					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P20					Názov dokumentu: **Politika ochrany koncových bodov a ochrany pred malvérom**							
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	Ochrana koncových bodov a kontroly proti malvéru sú vyžadované na splnenie cieľov systému manažérstva informačnej bezpečnosti (ISMS)
ISO/IEC 27002:2022	Kontroly 8.7, 8	Poskytuje technické kontroly a usmernenia pre antimalvérové opatrenia, ochranu koncových bodov a riešenie incidentov
NIST SP 800-53 Rev.5	SI-3, SI-4, CM-6	Definuje požiadavky na ochranu pred škodlivým kódom, centrálne monitorovanie a referenčnú konfiguráciu
GDPR EÚ	Článok 32	Ukladá primerané technické opatrenia na ochranu osobných údajov vrátane ochrany pred malvérom
Smernica EÚ NIS2	Článok 21(2)(d)	Vyžaduje nasadenie detekcie hrozieb a preventívnych opatrení na úrovni koncových bodov
Nariadenie EÚ DORA	Článok 9	Vyžaduje riadenie rizík IKT v oblasti malvéru a ochrany pred hrozbami vychádzajúcimi z koncových bodov
COBIT 2019	DSS05.01, DSS01.04, MEA	Ukladá ochranu, monitorovanie a hodnotenie kontrol koncových bodov

1. Účel

1.1 Táto politika stanovuje povinné kontroly a prevádzkové požiadavky na ochranu koncových bodov organizácie vrátane stolových počítačov, notebookov, mobilných zariadení a serverov pred malvérom a súvisiacimi hrozbami.

1.2 Stanovuje minimálne štandardy pre ochranu koncových bodov, detekciu malvéru, reakciu na zamedzenie šírenia a behaviorálne monitorovanie tak, aby systémy zostali odolné voči bežným aj pokročilým variantom malvéru.

1.3 Táto politika priamo podporuje súlad s ISO/IEC 27001:2022, kapitolou 8.1 a prílohou A, kontrolou 8.7, a je zosúladená s regionálnymi povinnosťami kybernetickej bezpečnosti podľa GDPR, NIS2 a DORA.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetky koncové body vrátane:

2.1.1 stolových počítačov, notebookov, mobilných zariadení a virtuálnych inštancií vo vlastníctve organizácie alebo spravovaných organizáciou,

2.1.2 súkromných zariadení povolených podľa politiky Používanie vlastných zariadení (BYOD), ak podliehajú inštalácii MDM alebo agentov koncových bodov,

2.1.3 serverov a infraštruktúrnych aktív vrátane virtuálnych strojov prevádzkovaných v cloudovom prostredí a okrajových zariadení,

2.1.4 operačných systémov, ovládačov, lokálnych služieb, agentov koncových bodov a bezpečnostných kontrol nainštalovaných na každom uzle.

2.2 Táto politika sa vzťahuje na všetkých pracovníkov s administrátorskou, technickou alebo prevádzkovou zodpovednosťou za akýkoľvek koncový bod vrátane:

2.2.1 interných zamestnancov a zmluvných pracovníkov,

2.2.2 poskytovateľov spravovaných služieb (MSP), externej podpory pracovných staníc a IT administrátorov tretích strán,

2.2.3 používateľov oprávnených používať prenosné systémy, notebooky s podnikovou VPN alebo mobilný prístup do sietí organizácie.

2.3 Pokrytie hrozieb podľa tejto politiky zahŕňa okrem iného:

2.3.1 vírusy, červy, trójske kone, ransomvér, spyware, rootkity, adware, keyloggery a botnety,

2.3.2 bezsúborový malvér, zero-day škodlivé zaťaženia, malvér na eskaláciu oprávnení a exploit kity pre prehliadače,

2.3.3 škodlivý kód doručovaný prostredníctvom prenosných médií, phishingových vektorov, drive-by downloadov alebo útokov cez USB.

