Doporučení na minimální požadavky pro logy, které musí být zajištěny pro spolehlivou ex-post analýzu kybernetických bezpečnostních incidentů

Tento dokument popisuje doporučené minimální požadavky pro logy, které musí být zajištěny pro spolehlivou ex-post analýzu kybernetických bezpečnostních incidentů. Vychází z dokumentu NIST800-92 [1].

Pro ex-post analýzu KBI je nezbytné disponovat provozními záznamy z doby jejího výskytu. Zařízení, které záznamy generují je nespočet, jedná se obecně o bezpečnostní nástroje (antivirus, IDS/IPS, proxy, router, switch, firewall,…), operační systémy (autentizace, privilegované spuštění, systémové události,…) a aplikace (komunikace mezi klientem a serverem, uživatelské události, přístupy,…).

Pro nasazení log managementu je klíčové:

- Správně nastavené časové značky na všech zdrojích (tj. synchronizovaný čas, jeho jednotný formát)[1].
- Zajištění dostatečné kapacity pro logování, pravidelné odesílání logů do centrálního log managementu a jejich uchovávání po určenou dobu.
- Pravidelná analýza logů v log managementu, nejlépe automatizované upozornění na výskyt abnormalit.
- Zajištění bezpečnosti a integrity log záznamů (ochrana před zneužitím, změněním nebo vymazáním) napříč celým log management systémem (dle možné závažnosti zneužití).
- Dostupnost logů i v případě poruchy systému (zálohování).

Zdroje logů můžeme rozdělit do několika kategorií:

- Skupinou **SEC** je myšleno bezpečnostní software a nástroje, jako antivirový/antimalware software, IPS a IDS systémy, VPN, web proxy, vulnerability management software, firewally a routery, autentizační servery apod.
- Skupina **OS** zahrnuje servery, pracovní stanice a síťové prvky (routery a switche). Jde převážně o dva typy logů:
    - systémové události (spuštění/zastavení služby, vypnutí/zapnutí stanice, selhání služeb, závažné chyby apod.)
    - události auditu (pokusy o ne/úspěšné přihlášení, přístupy k souborům, změny nastavení, využití oprávnění apod.)
- Skupina **APP** označuje logování chodu aplikací. Jde především o:
    - Komunikace klienta se serverem (**C<>S**) - klientské požadavky přijaté serverem a jejich odpovědi.
    - Využití účtů (**ACC** = Account info.) - Informace o přihlášení k aplikaci/službě (i neúspěšné pokusy), změny v účtech, změny oprávnění apod.

[1] *Pro KII a VIS podle ZoKB platí: (4)* Orgán a osoba uvedená v § 3 písm. c) až e) zákona zajišťuje nejméně jednou za 24 hodin synchronizaci jednotného systémového času technických aktiv patřících do informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému.

- Údaje o aktivitě uživatelů (**Aktivita**) - např. počty transakcí a jejich objem.
- Významné provozní akce (**Akce**) jako spuštění nebo ukončení aplikace, pády aplikace nebo její významné změny.

Následující tabulka specifikuje jednotlivé skupiny logů a stanovuje koeficient (počet dní) pro jednotlivé skupiny.

SEC	AV	IDS/IPS	Vzdálený přístup	Web proxy	Autentizační server	Vulnerability management	Routery	Switche	Radius
Počet dní	30	30	30	30	30	30	30	30	30
OS	**Systém**	**Audit**							
Počet dní	30	30							
APP	**C <> S**	**ACC**	**Aktivita**	**Akce**					
Počet dní	7	7	1	30					

Následující tabulku určuje doporučení pro kategorie (KII/VIS/ostatní) kde počet dní najdete výše.

Kategorie	Ostatní	VIS	KII[2]
Retence dat SEC	min. 1 * počet dní	min. 3 * počet dní	min. 6 * počet dní
Retence dat OS	min. 1 * počet dní	min. 3 * počet dní	min. 6 * počet dní
Retence dat APP	min. 1 * počet dní	min. 3 * počet dní	min. 6 * počet dní
Rotace logů	Každý týden nebo po dosažení 25MB	Mezi 6-24 hodinami nebo při dosažení 5MB	Mezi 15-60 minutami nebo při dosažení 1MB
Jak často zasílat do log managementu	Každé 3-24 hodin	Každých 15-60 minut	Nejpozději každých 5 minut
Kontrola integrity (rotace)	Volitelná	Ano	Ano
Šifrování logů	Volitelné	Ano	Ano
Šifrovaný přenos logů do log managementu	Volitelný	Ano	Ano

Reference

[1] M. S. Karen Kent, „Guide to Computer Security Log Management,“ 2006. Dostupné online ' http://csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf '.

[2] Pro *KII podle ZoKB platí: (3)* Orgán a osoba uvedená v § 3 písm. c) a d) zákona záznamy činností zaznamenané podle odstavce 2 uchovává nejméně po dobu 3 měsíců.