					Sem vložte název registrované právnické osoby							
Číslo dokumentu: P23					Název dokumentu: **Politika synchronizace času**							
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	Clause 8	-
ISO/IEC 27002:2022	Opatření 8	-
NIST SP 800-53 Rev.5	SC-45, AU-8	-
GDPR	Article 32	-
směrnice NIS2	Article 21(2)(e)	-
nařízení DORA	Articles 9, 10	-
COBIT 2019	DSS05.04, MEA	-

1. Účel

1.1 Účelem této politiky je zajistit, aby všechny systémy, aplikace, zařízení a cloudové služby organizace udržovaly konzistentní a přesná časová nastavení prostřednictvím synchronizace s určenými důvěryhodnými zdroji času.

1.2 Přesná synchronizace času je nezbytná pro spolehlivé protokolování, bezpečnou komunikaci, auditní stopu, reakci na incidenty a forenzní šetření. Nesoulad času může vést k nekorelovatelným logům, selhání autentizace a neúplnému regulatornímu reportingu.

1.3 Tato politika podporuje opatření 8.17 přílohy A normy ISO/IEC 27001 a související mezinárodní normy tím, že prosazuje přesnost času a detekci odchylek systémového času v celém IT prostředí organizace.

2. Rozsah

2.1 Tato politika se vztahuje na:

2.1.1 všechny komponenty infrastruktury včetně serverů, pracovních stanic, síťových zařízení, firewallů a systémů internetu věcí (IoT)

2.1.2 virtuální a cloudová prostředí (např. AWS, Azure, Google Cloud)

2.1.3 všechny systémy zapojené do protokolování, autentizace, zpracování transakcí nebo korelace bezpečnostních událostí

2.1.4 interní zaměstnance, smluvní pracovníky a poskytovatele služeb třetích stran odpovědné za systémy citlivé na čas

2.2 Za součást rozsahu se považují systémy, které vytvářejí nebo využívají záznamy s časovým razítkem, jako jsou položky logů, upozornění, záznamy o aktivitě uživatelů nebo forenzní důkazy.

3. Cíle

3.1 Definovat konzistentní centralizovanou architekturu synchronizace času využívající schválené zdroje NTP nebo jejich ekvivalent.

3.2 Zajistit, aby všechny systémy synchronizovaly svůj čas v definovaných intervalech a aby jakákoli odchylka byla detekována a odstraněna automaticky nebo s minimálním zásahem.

3.3 Udržovat přesnost času v hybridním režimu, v on-premise prostředích i v cloudu tak, aby bylo možné zajistit:

3.3.1 spolehlivou korelaci událostí a reakci na incidenty

3.3.2 soulad s normami a právními předpisy, jako jsou ISO 27001, GDPR, směrnice NIS2 a nařízení DORA

3.3.3 ochranu proti replay útokům a selháním autentizace založeným na čase

3.4 Stanovit jasné role, postupy pro řešení výjimek a auditní mechanismy pro zajištění uplatňování této politiky.

3.5 Zajistit, aby anomálie související s časem byly protokolovány, aby na ně byla generována upozornění a aby byly eskalovány při překročení stanovených tolerancí.

4. Role a odpovědnosti

4.1 ředitel informační bezpečnosti (CISO)

4.1.1 odpovídá za tuto politiku a zajišťuje její soulad s provozními opatřeními ISMS a regulatorními požadavky.

4.1.2 schvaluje výběr podnikových zdrojů času a ověřuje procesy reportingu synchronizace času.

4.2 manažer infrastrukturních služeb / vedoucí síťového inženýrství

4.2.1 spravuje primární a sekundární NTP servery organizace nebo určenou konfiguraci zdrojů času.

4.2.2 zajišťuje, aby všechna síťově připojená zařízení a virtuální instance synchronizovaly čas ve vhodných intervalech.

4.2.3 monitoruje logy synchronizace času, upozornění na odchylky systémového času a chybové stavy.

[... 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 jednou ročně nebo dříve za následujících podmínek:

9.1.1 zjištění exploitů založených na čase nebo selhání protokolování

9.1.2 změny v klíčové časové infrastruktuře (např. nové podnikové NTP servery nebo aktualizace protokolů)

9.1.3 odchylky synchronizace času cloudové platformy nebo změny regionálních služeb

9.1.4 zjištění po incidentu, která identifikují nesoulad času jako přispívající faktor

9.2 Přezkum koordinuje vedoucí infrastruktury, přičemž je vyžadován vstup od SOC, bezpečnosti aplikací a zainteresovaných stran v oblasti compliance.

