Informace o zabezpečení e-infrastruktury CESNET

Systém řízení bezpečnosti informací ve sdružení CESNET

Sdružení CESNET má již řadu let zavedený systém řízení bezpečnosti informací, který:

- odpovídá požadavkům normy ISO/IEC 27001, kdy sdružení CESNET je držitelem certifikace dle ČSN EN ISO/IEC 27001:2023,
- plní požadavky zákona č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „ZKB“), neboť sdružení CESNET je provozovatelem regulovaných služeb ve smyslu ZKB, a to v režimu vyšších povinností,
- zahrnuje též problematiku ochrany osobních údajů a zajišťování bezpečnosti dat.

V rámci systému řízení bezpečnosti informací ve sdružení CESNET:

- byl zřízen výbor pro řízení kybernetické bezpečnosti a obsazeny požadované bezpečnostní role, a to včetně pověřence pro ochranu osobních údajů,
- pomocí metody PDCA cyklu dochází k pravidelnému plánování, realizaci, kontrole a zlepšování stavu kybernetické a informační bezpečnosti,
- jsou stanoveny a pravidelně revidovány bezpečnostní politiky a důsledně vedena bezpečnostní dokumentace, a to včetně záznamů o činnostech zpracování osobních údajů.

Vedle systému řízení bezpečnosti informací sdružení CESNET zavedlo compliance program, v rámci kterého je systematicky a soustavně monitorován nejen soulad činností sdružení CESNET s požadavky vyplývajícími z legislativy, ale také soulad se smluvními a dalšími závazky sdružení CESNET.

Řízení rizik

Systém řízení bezpečnosti informací ve sdružení CESNET je založený na principu řízení rizik, který spočívá v soustavné identifikaci hrozeb a zranitelností a v následném provádění analýz jejich dopadů na jednotlivá aktiva sdružení CESNET. Zvláštní důraz je kladen na aktiva, která souvisí s poskytováním regulovaných služeb dle ZKB nebo k nimž mají přístup jiné subjekty (dodavatelé, spolupracující organizace apod.).

Ke zmírnění identifikovaných rizik se stanovují bezpečnostní opatření, která se následně promítají do bezpečnostních politik sdružení CESNET. Bezpečnostní politiky jsou závazné pro všechny zaměstnance, členy orgánů sdružení CESNET i vybrané dodavatele.

Bezpečnost lidských zdrojů

Jedním z nejdůležitějších prvků kybernetické a informační bezpečnosti je zajišťování bezpečnosti lidských zdrojů, které ve sdružení CESNET zahrnuje:

- povinná školení zaměstnanců, členů orgánů sdružení CESNET i vybraných dodavatelů o obsahu bezpečnostních politik, mj. s důrazem na zachovávání mlčenlivosti a ochranu soukromí uživatelů,
- pravidelná školení za účelem zvyšování obecného povědomí o problematice informační a kybernetické bezpečnosti,
- průběžné ověřování úrovně znalostí prostřednictvím testování a interních kontrol.

Řízení přístupů

V oblasti řízení přístupů sdružení CESNET zavedlo tato bezpečnostní opatření:

- přístupová oprávnění jsou řízena na základě *role-based* modelu,
- jsou důsledně oddělovány role administrátorů a uživatelů,
- přístupy jsou přidělovány podle principu minimalizace a principu *need-to-know,*
- rozsah uživatelských oprávnění je průběžně prověřován v rámci celého životního cyklu uživatelské identity,
- pro přístup k aktivům je nastavena silná heslová politika a jsou využívány mechanismy vícefaktorové autentizace (MFA).

K zajištění autentizace a autorizace sdružení CESNET využívá:

- věrohodné zdroje identit, mezi něž patří (kromě IdP provozovaného přímo sdružením CESNET) federace eduID,
- nástroj pro řízení přístupů ke zdrojům a službám Perun.

Výše uvedená pravidla pro řízení přístupů přenáší sdružení CESNET v relevantních případech i na své dodavatele a partnery.

Technická opatření pro zajištění bezpečnosti e-infrastruktury CESNET

Pro zajištění bezpečnosti e-infrastruktury CESNET jsou využívány *state-of-the-art* technické a programové prostředky.

