					Ide írja be a bejegyzett jogi személy nevét							
Dokumentumszám: P20					Dokumentum címe: **Végpontvédelem / Malware elleni védelem szabályzat**							
Verzió: 1.0		Hatálybalépés dátuma: 01.01.2025			A dokumentum tulajdonosa:							
X	Szabályzat		Szabvány		Eljárás		Űrlap		Nyilvántartás		Egyéb	

Felülvizsgálati előzmények				
Felülvizsgálat száma	**Felülvizsgálat dátuma**	**Változások**	**Felülvizsgálta**	**A folyamat tulajdonosa**

Jóváhagyások			
Név	**Beosztás**	**Dátum**	**Aláírás**

Vonatkozó szabványokkal és jogszabályokkal összhangban

Szabvány/jogszabály	Pont/cikk	Megjegyzés
ISO/IEC 27001:2022	8. pont	A végpontvédelemre és a malware elleni kontrollokra vonatkozó követelmények szükségesek az ISMS céljainak teljesítéséhez
ISO/IEC 27002:2022	8.7 és 8. kontroll	Technikai kontrollokat és útmutatást biztosít a malware elleni védelemhez, a végpontvédelemhez és az incidenskezeléshez
NIST SP 800-53 Rev.5	SI-3, SI-4, CM-6	Meghatározza a rosszindulatú kód elleni védelemre, a központi megfigyelésre és az alapkonfigurációkra vonatkozó követelményeket
GDPR	32. cikk	Előírja a személyes adatok védelmét szolgáló megfelelő technikai intézkedések alkalmazását, beleértve a malware elleni védelmet
NIS2 irányelv	21. cikk (2) bekezdés d) pont	Előírja a végponti fenyegetésészlelési és megelőző intézkedések bevezetését
DORA-rendelet	9. cikk	Előírja az IKT-kockázatkezelést a malware és a végpontokról eredő fenyegetések elleni védelem érdekében
COBIT 2019	DSS05.01, DSS01.04, MEA	Előírja a végponti kontrollok védelmét, megfigyelését és értékelését

1. Cél

1.1 Jelen szabályzat meghatározza a szervezeti végpontok - ideértve az asztali számítógépeket, hordozható számítógépeket, mobileszközöket és szervereket - malware és kapcsolódó fenyegetések elleni védelméhez szükséges kötelező kontrollokat és működési követelményeket.

1.2 Meghatározza a végpontvédelem, a malware-észlelés, az elhatárolási válaszintézkedések és a viselkedésalapú megfigyelés minimumkövetelményeit annak biztosítására, hogy a rendszerek ellenállóak maradjanak mind az általánosan elterjedt, mind a fejlett malware-változatokkal szemben.

1.3 A szabályzat közvetlenül támogatja az ISO/IEC 27001:2022 8.1 pontjának és az A melléklet 8.7 kontrolljának való megfelelést, továbbá összhangban áll a GDPR, a NIS2 és a DORA szerinti regionális kiberbiztonsági kötelezettségekkel.

2. Hatály

2.1 Jelen szabályzat az összes végpontra kiterjed, beleértve az alábbiakat:

2.1.1 A szervezet tulajdonában lévő vagy általa kezelt asztali számítógépek, hordozható számítógépek, mobileszközök és virtuális példányok

2.1.2 A BYOD szabályzat alapján engedélyezett saját tulajdonú eszközök, MDM vagy végponti ügynök telepítéséhez kötötten

2.1.3 Szerverek és infrastrukturális eszközök, beleértve a felhőben üzemeltetett virtuális gépeket és a peremhálózati eszközöket

2.1.4 Az egyes csomópontokon telepített operációs rendszerek, illesztőprogramok, helyi szolgáltatások, végponti ügynökök és biztonsági kontrollok

2.2 A szabályzat hatálya kiterjed minden olyan személyre, aki bármely végponttal kapcsolatban adminisztratív, műszaki vagy üzemeltetési felelősséget visel, beleértve az alábbiakat:

2.2.1 Belső munkavállalók és szerződéses közreműködők

2.2.2 Menedzselt szolgáltatók (MSP-k), kiszervezett munkaállomás-támogatási szolgáltatók és külső IT-adminisztrátorok

2.2.3 Azok a felhasználók, akik jogosultak hordozható rendszerek, VPN-képes hordozható számítógépek vagy a szervezeti hálózatokhoz történő mobil hozzáférés használatára

