UNIVERZITA J. E. PURKYNĚ V ÚSTÍ NAD LABEM
Přírodovědecká fakulta

SMĚRNICE DĚKANA PŘÍRODOVĚDECKÉ FAKULTY

č. 2 / 2024

Politika kybernetická bezpečnost na Přírodovědecké fakultě Univerzity J. E. Purkyně v Ústí nad Labem

doc. RNDr. Michal Varady, Ph.D., děkan

Platná od: 1. *9. 2024*
Zpracoval/a: *Bc. Jaroslav Tichý*
Ruší:

Čl. 1

Úvodní ustanovení

Tato směrnice (Politika) stanovuje zásady pro nasazení a používání nástrojů určených k detekci kybernetických bezpečnostních událostí. Detekce, záznam, evidence, sběr a vyhodnocení bezpečnostních událostí jsou klíčové pro zajištění bezpečného provozu a ochrany informačních systémů. Politika definuje potřebné nástroje pro efektivní detekci a stanovuje postupy pro jejich implementaci a správu, aby bylo možné včas reagovat na potenciální hrozby a minimalizovat rizika.

Čl. 2

Obecné ustanovení

Na Přírodovědecké fakultě UJEP řeší záležitosti týkající se kybernetické bezpečnosti Centrum infrastrukturních technologií (CIT) Přírodovědecké fakulty (organizace) Univerzity Jana Evangelisty Purkyně (UJEP) v Ústí nad Labem v úzké kooperaci s Centrem informatiky UJEP (CI) a manažerem kybernetické bezpečnosti UJEP.

CIT je v oblasti kybernetické bezpečnosti vázáno interními předpisy univerzity:

- Směrnice rektora č. 7/2023, která odkazuje na politiky dostupné na odkaze https://grc.ci.ujep.cz/portal/policy,
- Směrnice prorektora pro rozvoj a informatizaci č. 1/2012,
- Příkaz rektorky č. 1/2008.

Všechny postupy a pravidla uvedené v tomto dokumentu musí být v souladu s těmito interními předpisy, které upravují správu a optimalizaci nástrojů pro detekci kybernetických bezpečnostních událostí. Je nezbytné pravidelně kontrolovat a aktualizovat postupy, aby odpovídaly aktuálním požadavkům uvedeným v interních předpisech univerzity a dalších relevantních dokumentech.

Politika vychází a reflektuje tyto základní veřejné směrnice, nařízení a normy:

- Zákon č. 181/2014 Sb. ve znění pozdějších předpisů (Zákon č. 205/2017 Sb.),
- Směrnice Evropského parlamentu a Rady (EU) 2016/1148 - Směrnice o bezpečnosti sítí a informačních systémů (NIS) - Vyhláška č. 82/2018 Sb.,
- Nařízení Evropského parlamentu a Rady (EU) 2016/679 - Obecné nařízení o ochraně osobních údajů (GDPR) - Zákon č. 110/2019 Sb.,
- Směrnice Evropského parlamentu a Rady (EU) 2018/1972 - Směrnice o evropském kodexu elektronických komunikací,
- Nařízení Evropského parlamentu a Rady (EU) 2019/881 - Nařízení o kybernetické bezpečnosti (Cybersecurity Act),
- Směrnice Evropského parlamentu a Rady (EU) 2019/770 - Směrnice o smlouvách o poskytování digitálních služeb (DSA),
- Nařízení (EU) 2022/858 - Nařízení o bezpečnosti a odolnosti veřejných infrastruktur,
- Nařízení Evropského parlamentu a Rady (EU) 2022/2554 - Nařízení o kybernetické odolnosti v souvislosti s dodavatelskými řetězci (Cyber Resilience Act),
- Směrnice Evropského parlamentu a Rady (EU) 2022/2555 - Směrnice o ochraně osobních údajů v souvislosti s poskytováním služeb v oblasti elektronických komunikací (NIS2),

- ISO/IEC 22301:2019 - Systémy řízení kontinuity činnosti,
- ISO/IEC 27001:2013 - Systémy řízení bezpečnosti informací (ISMS),
- ISO/IEC 27002:2022 - Kodex praktických opatření pro bezpečnost informací,
- ISO/IEC 27004:2020 - Měření a vyhodnocování systému řízení bezpečnosti informací,
- ISO/IEC 27005:2018 - Řízení rizik v oblasti bezpečnosti informací,
- ISO/IEC 27035:2016 - Řízení incidentů v oblasti bezpečnosti informací,
- ISO/IEC 27036:2014 - Bezpečnost informací v dodavatelských řetězcích.

