# Plán reakce na incident (Incident Response Plan)

## Úvod

**Kybernetickým bezpečnostním incidentem** je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.[[1]](#footnote-1)

Základní prvky Plánu reakce na incident jsou:

* **Rozpoznání incidentu:** o jaký incident se jedná a jakých systémů se týká;
* **Odpovědná osoba:** kdo má na starosti řešení incidentu;
* **Kontaktní údaje:** seznam dalších klíčových osob a institucí;
* **Oznámení incidentu:** komu a jakým způsobem nahlásit problém – včetně pokynů, co dělat či nedělat v dané situaci;
* **Řešení incidentu:** jaké kroky učinit pro řešení situace;
* **Obnovení systémů:** jak postupovat při obnově chodu systémů;
* **Evidence incidentů:** co a jak zaznamenat pro zpětné vyhodnocení a případné poučení.

## Vzor

|  |  |  |
| --- | --- | --- |
| Název školy: |  | |
| Krizový tým | Jméno | Odpovědnost |
| Zodpovědná osoba koordinující reakci: |  |  |
| Ředitel / zástupce ředitele |  |  |
| ICT koordinátor |  |  |
| ICT expert / správce sítě/ správce ICT |  |  |
| Správce dat / pověřenec pro ochranu osobních údajů |  |  |

1. Identifikace incidentu
2. Ransomware
3. Phishing
4. DDoS útok
5. Kompromitace školní sítě
6. Napadení wi-fi
7. Kompromitace DNS záznamů
8. Útok na webové stránky
9. Jiný (další klasifikace viz [taxonomie kybernetických incidentů](https://www.enisa.europa.eu/sites/default/files/publications/WP2017%20O-3-1-1%20Good%20practice%20guide%20on%20how%20to%20improve%20CSIRT%20capabilities.pdf) dle organizace ENISA)

Jak jednotlivé útoky rozpoznat, naleznete *v* [*#kyberšanonu*](https://myjsmenpi.sharepoint.com/:w:/r/sites/D_AIDIG-Kyberbezpenost/Sdilene%20dokumenty/00_Odesláno%20ke%20schválení/KYBER%20-%20nová%20struktura/01_Kyberšanon_souhrn.docx?d=w2857530902ef4fa0be4a83f5a63eed1a&csf=1&web=1&e=Pc36Z9)*). Můžete použít i nějaký AI nástroj. Když zde popíšete situaci, poradí vám s identifikací útoku.*

### 1. Rozsah incidentu

|  |  |
| --- | --- |
| Které systémy byly zasaženy?   * + Měl incident vliv pouze na jednotlivé síťové prvky, nebo na celou síť? |  |
| Došlo ke ztrátě důležitých dat? |  |
| Došlo ke ztrátě osobních nebo citlivých údajů? | ANO/NE  Pokud ano, je potřeba kontaktovat [ÚOOÚ](https://uoou.gov.cz/profesional/poruseni-zabezpeceni-osobnich-udaju). |
| Jak k incidentu došlo?   * Jaký byl vstupní bod pro útok? (počítač, uživatel, síťový prvek aj.) |  |
| Kdo na incident přišel? |  |
| Byly napadeny nějaké kritické systémy, které nelze vypnout? | ANO/NE  Pokud ano, které: |

### 2. Okamžitá reakce

* Izolace napadených systémů.
* Napadené systémy byly vypojeny ze sítě.
* Přístup do sítě byl omezen jen pro interní zařízení.
* Všechna hesla byla změněna.
  + Wi-fi
  + Administrátorské účty
  + Uživatelské účty (pokud je to nutné)
  + Bylo nastaveno vícefaktorové ověřování (minimálně na admin účtech).

