					Sem zadajte názov registrovanej právnickej osoby							
Číslo dokumentu: P38					Názov dokumentu: **Politika bezpečnej komunikácie a viacfaktorovej autentifikácie**							
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**

V súlade s normami a predpismi

Norma/predpis	Kapitola/článok	Poznámka
ISO/IEC 27001:2022	5.30, 5.31, 8.24	
ISO/IEC 27002:2022	5.15, 5.17, 5.18, 8.24, 8.28	
NIST SP 800-53 Rev. 5	IA-2, IA-3, IA-5, IA-8, SC-12, SC-13, SC-31	
Nariadenie EÚ GDPR	Čl. 32 ods. 1 písm. b)	
Smernica EÚ NIS2	Čl. 21 ods. 2 písm. j)	
Nariadenie EÚ DORA	Čl. 9 ods. 2 písm. d), Čl. 11	
COBIT 2019	DSS05.04, DSS05.05, DSS05	

1. Účel

1.1 Stanoviť požiadavky na používanie viacfaktorovej autentifikácie (MFA) alebo riešení priebežnej autentifikácie pri prístupe do systémov v súlade s článkom 21 ods. 2 písm. j) smernice EÚ NIS2.

1.2 Zaviesť kontroly bezpečnej hlasovej, obrazovej, textovej a núdzovej komunikácie s cieľom chrániť dôvernosť a integritu informácií.

2. Rozsah

2.1 Táto politika sa vzťahuje na všetky mechanizmy autentifikácie a komunikačné systémy (hlasové hovory, videokonferencie, správy a systémy núdzových notifikácií), ktoré organizácia používa.

2.2 Vzťahuje sa na všetkých zamestnancov, zmluvných pracovníkov a všetky externé strany, ktoré používajú komunikačné kanály organizácie alebo pristupujú k jej sieťovým a informačným systémom.

3. Ciele

3.1 Zabezpečiť, aby prístup do systémov získali iba primerane autentifikovaní používatelia, a znížiť riziko neoprávneného prístupu prostredníctvom zavedenia viacfaktorovej autentifikácie (MFA).

3.2 Zabezpečiť, aby sa interná a núdzová komunikácia prenášala bezpečnými metódami (napr. prostredníctvom šifrovaných komunikačných kanálov), čím sa predíde odpočúvaniu alebo neoprávnenej manipulácii.

3.3 Plniť požiadavky smernice EÚ NIS2 na silnú autentifikáciu a bezpečnú komunikáciu a tým posilniť celkovú kybernetickú odolnosť.

4. Roly a zodpovednosti

4.1 Riaditeľ informačnej bezpečnosti (CISO) / tím IT bezpečnosti: Definuje a udržiava mechanizmy viacfaktorovej autentifikácie (MFA) a nástroje bezpečnej komunikácie; zabezpečuje technické presadzovanie tejto politiky.

4.2 IT administrátori: Zavádzajú viacfaktorovú autentifikáciu (MFA) pre relevantné systémy a konfigurujú schválené platformy bezpečnej komunikácie; monitorujú súlad.

[... Sekcie 4.3–8 nie sú súčasťou tohto náhľadu. Pre prístup k úplnému obsahu si zakúpte celý dokument. ...]

9. Monitorovanie a audit

9.1 IT bezpečnosť musí nepretržite monitorovať autentifikačné záznamy s cieľom identifikovať akékoľvek pokusy o prihlásenie iba jedným faktorom alebo anomálne zlyhania viacfaktorovej

autentifikácie (MFA). Záznamy systémov bezpečnej komunikácie (ak sú dostupné) sa musia monitorovať s cieľom odhaliť pokusy o neoprávnený prístup alebo zmeny konfigurácie.

9.2 Funkcia vnútorného auditu a compliance každoročne preskúma dodržiavanie požiadaviek na nasadenie viacfaktorovej autentifikácie (MFA), overí, že všetky kritické systémy ju vynucujú, a preverí, že na citlivú komunikáciu sa používajú výlučne schválené bezpečné kanály. Zistenia sa predkladajú manažmentu spolu s odporúčaniami.

10. Preskúmanie a údržba

10.1 Táto politika sa preskúmava najmenej raz ročne a pri každom významnom bezpečnostnom incidente alebo novo identifikovanom riziku súvisiacom s autentifikáciou alebo komunikáciou (napr. nové vektory hrozieb proti viacfaktorovej autentifikácii (MFA), zistenie používania nebezpečnej komunikácie).

10.2 Revízie sa vykonávajú podľa potreby s cieľom reagovať na vývoj technológií (napr. zavedenie robustnejších riešení priebežnej autentifikácie) alebo zabezpečiť súlad s aktualizovanými regulačnými usmerneniami (napríklad budúcimi odporúčaniami ENISA pre bezpečnú komunikáciu).

11. Súvisiace politiky a väzby

11.1 P01 – Politika informačnej bezpečnosti. Stanovuje opatrenia autentifikácie a ochrany komunikácie na úrovni celej organizácie.

11.2 P04 – Politika riadenia prístupu. Zavádza riadenie a správu prístupov, ktoré P38 presadzuje prostredníctvom viacfaktorovej autentifikácie (MFA).

11.3 P11 – Politika správy používateľských účtov a oprávnení. Prepája viacfaktorovú autentifikáciu (MFA) so životným cyklom privilegovaného prístupu.

11.4 P18 – Politika kryptografických kontrol. Určuje schválené kryptografické postupy a správu kľúčov pre bezpečnú komunikáciu.

11.5 P21 – Politika bezpečnosti sietí. Zabezpečuje prenosové kanály používané pre hlasovú, obrazovú a správovú komunikáciu.

11.6 P22 – Politika logovania a monitorovania. Monitoruje autentifikačné udalosti a používanie bezpečných kanálov.

11.7 P32 – Politika kontinuity činností a obnovy po havárii. Zabezpečuje núdzovú komunikáciu počas krízových situácií.

11.8 P08 – Politika povedomia a školenia o informačnej bezpečnosti. Školí používateľov o viacfaktorovej autentifikácii (MFA) a hygiene používania komunikačných kanálov.

12. Referencie

12.1 Smernica NIS2 (EÚ 2022/2555), článok 21 ods. 2 písm. j) (používanie viacfaktorovej autentifikácie a zabezpečenej komunikácie)

12.2 Vykonávacie nariadenie Komisie (EÚ) 2024/2690, príloha, oddiel 11 (požiadavky na riadenie prístupu vrátane viacfaktorovej autentifikácie pre privilegované účty)

12.3 ISO/IEC 27001:2022 a ISO/IEC 27002:2022