Čl. 3

Význam a benefity

Politika nasazení a používání nástrojů pro detekci kybernetických bezpečnostních událostí je klíčová pro ochranu informačních systémů a dat. Její význam spočívá v systematickém přístupu k identifikaci a řešení bezpečnostních hrozeb, které mohou ohrozit integritu, dostupnost a důvěrnost informací a služeb. Efektivní detekce a správné vyhodnocení bezpečnostních událostí umožňuje rychlou reakci na incidenty, minimalizaci škod a prevenci budoucích útoků. Mezi hlavní benefity patří zvýšení schopnosti CIT reagovat na kybernetické hrozby v reálném čase, zlepšení řízení bezpečnosti a posílení celkové odolnosti proti kybernetickým útokům, což přispívá k ochraně a důvěryhodnosti organizace.

Čl. 4

Rozsah

Tato politika se vztahuje na všechny bezpečnostní události, které mohou mít nebo mají dopad na bezpečnost informací, tj. jejich důvěrnost, dostupnost nebo integritu. Bezpečnostní událostí se rozumí jakákoli událost, která, ačkoliv sama o sobě nemusí bezprostředně způsobit incident, je významná a její ignorování může v budoucnu vést k závažnějším problémům.

Mezi příklady bezpečnostních událostí, které spadají do rozsahu této politiky, patří:

1. Detekovaný nepovedený pokus o přístup do systému nebo k informacím, například zapomenuté heslo.
2. Plánovaná (avizovaná) nedostupnost systému, například z důvodu údržby, nebo jakákoli událost, jejíž opakovaný nebo mnohonásobný výskyt by mohl ohrozit dostupnost.
3. Škodlivý kód detekovaný a zachycený antivirovou ochranou dříve, než byly napáchány jakékoli škody.
4. Detekovaný pokus o překonání technického opatření.
5. Tato politika se rovněž vztahuje na události hlášené fyzickými nebo právnickými osobami, které mohou ovlivnit bezpečnostní stav systému. Uplatnění této politiky je v souladu s vyhláškou č. 82/2018 Sb. o kybernetické bezpečnosti, zejména § 22, 23 a 24.

Čl. 5

Chráněná aktiva

CIT je povinno analyzovat a případně řešit kybernetické bezpečnostní události v rozsahu odpovídajícím důležitosti jednotlivých aktiv, která zahrnují:

1. **Koncové stanice:** Počítače, pracovní stanice, notebooky a další koncová zařízení připojené k síti, která mohou být cílem nebo zdrojem bezpečnostních událostí.
2. **Servery:** Fyzické nebo virtuální servery, které hostují aplikace a data, a tudíž vyžadují detekci bezpečnostních incidentů.
3. **Datová úložiště a výměnné datové nosiče:** Systémy pro uchovávání dat, včetně externích disků, flash disků a jiných médií pro přenos dat, které musí být monitorovány pro ochranu proti ztrátě nebo neautorizovanému přístupu.
4. **Síťové aktivní prvky:** Routery, switche, firewall a další síťová zařízení, která jsou klíčová pro správné fungování a zabezpečení síťové infrastruktury.
5. **Uživatelé:** zahrnuje všechny osoby, které aktivně využívají služby IT poskytované organizací. Uživatelé jsou klíčovým prvkem IT infrastruktury a jejich správné řízení a ochrana jsou zásadní pro zajištění bezpečnosti informací a systémů organizace. Do této kategorie spadají:
    a. **Zaměstnanci:** Osoby, které jsou zaměstnány organizací a mají přístup k IT systémům a datům v rámci své pracovní činnosti.
    b. **Studenti:** Osoby, které jsou registrovány na organizaci a využívají IT služby pro studijní účely a přístup k poskytovaným službám.
6. **Jiná aktiva:** Jakékoli další komponenty a zařízení, které mohou být součástí IT infrastruktury a které mohou ovlivnit bezpečnost informací.