Bezpečnostní politiky sdružení CESNET vyžadují po správcích technických aktiv a souvisejících služeb dodržování řady opatření a principů vedoucích k zajištění dostupnosti, důvěrnosti a integrity, mj.:

- využívání bezpečnostních protokolů (kryptografické algoritmy, šifrování apod.), firewallu a politiky správy služeb, a to s cílem zamezit tomu, aby neoprávněné osoby během přenosu informací či dat mohly tyto informace či data číst, kopírovat, měnit nebo svévolně odstraňovat,
- zavedení pravidel pro zajištění fyzické bezpečnosti lokalit, a to za účelem ochrany pracovišť, technických aktiv i případných informací v listinné podobě před neoprávněným přístupem či jejich fyzickým zničením.

Technická opatření směřující k zabezpečení síťové části e-infrastruktury CESNET mají za cíl:

- zamezit zahlcení páteřní infrastruktury,
- zamezit zahlcení přípojek připojených organizací,
- zamezit zahlcení externích propojení,
- eliminovat nelegitimní provoz,
- ošetřit anomální jevy na úrovni síťového transportu s minimalizací rizik spojených s potenciálním *false-positive* vyhodnocením jevů.

Základem obrany e-infrastruktury CESNET, jejích služeb, informací a dat jsou bezpečnostní prvky a mechanismy na bázi specifického nastavení a architektury sítě, pokročilého síťového monitoringu a detekcí anomálií. Ty jsou využívány ve všech vrstvách a topologických částech sítě (na vnějším perimetru sítě, v páteřní infrastruktuře, na perimetru mezi páteří a připojenými institucemi i v koncových

sítích hostujících služby). Nastavení a aplikovaná opatření jsou průběžně vyhodnocována a optimalizována.

E-infrastruktura CESNET využívá hierarchizovaný monitorovací systém, pro který platí:

- je zajišťován dohledovým pracovištěm stálé služby (ServiceDesk) v režimu 24/7,
- každý podsystém má vlastní sadu monitorovacích nástrojů, které odesílají reporty do globálního rozhraní,
- na zjištěné či od připojených organizací oznámené problémy související s funkcionalitou sítě reaguje pracoviště stálé služby (ServiceDesk) do 1 hod.

Zároveň jsou v e-infrastruktuře CESNET nasazeny nástroje FTAS a ExaFS, které umožňují regulaci a eliminaci nežádoucího provozu a útoků významného objemu z externích sítí (DoS volumetrické a agresivní útoky) a dalších anomálních jevů v síťovém provozu (dlouhodobé/agresivnější skeny, podvržení IP adres apod.). Regulace provozu probíhá:

- automaticky na základě monitoringem zjištěného nestandardního chování infrastruktury (*event driven*), a to v režimu 24/7;
- na základě požadavku připojené organizace (např. eliminace nestandardního provozu z/do sítě připojené organizace), kdy na tyto požadavky reaguje pracoviště stále služby (ServiceDesk) do 1 hod.

Připojené organizace mohou požádat o přístup do globální instance systému FTAS, kde jim jsou v režimu 24/7 zpřístupňovány informace o jejich IP provozu. Zároveň je připojeným organizacím poskytován nástroj ExaFS také pro samoobslužnou regulaci vlastního provozu, kdy své požadavky mohou zadávat přímo do uživatelského rozhraní.

Zvládaní kybernetických bezpečnostních incidentů

Sdružení CESNET provozuje mezinárodně etablovaný bezpečnostní tým CESNET-CERTS. Ten je zodpovědný za zvládání kybernetických bezpečnostních událostí a incidentů v e-infrastruktuře CESNET, kdy tato činnost zahrnuje:

- nastavení procesu pro oznamování bezpečnostních událostí či incidentů ze strany zaměstnanců sdružení CESNET, uživatelů i dodavatelů a šíření osvěty o tomto procesu,
- provoz automatizovaných nástrojů pro detekci, zaznamenávání a mitigaci bezpečnostních událostí v souladu s legislativními požadavky
- *provoz centralizovaného log management zajišťující sběr z bezpečnostní telemetrie*, s pravidelnou kontrolou kvality a dostatečnosti zaznamenávaných informací,
- provádění analýz a vyhodnocování detekovaných událostí za účelem identifikace kybernetických bezpečnostních incidentů, práce s dalšími zdroji *threat inteligence,*
- *systematické skenování sítě a provozovaných služeb na výskyt zranitelností s denním monitoringem nově objevených zranitelností,*
- nastavení pravidel pro účinnou reakci na kybernetické bezpečnostní incidenty (fungování krizového týmu, postupy při komunikaci s dotčenými uživateli a s NÚKIB, přijímání opatření pro odvrácení a zmírnění dopadů incidentu, zjišťování příčin, vedení záznamů apod.).

