					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P19S					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**

V súlade s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	Kapitola 8	
ISO/IEC 27002:2022	Kontroly 8.8, 8.9	
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2	
Smernica EÚ NIS2	Články 21 ods. 2 písm. d), 21 ods. 2 písm. e)	
Nariadenie EÚ DORA	Články 8 ods. 1, 10 ods. 2	
COBIT 2019	DSS05.02, APO12	
Nariadenie EÚ GDPR	Článok 32 ods. 1 písm. b)	

1. Účel

1.1 Táto politika stanovuje spôsob, akým organizácia identifikuje, vyhodnocuje a zmierňuje zraniteľnosti v systémoch, aplikáciách a infraštruktúre.

1.2 Jej účelom je znižovať kybernetické riziko prostredníctvom včasného záplatovania a opatrení na nápravu založených na riziku, primeraných pre malé a stredné podniky (MSP).

1.3 Táto politika podporuje súlad s požiadavkami ISO/IEC 27001:2022 a napomáha plneniu regulačných povinností podľa GDPR, NIS2 a DORA tým, že vyžaduje proaktívne riadenie technických zraniteľností.

1.4 Organizácia uznáva, že nezaplátané systémy predstavujú významnú hrozbu pre informačnú bezpečnosť a musia sa riešiť systematicky a bezodkladne.

2. Rozsah

2.1 Táto politika sa vzťahuje na:

2.1.1 všetky servery, stolové počítače, notebooky, mobilné zariadenia, sieťové zariadenia a cloudové platformy používané organizáciou,

2.1.2 všetky operačné systémy, softvér tretích strán, zásuvné moduly a aplikácie používané v prevádzke organizácie,

2.1.3 interný IT personál alebo externých poskytovateľov služieb zodpovedných za údržbu systémov, aktualizácie alebo monitorovanie,

2.1.4 akýkoľvek interne vyvíjaný kód alebo vstavaný softvér, ktorý organizácia spravuje sama alebo prostredníctvom tretej strany.

2.2 Politika sa vzťahuje na infraštruktúru riadenú priamo organizáciou aj na systémy spravované zmluvnými dodávateľmi alebo poskytovateľmi hostingu.

3. Ciele

3.1 Včasne a konzistentne identifikovať a posudzovať známe zraniteľnosti vo všetkých IT aktívach.

3.2 Aplikovať záplaty a aktualizácie softvéru podľa ich závažnosti a rizika pre prevádzku organizácie alebo osobné údaje.

3.3 Predchádzať zneužitiu technických slabín, ktoré by mohli viesť k prerušeniu služieb, porušeniu ochrany údajov alebo nesúladu s právnymi požiadavkami.

3.4 Udržiavať presné záznamy o aplikovaných záplatách, otvorených problémoch a výnimkách na účely auditnej pripravenosti.

3.5 Používať nástroje a procesy primerané veľkosti organizácie a prevádzkovej zložitosti bez zníženia ich účinnosti.

3.6 Podporovať právny a regulačný súlad vrátane článku 32 GDPR a prílohy A normy ISO, kontrola 8.

4. Roly a zodpovednosti

4.1 Generálny manažér (GM)

4.1.1 Nesie celkovú zodpovednosť za zabezpečenie vykonávania činností záplatovania a riadenia zraniteľností.

4.1.2 Schvaľuje rizikové výnimky v prípadoch, keď záplaty nemožno aplikovať, a preskúmava súvisiace stratégie zmierňovania.

4.1.3 Preskúmava správy o stave záplatovania a zabezpečuje dostupnosť zdrojov potrebných na plnenie povinností v oblasti záplatovania.

4.2 Poskytovateľ IT podpory / interný IT administrátor

4.2.1 Monitoruje systémy z hľadiska zraniteľností a dostupných záplat prostredníctvom upozornení dodávateľov, spravodajstva o hrozbách a oznámení na úrovni operačného systému.

4.2.2 Aplikuje aktualizácie operačných systémov, firmvéru a aplikácií v stanovených lehotách.

4.2.3 Vedie formálnu evidenciu záplat a dokumentuje nevyriešené alebo odložené aktualizácie.

4.2.4 Vykonáva testovanie a plánovanie kritických aktualizácií s cieľom minimalizovať prevádzkové narušenia.

[... 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 Ročné preskúmanie

9.1.1 Túto politiku musí najmenej raz ročne preskúmať Generálny manažér (GM) na základe vstupov od poskytovateľa IT a koordinátora ochrany osobných údajov.

