					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P19					Názov dokumentu: **Politika riadenia zraniteľností a záplat**							
Verzia: 1.0		Dátum nadobudnutia účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Štandard		Postup		Formulár		Register		Iné	

História revízií				
Číslo revízie	**Dátum revízie**	**Zmeny**	**Preskúmal**	**Vlastník procesu**

Schválenia			
Meno	**Pozícia**	**Dátum**	**Podpis**

Súlad s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitola 8	Systematické ošetrovanie technických zraniteľností; priebežná účinnosť bezpečnostných kontrol.
ISO/IEC 27002:2022	Kontroly 8.8, 8.9, 5	Implementačné usmernenia pre záplatovanie, skenovanie zraniteľností, integritu softvéru, bezpečnú konfiguráciu a inventarizáciu aktív.
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2, CM-6	Vyžaduje časté skenovanie, odstraňovanie nedostatkov a riadenie konfigurácie.
Nariadenie EÚ GDPR	Článok 32, odôvodnenie 49	Technické opatrenia na bezodkladné záplatovanie, ošetrovanie zraniteľností a zachovanie kontinuity bezpečnosti.
Smernica EÚ NIS2	Článok 21(2)(d)	Detekcia, reakcia a zmierňovanie zraniteľností na udržanie vysokej úrovne kybernetickej hygieny.
Nariadenie EÚ DORA	Články 8, 10(2)(f)	Včasné odstraňovanie zraniteľností IKT; nepretržité hodnotenia riadené hrozbami.
COBIT 2019	DSS05.02, DSS01.03, MEA	Skenovanie, sledovanie a zmierňovanie technických slabín; monitorovanie známok zneužitia; auditovanie účinnosti vrátane stavu záplat.

1. Účel

1.1 Táto politika stanovuje záväzné požiadavky organizácie na identifikáciu, klasifikáciu, nápravu a monitorovanie technických zraniteľností a chýb softvéru vo všetkých informačných systémoch a aktívach v rozsahu systému manažérstva informačnej bezpečnosti (ISMS).

1.2 Zabezpečuje, aby všetky známe zraniteľnosti boli posúdené a riešené včas a na základe rizika prostredníctvom koordinovaného záplatovania, úprav konfigurácie alebo kompenzačných kontrol v súlade s potrebami organizácie a povinnosťami v oblasti súladu.

1.3 Táto politika podporuje súlad s kontrolou 8.8 prílohy A normy ISO/IEC 27001 a usmerneniami ISO/IEC 27002 a zohľadňuje regulačné požiadavky podľa článku 8 nariadenia DORA, článku 21 smernice NIS2, článku 32 GDPR a domén DSS a APO rámca COBIT 2019.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetky informačné systémy, aktíva a prostredia, ktoré uchovávajú, spracúvajú alebo prenášajú údaje podliehajúce správe ISMS, vrátane:

2.1.1 operačných systémov, aplikácií, sieťových zariadení, firmvéru, cloudových platforiem, API a softvéru tretích strán.

2.1.2 systémov vo vývoji, prostredí staging, produkčných, zálohovacích a prostredí obnovy po havárii.

2.1.3 koncových staníc, serverov, zariadení IoT, virtualizačnej infraštruktúry a kontajnerov.

2.2 Je záväzná pre:

2.2.1 interný personál: administrátorov IT, systémových inžinierov, vývojárov aplikácií, bezpečnostných analytikov a tímy infraštruktúry.

2.2.2 externé strany: zmluvných dodávateľov, poskytovateľov riadených služieb (MSP), dodávateľov softvéru a systémových integrátorov s technickou zodpovednosťou za aktíva v rozsahu pôsobnosti.

2.3 Politika pokrýva celý životný cyklus riadenia zraniteľností a záplat vrátane:

2.3.1 skenovania a detekcie,

2.3.2 klasifikácie a prioritizácie rizík,

2.3.3 získania, testovania, nasadenia záplat a návratu zmien,

2.3.4 ošetrovania výnimiek a plánovania kompenzačných kontrol,

2.3.5 logovania, vykazovania a auditnej sledovateľnosti.