Zpracování přijatých hlášení bezpečnostních incidentů, příp. jejich předání k řešení připojené organizaci, provádí bezpečnostní tým CESNET-CERTS v pracovní dny v době od 9 do 17 hod. Standardní reakční doba jsou 2 hodiny.

V případě bezpečnostních incidentů, které byly předány k řešení připojené organizaci, nabízí bezpečnostní tým organizaci spolupráci či asistenci, které jsou poskytovány ve standardní pracovní době, příp. v době dle dohody s dotčenou organizací.

Bezpečnostní tým při své práci využívá nástroje a služby, které jsou dostupné také organizacím připojeným k e-infrastruktuře CESNET, mj.:

- nástroje pro management bezpečnostních událostí Warden a Mentat,
- skenovací nástroje pro vyhledávání zranitelností,
- nástroje pro hodnocení zabezpečení sítě,
- nástroje a služby pro sdílení podpůrných informací pro řešení bezpečnostních incidentů PassiveDNS, NERD, apod.

Řízení kontinuity činností

S tématem zvládání bezpečnostních incidentů úzce souvisí i řízení kontinuity činností. Pravidla pro řízení kontinuity činností jsou stanovena příslušnou bezpečnostní politikou sdružení CESNET, na základě které:

- je prováděna analýza dopadů bezpečnostních incidentů na aktiva, a to zejména ve vztahu k zajišťování dostupnosti služeb, informací a dat, a výsledky analýzy dopadů jsou zohledňovány při řízení rizik,
- jsou identifikována aktiva a související činnosti a procesy, které jsou klíčové z pohledu zajišťování kontinuity činností,
- jsou stanovovány postupy, lhůty a odpovědnosti při obnovování činností a dostupnosti služeb, informací a dat,
- se zpracovávají a pravidelně testují plány obnovy ve vztahu ke klíčovým aktivům,
- jsou zaváděna technická opatření, která jsou dle výsledků analýzy rizik nezbytná pro zajišťování dostupnosti služeb, informací a dat, a to zejména v oblastech:
  - zajišťování odolnosti a redundance aktiv,
  - zálohování konfigurací a nastavení technických aktiv, zálohování informací a dat,
  - zajišťování bezpečnosti záloh, kontrola jejich konzistence a testování jejich obnovitelnosti,
- se využívají principy krizového řízení ve všech fázích zajišťování kontinuity činností.

Řízení změn a zajišťování bezpečnosti aktiv při jejich akvizici, vývoji a údržbě

Sdružení CESNET soustavně pracuje na zvyšování úrovně svých služeb i jejich bezpečnosti. U těchto i dalších změn v činnostech sdružení CESNET jsou průběžně vyhodnocovány jejich dopady na bezpečnost. Obdobně to platí i pro akvizice, vývoj a údržbu aktiv.

Při realizaci změn, akvizic, vývoje i údržby aktiv jsou prováděny analýzy rizik, které zohledňují hodnotu dotčených aktiv a závažnost dopadů na jejich bezpečnost. Samozřejmostí je dodržování bezpečnostních opatření při realizaci těchto činností, jak požadovaných legislativou, tak vyplývajících z dobré praxe a aktuálních trendů.

Zásadní změny s dopady do oblasti bezpečnosti oznamuje sdružení CESNET v relevantním rozsahu svým uživatelům, partnerům a dodavatelům.

Likvidace informací a dat

Způsoby likvidace informací a dat vyplývají z jejich charakteru a z hodnoty aktiv, ke kterým se vztahují, kdy pro likvidaci platí ve sdružení CESNET tato pravidla:

- pro všechna data je v rámci řízení jejich životního cyklu stanovena doba, po jejímž uplynutí jsou zlikvidována,
- likvidace dat probíhá buď automatizovaně (typicky mazání starých logů, anonymizace neaktivních uživatelských účtů apod.), nebo ručně (např. při ukončení služby, na základě uplatnění práva být zapomenut ze strany subjektu údajů apod.),
- až do okamžiku likvidace dotčených informací a dat je dbáno na dodržování všech opatření pro zajištění jejich důvěrnosti (tj. dodržování pravidel pro řízení přístupů, smluvní ošetření likvidace dat jiným subjektem atd.)
- fyzickou likvidaci nosičů informací a dat zajišťují pouze k tomu proškolení zaměstnanci,
- o likvidaci dat jsou uchovávány záznamy (logy, protokoly apod.).

