Zásady práce bezpečnostního týmu CSIRT-ZONER

Název dokumentu: Zásady práce bezpečnostního týmu CSIRT-ZONER
Verze: 1.0
Platnost od: 15.5.2025
Zodpovědný útvar: CSIRT-ZONER
Schválil: Ing. Jindřich Zechmeister, manažer KB

1. Poslání týmu

Posláním CSIRT-ZONER je chránit informační aktiva společnosti ZONER, a.s. před kybernetickými hrozbami, poskytovat expertní podporu při řešení incidentů a zvyšovat úroveň kybernetické odolnosti společnosti.

ZONER, a.s. je provozovatelem základní služby dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti, konkrétně v oblasti poskytování služeb systému doménových jmen (DNS). CSIRT-ZONER plní roli interního týmu dle vyhlášky č. 82/2018 Sb., který zajišťuje organizační opatření pro zvládání bezpečnostních incidentů.

2. Kompetence týmu

- Analýza hrozeb a incidentů
- Koordinace reakce na bezpečnostní incidenty
- Komunikace s externími partnery (např. NÚKIB, CERT.CZ)
- Správa nástrojů detekce a monitoringu
- Školení a informování uživatelů

3. Hodnoty a principy

- Důvěrnost
- Odbornost
- Rychlost a přesnost
- Transparentnost

4. Koordinace a spolupráce

CSIRT-ZONER spolupracuje s IT oddělením, Compliance, právním oddělením, managementem a s externími partnery a CSIRT/CERT týmy, zejména v rámci ostatních webhostingových společností.

5. Nástroje a infrastruktura

Tým využívá nástroje pro monitoring sítí a systémů, detekci a analýzu malwaru, správu ticketů, forenzní analýzu a threat intelligence.

6. Provozní režim

Tým funguje v režimu běžného provozu s on-call službou pro kritické incidenty mimo pracovní dobu. Dozor na síťovým provozem zajišťuje dozor/NOC v režimu 24/7.
Reakční doby jsou stanoveny dle klasifikace incidentů.

7. Kontinuita činnosti

CSIRT-ZONER má vlastní plán kontinuity činnosti a obnovy pro případ výpadku klíčových členů nebo nástrojů.

ZONER a.s. [IČ 49437381]

Digitálně podepsal ZONER a.s. [IČ 49437381]
Datum: 2025.05.15 10:30:18 +02'00'