Standard č. 1

Manažera kybernetické bezpečnosti MD

Věc: Požadavky na bezpečnostní monitoring aplikací

Informační systém	Všechny aplikace Ministerstva dopravy ČR, zařazené do Systému řízení kybernetické bezpečnosti (SŘKB)
Zodpovědná osoba	Správci a provozovatelé jednotlivých aplikací

Odůvodnění standardu

Základní pravidla a principy bezpečnosti informací jsou obsaženy v politice/koncepci/strategii MD. Podrobnější požadavky, které plynou z aktualizací právních úprav, správných praxí, incidentů atd. řeší standardy, závazné pro všechny aplikace, zařazené do Systému řízení kybernetické bezpečnosti.

Tento standard upřesňuje požadavky Části VI, kapitoly 4 (Monitorování) přílohy č. 4 Bezpečnostní politiky informací MD (Požadavky na auditní záznamy) v souladu s požadavky § 22, odst. 2, písm. b) aktuálního znění Vyhlášky o kybernetické bezpečnosti č. 82/2018 Sb.

Upřesněné požadavky na bezpečnostní monitoring aplikací

1. Obsah auditních záznamů

Bezpečnostní politika informací MD stanovuje, že každý záznam v logu musí obsahovat minimálně tyto informace:

- datum a čas, kdy k události došlo,
- ID uživatele (či automatu),
- zdroj (IP adresa, lokální konzole a podobně),
- vlastní auditní informaci.

Tento standard upřesňuje výše uvedený obsah logů. Pro potřeby monitoringu aplikací je nutné do logů zaznamenávat tyto informace:

- datum a čas včetně specifikace časového pásma,
- typ činnosti,
- identifikaci technického aktiva, které činnost zaznamenalo,
- jednoznačnou identifikaci účtu, pod kterým byla činnost provedena,
- jednoznačnou síťovou identifikaci zařízení původce,
- úspěšnost nebo neúspěšnost činnosti.

2. Sběr a vyhodnocování kybernetických bezpečnostních událostí

Bezpečnostní politika informací MD neobsahuje konkrétní požadavky na nástroj pro sběr a nepřetržité vyhodnocování kybernetických bezpečnostních událostí, protože ty závisejí do značné míry na aktuálním způsobu řešení.

Tento standard odráží aktuálně používaný nástroj pro sběr a vyhodnocování kybernetických bezpečnostních událostí, kterým je SIEM, provozovaný bezpečnostním dohledem O2. Požadavky na sběr a způsob nepřetržitého vyhodnocování kybernetických bezpečnostních událostí jsou tyto:

- auditní záznamy jsou pořizovány v rozsahu bodu č. 1 a následně jsou odesílány do centrálního SIEM, provozovaného O2,
- auditní záznamy jsou do SIEM odesílány "on-line", povoleno je odesílání těchto záznamů dávkově v intervalu, který s ohledem na provozní zatížení systému nepřesahuje jednotky minut,
- auditní záznamy jsou vyhodnocovány nejen "ručně", ale také automatizovaně na základě aktualizovaného seznamu korelačních pravidel,
- je definován proces pro aktualizaci seznamu korelačních pravidel na základě průběžného vyhodnocování jejich účinnosti, pro případ reakce na bezpečnostní incidenty a podobně,
- je definován proces, jakým jsou relevantní osoby (administrátoři provozovatelů, Manažer kybernetické bezpečnosti a podobně) informovány o kybernetické bezpečnostní události,
- je definován proces zpřístupnění auditních záznamů řešitelům kybernetických bezpečnostních událostí, pokud o to požádají.

Výše uvedené požadavky na zpřístupnění relevantních auditních záznamů řešitelům kybernetických bezpečnostních událostí je nutné zajistit i v případě provozovatelů, se kterými nemá MD přímý smluvní vztah. Zejména se jedná o provoz CMS, JIP/KAAS, NIA a podobně.

V Praze dne dle elektronického podpisu

Ing. Josef Svozilík

Digitálně podepsal Ing. Josef Svozilík
Datum: 2021.04.15 14:30:13 +02'00'

Ing. Josef Svozilík
Manažer kybernetické bezpečnosti MDČR