Prvních 60 minut po kybernetickém incidentu

Praktický checklist pro organizace

Úvod

Kybernetický incident může mít podobu napadení účtu, škodlivého e-mailu, úniku dat, nedostupnosti služby nebo jiného narušení bezpečnosti.

První hodina po odhalení incidentu bývá rozhodující pro omezení škod a zajištění rychlé obnovy provozu. Cílem není problém okamžitě vyřešit, ale získat kontrolu nad situací, zabránit dalšímu šíření incidentu a zajistit dostatek informací pro další postup.

Tento dokument poskytuje jednoduchý přehled kroků, které by měly být provedeny bezprostředně po zjištění incidentu.

Základní checklist při incidentu

Identifikace a oznámení

- [ ] Je incident zaznamenán (čas, systém, stručný popis)?
- [ ] Byla informována odpovědná osoba?
- [ ] Je znám rozsah incidentu (co je zasaženo) nebo alespoň jeho předpokládaný dopad?
- [ ] Byly identifikovány možné příčiny?

Omezení dopadů a obnova

- [ ] Bylo zabráněno dalšímu šíření incidentu?
- [ ] Byly odpojeny nebo omezeny dotčené systémy, zařízení nebo účty?
- [ ] Byly zahájeny kroky k obnovení provozu?
- [ ] Byla ověřena správná funkčnost systémů?

Spolufinancováno Evropskou unií

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

CYLANCES

Dokumentace

- [ ] Jsou zaznamenány všechny kroky?
- [ ] Jsou evidována přijatá opatření?
- [ ] Jsou zaznamenány časy jednotlivých událostí?
- [ ] Jsou uchovány relevantní důkazy (logy, screenshoty, e-maily)?

Co dělat v prvních 60 minutách

První fáze řešení incidentu je zásadní. V této době se rozhoduje o tom, jak velký dopad bude mít incident na organizaci.

Hlavním cílem není okamžité odstranění problému, ale:

- potvrdit existenci incidentu,
- zabránit jeho dalšímu šíření,
- zajistit důležité informace,
- zahájit koordinovanou reakci organizace.

0–15 minut: Rozpoznání a oznámení

- [ ] Je potvrzeno, že se skutečně jedná o bezpečnostní incident?
- [ ] Byla informována odpovědná osoba nebo bezpečnostní tým?
- [ ] Byly zaznamenány základní informace o situaci?
- [ ] Nedochází k nevratným zásahům (mazání, restart bez evidence)?

15–30 minut: Omezení šíření

- [ ] Byly odpojeny napadené systémy nebo zařízení?
- [ ] Byly zablokovány kompromitované účty?
- [ ] Je zabráněno dalšímu šíření incidentu?
- [ ] Jsou průběžně evidovány všechny provedené kroky?

Spolufinancováno Evropskou unií

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

CYLANCES

30–60 minut: Vyhodnocení a rozhonutí

- [ ] Je znám alespoň přibližný rozsah incidentu?
- [ ] Byla určena priorita řešení?
- [ ] Bylo rozhodnuto o dalším postupu?
- [ ] Byla posouzena potřeba eskalace?
- [ ] Byla posouzena případná oznamovací povinnost?

Průběžně po celou dobu

- [ ] Jsou dokumentovány provedené kroky?
- [ ] Je komunikace řízena a koordinována?
- [ ] Jsou chráněny důkazy pro následnou analýzu?
- [ ] Jsou průběžně informovány odpovědné osoby?

Čemu se při incidentu vyhnout

Při řešení incidentu mohou neuvážené zásahy způsobit větší škody než samotný útok.

Proto se doporučuje:

- nemažte podezřelé soubory bez konzultace s odpovědnou osobou,
- neprovádějte restart zařízení bez zaznamenání důvodů a stavu systému,
- neinstalujte neověřené nástroje pro „rychlou opravu“,
- nereagujte na požadavky útočníka bez schválení vedením organizace,
- nesdílejte informace o incidentu mimo určené komunikační kanály,
- neprovádějte změny, které mohou zničit důkazy potřebné pro analýzu.

Následná opatření

Řešením incidentu proces nekončí. Každý významnější incident představuje příležitost ke zlepšení bezpečnosti organizace.

Spolufinancováno Evropskou unií

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

CYLANCES

Čemu se při incidentu vyhnout

Po ukončení řešení by měla být provedena analýza příčin, která pomůže identifikovat:

- proč incident vznikl,
- jaké byly jeho dopady,
- zda byla reakce organizace dostatečná,
- jak lze podobným situacím předcházet v budoucnu.

Na základě získaných zkušeností je vhodné:

- aktualizovat bezpečnostní opatření,
- upravit interní postupy,
- doplnit školení zaměstnanců,
- aktualizovat analýzu rizik,
- ověřit účinnost přijatých opatření.

Spolufinancováno Evropskou unií

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Projekt financovaný v rámci grantové dohody č. 101249300 je podporován Evropským průmyslovým, technologickým a výzkumným centrem kompetencí pro kybernetickou bezpečnost.

CYLANCES