3. Ciele

3.1 Chrániť integritu, dostupnosť a dôvernosť systémov koncových bodov a údajov, ktoré spracúvajú, prostredníctvom spoľahlivej prevencie, detekcie a reakcie na malvér.

3.2 Zamedziť spusteniu alebo šíreniu škodlivého kódu v sieťach organizácie uplatňovaním technických ochranných opatrení, hardeningu podľa referenčnej konfigurácie a telemetrie v reálnom čase.

3.3 Integrovať ochranu koncových bodov s ďalšími kontrolami ISMS vrátane riadenia zraniteľností, riadenia prístupu, auditného logovania a monitorovania a reakcie na incidenty.

3.4 Zabezpečiť nepretržitú viditeľnosť koncových bodov prostredníctvom centrálne spravovaných platforiem ochrany vrátane antivírusového softvéru/antimalvérových agentov, EDR (Endpoint Detection and Response) a telemetrie SIEM.

3.5 Zabezpečiť súlad so zákonnými, regulačnými a normatívnymi požiadavkami vyžadujúcimi zabezpečenie koncových bodov, napríklad podľa článku 32 GDPR, článku 21 NIS2 a článku 9 DORA.

3.6 Stanoviť jasne pridelené zodpovednosti, uplatňovať SLA pre záplatovanie a reakciu na upozornenia a zabezpečiť pripravenosť na audit prostredníctvom dokumentácie a reportingu.

4. Roly a zodpovednosti

4.1 Riaditeľ informačnej bezpečnosti (CISO)

4.1.1 Zodpovedá za túto politiku a zabezpečuje jej súlad s ISMS a celkovou bezpečnostnou stratégiou.

4.1.2 Štvrťročne preskúmava metriky ochrany koncových bodov, trendy incidentov a účinnosť nástrojov.

4.1.3 Schvaľuje výnimky a akceptáciu reziduálneho rizika súvisiacu s pokrytím koncových bodov.

4.2 Vedúci bezpečnosti koncových bodov / manažér SOC

4.2.1 Spravuje systémy ochrany koncových bodov, napríklad AV, EDR a MDM.

4.2.2 Dohliada na uplatňovanie politiky, ladenie detekcie hrozieb a playbooky reakcie.

4.2.3 Udržiava štatistiky pokrytia, záznamy o incidentoch s malvérom a referenčné konfigurácie upozornení.

[... 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 sa musí preskúmať raz ročne alebo vtedy, keď:

9.1.1 dôjde k významným malvérovým kampaniam alebo incidentom bezpečnosti koncových bodov,

9.1.2 nové typy hrozieb, napríklad bezsúborový malvér alebo varianty ransomvéru, vyžadujú aktualizované stratégie detekcie alebo reakcie,

9.1.3 sa významne zmenia platformy ochrany koncových bodov alebo architektúry agentov,

9.1.4 sa aktualizujú zákonné alebo regulačné požiadavky ovplyvňujúce kontroly koncových bodov.

9.2 Preskúmanie iniciuje Vedúci bezpečnosti koncových bodov a koordinuje ho s funkciami CISO, právnych záležitostí, riadenia rizík a auditu.

9.3 Schválené revízie musia byť zdokumentované v registri riadenia dokumentácie ISMS, musí im byť priradený nový identifikátor verzie a musia byť oznámené všetkým dotknutým stranám.

9.4 Nahradené verzie musia byť archivované s obmedzeným prístupom a uchovávané na zachovanie integrity auditnej stopy podľa lehôt uchovávania ISMS.

10. Súvisiace politiky a väzby

10.1 P1 - Politika informačnej bezpečnosti. Stanovuje základné princípy ochrany systémov, údajov a sietí. Táto politika uplatňuje tieto princípy na úrovni koncových bodov prostredníctvom technických a procesných kontrol ochrany pred malvérom.