Čl. 6

Pravidla a postupy nasazení nástroje pro detekci kybernetických bezpečnostních událostí

Tyto pravidla a postupy mají za cíl zajistit efektivní detekci kybernetických bezpečnostních událostí a poskytnout organizaci nástroje a postupy potřebné k jejich správnému řízení a vyhodnocení.

1. **Způsoby detekce a záznamu událostí:**
    a. **Oznámení zaměstnanců a zainteresovaných stran:** hlášení od zaměstnanců a dalších relevantních osob, včetně případných dodavatelů a externích partnerů. Oznámení je realizováno prostřednictvím stanovených kanálů:
        i. e-mail: cit@rt.ujep.cz
        ii. telefonicky: 720 060 280 nebo interní klapky: 6729, 6730, 6735
    b. **Antivirové řešení:** ESET Antivirus je centrální univerzitní řešení, které musí být instalováno na všech relevantních zařízeních.
    c. **Penetrační testování:** v pravidelných intervalech, dle možností nejméně však jednou ročně, provádí CIT testování kybernetické bezpečnosti provozovaných technologií a služeb.
    d. **Security Operation Center:** CIT implementuje a udržuje různé nástroje pro detekci událostí, k zajištění používá:
        i. Security Information and Event Management (SIEM) – Centralizované shromažďování, analýzu a korelace bezpečnostních událostí,
        ii. centralizované shromažďování bezpečnostních logů,
        iii. monitorování a správu IT infrastruktury,
        iv. další relevantní nástroje, které jsou aplikovány podle potřeby a specifických požadavků organizace.
2. **Funkce nástroje pro detekci:**
    a. **Ověření a kontrola přenášených dat:** Nástroj musí zajistit ověření a kontrolu všech dat přenášených v rámci komunikační sítě a mezi různými komunikačními

sítěmi. To zahrnuje monitorování datových toků a detekci neobvyklého nebo podezřelého chování.

b. **Ověření a kontrola na perimetru:** Nástroj musí poskytovat ochranu na perimetru komunikační sítě, což zahrnuje sledování a analýzu dat, která vstupují nebo opouštějí síť.

c. **Blokování nežádoucí komunikace:** Musí být schopný automaticky blokovat nebo oznámit pokusy o nežádoucí nebo neautorizovanou komunikaci.

3. **Rozsah záznamů:**

   a. **Komplexita informací:**

      i. pro kritické systémy musí obsahovat všechny relevantní informace o událostech a aktivitách, které mohou souviset s bezpečnostními incidenty. To zahrnuje podrobnosti o příčinách, důsledcích a způsobech reakce,

      ii. pro ostatní systémy musí obsahovat informace o incidentu a události stupně Error/Critical.

   b. **Poskytování informací pro bezpečnostní role:** Záznamy musí být strukturovány tak, aby poskytovaly informace potřebné pro analýzu a rozhodování bezpečnostních odborníků a dalších určených rolí.

   c. **Uchování důkazů:** Organizace zajistí, že záznamy jsou uchovávány v souladu s právními a regulačními požadavky, minimálně 6 měsíců a aby bylo možné v případě potřeby provádět forenzní analýzy.

Čl. 7

Provozní postupy pro vyhodnocování a reagování na detekované kybernetické bezpečnostní události

Politika stanovuje následující postupy zajišťující, že detekované kybernetické bezpečnostní události jsou správně vyhodnoceny a efektivně řízeny, čímž se minimalizují potenciální škody a zajišťuje se odpovídající reakce na bezpečnostní incident.

1. **Reakce na detekované události:** Po detekci bezpečnostní události je nezbytné ji správně klasifikovat. Události, které jsou považovány za potenciální incidenty nebo mají významný dopad, musí být operativně řešeny a reportovány manažerovi kybernetické bezpečnosti UJEP. Klasifikace událostí zahrnuje hodnocení jejich závažnosti a potenciálních dopadů na organizaci.