9.3 Revize musí být zdokumentovány v registru dokumentů ISMS a oznámeny dotčeným interním i externím zainteresovaným stranám.

9.4 Historické verze politiky musí být bezpečně archivovány, vedeny v režimu správy verzí a zpřístupněny pro požadavky interního auditu, auditu souladu nebo právního auditu.

10. Související politiky a vazby

10.1 P1 – Politika informační bezpečnosti. Stanoví zastřešující požadavek na zajištění integrity a dohledatelnosti všech informačních systémů, pro které je přesnost času základním předpokladem.

10.2 P5 – Politika řízení změn. Upravuje změny konfigurací systémů včetně úprav zdrojů času a zajišťuje řádnou dokumentaci, testování a plány návratu změn.

10.3 P22 – Politika protokolování a monitorování. Je přímo závislá na synchronizovaném čase, aby byla zajištěna posloupnost událostí, korelace logů a integrita vyšetřování incidentů napříč různorodými systémy.

10.4 P30 – Politika reakce na incidenty (P30). Je závislá na přesných časových razítkách pro forenzní vyšetřování, časové osy incidentů a důkazy v rámci řetězce svěření. Nepřesný čas snižuje důvěryhodnost zpráv o incidentech.

10.5 P20 – Politika ochrany koncových bodů / ochrany před malwarem. Vyžaduje časově přesné upozorňování a behaviorální analytiku pro detekci šíření malwaru, laterálního pohybu a anomálií přístupu.

10.6 P6 – Politika řízení rizik. Definuje desynchronizaci jako potenciální provozní a forenzní riziko a vyžaduje opatření definovaná v této politice ke zmírnění dopadu.

11. Referenční normy a rámce

11.1 ISO/IEC 27001

11.1.1 Clause 8.1 – Provozní plánování a řízení: Vyžaduje integraci přesných technických opatření, jako jsou synchronizované systémové hodiny, pro spolehlivé provádění provozních činností.

11.2 ISO/IEC 27002:2022 – Opatření 8

11.2.1 Posiluje požadavek na přesnost času a ukládá organizační konzistenci systémového času za účelem usnadnění porovnávání logů, vyšetřování a bezpečné validace transakcí.

11.3 NIST SP 800-53 Rev.

11.3.1 SC-45 – Synchronizace systémového času: Vyžaduje synchronizaci času pomocí autoritativních zdrojů napříč všemi komponentami v rámci hranice systému.

11.3.2 AU-8 – Časová razítka: Zajišťuje, aby události byly přesně opatřeny časovým razítkem, a poskytuje dohledatelnost pro audit a reakci na incidenty.

11.4 GDPR (2016/679)

11.4.1 Článek 32 – Zabezpečení zpracování: Ačkoli explicitně neuvádí čas, vyžaduje použití odpovídajících technických opatření, včetně auditních stop a logů, jejichž platnost a integrita jsou přirozeně závislé na synchronizovaných časových razítkách.

11.5 směrnice NIS2 (2022/2555)

11.5.1 Článek 21(2)(e): Vyžaduje schopnosti protokolování a detekce, které předpokládají přesnou synchronizaci času pro korelaci napříč systémy a včasnou reakci.

11.6 nařízení DORA (2022/2554)

11.6.1 Článek 9 – Řízení rizik v oblasti ICT: Ukládá přesnou systémovou telemetrii pro monitorování rizik a detekci anomálií, což závisí na přesné synchronizaci systémového času.

11.6.2 Článek 10 – kontinuita činností v oblasti ICT: Prosazuje opatření zajišťující integritu systémů během narušení, včetně časově sladěných záznamů událostí.

11.7 COBIT 2019

11.7.1 DSS05.04 – Monitorování bezpečnostních událostí: Vyžaduje integritu časových razítek pro účinnou analýzu logů a detekci hrozeb.

11.7.2 MEA03 – Monitorování, vyhodnocování a posuzování souladu: Synchronizace času podporuje přesný audit souladu a cykly reportingu.