Problematika logování a práce se SIEM

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

Obsah

- **Jaký je stav** z pohledu kontroly (aktuální Vyhlášky o kybernetické bezpečnosti)
  - § 22
  - § 24
  - Nejčastější problémy
  - Shrnutí

- **Jak zlepšit tento** stav – základní koncepty užitečného logování a práce se SIEM
  - **Plánování**
  - **Tipy a triky** pro konkrétní oblasti práce s logy v SIEM (analýza logů)
    - Služby a protokoly
    - Koncové stanice a uživatelé
    - Zpětná analýza

Úvod

- Co jsou to logy?

- Co je to SIEM (Security Information and Event Management)?

Vyhláška o kybernetické bezpečnosti

Aktuality

07.09.2022 NÚKIB představuje evropskou směrnici NIS2

25.08.2022 NÚKIB spouští webové stránky ke směrnici NIS2

Národní úřad pro kybernetickou a informační bezpečnost
24. srpen v 15:05 ·

✔ Spustili jsme stránky ke směrnici NIS2. Na https://nis2.nukib.cz/ nyní najdete relevantní informace přehledně na jednom místě.

ℹ Nová směrnice EU o kybernetické bezpečnosti, tzv. NIS2, přináší mnoho změn. Vybrali jsme pro vás 10 nejzajímavějších a nejdůležitějších z nich, které se s touto blížící se právní úpravou pojí. Vše budeme průběžně doplňovat.

#nukib #nis2

NÚKIB představuje evropskou směrnici NIS2

Do roku 2024 by měla mít Česká republika ve svém právním řádu implementovány požadavky nové směrnice Evropského parlamentu a Rady Evropské unie o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii, tzv. směrnice NIS2. Ta přináší mnoho změn v oblasti zajišťování kybernetické bezpečnosti a týká se nejen organizací, které jsou již dnes ze zákona o kybernetické bezpečnosti povinny své systémy

§ 22 odst. 1

(1) *Povinná osoba*

a) *zaznamenává* ***bezpečnostní*** *a* ***potřebné provozní*** *události* ***důležitých*** *aktiv informačního a komunikačního systému a*

b) *na základě* ***hodnocení důležitosti aktiv aktualizuje rozsah*** *aktiv, u kterých je zaznamenávání bezpečnostních a provozních událostí prováděno.*

§ 22 odst. 2

(2) *Povinná osoba pro zaznamenávání bezpečnostních a provozních událostí podle odstavce 1 zajišťuje*

a) ***jednoznačnou síťovou identifikaci*** *zařízení původce, je-li v komunikační síti použit nástroj, který* ***mění*** *jeho síťovou identifikaci,*

b) *sběr informací o bezpečnostních a provozních událostech; zejména zaznamenává*

1. *datum a čas včetně specifikace časového pásma,*
2. *typ činnosti,*
3. *identifikaci technického aktiva, které činnost zaznamenalo,*
4. *jednoznačnou identifikaci účtu, pod kterým byla činnost provedena,*
5. *jednoznačnou síťovou identifikaci zařízení původce a*
6. *úspěšnost nebo neúspěšnost činnosti,*

c) ***ochranu informací*** *získaných podle písmen a) a b) před neoprávněným čtením a jakoukoli změnou,*

d), e)

(d) *zaznamenávání*

1. *přihlašování a odhlašování ke všem účtům, a to včetně neúspěšných pokusů,*

2. *činností provedených administrátory,*

3. *úspěšné i neúspěšné manipulace s účty, oprávněními a právy,*

4. *neprovedení činností v důsledku nedostatku přístupových práv a oprávnění,*

5. *činností uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému,*

6. *zahájení a ukončení činností technických aktiv,*

7. *kritických i chybových hlášení technických aktiv a*

8. *přístupů k záznamům o událostech, pokusy o manipulaci se záznamy o událostech a změny nastavení nástrojů pro zaznamenávání událostí a*

e) synchronizaci **jednotného času** technických aktiv nejméně jednou za 24 hodin

§ 22 odst. 3, 4

(3) Povinná osoba uvedená v § 3 písm. c), d) a f) zákona uchovává záznamy událostí zaznamenaných podle odstavce 2 nejméně po dobu **18 měsíců**.
(4) Povinná osoba uvedená v § 3 písm. e) zákona uchovává záznamy událostí zaznamenaných podle odstavce 2 nejméně po dobu **12 měsíců**.

§ 24 písm. a), b), c)

Povinná osoba uvedená v § 3 písm. c), d) a f) zákona používá nástroj pro ***sběr a nepřetržité vyhodnocení kybernetických bezpečnostních událostí****, který umožní*

a) *sběr a vyhodnocování událostí zaznamenaných podle § 22 a 23,*

b) *vyhledávání a seskupování souvisejících záznamů,*

c) *poskytování informací pro určené bezpečnostní role o detekovaných kybernetických bezpečnostních událostech,*

§ 24 písm. d), e), f)

d) *vyhodnocování kybernetických bezpečnostních událostí s cílem* ***identifikace kybernetických bezpečnostních incidentů****, včetně* ***včasného*** *varování určených bezpečnostních rolí,*

e) *omezení případů* ***nesprávného vyhodnocení*** *událostí pravidelnou aktualizací nastavení pravidel pro*

1. *vyhodnocování kybernetických bezpečnostních událostí a*
2. *včasné varování a*

f) *využívání informací získaných nástrojem pro sběr a vyhodnocení kybernetických bezpečnostních událostí pro optimální* ***nastavení bezpečnostních opatření*** *informačního a komunikačního systému.*

