| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Sem vložte název registrované právnické osoby | | | | | | | |
| Číslo dokumentu:<br>P20 | | | | | Název dokumentu:<br>**Politika ochrany koncových bodů / malwaru** | | | | | | | |
| Verze:<br>1.0 | | Datum účinnosti:<br>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 | Ochrana koncových bodů a ochrana proti malwaru jsou vyžadovány pro naplnění cílů ISMS |
| ISO/IEC 27002:2022 | Opatření 8.7, 8 | Poskytuje technická opatření a pokyny pro ochranu proti malwaru, ochranu koncových bodů a zvládání incidentů |
| NIST SP 800-53 Rev.5 | SI-3, SI-4, CM-6 | Definuje požadavky na ochranu proti škodlivému kódu, centralizované monitorování a výchozí konfigurace |
| GDPR EU | Článek 32 | Vyžaduje přiměřená technická opatření k ochraně osobních údajů, včetně ochrany proti malwaru |
| směrnice EU NIS2 | Článek 21 odst. 2 písm. d) | Vyžaduje nasazení detekce hrozeb na úrovni koncových bodů a preventivních opatření |
| nařízení EU DORA | Článek 9 | Vyžaduje řízení rizik v oblasti ICT pro ochranu proti malwaru a hrozbám přenášeným prostřednictvím koncových bodů |
| COBIT 2019 | DSS05.01, DSS01.04, MEA | Vyžaduje ochranu, monitorování a hodnocení opatření na ochranu koncových bodů |

## 1. Účel

1.1 Tato politika stanoví povinná opatření a provozní požadavky na ochranu koncových bodů organizace, včetně stolních počítačů, notebooků, mobilních zařízení a serverů, před malwarem a souvisejícími hrozbami.

1.2 Stanoví minimální standardy pro ochranu koncových bodů, detekci malwaru, reakci za účelem zamezení šíření a behaviorální monitorování tak, aby systémy zůstaly odolné vůči běžným i pokročilým variantám malwaru.

1.3 Tato politika přímo podporuje soulad s ISO/IEC 27001:2022, kapitolou 8.1 a přílohou A, opatřením 8.7, a je v souladu s regionálními povinnostmi v oblasti kybernetické bezpečnosti podle GDPR, NIS2 a DORA.

## 2. Rozsah

**2.1 Tato politika se vztahuje na všechny koncové body, včetně:**

2.1.1 stolních počítačů, notebooků, mobilních zařízení a virtuálních instancí vlastněných organizací nebo jí spravovaných

2.1.2 soukromých zařízení schválených podle Politiky používání vlastních zařízení (BYOD), za předpokladu instalace MDM nebo agentů koncových bodů

2.1.3 serverů a infrastrukturních aktiv, včetně virtuálních strojů hostovaných v cloudu a okrajových zařízení

2.1.4 operačních systémů, ovladačů, lokálních služeb, agentů koncových bodů a bezpečnostních opatření nainstalovaných na každém uzlu

**2.2 Tato politika se vztahuje na veškerý personál s administrativní, technickou nebo provozní odpovědností za jakýkoli koncový bod, včetně:**

2.2.1 interních zaměstnanců a smluvních pracovníků

2.2.2 poskytovatelů řízených služeb (MSP), externě zajišťované podpory desktopů a IT administrátorů třetích stran

2.2.3 uživatelů oprávněných používat přenosné systémy, notebooky s aktivovanou VPN nebo mobilní přístup do sítí organizace

**2.3 Pokrytí hrozeb podle této politiky zahrnuje mimo jiné:**

2.3.1 viry, červy, trojské koně, ransomware, spyware, rootkity, adware, keyloggery a botnety

2.3.2 fileless malware, zero-day payloady, malware pro eskalaci oprávnění a sady exploitů pro prohlížeče

2.3.3 škodlivý kód doručený prostřednictvím vyměnitelných médií, phishingových vektorů, drive-by downloadů nebo útoků přes USB

**3. Cíle**

3.1 Chránit integritu, dostupnost a důvěrnost systémů koncových bodů a dat, která zpracovávají, prostřednictvím spolehlivé prevence malwaru, detekce a reakce.

3.2 Zabránit spuštění nebo šíření škodlivého kódu v sítích organizace uplatňováním technických ochranných opatření, hardeningu výchozí konfigurace a telemetrie v reálném čase.

3.3 Integrovat ochranu koncových bodů s dalšími opatřeními ISMS, včetně řízení zranitelností, řízení přístupu, protokolování a monitorování a reakce na incidenty.

3.4 Zajistit nepřetržitou viditelnost koncových bodů prostřednictvím centrálně spravovaných platforem ochrany, včetně agentů antiviru/ochrany proti malwaru, EDR (detekce a reakce na koncových bodech) a telemetrie SIEM.

3.5 Zajistit soulad s právními, regulačními a normativními požadavky vyžadujícími zabezpečení koncových bodů (např. článek 32 GDPR, článek 21 NIS2, článek 9 DORA).

3.6 Vymezit odpovědné role, vynucovat SLA pro záplatování a reakci na upozornění a zajistit připravenost na audit prostřednictvím dokumentace a reportingu.

**4. Role a odpovědnosti**

**4.1 ředitel informační bezpečnosti (CISO)**

4.1.1 Odpovídá za tuto politiku a zajišťuje její soulad s ISMS a celkovou bezpečnostní strategií.

4.1.2 Čtvrtletně přezkoumává metriky ochrany koncových bodů, trendy incidentů a účinnost nástrojů.