2. **Postupy seskupování záznamů:**

   a. **Dohledání a analýza informací:** CIT má jasně definované postupy pro seskupování a dohledání záznamů souvisejících s událostmi. To zahrnuje shromáždění potřebných parametrů, jako jsou:

      i. ID osoby: Identifikace uživatele nebo systému zapojeného do události.

      ii. Čas: Datum a čas, kdy událost nastala.

      iii. IP adresa: Adresa zařízení zapojeného do události.

      iv. MAC adresa: Fyzická adresa síťového zařízení.

      v. Protokol: Síťový protokol používaný při události.

      vi. Využité služby: Služby nebo aplikace, které byly zapojené do události.

   b. **Sledování řetězce informací:** Sledováním řetězce událostí a jejich souvisejících aktivit CIT zkouší identifikovat další/závažnější incidenty.

3. **Postupy včasného varování:**

   a. **Včasné varování:** CIT má nastavené postupy pro včasné varování o potenciálních hrozbách a zranitelnostech. To zahrnuje:

b. **Monitorování a výstrahy (alerty):** Automatické monitorování systému a generování varovných hlášení v případě detekce podezřelých aktivit.
c. **Informování:** Poskytování relevantních informací odpovědným osobám pro zajištění včasné reakce a přizpůsobení bezpečnostních opatření.
d. **Nastavení bezpečnostních opatření:** Na základě získaných informací a včasných varování CIT realizuje bezpečnostní opatření, aby minimalizovalo rizika a zranitelnosti.

Čl. 8

Pravidla a postupy pro optimalizaci nastavení nástroje pro detekci kybernetických bezpečnostních událostí

1. **Evidence:** Záznamy o bezpečnostních událostech jsou systematicky ukládány do centralizovaného úložiště, aby bylo možné provádět analýzu a audit.
2. **Zálohování:** Detekované události a související data jsou pravidelně zálohována, aby byla zajištěna jejich dostupnost a integrita v případě potřeby obnovy.
3. **Automatické aktualizace:** Používané technologie jsou běžně konfigurovány na automatické stahování a instalaci bezpečnostních aktualizací.
4. **Manuální aktualizace:** U vybraných infrastrukturních prvků jsou pravidelně prováděny ruční aktualizace pro zajištění funkčnosti dle doporučení výrobců.
5. **Testování a ladění:** Jsou pravidelně používány automatické i manuální testovací a ladící nástroje, aby se zajistila efektivita a přesnost v detekci událostí.

Čl. 9

Preventivní opatření

1. **Správa přístupových práv:** Definice rolí a odpovědností.
2. **Autentifikace a autorizace:** Silné autentifikační mechanismy (2FA/certifikáty) a bezpečná hesla.
3. **Školení a osvěta:** Školení a osvěta o bezpečnostních hrozbách, politikách a postupech, včetně phishingu a ochrany osobních údajů.
4. **Testování povědomí:** Provádění testů a simulací pro ověření úrovně povědomí a připravenosti uživatelů.
5. **Monitorování aktivit:** Zavedení mechanismů pro monitorování a zaznamenávání aktivit uživatelů na IT systémech a sítích ve správě CIT.
6. **Ochrana dat a soukromí:** Zajištění, že osobní údaje uživatelů a jiná citlivá data jsou chráněny v souladu s právními a regulačními požadavky včetně šifrování a kontroly přístupu.
7. **Zálohování dat:** Zajištění pravidelného zálohování dat generovaných a využívaných uživateli, stejně jako dat systémů provozovaných služeb.
8. **Správa koncových zařízení:** Implementace bezpečnostních opatření na koncových zařízeních organizace (počítače, mobilní zařízení) používaných uživateli.
9. **Inventarizace HW a SW:** Automatická inventarizace hardware a software, včetně zaznamenávání a správy majetku a licencí. Inventarizace musí zahrnovat sledování přidělených a používaných zařízení, jejich umístění a konfiguraci, stejně jako aktualizaci údajů o softwarových licencích a verzích.
10. **Kontrola a údržba:** Pravidelná kontrola a údržba koncových zařízení pro zajištění jejich bezpečnosti.

11. **Zabezpečení připojení a komunikace:** Používání šifrovaných kanálů pro komunikaci a přenos citlivých informací mezi uživateli a systémy.
12. **Bezpečné připojení:** Zajištění bezpečného připojení k IT systémům, například pomocí VPN pro vzdálený přístup.