2.3 A jelen szabályzat szerinti fenyegetési kör többek között az alábbiakat foglalja magában:

2.3.1 Vírusok, férgek, trójai programok, zsarolóvírusok, kémprogramok, rootkitek, reklámprogramok, billentyűzetfigyelők, botnetek

2.3.2 Fájl nélküli malware, nulladik napi káros terhek, jogosultságkiterjesztésre szolgáló malware és böngészőalapú exploitkészletek

2.3.3 Cserélhető adathordozón, adathalász támadási vektorokon, drive-by letöltéseken vagy USB-alapú támadásokon keresztül terjesztett rosszindulatú kód

3. Célkitűzések

3.1 A végpontrendszerek és az általuk kezelt adatok sértetlenségének, rendelkezésre állásának és bizalmasságának védelme megbízható malware-megelőzési, -észlelési és -kezelési intézkedésekkel.

3.2 A rosszindulatú kód végrehajtásának vagy terjedésének megelőzése a szervezeti hálózatokon technikai védelmi intézkedések, előírt alapkonfigurációk megerősítése és valós idejű telemetria alkalmazásával.

3.3 A végpontvédelem integrálása az ISMS egyéb kontrolljaival, beleértve a sérülékenységkezelést, a hozzáférés-szabályozást, a naplózást és megfigyelést, valamint az incidenskezelést.

3.4 A végpontok folyamatos láthatóságának biztosítása központilag kezelt védelmi platformokkal, ideértve a vírusvédelmi/malware elleni ügynököket, az EDR-t (Endpoint Detection and Response) és a SIEM-telemetriát.

3.5 A végpontbiztonságra vonatkozó jogi, szabályozási és szabványalapú követelmények teljesítése (pl. GDPR 32. cikk, NIS2 21. cikk, DORA 9. cikk).

3.6 Az elszámoltatható szerepkörök meghatározása, a javításkezelési és riasztáskezelési SLA-k érvényesítése, valamint az auditra való felkészültség biztosítása dokumentáció és jelentéstétel útján.

4. Szerepkörök és felelősségek

4.1 Információbiztonsági vezető (CISO)

4.1.1 Felelős a szabályzatért, és biztosítja annak összhangját az ISMS-sel és az átfogó biztonsági stratégiával.

4.1.2 Negyedévente felülvizsgálja a végpontvédelmi mutatókat, az incidensek trendjeit és az eszközök hatékonyságát.

4.1.3 Jóváhagyja a végponti lefedettséghez kapcsolódó kivételeket és a fennmaradó kockázatok elfogadását.

4.2 Végpontbiztonsági vezető / SOC-vezető

4.2.1 Kezeli a végpontvédelmi rendszereket (pl. AV, EDR, MDM).

4.2.2 Felügyeli a szabályzat alkalmazását, a fenyegetésészlelés finomhangolását és a válaszintézkedési forgatókönyveket.

4.2.3 Fenntartja a lefedettségi statisztikákat, a malware-incidensek naplóit és a riasztási konfigurációk alapkonfigurációit.

[... A 4.3–8. szakaszok nem szerepelnek ebben az előnézetben. A teljes tartalom eléréséhez vásárolja meg a teljes dokumentumot. ...]

9. Felülvizsgálati és frissítési követelmények

9.1 Jelen szabályzatot évente, illetve az alábbi esetekben kell felülvizsgálni:

9.1.1 Jelentős malware-kampány vagy végpontbiztonsági incidens esetén

9.1.2 Ha új fenyegetéstípusok (pl. fájl nélküli malware, zsarolóvírus-változatok) módosított észlelési vagy válaszstratégiát tesznek szükségessé

9.1.3 Ha a végpontvédelmi platformok vagy ügynökarchitektúrák jelentősen megváltoznak

9.1.4 Ha a végponti kontrollokat érintő jogi vagy szabályozási követelmények módosulnak

9.2 A felülvizsgálatot a végpontbiztonsági vezető kezdeményezi, és azt a CISO-val, valamint a jogi, kockázatkezelési és audit funkciókkal összehangoltan kell végrehajtani.

9.3 A jóváhagyott módosításokat dokumentálni kell az ISMS dokumentumkezelési nyilvántartásában, új verzióazonosítóval kell ellátni, és azokat minden érintett féllel közölni kell.

9.4 A hatályon kívül helyezett verziókat archiválni kell, hozzáférésüket korlátozni kell, és az ISMS megőrzési ütemterve szerint meg kell őrizni az auditnyom sértetlenségének biztosítása érdekében.