3. Ciele

3.1 Zabezpečiť, aby všetky známe zraniteľnosti boli identifikované, vyhodnotené a odstránené spôsobom, ktorý minimalizuje vystavenie riziku a je v súlade s prevádzkovými prioritami.

3.2 Zaviesť konzistentné procesy riadenia zraniteľností v celej organizácii pre skenovanie zraniteľností, klasifikáciu závažnosti (napr. CVSS) a riadenie záplat vrátane núdzového riešenia a plánovania návratu zmien.

3.3 Umožniť riadenie bezpečnej konfigurácie prostredníctvom zosúladenia s referenčnými konfiguráciami hardeningu, postupmi riadenia zmien a aktuálnym spravodajstvom o hrozbách.

3.4 Zabezpečiť merateľný súlad s regulačnými a normatívnymi kontrolami týkajúcimi sa integrity systémov, disciplíny záplatovania a včasného odstraňovania chýb.

3.5 Vymedziť zodpovednosti a preukázateľnú zodpovednosť jednotlivých rolí za celý životný cyklus riadenia zraniteľností tak, aby všetky zainteresované strany konali v rámci definovaných dohôd o úrovni služieb (SLA) a vykazovaných metrík kontrol.

3.6 Podporiť pripravenosť na audit a zvýšiť odolnosť voči novým hrozbám vrátane zero-day zraniteľností, aktívnych reťazcov zneužitia a významných oznámení dodávateľov.

4. Roly a zodpovednosti

4.1 Riaditeľ informačnej bezpečnosti (CISO)

4.1.1 Je vlastníkom tejto politiky a zabezpečuje jej integráciu v rámci ISMS.

4.1.2 Definuje rizikový profil organizácie a zabezpečuje súlad s regulačnými požiadavkami a očakávaniami v oblasti kontrol.

4.2 Vedúci riadenia zraniteľností / manažér bezpečnostných operácií

4.2.1 Zodpovedá za komplexné riadenie činností súvisiacich so zraniteľnosťami a záplatami.

4.2.2 Koordinuje harmonogramy skenovania, modely prioritizácie a lehoty nápravy.

4.2.3 Vedie register zraniteľností a spolupracuje pri hodnotení kompenzačných kontrol.

[... Sekcie 4.3–8 nie sú súčasťou tohto náhľadu. Pre prístup k úplnému obsahu si zakúpte celý dokument. ...]

9. Požiadavky na preskúmanie a aktualizáciu

9.1 Táto politika musí byť preskúmaná najmenej raz ročne alebo pri:

9.1.1 významných regulačných aktualizáciách (napr. zmeny v DORA, NIS2),

9.1.2 zmenách rámcov prioritizácie zraniteľností (napr. aktualizácie CVSS),

9.1.3 významných zmenách IT prostredia (napr. migrácia do cloudového prostredia, zásadná zmena EDR),

9.1.4 významných porušeniach bezpečnosti alebo externých upozorneniach vyžadujúcich sprísnenie politiky.

9.2 Preskúmania vykonáva CISO v spolupráci s bezpečnostnými operáciami, riadením rizík a vedením infraštruktúry.

9.3 Aktualizácie politiky musia byť:

9.3.1 zdokumentované v registri riadenia dokumentácie ISMS,

9.3.2 preskúmané a schválené výkonným manažmentom,

9.3.3 oznámené všetkým dotknutým zainteresovaným stranám vrátane poskytovateľov služieb tretích strán.

9.4 Historické verzie musia byť bezpečne uchovávané na účely auditu a preukázateľnej zodpovednosti.

10. Súvisiace politiky a väzby

10.1 P1 - Politika informačnej bezpečnosti. Stanovuje celkový záväzok chrániť systémy a údaje vrátane proaktívneho riadenia zraniteľností a zabezpečenia integrity softvéru.