10.2 P4 - Politika riadenia prístupu. Definuje obmedzenia prístupu používateľov, ktoré sa uplatňujú na vrstve koncových bodov, vrátane ochrany pred eskaláciou oprávnení a neoprávnenými inštaláciami nepreverereného softvéru.

10.3 P5 - Politika riadenia zmien. Zabezpečuje, aby aktualizácie softvéru ochrany koncových bodov, pravidiel politiky alebo konfigurácií agentov podliehali schváleniu a riadeným procesom nasadenia.

10.4 P12 - Politika správy aktív. Poskytuje základ klasifikácie aktív a inventarizácie potrebný na viditeľnosť koncových bodov, pokrytie záplatovaním a vymedzenie rozsahu ochrany pred malvérom.

10.5 P22 - Politika logovania a monitorovania. Umožňuje integráciu upozornení z koncových bodov, stavu agentov a spravodajstva o hrozbách do centralizovaných systémov SIEM na detekciu v reálnom čase a forenznú sledovateľnosť.

10.6 P30 - Politika reakcie na incidenty (P30). Prepája incidenty s malvérom na úrovni koncových bodov so štandardizovanými pracovnými postupmi pre zamedzenie šírenia, odstránenie, vyšetrovanie a obnovu s pridelenými rolami a prahovými hodnotami eskalácie.

11. Referenčné normy a rámce

11.1 ISO/IEC 27001:

11.1.1 Kapitola 8.1 - Prevádzkové plánovanie a riadenie: Vyžaduje implementáciu technických kontrol vrátane ochranných opatrení na koncových bodoch na udržanie cieľov ISMS.

11.2 ISO/IEC 27002:2022 - Kontroly 8.7, 8:

11.2.1 Poskytuje podrobné technické usmernenia k antimalvérovým opatreniam, bezpečnému nasadeniu softvéru, monitorovaniu a pripravenosti na incidenty v prostrediach koncových bodov.

11.3 NIST SP 800-53 Rev.5:

11.3.1 SI-3 - Ochrana pred škodlivým kódom: Vyžaduje používanie antimalvérových nástrojov so skenovaním v reálnom čase, pri prístupe a s behaviorálnou analýzou.

11.3.2 SI-4 - Monitorovanie systému: Podporuje integráciu telemetrie s centralizovanými platformami detekcie.

11.3.3 CM-6 - Nastavenia konfigurácie: Posilňuje referenčné nastavenia kontrol na koncových bodoch vrátane uplatňovania ochranných agentov.

11.4 Nariadenie EÚ GDPR (2016/679):

11.4.1 Článok 32 - Bezpečnosť spracúvania: Vyžaduje, aby organizácie zaviedli primerané technické opatrenia na ochranu osobných údajov vrátane ochrany pred malvérovými hrozbami.

11.5 Smernica EÚ NIS2 (2022/2555):

11.5.1 Článok 21(2)(d): Ukladá subjektom povinnosť nasadiť opatrenia detekcie a prevencie hrozieb vrátane mechanizmov ochrany pred malvérom na úrovni koncových bodov.

11.6 Nariadenie EÚ DORA (2022/2554):

11.6.1 Článok 9 - Požiadavky na riadenie rizík IKT: Vyžaduje, aby finančné subjekty prijali ochranné opatrenia na prevenciu, detekciu a reakciu na malvér a hrozby vychádzajúce z koncových bodov.

11.7 COBIT 2019:

11.7.1 DSS05.01 - Ochrana pred malvérom: Ukladá detekciu a zmierňovanie malvéru naprieč všetkými koncovými bodmi organizácie.

11.7.2 DSS01.04 - Riadenie dostupnosti a kapacity: Zabezpečuje, aby bola ochrana pred malvérom vyvážená s výkonom systémov a kontinuitou činností.

11.7.3 MEA03 - Monitorovanie, hodnotenie a posudzovanie súladu: Vyžaduje pravidelný audit kontrol koncových bodov a účinnosti ochrany.