### 3. Komunikace

* Byl kontaktován ICT expert / správce ICT či jiný poskytovatel (např. webového hostingu), je připraven ke spolupráci.
* Dotčení uživatelé byli informováni a obdrželi jasné instrukce, co mají a nemají dělat. (např.: „Neotvírejte přílohu e-mailu s předmětem …, příloha je nositelem viru!“)
* Zřizovatel byl informován, je připraven pomoci (např. právní pomoc).
* Všichni zaměstnanci vědí, co mají a nemají dělat.
* Byla kontaktována Policie ČR (v případě cíleného útoku, ransomwaru aj.).
* Byl kontaktován [NÚKIB](https://nukib.gov.cz/cs/kontakty/hlaseni-incidentu/) (v případě cíleného útoku na školu většího rozsahu).
* Byl kontaktován [ÚOOÚ](https://uoou.gov.cz/profesional/poruseni-zabezpeceni-osobnich-udaju) (v případě úniku osobních údajů).

### 4. Zajištění provozu IT

* Základní provoz ve škole byl zajištěn (např.: vedení školy, ekonomický úsek, stravování).
* Běžný provoz ve škole byl zajištěn (např.: připojení k internetu pro vyučující, školní informační systém).
* Obnovení ze záloh – zálohy jsou k dispozici.
* Obnovení ze záloh – zálohy jsou konzistentní a úplné.
* Obnovení ze záloh – zálohy nejsou kompromitovány útokem.
* Použití záloh k obnovení systémů

### 5. Důkazy

Byly pořízeny důkazy o útoku:

* Základní informace o útoku:

|  |  |
| --- | --- |
| Datum incidentu: |  |
| Vyšetřující osoba/osoby: |  |
| Popis incidentu: |  |
| Kde incident vznikl (fyzické místo nebo technologie): |  |
| Příčina vzniku incidentu: |  |
| Dopad incidentu: |  |
| Přijatá opatření: |  |

* Printscreeny, fotografie – k dispozici na: \_\_\_\_\_\_\_\_\_\_\_\_\_\_
* E-maily – k dispozici na: \_\_\_\_\_\_\_\_\_\_\_\_\_
* Logy, vstupy do sítě – k dispozici na: \_\_\_\_\_\_\_\_\_\_\_\_\_\_
* Jiné \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_k dispozici na: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

### 6. Odstranění infekce a náprava

* Napadené systémy byly vyčištěny od malwaru.
* Zálohy byly aktivovány.
* Ukradená data byla:
  + Získána zpět – dešifrována.
  + Ztracena, jedná se o tato data: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

### 7. Nové nastavení ochrany

* Antivirový software byl aktualizován.
* Firewall byl aktualizován a správně nastaven.
* Hesla byla resetována.
* Bylo nastaveno vícefaktorové ověřování (minimálně u administrátorských účtů a zaměstnaneckých účtů mimo budovu).

### 8. Další úkony

* Proběhla reflexe útoku a reakce na něj (incident review meeting).
* [Checklist](https://digitalizace.rvp.cz/files/kyberprevence-check-list-pro-vedeni.pdf) kybernetické bezpečnosti je splněn. kybernetické bezpečnosti je splněn. kybernetické bezpečnosti je splněn.
* Plán reakce na incident byl v reakci na útok upraven.
* Bezpečnostní směrnice a další nastavení byly v reakci na útok upraveny.
* Všichni uživatelé byli znovu vyškoleni.
* Nový plán byl otestován.

Tento plán má škole pomoci zvládnout kybernetický incident či útok co nejlépe a co nejrychleji. Když ho budou všichni znát a občas si ho společně projdete, zvládnete i složité situace s větším klidem a jistotou.

Vytiskněte si ho a uložte do #kyberšanonu, abyste ho měli kdykoliv po ruce.

1. <https://www.e-sbirka.cz/sb/2014/181?zalozka=text>

   2 Více viz <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf> nebo <https://o2cybernews.cz/clanky/jak-vytvorit-ucinny-incident-response-plan-v-souladu-s-nis2?utm_source=chatgpt.com> [↑](#footnote-ref-1)