# ****2. Plán reakcie na kybernetické incidenty (PRI) – WebCreators.sk****

### 1. Účel

Účelom tohto dokumentu je zabezpečiť rýchlu a efektívnu reakciu na kybernetické incidenty, minimalizovať ich dopad na služby a zabezpečiť oznamovanie incidentov v súlade s NIS2 a požiadavkami NBÚ.

### 2. Definícia incidentu

Incident je akákoľvek udalosť, ktorá:

* ohrozuje dostupnosť, dôvernosť alebo integritu IT služieb,
* spôsobuje narušenie prevádzky systémov alebo dát,
* má potenciálny vplyv na klientov alebo infraštruktúru,
* spĺňa definíciu **významného incidentu** podľa § 3 zákona č. 69/2018 Z. z.

### 3. Fázy reakcie na incident

#### ****3.1 Detekcia a identifikácia****

* Využívame automatizované nástroje (napr. IDS/IPS, SIEM).
* Incidenty môžu byť nahlásené aj manuálne (zákazník, zamestnanec).
* Každý incident je zaznamenaný do interného incidentného registra.

#### ****3.2 Klasifikácia incidentu****

Incidenty sa triedia podľa závažnosti:

| **Úroveň** | **Popis** | **Príklad** |
| --- | --- | --- |
| Nízka | Lokálny problém bez dopadu na služby | Pokus o phishing na 1 e-mail |
| Stredná | Čiastočné obmedzenie služby | Výpadok zálohovacieho servera |
| Vysoká | Ohrozenie dostupnosti alebo úniku dát | Ransomvér, kompromitácia systému |

#### ****3.3 Reakcia a eskalácia****

* Incidenty vyššej závažnosti rieši **Incident Response Tím (IRT)**.
* Kritické incidenty sa do 24 hodín hlásia NBÚ cez CSIRT.SK.
* Klientov informujeme podľa úrovne dopadu a platných zmlúv.

#### ****3.4 Náprava a obnova****

* Odstránenie príčiny incidentu (napr. zablokovanie IP, obnova systému).
* Obnovenie prevádzky podľa DRP (Disaster Recovery Plan).
* Zabezpečenie logov a dôkazového materiálu pre analýzu.

#### ****3.5 Analýza a poučenie****

* Do 5 pracovných dní vyhotovíme správu o incidente.
* Prijmeme nápravné opatrenia (napr. zmena konfigurácie, školenie).
* Incident sa archivuje na min. 3 roky.

### 4. Zodpovednosti

| **Rola** | **Zodpovednosť** |
| --- | --- |
| IT administrátor | Prvotná detekcia, eskalácia |
| Vedúci IRT (Incident Response Team) | Koordinácia reakcie a komunikácia s NBÚ |
| Zodpovedná osoba za kyberbezpečnosť (ZKB) | Kontrola postupu a schválenie správy |
| Vedenie spoločnosti | Informovanie partnerov, schválenie výdavkov |

### 5. Komunikácia s externými stranami

* **NBÚ/CSIRT.SK:** notifikácia do 24 hodín, doplňujúca správa do 72 hodín.
* **Zákazníci:** informácia prostredníctvom e-mailu, status stránky alebo ticket systému.
* **Dodávatelia:** notifikácia podľa SLA (ak incident vznikol u nich).

### 6. Testovanie a aktualizácia

* Simulovaný test incidentu vykonávame min. 1× ročne.
* Plán je prehodnocovaný po každom vážnom incidente alebo legislatívnej zmene.