					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P19					Název dokumentu: **Politika řízení zranitelností a záplat**							
Verze: 1.0		Datum účinnosti: 01.01.2025			Vlastník dokumentu:							
X	Politika		Standard		Postup		Formulář		Registr		Jiné	

Historie revizí				
Číslo revize	**Datum revize**	**Změny**	**Přezkoumal**	**Vlastník procesu**

Schválení			
Jméno	**Funkce**	**Datum**	**Podpis**

V souladu s normami a právními předpisy

Norma/právní předpis	Kapitola/článek	Komentář
ISO/IEC 27001:2022	Kapitola 8	Systematické ošetřování technických zranitelností; průběžné zajišťování účinnosti bezpečnostních opatření.
ISO/IEC 27002:2022	Opatření 8.8, 8.9, 5	Pokyny k implementaci pro záplatování, skenování zranitelností, integritu softwaru, bezpečnou konfiguraci a evidenci aktiv.
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2, CM-6	Vyžaduje časté skenování, odstraňování zjištěných nedostatků a řízení konfigurace.
GDPR	Článek 32, bod odůvodnění 49	Technická opatření pro včasné záplatování, ošetřování zranitelností a zajištění kontinuity bezpečnosti.
směrnice NIS2	Článek 21(2)(d)	Detekce, reakce a zmírňování zranitelností za účelem dosažení vysoké úrovně kybernetické hygieny.
nařízení DORA	Články 8, 10(2)(f)	Včasná náprava zranitelností ICT; průběžná hodnocení založená na hrozbách.
COBIT 2019	DSS05.02, DSS01.03, MEA	Skenování, sledování a zmírňování technických slabin; monitorování známek zneužití; audit účinnosti včetně stavu záplat.

1. Účel

1.1 Tato politika stanoví závazné požadavky organizace na identifikaci, klasifikaci, nápravu a monitorování technických zranitelností a softwarových chyb ve všech informačních systémech a aktivech v rozsahu systému řízení bezpečnosti informací (ISMS).

1.2 Zajišťuje, aby všechny známé zranitelnosti byly posuzovány a řešeny včas a na základě rizik prostřednictvím koordinovaného záplatování, úprav konfigurace nebo kompenzačních opatření, v souladu s obchodními potřebami a povinnostmi v oblasti souladu.

1.3 Tato politika podporuje soulad s ISO/IEC 27001, přílohou A, opatřením 8.8 a pokyny ISO/IEC 27002 a zohledňuje regulační požadavky podle článku 8 nařízení DORA, článku 21 směrnice NIS2, článku 32 GDPR a domén DSS a APO COBIT 2019.

2. Rozsah

2.1 Tato politika se vztahuje na všechny informační systémy, aktiva a prostředí, která ukládají, zpracovávají nebo přenášejí data spravovaná v rámci ISMS, včetně:

2.1.1 operačních systémů, aplikací, síťových zařízení, firmwaru, cloudových platforem, rozhraní API a softwaru třetích stran.

2.1.2 systémů ve vývoji, ve staging prostředí, v produkčním prostředí, v prostředích pro zálohování a v prostředí pro obnovu po havárii.

2.1.3 koncových bodů, serverů, zařízení IoT, virtualizační infrastruktury a kontejnerů.

2.2 Je závazná pro:

2.2.1 interní pracovníky: správce IT, systémové inženýry, vývojáře aplikací, bezpečnostní analytiky a infrastrukturní týmy.

2.2.2 externí strany: dodavatele a poskytovatele služeb třetích stran, poskytovatele řízených služeb (MSP), dodavatele softwaru a systémové integrátory s technickou odpovědností za aktiva v rozsahu této politiky.

2.3 Politika pokrývá celý životní cyklus řízení zranitelností a záplat, včetně:

2.3.1 skenování a detekce

2.3.2 klasifikace a prioritizace rizik

2.3.3 získávání, testování, nasazování a vracení záplat

2.3.4 řešení výjimek a plánování kompenzačních opatření

2.3.5 protokolování, reportování a dohledatelnosti pro účely auditu

3. Cíle

3.1 Zajistit, aby všechny známé zranitelnosti byly identifikovány, vyhodnoceny a odstraněny způsobem, který minimalizuje zbytkovou expozici a odpovídá provozním prioritám.

3.2 Zavést konzistentní celopodnikové procesy pro skenování zranitelností, klasifikaci závažnosti (např. CVSS) a řízení záplat, včetně řešení nouzových situací a plánování vrácení změn.

3.3 Umožnit účinné řízení bezpečné konfigurace prostřednictvím souladu s výchozí konfigurací, postupy řízení změn a informacemi o hrozbách v reálném čase.

3.4 Poskytovat měřitelný soulad s regulačními požadavky a požadavky norem souvisejícími s integritou systémů, hygienou záplat a včasným odstraňováním chyb.

3.5 Vymezit pravomoci a odpovědnosti napříč rolemi pro celý životní cyklus řízení zranitelností tak, aby všechny zainteresované strany jednaly v souladu s definovanými dohodami o úrovni služeb (SLA) a vykazovanými metrikami kontrol.

3.6 Posilovat připravenost na audit a zvyšovat odolnost vůči nově vznikajícím hrozbám, včetně zranitelností typu zero-day, aktivních řetězců zneužití a významných oznámení dodavatelů.

4. Role a odpovědnosti

4.1 ředitel informační bezpečnosti (CISO)

4.1.1 Odpovídá za tuto politiku a zajišťuje její začlenění do ISMS.

4.1.2 Stanovuje postoj k riziku na úrovni podniku a zajišťuje soulad s regulačními požadavky a očekáváními v oblasti kontrol.

