatelských aplikací, povolte jen funkcionalitu, která je vyžadována pro práci uživatelů. Dodatečné funkce (např. Java a Flash ve webovém prohlížeči, makra v MS Office) povolte pouze, je-li to nutné.
- Používejte obecné preventivní mechanismy, které mohou pomoci ochránit systém před zero-day zranitelnostmi, jako např. DEP (Data Execution Prevention) nebo SELinux v linuxových systémech.
- Aktivujte IDS/IPS systémy na koncových stanicích detekující anomální chování jako např. injekci kódu do jiných procesů, změnu chráněných registrových klíčů, zachytávání stisků kláves, načítání neznámých ovladačů, snahu o zajištění perzistence a další.

Bezpečnostní doporučení pro administrátory

Stanice a servery

- Zajistěte centralizované a časově synchronizované logování síťových událostí (povolených a blokovaných) s okamžitým automatickým vyhodnocováním a uložením po dobu minimálně 18 měsíců.
- Filtrujte obsah e-mailů a propouštějte pouze relevantní druhy příloh po důkladné analýze chování uživatelů určete typy souborů, které potřebují posílat emailem. Ostatní formáty příloh blokujte – především spustitelný kód. Dále ověřujte soulad přípony souboru a jeho skutečného formátu.
- Pravidelně zálohujte důležitá a citlivá data, jako např. obsah webového serveru, databází nebo konfiguraci služeb. Zálohu umístěte do odděleného prostředí mimo produkční síť. Pravidelně testujte, jestli dokážete data obnovit a jestli jsou data po obnově funkční.
- Zaveďte standard operating environment (SOE) se standardizovanou konfigurací pro pracovní stanice i servery, kde budou vypnuty všechny nevyžádané funkcionality.
- Zamezte přímému přístupu pracovních stanic na internet a směrujte provoz přes split DNS server, e-mailový server nebo autentizovaný web proxy server. Nezapomeňte vynutit pro IPv4 i IPv6.
- Používejte antivirový a bezpečnostní software a nástroje, které zakazují spouštění nebezpečných aplikací (mimo přesně definovaný seznam privilegovaných aplikací), či nástroje, které pomáhají chránit systém v době, kdy nejsou dostupné klasické bezpečnostní aktualizace.

Bezpečnostní doporučení pro administrátory

Stanice a servery

- Šifrujte disky zejména u přenosných počítačů – včetně centrální evidence klíčů.
- Využívejte trusted platform module (TPM), tedy zabezpečený kryptografický modul pro generování a uložení hesel a kryptografických klíčů, je-li jím počítač vybaven.
- Nastavte heslo UEFI/BIOS unikátní pro každou stanici s centrální správou hesel.
- Vynucujte secure boot a nastavte pořadí zařízení určených pro boot systému. Boot manager musí být zabezpečen heslem.
- Chraňte se před útoky na hesla u všech služeb, kam se přihlašují uživatelé. Například pomocí fail2ban, využití funkcí určených pro ukládání hesel (Argon2, bcrypt, scrypt, PBKDF2) nebo CAPTCHA.
- Pro správu serverů pomocí SSH využívejte pro přihlášení klíče, zakažte hesla.
  Pro svázání otisku klíče se serverem, kde je použitý, využívejte SSHFP záznamy v DNS ideálně v kombinaci s DNSSEC, který zajistí autenticitu odpovědi obsahující SSHFP záznam.
- Provádějte hardening konfigurace serverových aplikací, tj. databází, webových aplikací, CRM systémů, účetních systémů, HR systémů a dalších systémů ukládání dat.
- Kontrolujte přenosná média jako součást širší strategie prevence ztráty dat, včetně vedení seznamu povolených USB zařízení, jejich skladování, šifrování, mazání a likvidace.
- Omezte přístup k server message blocku (SMB) a netbiosu na pracovních stanicích a serverech, kdekoliv je to možné.

Bezpečnostní doporučení pro administrátory

Stanice a servery

- Používejte režim chráněného přístupu při práci se soubory na úrovni pracovních stanic, může se např. jednat o Protected View nebo Protected mode.
- Vynuťte vytáčení VPN pokud se zařízení připojuje mimo síť organizace. Omezte síťovou aktivitu, dokud není navázáno VPN spojení.
- Zajistěte fyzickou bezpečnost IT techniky.

Bezpečnostní doporučení pro administrátory

Správa účtů

- Zaveďte centrální správu uživatelských účtů a oprávnění a nastavte jednotnou bezpečnostní politiku. Účtům, u kterých to není vyžadováno, odeberte rozšířená oprávnění a zakažte spouštění skriptů, instalaci softwaru, úpravy registru atd.
- Vynucujte vícefaktorovou autentizaci zejména pro akce vyžadující vyšší úroveň oprávnění a kritické operace jako vzdálený přístup nebo přístup k citlivým informacím.
- Oddělte administrátorské účty. Pro správu používejte speciální účty pro administraci systémů. Pro své ostatní pracovní aktivity (e-mail, web atd.) používejte běžný neprivilegovaný účet. Účet s oprávněním doménového administrátora je použit pouze ke správě Domain Controlleru (tzn. nepřistupuje na klientské stanice a servery).
- Přidělte každému administrátorovi vlastní účet pro správu systémů. Nepoužívejte sdílené účty.
- Zabezpečte lokální administrátorské účty. Nastavte unikátní heslo na každé stanici, v prostředí Windows můžete využít například LAPS (Local Administrator Password Solution).
- Vynuťte používání silných hesel s ohledem na vyžadovanou složitost, délku a dobu platnosti. Zamezte opakovanému použití stejných hesel a používání slovníkových výrazů. Vynuťte změnu hesla, existuje-li podezření, že bylo kompromitováno.
- Pravidelně kontrolujte uživatelské účty a jejich oprávnění a to jak lokální, tak centrálně spravované.

Děkujeme za dodržování bezpečnostních pravidel ČD