Standard č. 4

Manažera kybernetické bezpečnosti MD

Věc: Minimální korelační pravidla

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 stanoví minimální korelační pravidla pro události, které budou ukládány a automatizovaně vyhodnocovány v SIEM na základě požadavků Části VI, kapitola 4 (Monitorování) Přílohy č. 4 Bezpečnostní politiky informací MD (Pravidla pro provozovatele) a v souladu s požadavky § 24, písm. d) aktuálního znění Vyhlášky o kybernetické bezpečnosti č. 82/2018 Sb. (dále jen VoKB).

Pravidla pro implementaci minimálních korelačních pravidel:

- Níže uvedená korelační pravidla jsou nedílnou součástí bezpečnostních požadavků na každou aplikaci, která je součástí systému řízení kybernetické bezpečnosti, ve smyslu §13 VoKB (Akvizice, vývoj a údržba).
- Níže uvedená korelační pravidla musí být součástí souboru korelačních pravidel aplikovaných u každého informačního systému MD, který je součástí Systému řízení kybernetické bezpečnosti.
- Při implementaci každého z níže uvedených pravidel v rámci konkrétní aplikace je nutné se řídit cílem, který má dané pravidlo naplnit.

Pokud není z logiky práce s danou aplikací možné některé z níže uvedených pravidel aplikovat, musí být toto zdůvodněno v její dokumentaci.

Minimální korelační pravidla:

1. Princip „bezpečné přístupové lokality“

Detekovat uživatelský účet, ke kterému se uživatel připojil z jiného počítače/jiné IP adresy, než je „standardní“.

Důvod: Pokud není fixovaný uživatel na daný počítač, toto pravidlo umožní sledovat pohyb uživatelů z jednoho přístroje na druhý. Změna přístrojů může být bezpečnostní riziko, riziko úniku informací či přistup neoprávněné osoby do systému. V případě, že taková situace nastane, bude nástroj ke zjištění konkrétního zařízení a bude dále možné zjistit okolnosti události.

Cíl: Zajištění přístupových bodů do systému a omezení přístupu neoprávněných zařízení (PC).

2. Princip „jeden uživatel, jedno připojení“

Detekovat uživatelský účet, u kterého byl zaznamenán pokus o vícenásobné připojení.

Důvod: Není žádný oprávněný důvod, proč by se dvě osoby měly simultánně připojovat k jednomu účtu. Pokud taková situace nastane, znamená to, že přístup (uživatelské jméno, heslo) k účtu do systému může znát neoprávněná osoba. Tento nástroj umožní zjistit kdy a kdo se pokoušel připojit k již připojenému účtu. Předpokládá se, že pro standardní činnost uživatele je dostačující připojení jedním účtem z jednoho zařízení.

Cíl: Zajistit a pojistit bezpečnost účtů uživatelů a přístup do systému.

3. Princip sledování proměnných IP adres

Detekovat uživatelský účet, u kterého dojde ke změně IP adresy během připojení k účtu.

Důvod: Vyvarovat se fenoménu „jumping IP“. Tento postup spočívá ve vzdáleném průniku do počítače uživatele systému a zneužití aktuálně přihlášených aplikací. V takovém případě může být IP adresa uživatele na vteřiny zaměněna za IP adresu útočníka a zase navrácena na IP uživatele, ale útočník již získá přístup k určitým datům ze systému, resp. tato data.

Cíl: Zajistit bezpečnost uživatelů a vyvarování se falešného obviňování**.**

4. Princip ochrany před útokem hrubou silou

Detekovat neobvyklý počet pokusů o přihlášení k uživatelskému účtu.

Důvod: Toto pravidlo detekuje útoky na autentizaci k OS a/nebo aplikaci hrubou silou. Pravidlo se spustí, když je překročen počet neúspěšných pokusů o přihlášení ke stejnému účtu za daný časový úsek.

Cíl: Zamezit útoku na přihlašovací údaje hrubou silou – systematické zkoušení přihlašovacích pokusů, provedené automatem.

5. Princip „pracovní doby“

Detekovat přihlášení k uživatelskému účtu:

- ke kterému dojde mimo pracovní nebo jinak omezenou dobu, pokud je tato pro danou aplikaci stanovena (např. pouze pracovní dny 7-18, pouze pracovní dny bez dalšího omezení, …),
- jiným, než “standardním” způsobem (např. přístup pomocí uživatelského prostředí, přístup na API, …).

Důvod: Přihlášení uživatele, který nemá „pracovní“ důvod pro přístup k aplikaci mimo stanovenou dobu, může znamenat pokus o zneužití získaných přístupových údajů, kdy se útočník snaží eliminovat riziko detekce násobného přístupu jednoho uživatele.

Cíl: Zajistit a pojistit bezpečnost účtů uživatelů a přístup do systému.

6. Princip „odhlášení“

Detekovat uživatelský účet, který je přihlášený déle než je maximální povolená doba (např. 16 hodin).

Důvod: Identifikovat situaci, kdy útočník provede „únos“ uživatelské session. Takový „únos“ může útočníkovi umožnit práci pod účtem uživatele, aniž by musel zadat jeho uživatelské jméno a heslo.

Útočník se snaží udržet session aktivní, aby nedošlo k automatickému odhlášení z důvodu nečinnosti (bezpečnostní politika požaduje odhlášení účtu po 15 minutách nečinnosti). Důsledkem je, že uživatelský účet je přihlášen netypicky dlouho.

Cíl: Zvýšit bezpečnost účtů uživatelů a přístupu do systému.

V Praze dne dle elektronického podpisu

Ing. Josef Svozilík

Digitálně podepsal Ing. Josef Svozilík
Datum: 2021.04.15 21:07:57 +02'00'

.....

Ing. Josef Svozilík
Manažer kybernetické bezpečnosti