10.2 P5 - Politika riadenia zmien. Upravuje všetky nasadenia záplat a úpravy konfigurácie a vyžaduje dokumentáciu, testovanie, schválenie a postupy návratu zmien, ktoré dopĺňajú procesy odstraňovania zraniteľností.

10.3 P6 - Politika riadenia rizík. Podporuje klasifikáciu a ošetrenie neodstránených zraniteľností prostredníctvom štruktúrovaných posúdení rizík, analýzy vplyvu a postupov akceptácie reziduálneho rizika.

10.4 P12 - Politika správy aktív. Zabezpečuje, aby boli systémy presne evidované a klasifikované, čo umožňuje konzistentné skenovanie zraniteľností, priradenie vlastníctva a pokrytie záplatovaním počas celého životného cyklu.

10.5 P22 - Politika logovania a monitorovania. Definuje požiadavky na detekciu udalostí a vytváranie auditnej stopy. Táto politika podporuje viditeľnosť činností záplatovania, neautorizovaných zmien a pokusov o zneužitie zameraných na známe zraniteľnosti.

10.6 P30 - Politika reakcie na incidenty (P30). Stanovuje eskalačné postupy a stratégie zamedzenia šírenia pri zneužitých zraniteľnostiach, vyšetrovaniach porušení a nápravných opatreniach zosúladených s kontrolami tejto politiky.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001: Kapitola 8.1 - Prevádzkové plánovanie a riadenie: Vyžaduje systematické ošetrovanie technických zraniteľností s cieľom zabezpečiť priebežnú účinnosť bezpečnostných kontrol.

11.2 ISO/IEC 27002:2022 - Kontroly 8.8, 8.9, 5: Poskytuje implementačné usmernenia pre záplatovanie, skenovanie zraniteľností, integritu softvéru a integráciu s bezpečnou konfiguráciou a inventarizáciou aktív.

11.3 NIST SP 800-53 Rev.: RA-5 - Monitorovanie a skenovanie zraniteľností: Vyžaduje časté skenovanie a sledovanie nápravy. SI-2 - Odstraňovanie chýb: Vyžaduje bezodkladné vyhodnotenie a zmiernenie chýb dostupnými záplatami alebo inými opatreniami. CM-2 / CM-6 - Referenčné konfigurácie a kontroly riadenia konfigurácie: Vytvára základ pre bezpečné konfigurácie systémov naviazané na uplatňovanie záplat.

11.4 Nariadenie EÚ GDPR (2016/679): Článok 32 - Bezpečnosť spracúvania: Vyžaduje zavedenie primeraných technických opatrení, ako je bezodkladné záplatovanie a ošetrovanie zraniteľností, na

zabezpečenie dôvernosti a odolnosti systémov. Odôvodnenie 49: Podporuje zavádzanie preventívnych kontrol proti známym hrozbám na podporu bezpečnosti a kontinuity.

11.5 Smernica EÚ NIS2 (2022/2555): Článok 21(2)(d): Ukladá základným a dôležitým subjektom povinnosť detegovať, riešiť a zmierňovať zraniteľnosti systémov a udržiavať vysokú úroveň kybernetickej hygieny.

11.6 Nariadenie EÚ DORA (2022/2554): Článok 8 - Riadenie rizík IKT: Vyžaduje identifikáciu a včasné odstraňovanie zraniteľností v informačných a komunikačných technológiách používaných vo finančných systémoch. Článok 10(2)(f): Zdôrazňuje nepretržité hodnotenia zraniteľností riadené hrozbami a záplatovanie ako súčasť prevádzkovej odolnosti.

11.7 COBIT 2019: DSS05.02 - Riadenie bezpečnostných zraniteľností: Usmerňuje organizácie, aby skenovali, sledovali a zmierňovali známe technické slabiny. DSS01.03 - Monitorovanie infraštruktúry: Zabezpečuje, aby boli systémy monitorované na známky zneužitia alebo slabín. MEA03 - Monitorovanie, hodnotenie a posudzovanie súladu: Vyžaduje pravidelné auditovanie účinnosti kontrol vrátane stavu záplat a ošetrovania výnimiek.