4.1.3 Schvaluje výjimky a akceptaci zbytkového rizika související s pokrytím koncových bodů.

**4.2 Vedoucí ochrany koncových bodů / manažer SOC**

4.2.1 Spravuje systémy ochrany koncových bodů (např. AV, EDR, MDM).

4.2.2 Zajišťuje uplatňování politiky, ladění detekce hrozeb a playbooky reakce.

4.2.3 Udržuje statistiky pokrytí, logy incidentů souvisejících s malwarem a základní konfigurace upozornění.

[ ... 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 přezkoumávána každoročně nebo pokud:

9.1.1 dojde k rozsáhlým malwarovým kampaním nebo incidentům v oblasti zabezpečení koncových bodů

9.1.2 nové typy hrozeb (např. fileless malware, varianty ransomwaru) vyžadují aktualizované strategie detekce nebo reakce

9.1.3 se významně změní platformy ochrany koncových bodů nebo architektury agentů

9.1.4 jsou aktualizovány právní nebo regulační požadavky ovlivňující opatření pro koncové body

9.2 Přezkum zahajuje Vedoucí ochrany koncových bodů a koordinuje jej s funkcemi CISO, právní a compliance, řízení rizik a auditu.

9.3 Schválené revize musí být zdokumentovány v registru řízení dokumentace ISMS, musí jim být přiřazen nový identifikátor verze a musí být oznámeny všem dotčeným stranám.

9.4 Nahrazené verze musí být archivovány, jejich přístup omezen a musí být uchovávány pro zachování integrity auditní stopy podle retenčních lhůt ISMS.

## 10. Související politiky a vazby

10.1 P1 - Politika informační bezpečnosti. Stanoví základní zásady pro ochranu systémů, dat a sítí. Tato politika tyto zásady uplatňuje na úrovni koncových bodů prostřednictvím technických a procesních opatření proti malwaru.

10.2 P4 - Politika řízení přístupu. Definuje omezení přístupu uživatelů, která jsou vynucována na vrstvě koncových bodů, včetně ochrany proti eskalaci oprávnění a neoprávněným instalacím neprověřeného softwaru.

10.3 P5 - Politika řízení změn. Zajišťuje, aby aktualizace softwaru ochrany koncových bodů, pravidel politiky nebo konfigurací agentů podléhaly schválení a řízenému procesu nasazení.

10.4 P12 - Politika správy aktiv. Poskytuje základ pro klasifikaci aktiv a evidenci aktiv potřebný pro viditelnost koncových bodů, pokrytí záplatami a vymezení rozsahu ochrany proti malwaru.

10.5 P22 - Politika protokolování a monitorování. Umožňuje integraci upozornění z koncových bodů, stavu agentů a informací o hrozbách do centralizovaných systémů SIEM pro detekci v reálném čase a forenzní dohledatelnost.

10.6 P30 - Politika reakce na incidenty (P30). Propojuje incidenty malwaru na úrovni koncových bodů se standardizovanými pracovními postupy pro zamezení šíření, eradikaci, vyšetřování a obnovu s přiřazenými rolemi a prahovými hodnotami eskalace.

## 11. Referenční normy a rámce

### 11.1 ISO/IEC 27001:

11.1.1 Kapitola 8.1 - Provozní plánování a řízení: Vyžaduje implementaci technických opatření, včetně ochranných opatření koncových bodů, k udržení cílů ISMS.

### 11.2 ISO/IEC 27002:2022 - Opatření 8.7, 8:

11.2.1 Poskytuje podrobné technické pokyny k opatřením proti malwaru, bezpečnému nasazení softwaru, monitorování a připravenosti na incidenty v prostředích koncových bodů.

### 11.3 NIST SP 800-53 Rev.5:

11.3.1 SI-3 - Ochrana proti škodlivému kódu: Vyžaduje používání nástrojů ochrany proti malwaru se skenováním v reálném čase, skenováním při přístupu a behaviorální analýzou.

11.3.2 SI-4 - Monitorování systému: Podporuje integraci telemetrie s centralizovanými platformami detekce.

11.3.3 CM-6 - Nastavení konfigurace: Posiluje výchozí nastavení opatření na koncových bodech, včetně vynucování ochranných agentů.

**11.4 GDPR EU (2016/679):**

11.4.1 Článek 32 - Zabezpečení zpracování: Vyžaduje, aby organizace implementovaly přiměřená technická opatření k ochraně osobních údajů, včetně ochrany proti hrozbám malwaru.

**11.5 směrnice EU NIS2 (2022/2555):**

11.5.1 Článek 21 odst. 2 písm. d): Ukládá subjektům nasadit opatření pro detekci a prevenci hrozeb, včetně mechanismů ochrany proti malwaru na úrovni koncových bodů.

**11.6 nařízení EU DORA (2022/2554):**

11.6.1 Článek 9 - Požadavky na řízení rizik v oblasti ICT: Vyžaduje, aby finanční subjekty přijaly ochranná opatření k prevenci, detekci a reakci na malware a hrozby přenášené prostřednictvím koncových bodů.

**11.7 COBIT 2019:**

11.7.1 DSS05.01 - Ochrana proti malwaru: Vyžaduje detekci a zmírňování malwaru napříč všemi koncovými body organizace.

11.7.2 DSS01.04 - Řízení dostupnosti a kapacity: Zajišťuje, aby ochrana proti malwaru byla vyvážena s výkonností systému a kontinuitou činností.

11.7.3 MEA03 - Monitorování, hodnocení a posuzování souladu: Vyžaduje pravidelný audit opatření pro koncové body a účinnosti ochrany.