V případě likvidace informací a dat jiného subjektu (odběratelé služeb sdružení CESNET) se kromě výše uvedených pravidel uplatní také smluvně ujednané postupy pro likvidaci.

V případě ukončování poskytování některé ze služeb, je nezbytné s připojenou organizací vypořádat také otázku „*exit strategy*“, tj, nejen pravidla pro likvidaci dat ze strany sdružení CESNET, ale také jejich případného vydání připojené organizaci. Ujednání ohledně *exit strategy* jsou proto standardní součástí smluv o poskytování služeb sdružení CESNET. Vedle toho sdružení CESNET nabízí možnost konzultace s garanty služeb sdružení CESNET ohledně nejvhodnějšího postupu.

Řízení dodavatelů

Přísná bezpečnostní opatření sdružení CESNET vyžaduje i od svých dodavatelů, kdy cílem těchto opatření je zmírnit rizika spojená s přístupem dodavatelů k aktivům, příp. se závislostí bezpečnosti aktiv na jiném subjektu.

Součástí procesu výběru dodavatele zboží či služeb je povinné provedení analýzy rizik. Na ni navazuje stanovení bezpečnostních opatření pro snížení rizik souvisejících s předmětnou dodávkou. Bezpečnostní opatření směřují nejen do oblasti vnitřních postupů ve sdružení CESNET, ale ovlivňují přímo i obsah smlouvy s dodavatelem. Do smluvního vztahu s dodavateli jsou automaticky zahrnuta:

- ujednání o mlčenlivosti, o nakládání s duševním vlastnictvím (mj. licenční ujednání), o řešení bezpečnostních incidentů, o nakládání s osobními údaji apod.,
- bezpečnostní opatření vyplývající z analýz rizik a vydaných protiopatření NÚKIB,
- další požadavky na smlouvy s dodavateli, které vyplývají z prováděcích vyhlášek k ZKB či jiných právních předpisů.

Ve sdružení CESNET je prováděno průběžné hodnocení všech dodavatelů, na jehož základě jsou následně upravovány požadavky na zavádění bezpečnostních opatření.

Ověřování účinnosti systému řízení bezpečnosti informací ve sdružení CESNET

Nedílnou součástí provozu systému řízení bezpečnosti informací ve sdružení CESNET je provádění pravidelného hodnocení účinnosti tohoto systému, a to mj. na základě informacích zjištěných při:

- analýzách rizik a interních kontrolách dodržování stanovených bezpečnostních opatření,
- testování zabezpečení aktiv prostřednictvím služeb Forenzní laboratoře sdružení CESNET (FLAB), jako jsou penetrační testy či testy sociálního inženýrství,
- interních auditech realizovaných v legislativou stanovených lhůtách,
- certifikačních a dozorových auditech dle normy ISO/IEC 27001.

Hodnocení účinnosti systému řízení bezpečnosti informací je ve sdružení CESNET prováděno pravidelně, s jeho výsledky je každoročně seznamováno vrcholné vedení prostřednictvím zprávy o přezkoumání systému řízení bezpečnosti informací. Na jeho základě probíhá aktualizace celého systému řízení bezpečnosti informací a související dokumentace a stanovování cílů na další sledované období.

Bezpečnost komunity

K bezpečnosti e-infrastruktury CESNET přispívá i bezpečnost infrastruktur připojených organizací. Proto je nedílnou součástí činností sdružení CESNET také sdílení zdrojů *threat inteligence*, poskytování součinnosti bezpečnostního týmu při řešení bezpečnostních událostí a incidentů, poskytování konzultací, pořádání seminářů apod.

Do e-infrastruktury CESNET jsou připojeny organizace s vysokými potřebami v oblasti kybernetické bezpečnosti. Připojeným organizacím proto sdružení CESNET nabízí služby, které jsou využívány i při zajišťování bezpečnosti e-infrastruktury CESNET a které byly v řadě případů ve sdružení CESNET přímo vyvinuty.

Na základě individuální dohody mezi sdružením CESNET a připojenou organizací je možné aplikovat specifická opatření dle bezpečnostních potřeb připojené organizace.

Poslední aktualizace dne 23. 3. 2026