Nejčastější problémy

- Není přehled o tom, co se kde loguje, detekuje a co z toho jde do SIEM
- Nikdo se SIEM nepracuje (analytika logů, false positive, alerty,…)
- SIEM je používán jako skladiště logů, absence log manageru
- Do SIEM není zapojeno to, co by určitě mělo být
- Zpětná vazba ze SIEM není nijak využita

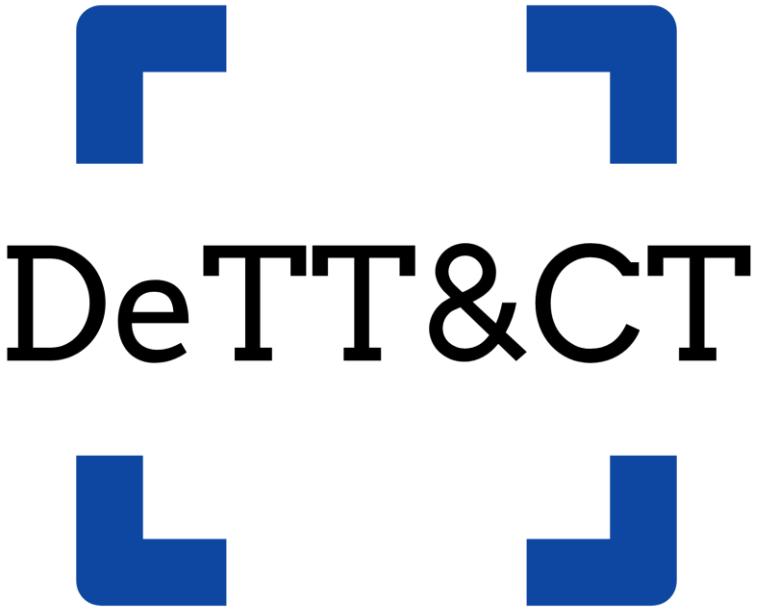
Shrnutí

- Nedostatečné plánování
  - Znalost vlastní infrastruktury, zejména možných zdrojů logů
  - Skladiště logů
  - Lidské zdroje se znalostmi a časem pro práci se SIEM
  - Vhodnost daného řešení pro daný systém, situaci a potřeby organizace
  - (Proof of Concept)

Jak zlepšit tento stav?

Plánování 1/2

- Inventura zdrojů logů, aneb co všechno chceme napojit do SIEM
- Možné způsoby plánování
  - Podle vstupů (co máme)
  - Podle výstupů (co chceme)
  - Kombinace
- Events per Second (peak)
- Uložiště logů
- **Lidské zdroje (analytici)**



Plánování je časově náročné, ale vyplatí se

Plánování 2/2

- Po pořízení SIEM
  Práce bohužel zdaleka nekončí, spíše začíná

- Přizpůsobení logů pro potřeby analýzy

  - Filtrování

  - Osekávání a obohacování

  - **Tagování**

  - **Údržba** a **změny**

Co Vás zajímá?

www. slido.com #Cybercon

Tipy a triky – služby a protokoly

- SMTP (Simple Mail Transfer Protocol)
  1. Detekce phishingových e-mailů
  2. Kompromitovaná e-mailová schránka spamuje
  3. Malware posílá e-maily

- DNS (Domain Name System)
  4. Základní pravidlo pro neutopení se v DNS logování
  5. Neautorizované DNS dotazování
  6. Rozpoznání náhodně generovaných domén
  7. Rozpoznání nových domén
  8. Jak poznat DNS tunneling
  9. Podezřelý provoz neužívající DNS
  10. Odkud vítr fouká

Tipy a triky – služby a protokoly

- HTTP (Hyper Text Transfer Protocol)
  11. Detekce HTTP Proxy (možný Man-in-the-Middle)
  12. Detekce Meterpreter přes HTTP
  13. Pokus o SQL Injection
  14. Detekce skenerů zranitelností
  15. Podezřelé HTTP requesty vůči IP adrese (absence DNS)
  16. Co mohou znamenat podezřelé délky URL (uvnitř sítě)
  17. Odkud vítr fouká 2.0

- TLS (Transport Layer Security)
  18. V tomto certifikátu něco chybí…
  19. Problém s neplatnými a self-signed certifikáty

Tipy a triky – koncové stanice a uživatelé

- Windows
  20. Jaké Windows Eventy mě mají zajímat, abych splnil požadavky VKB?
  21. Pokusy o prolomení hesla, které většina z nás nedetekuje (není to bruteforcing)
  22. Manipulace s uživateli, oprávněními nebo skupinami
  23. Manipulace se soubory
  24. Manipulace s registry
  25. Nové plánované úlohy (služby)
  26. Vyměnitelná zařízení
  27. Kdy je ok mazat logy?
  28. Logování PowerShell/cmd

- Linux
  29. Jak zabezpečit přenos logů
  30. iptables

Tipy a triky – Zpětná analýza

- Analýza historických logů
  31. Proč bych se měl zabývat logy, které už jsou „staré“ a v SIEM už byly?
  32. Detekce malware
  33. Detekce C2 nebo exfiltrace

Pavel Mazánek

Technický specialista informační/kybernetické bezpečnosti, Odbor kontroly

E-mail: p.mazanek@nukib.cz
Mobil: +420 722 975 021