4.2 vedoucí řízení zranitelností / manažer bezpečnostního provozu

4.2.1 Zajišťuje dohled nad celým procesem řízení zranitelností a záplat.

4.2.2 Koordinuje harmonogramy skenování, modely prioritizace a lhůty pro nápravu.

4.2.3 Spravuje registr zranitelností a spolupracuje na vyhodnocování kompenzačních opatření.

[... Oddíly 4.3–8 nejsou součástí tohoto náhledu. Pro přístup k úplnému obsahu zakupte celý dokument. ...]

9. Požadavky na přezkoumávání a aktualizaci

9.1 Tato politika musí být přezkoumána nejméně jednou ročně nebo při:

9.1.1 významných regulačních změnách (např. změny v nařízení DORA, směrnici NIS2)

9.1.2 změnách rámců pro prioritizaci zranitelností (např. aktualizace CVSS)

9.1.3 významných změnách IT prostředí (např. migrace do cloudu, zásadní změna EDR)

9.1.4 závažných bezpečnostních incidentech nebo externích upozorněních vyžadujících posílení politiky

9.2 Přezkumy provádí CISO ve spolupráci s bezpečnostním provozem, řízením rizik a vedením infrastruktury.

9.3 Aktualizace politiky musí být:

9.3.1 zdokumentovány v registru řízení dokumentace ISMS

9.3.2 přezkoumány a schváleny vrcholovým vedením

9.3.3 oznámeny všem dotčeným zainteresovaným stranám, včetně zpracovatelů třetích stran

9.4 Historické verze musí být bezpečně uchovávány pro účely auditu a odpovědnosti.

10. Související politiky a vazby

10.1 P1 - Politika informační bezpečnosti. Stanoví celkový závazek chránit systémy a data, včetně proaktivního řízení zranitelností a zajištění integrity softwaru.

10.2 P5 - Politika řízení změn. Řídí veškeré nasazování záplat a úpravy konfigurace a vyžaduje dokumentaci, testování, schválení a postupy vrácení změn, které doplňují procesy nápravy zranitelností.

10.3 P6 - Politika řízení rizik. Podporuje klasifikaci a ošetření neodstraněných zranitelností prostřednictvím strukturovaného hodnocení rizik, analýzy dopadů a postupů přijetí zbytkového rizika.

10.4 P12 - Politika správy aktiv. Zajišťuje, aby systémy byly přesně evidovány a klasifikovány, což umožňuje konzistentní skenování zranitelností, přiřazení vlastnictví a pokrytí záplatami v celém životním cyklu.

10.5 P22 - Politika protokolování a monitorování. Definuje požadavky na detekci událostí a vytváření auditní stopy. Tato politika podporuje viditelnost činností záplatování, neoprávněných změn a pokusů o zneužití známých zranitelností.

10.6 P30 - Politika reakce na incidenty (P30). Specifikuje eskalační postupy a strategie omezení šíření pro zneužité zranitelnosti, vyšetřování bezpečnostních incidentů a nápravná opatření v souladu s kontrolami této politiky.

11. Referenční normy a rámce

11.1 ISO/IEC 27001: Kapitola 8.1 - Provozní plánování a řízení: Vyžaduje systematické ošetřování technických zranitelností za účelem zajištění průběžné účinnosti bezpečnostních opatření.

11.2 ISO/IEC 27002:2022 - Opatření 8.8, 8.9, 5: Poskytuje pokyny k implementaci pro záplatování, skenování zranitelností, integritu softwaru a integraci s bezpečnou konfigurací a evidencí aktiv.

11.3 NIST SP 800-53 Rev.5: RA-5 - Monitorování a skenování zranitelností: Vyžaduje časté skenování a sledování nápravy. SI-2 - Náprava chyb: Vyžaduje bezodkladné vyhodnocení a zmírnění chyb dostupnými záplatami nebo jinými opatřeními. CM-2 / CM-6 - Výchozí stavy a opatření řízení konfigurace: Vytváří základ pro bezpečné konfigurace systémů navázané na vynucování záplat.

11.4 GDPR (2016/679): Článek 32 - Zabezpečení zpracování: Vyžaduje zavedení odpovídajících technických opatření, jako je včasné záplatování a ošetřování zranitelností, za účelem zajištění důvěrnosti a odolnosti systémů. Bod odůvodnění 49: Podporuje zavádění preventivních kontrol proti známým hrozbám na podporu bezpečnosti a kontinuity.

11.5 směrnice NIS2 (2022/2555): Článek 21(2)(d): Ukládá základním a významným subjektům povinnost detekovat zranitelnosti systémů, reagovat na ně a zmírňovat je a udržovat vysokou úroveň kybernetické hygieny.

11.6 nařízení DORA (2022/2554): Článek 8 - Řízení rizik v oblasti ICT: Vyžaduje identifikaci a včasnou nápravu zranitelností v informačních a komunikačních technologiích používaných ve finančních

systémech. Článek 10(2)(f): Zdůrazňuje průběžná hodnocení zranitelností a záplatování řízené hrozbami jako součást provozní odolnosti.

11.7 COBIT 2019: DSS05.02 - Řízení bezpečnostních zranitelností: Ukládá organizacím skenovat, sledovat a zmírňovat známé technické slabiny. DSS01.03 - Monitorování infrastruktury: Zajišťuje monitorování systémů z hlediska známek zneužití nebo slabin. MEA03 - Monitorování, hodnocení a posuzování souladu: Vyžaduje pravidelný audit účinnosti opatření, včetně stavu záplat a řešení výjimek.