# ****3. Prehľad implementovaných bezpečnostných opatrení podľa článku 21 NIS2 – WebCreators.sk****

| **Oblasť opatrenia podľa NIS2** | **Implementované opatrenia v praxi WebCreators.sk** |
| --- | --- |
| **a) Politika a riadenie rizík** | - Interný dokument "Bezpečnostná politika" platný od 01.04.2025 - Ročné hodnotenie rizík podľa ISO 27005 - Priebežná evidencia aktív a zraniteľností |
| **b) Reakcia na incidenty** | - Vypracovaný "Plán reakcie na incidenty (PRI)" - Interný incidentný register a eskalačný systém - Oznamovanie incidentov NBÚ do 24 h - Simulované testy incidentov 1× ročne |
| **c) Kontinuita činností a obnova** | - Vypracovaný DRP a plán obnovy infraštruktúry - Denné zálohy (min. 30-dňová retencia) - Zálohy testované kvartálne |
| **d) Zabezpečenie dodávateľského reťazca** | - Bezpečnostné klauzuly v zmluvách s dodávateľmi - Overovanie certifikácií (napr. ISO 27001 u cloud partnerov) - Pravidelný prehľad kritických dodávateľov |
| **e) Bezpečnostná architektúra a segmentácia siete** | - Virtuálna segmentácia infraštruktúry - DMZ pre verejne dostupné služby - Oddelené prostredia (produkcia, testovanie) |
| **f) Riadenie prístupu a identít (IAM)** | - Viacfaktorová autentifikácia pre administratívne účty - Centrálne riadenie oprávnení (IAM systém) - Revízia prístupov 1× mesačne |
| **g) Ochrana informácií a systémov** | - Šifrovanie pri prenose (TLS 1.3), šifrovanie databáz - IDS/IPS systém - Automatizovaný patch management a aktualizácie |
| **h) Politika používania kryptografie** | - Povinné používanie šifrovania pre všetky klientské dáta - Certifikáty spravované centrálne (Let's Encrypt, EV certifikáty) - Nepoužívame zastarané algoritmy |
| **i) Školenia a zvyšovanie povedomia** | - Onboarding školenie pre nových zamestnancov - Ročné školenia pre všetkých - Simulácie phishingových útokov 2× ročne |
| **j) Zásady používania aktív** | - Interný zoznam IT aktív - Pravidelné inventúry hardvéru a softvéru - Politika pre firemné zariadenia a BYOD |
| **k) Zabezpečenie akvizícií a vývoja IT systémov** | - Bezpečnostné testy pred nasadením do produkcie - Code review a bezpečnostné checklisty pri vývoji - CI/CD pipeline s kontrolou bezpečnosti |
| **l) Používanie viacfaktorovej autentifikácie** | - MFA implementovaná pre všetkých adminov a manažérov - Povinná pre prístup do serverového a cloudového prostredia |
| **m) Bezpečnostné testovanie a audit** | - Penetračné testy raz ročne (externý partner) - Interné audity bezpečnostných opatrení podľa ISO 27001 rámca - Vlastné logovanie a SIEM nástroje na detekciu anomálií |