Čl. 10

Preventivní opatření

Tento článek specifikuje kontrolní mechanismy, které zajišťují, že politika kybernetické bezpečnosti je efektivně implementována a udržována. Kontrolní mechanismy zahrnují pravidelný reporting a interní audit, které pomáhají monitorovat, vyhodnocovat a zlepšovat bezpečnostní postupy a nástroje.

1. **Reporting**
    a) Cíl reportingu:
        i. Monitorování výkonu: Reporting slouží k monitorování účinnosti nástrojů a procesů pro detekci kybernetických bezpečnostních událostí.
        ii. Identifikace problémů: Umožňuje identifikovat a reagovat na případné problémy, zranitelnosti nebo nedostatky v bezpečnostních opatřeních.
    b) Typy reportů:
        i. Automatické testování: Zprávy z pravidelných automatických testů a skenování, které obsahují detaily o nalezených zranitelnostech a doporučení pro nápravná opatření.
        ii. Incidenty a události: Reporty o detekovaných bezpečnostních událostech a incidentech, včetně detailních informací o zjištěných příčinách, dopadech a provedených opatřeních.
        iii. Výkonnostní zprávy: Zprávy o výkonu nástrojů a systémů pro detekci bezpečnostních událostí, včetně statistik o počtu a typu detekovaných událostí.
    c) Frekvence: Reporty jsou generovány pravidelně (např. měsíčně, čtvrtletně), dle povahy provozované služby, a ad-hoc podle potřeby, například v případě závažného incidentu.
    d) Zodpovědnost: Odpovědnost za tvorbu a distribuci reportů nese tým kybernetické bezpečnosti CIT (CERT). Výsledky reportů jsou k dispozici managementu organizace a relevantním zainteresovaným stranám formou sdíleného úložiště.
    e) Formát: Reporty budou poskytovány v jasném a přehledném formátu, který usnadňuje jejich analýzu a rozhodování.
2. **Interní audit**
    a) Cíl interního auditu:
        i. Ověření shody: Interní audit slouží k ověření dodržování politiky kybernetické bezpečnosti, interních předpisů a regulačních požadavků.
        ii. Zlepšení postupů: Identifikace oblastí, kde je možné zlepšit procesy a postupy v oblasti kybernetické bezpečnosti.
    b) Typy auditů:
        i. Pravidelný audit: Prováděný v přibližně ročním intervalu s cílem ověřit efektivitu a shodu s politikou kybernetické bezpečnosti.
        ii. Speciální audit: Prováděný na základě specifických potřeb, například v reakci na nově vzniklé hrozby nebo po zásadních změnách v infrastruktuře či personálním zabezpečení.
    c) Proces auditu:

i. Plánování: Příprava plánu auditu, který zahrnuje rozsah, cíle, kritéria a harmonogram auditu.
ii. Provádění: Shromažďování důkazů, vyhodnocování procesů, systémů a dokumentace v souladu s auditními standardy.
iii. Vyhodnocení: Analýza zjištění a příprava závěrečné zprávy obsahující doporučení pro zlepšení.

d) Zodpovědnost: Zadání auditu bude formulovat CERT a prováděn Oddělením interního auditu UJEP nebo externím subjektem.
e) Akční plán:
i. Implementace doporučení: Na základě závěrů auditních zpráv bude vypracován akční plán pro implementaci doporučených opatření.
ii. Sledování pokroku: Pokrok v implementaci doporučení bude pravidelně monitorován a hlášen proděkance/proděkanovi pro rozvoj a kvalitu PřF UJEP.

3. **Údržba a revize kontrolních mechanismů:** Kontrolní mechanismy budou pravidelně revidovány a aktualizovány, aby odpovídaly aktuálním požadavkům a legislativním změnám v kybernetické bezpečnosti. Kromě toho budou optimalizovány na základě zjištění získaných z reportů a auditů.

Čl. 11

Přechodná a závěrečná ustanovení

1. Tato směrnice vstupuje v platnost dne 1. září 2024.

doc. RNDr. Michal Varady, Ph.D.

Digitally signed by doc. RNDr. Michal Varady, Ph.D.
Date: 2024.09.10 09:07:56 +02'00'

doc. RNDr. Michal Varady, Ph.D.
děkan