Provozní řád CSIRT týmu při CIT VŠB-TUO

Cílem tohoto dokumentu je definovat pravidla a postupy při zjišťování, vyhodnocování a řešení bezpečnostních incidentů v IT oblasti směřujících k porušování technických i zákonných norem.

CSIRT (Computer Security Incident Response Team) tým je pracovní skupina zabývající se zpracováním bezpečnostních incidentů. Kontaktní e-mail pro členy skupiny je abuse@vsb.cz.

Zdroje incidentů

- detekce incidentů analýzou provozu počítačové sítě
- přijímání incidentů od uživatelů VŠB-TUO
- přijímání incidentů od externích subjektů

Detekce incidentů analýzou počítačové sítě

CSIRT tým je složen z pracovníků oddělení CIT - Infrastruktura IT. CIT provádí takové technické kroky, které směřují k aktivnímu vyhledávání napadených a zranitelných koncových systémů v síti VŠB-TUO. Zachycovány a vyhledávány jsou zejména:

- projevy malware koncových stanic VŠB-TUO,
- příliš veliké datové přenosy vztahující se k jedné koncové stanici,
- projevy napadených nebo zranitelných koncových systémů.

Přijímání bezpečnostních incidentů od uživatelů

Bezpečnostní incidenty jsou přijímány od uživatelů sítě VŠB-TUO (zaměstnanci i studenti) a také od externích subjektů s dodržením následujících zásad:

1. Hlášení by mělo být zasláno prostřednictvím **jednoduchého textového e-mailu**, v případě potřeby s přílohou (v příloze by měl být tzv. “důkazní materiál”).
2. Hlášení by se mělo týkat jedné **IP adresy** nebo **jednoho adresového bloku**.

3. Předmět zprávy by měl obsahovat **IP adresu** nebo **adresový blok** a **typ incidentu** (spam, malware, skenování portů, DDOS, hacking, phishing, pharming, porušení autorských práv, …).

4. **Hlášení o skenování** musí obsahovat část logu obsahující záznamy o skenování:

    - časové známky (počátek a konec skenování) a časovou zónu
    - zdrojovou a cílovou IP adresu
    - zdrojový a cílový port
    - TCP/UDP/ICMP

5. **Hlášení o spamu** (“unsolicited commercial e-mails”) musí obsahovat kompletní nemodifikovanou hlavičku a tělo zprávy, která je považována za spam.

6. **Nahlášení porušení práva autorského** musí obsahovat následující informace:

    - časové známky a časovou zónu
    - zdrojovou a cílovou IP adresu, na které došlo k porušení autorských práv
    - služba použitá pro zveřejnění dat chráněných autorským právem
    - typ (název) dat chráněných autorským právem

7. **Hlášení o phishing nebo pharming** musí obsahovat URL a pokud možno i zdrojový kód webové stránky.

8. **Hlášení ostatních bezpečnostních** incidentů musí obsahovat část logu obsahující záznamy o útoku:

    - časové známky (počátek a konec útoku) a časovou zónu
    - zdrojovou a cílovou IP adresu, zdrojový a cílový port, typ protokolu (TCP/UDP/ICMP)
    - typ útoku

9. **Hlášení musí obsahovat základní kontaktní informace** - jméno ohlašovatele a jméno organizace.

10. **Hlášení musí být odesláno z validní e-mailové adresy.**

Postup při zpracování incidentů

1. Přijetí incidentu pracovníkem CSIRT týmu.

2. Zdokumentování pracovníkem CSIRT týmu.
3. Bude-li hrozba vyhodnocena jako ohrožující, provede se omezení běhu koncové stanice (např. blokace).
4. Pracovník CSIRT týmu vyrozumí o incidentu uživatele i správce koncové stanice, popř. zajistí publikaci informace.
5. Řešení incidentu provádí uživatel stanice, popř. příslušný správce stanice (např. fakultní, rektorátní). Po vyřešení informuje o způsobu a výsledcích pracovníka CSIRT týmu.
6. Pracovník CSIRT týmu dohlíží na řešení problému. Po přijetí informace o vyřešení od oprávněné osoby a po ověření tohoto faktu může incident uzavřít.
7. Při uzavření incidentu vyrozumí pracovník CSIRT o tomto faktu uživatele i správce koncové stanice a zajistí publikaci tohoto faktu v informačních systémech.

Při neřešení incidentu bude tento fakt eskalován nadřízenému příslušného pracovníka. Provoz koncových stanic nebo uživatelů může být omezen nebo zcela znemožněn a to až do doby úplného vyřešení incidentu.

Verze	Datum	Obsah změny/revize	Jméno garanta dokumentu
A	2.5.2018	Nový dokument	Ing. Martin Pustka, Ph.D.
B	7.6.2024	Aktualizace názvu univerzity	Ing. Martin Pustka, Ph.D.