9.2 Spúšťače preskúmania

9.2.1 Mimoriadne preskúmanie sa musí vykonať, ak:

9.2.1.1 závažná zraniteľnosť alebo exploit ovplyvní systémy v rozsahu tejto politiky,

9.2.1.2 dôjde k významným zmenám systémov alebo softvéru,

9.2.1.3 audit identifikuje nedostatky v procesoch záplatovania,

9.2.1.4 je zaznamenaný incident alebo porušenie súvisiace so záplatovaním.

9.3 Riadenie verzií politiky

9.3.1 Všetky aktualizácie musia byť zaznamenané v evidencii verzií spolu so súhrnom zmien.

9.3.2 Zmeny musia byť oznámené dotknutému personálu.

9.3.3 Neaktuálne verzie sa musia archivovať s obmedzeným prístupom.

10. Súvisiace politiky a väzby

10.1 Táto politika podporuje viaceré ďalšie politiky pre MSP a zároveň je od nich závislá:

10.1.1 P12S – Politika správy aktív: identifikuje vlastníctvo a klasifikáciu systémov a zabezpečuje, aby všetky aktíva vyžadujúce záplatovanie boli evidované v inventarizácii aktív.

10.1.2 P14S – Politika uchovávania a likvidácie údajov: zabezpečuje, aby systémy plánované na vyradenie boli bezpečne aktualizované alebo vymazané, čím sa znižuje vystavenie zraniteľnostiam.

10.1.3 P17S – Politika ochrany údajov a súkromia: uprednostňuje nápravu zraniteľností v systémoch spracúvajúcich osobné údaje s cieľom splniť právne požiadavky v oblasti súkromia.

10.1.4 P22S – Politika logovania a monitorovania: podporuje detekciu nezaplátaných systémov alebo podozrivého správania, ktoré môže signalizovať zneužitie zraniteľnosti.

10.1.5 P30S – Politika reakcie na incidenty: definuje postupy reakcie na zraniteľnosti, ktoré vedú k bezpečnostným incidentom, vrátane eskalácie a oznamovacích krokov.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001

11.1.1 Kapitola 8 – Vyžaduje implementáciu kontrol na riešenie prevádzkových rizík vrátane riadenia zraniteľností.

11.2 ISO/IEC 27002

11.2.1 Kontrola 8.8 – Špecifikuje procesy skenovania a odstraňovania známych slabín v systémoch.

11.2.2 Kontrola 8.9 – Zdôrazňuje bezpečnú konfiguráciu, overovanie záplat a riadenie zmien s cieľom predchádzať novým vystaveniam riziku počas aktualizácií.

11.3 NIST SP 800-53 Rev.5

11.3.1 RA-5 – Vyžaduje identifikáciu zraniteľností a ich nápravu v stanovených lehotách.

11.3.2 SI-2 – Ukladá bezodkladnú aplikáciu záplat a aktualizácií podľa závažnosti.

11.3.3 CM-2 – Upravuje referenčné konfigurácie systémov a dokumentovanie aktualizácií s cieľom zabezpečiť konzistentnú ochranu.

11.4 Nariadenie EÚ GDPR

11.4.1 Článok 32 ods. 1 písm. b) – Vyžaduje, aby organizácie zaviedli primerané technické opatrenia vrátane záplatovania na zachovanie bezpečnosti spracúvania.

11.5 Smernica EÚ NIS2

11.5.1 Článok 21 ods. 2 písm. d) – Vyžaduje riešenie zraniteľností prostredníctvom systematického skenovania a nápravy.

11.5.2 Článok 21 ods. 2 písm. e) – Ukladá bezpečnú konfiguráciu a riadenie záplat na zabezpečenie odolnosti IKT.

11.6 Nariadenie EÚ DORA

11.6.1 Článok 8 ods. 1 – Vyžaduje identifikáciu a zmierňovanie IKT rizík vrátane technických zraniteľností.

11.6.2 Článok 10 ods. 2 – Ukladá finančným subjektom odstrániť slabiny ovplyvňujúce systémy IKT a prevádzku.

11.7 COBIT 2019

11.7.1 DSS05.02 – Vyžaduje ošetrenie známych technických zraniteľností na zachovanie bezpečnej prevádzky.

11.7.2 APO12.01 – Zosúlaďuje riadenie rizík s proaktívnym monitorovaním a odstraňovaním systémových slabín.