10. Kapcsolódó szabályzatok és összefüggések

10.1 P1 - Információbiztonsági szabályzat. Meghatározza a rendszerek, adatok és hálózatok védelmének alapelveit. Jelen szabályzat ezeket az alapelveket végponti szinten, technikai és eljárási malware elleni kontrollok útján érvényesíti.

10.2 P4 - Hozzáférés-szabályozási szabályzat. Meghatározza a felhasználói hozzáférési korlátozásokat, amelyeket végponti szinten kell érvényesíteni, beleértve a jogosultságkiterjesztés és a nem ellenőrzött szoftverek jogosulatlan telepítése elleni védelmet.

10.3 P5 - Változáskezelési szabályzat. Biztosítja, hogy a végpontvédelmi szoftverek, szabályok vagy ügynökkonfigurációk módosításai jóváhagyáshoz és szabályozott bevezetési folyamathoz kötöttek legyenek.

10.4 P12 - Eszközkezelési szabályzat. Biztosítja azt az eszközbesorolási és leltározási alapot, amely a végponti láthatósághoz, a javítási lefedettséghez és a malware elleni védelem hatályának meghatározásához szükséges.

10.5 P22 - Naplózási és megfigyelési szabályzat. Lehetővé teszi a végponti riasztások, az ügynökök működési állapotának és a fenyegetésintelligenciának a központi SIEM-rendszerekbe történő integrálását valós idejű észlelés és igazságügyi visszakövethetőség céljából.

10.6 P30 - Incidenskezelési szabályzat. Összekapcsolja a végponti malware-incidenseket a szabványosított elhatárolási, eltávolítási, kivizsgálási és helyreállítási munkafolyamatokkal, kijelölt felelősségekkel és eszkalációs küszöbértékekkel.

11. Hivatkozott szabványok és keretrendszerek

11.1 ISO/IEC 27001:

11.1.1 8.1 pont - Operatív tervezés és kontroll: Előírja technikai kontrollok - ideértve a végponti védelmi intézkedéseket is - bevezetését az ISMS-célok fenntartása érdekében.

11.2 ISO/IEC 27002:2022 - 8.7 és 8. kontroll:

11.2.1 Részletes technikai útmutatást ad a malware elleni intézkedésekre, a biztonságos szoftverterítésre, a megfigyelésre és az incidensekre való felkészültségre végponti környezetekben.

11.3 NIST SP 800-53 Rev.5:

11.3.1 SI-3 - Rosszindulatú kód elleni védelem: Előírja malware elleni eszközök használatát valós idejű, hozzáféréskori vizsgálattal és viselkedéselemzéssel.

11.3.2 SI-4 - Rendszermegfigyelés: Támogatja a telemetria integrálását központi észlelési platformokkal.

11.3.3 CM-6 - Konfigurációs beállítások: Megerősíti az előírt végponti kontrollbeállításokat, beleértve a védelmi ügynökök alkalmazását.

11.4 GDPR (2016/679):

11.4.1 32. cikk - Az adatkezelés biztonsága: Előírja, hogy a szervezetek megfelelő technikai intézkedéseket vezessenek be a személyes adatok védelme érdekében, beleértve a malware-fenyegetésekkel szembeni védelmet.

11.5 NIS2 irányelv (2022/2555):

11.5.1 21. cikk (2) bekezdés d) pont: Kötelezi a szervezeteket fenyegetésészlelési és megelőzési intézkedések bevezetésére, beleértve a végponti malware elleni védelmi mechanizmusokat.

11.6 DORA-rendelet (2022/2554):

11.6.1 9. cikk - IKT-kockázatkezelési követelmények: Előírja, hogy a pénzügyi szervezetek olyan védelmi intézkedéseket alkalmazzanak, amelyek megelőzik, észlelik és kezelik a malware-t és a végpontokról eredő fenyegetéseket.

11.7 COBIT 2019:

11.7.1 DSS05.01 - Malware elleni védelem: Előírja a malware észlelését és mérséklését a szervezet valamennyi végpontján.

11.7.2 DSS01.04 - Rendelkezésre állás és kapacitás kezelése: Biztosítja, hogy a malware elleni védelem egyensúlyban legyen a rendszer teljesítményével és az üzletmenet-folytonossággal.

11.7.3 MEA03 - Megfelelés nyomon követése, értékelése és felmérése: Előírja a végponti kontrollok és a védelem hatékonyságának időszakos auditját.