LOGmanager

> Centrální úložiště logů
> Dostupný SIEM

SPLŇUJE POŽADAVKY ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI A ČSN ISO 27001

LOGmanager a súlad s požiadavkami zákona o kybernetickej bezpečnosti

Whitepaper ilustruje, ako nasadenie platformy LOGmanager pomáha zaistiť dodržiavanie požiadaviek zákona č. 69 z 30. januára 2018 o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len ZKB). Vyhlášky č. 164 Národného bezpečnostného úradu z 1. júna 2018, ktorou sa určujú identifikačné kritériá prevádzkovanej služby (kritériá základnej služby). Vyhlášky č. 165 Národného bezpečnostného úradu z 1. júna 2018, ktorou sa určujú identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov a podrobnosti hlásenia kybernetických bezpečnostných incidentov. Vyhlášky č. 362 VYHLÁŠKA Národného bezpečnostného úradu z 11. decembra 2018, ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len VKB).

Mnoho organizácií rieši otázku, aké kontrolné opatrenia a v akých oblastiach je podľa požiadaviek ZKB a VKB povinné dodržiavať. Taktiež sa zamýšľajú nad tým, aké systémy a riešenia im môžu spoľahlivé dodržiavanie týchto požiadaviek zaistiť. Tento dokument popisuje, ako možno dosiahnuť splnenie niektorých dôležitých požiadaviek týchto právnych noriem, a to zavedením vhodného systému centrálneho zberu a riadenia bezpečnostných udalostí postaveného na platforme LOGmanager.

Prehľad pre vedúcich pracovníkov na pozíciách CISO/CIO

Tento dokument pracuje s aktuálnym znením ZKB a VKB k 1. júnu 2019.

Stručne k ZKB:

- Upravuje organizáciu, pôsobnosť a povinnosti orgánov verejnej moci v oblasti kybernetickej bezpečnosti, národnú stratégiu a jednotný informačný systém kybernetickej bezpečnosti.
- Definuje postavenie a povinnosti prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb.
- Definuje jednotlivé sektory, prevádzkovateľov služieb a ústredné orgány, ktoré ich majú vo svojej pôsobnosti a druhy digitálnych služieb.
- Ďalej vo vyhláškach definuje identifikačné kritériá základnej služby, identifikačné kritériá pre jednotlivé kategórie závažných kybernetických bezpečnostných incidentov, podrobnosti hlásenia kybernetických bezpečnostných incidentov a obsah bezpečnostných opatrení, obsah a štruktúru bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

LOGmanager – stručný popis

LOGmanager bol vyvinutý ako systém pre centralizovanú správu protokolov udalostí (logov), poskytujúci jednoduché zobrazenie všetkých strojovo generovaných dát v organizácii. V prvom kroku LOGmanager zhromažďuje, unifikuje a dlhodobo uchováva protokoly udalostí a záznamy o udalostiach z aktívnych sieťových prvkov, bezpečnostných zariadení, operačných systémov a aplikačného softvéru. Následne v „takmer reálnom čase“ (near real-time) ukladá zhromaždené dáta do dobre definovanej výkonnej databázy, ku ktorej môžu IT bezpečnostní špecialisti pristupovať prostredníctvom preddefinovaných riadiacich panelov a štruktúrovaného i fulltextového vyhľadávania s grafickým zobrazením výsledkov. To môže byť použité, okrem iného, aj pri plnení vybratých povinností vychádzajúcich zo ZKB. Ide najmä o povinnosti pre prevádzkovateľov základnej služby, plnení bezpečnostných opatrení, riešenie kybernetických bezpečnostných incidentov a vykonanie auditu kybernetickej bezpečnosti. LOGmanager ďalej poskytuje základné SIEM funkcie, ako sú upozornenia s limitmi a jednoduché korelácie. Na nasadenie s cieľom získať súlad so ZKB sú tieto integrované SIEM funkcie dostatočné. Pokiaľ však zákazník požaduje pokročilé analytické a korelačné funkcie, LOGmanager poskytuje jednoduchú integráciu s ďalšími nástrojmi používanými na monitorovanie alebo analýzu dát, dátových tokov, aplikácií a operačných systémov. Pomocou LOGmanagera je možné rýchlo a jednoducho vizualizovať rôzne typy dát, a preto je vhodným riešením na implementáciu aj v takých zložitých a komplikovaných prostrediach, ako sú IoT a SCADA.

LOGmanager a jeho vzťah k ZKB

LOGmanager pomáha všetkým povinným subjektom predovšetkým s dodržiavaním povinností vyplývajúcich z nasledujúcich požiadaviek ZKB:

- Prijať organizačné a bezpečnostné opatrenia na riadenie rizík.
- Prijať opatrenia na predchádzanie incidentom narúšajúcim bezpečnosť.
- Viesť bezpečnostnú dokumentáciu.
- Hlásiť kybernetické bezpečnostné incidenty.
- Poskytovať úradu súčinnosť na posúdenie bezpečnosti.

Na vyššie uvedené povinnosti LOGmanager poskytuje mechanizmy protokolovania, upozorňovania a zaisťuje schopnosť spätne dohľadať aktivity systémov aj užívateľov a vykonávať ich priebežný aj nárazový audit. To je kriticky dôležité pre prevenciu, odhaľovanie alebo minimalizáciu vplyvov narušenia (kompromitácie) dát aj systémov. Vzhľadom na to, že LOGmanager v rámci jednoduchého zobrazenia poskytuje prístup ku všetkým strojovým dátam, je možné v prípade, že sa zistí problém, robiť podrobné sledovanie, aktivovať výstrahy a zaistiť detailnú analýzu. V skratke ide o aplikáciu na zhromažďovanie, ukladanie a analýzu protokolov udalostí, ktorá umožňuje nákladovo efektívnu automatizáciu bezpečnostných opatrení a proaktívnu ochranu informačných systémov a elektronických sietí.
LOGmanager spĺňa bez výhrad požiadavky normy STN EN ISO/IEC 27001:2013 na vytváranie auditných záznamov. Potvrdenie od autorizovaného audítora je na vyžiadanie u výrobcu LOGmanager riešenia k dispozícii.

Podrobnejšie o ZKB pre špecialistov bezpečnosti

Pre záujemcov o podrobné preštudovanie spomínaných právnych noriem sú tieto v úplnom znení k dispozícii na webovej adrese: https://www.sk-cert.sk/sk/legislativa/index.html

Na účely tohto dokumentu je dôležité, ako ZKB a VKB stanovujú organizačné a bezpečnostné opatrenia a akým spôsobom môže vhodne zvolený Security Event Management prispieť k naplneniu požiadaviek realizácie niektorých z týchto opatrení. Riešenie LOGmanager pomáha v rýchlej a jednoduchej orientácii spracovávaných logov. Ďalej sú v texte uvedené konkrétne ustanovenia ZKB/VKB, pri realizácii ktorých LOGmanager dopomáha k ich splneniu.

Bezpečnostné opatrenia a opatrenia na predchádzanie incidentom:

- Zabezpečiť dôkaz alebo dôkazny prostriedok tak, aby mohol byť použitý v trestnom konaní.
  LOGmanager bol navrhnutý podľa ISO 27001:2013 na vytváranie auditných záznamov a vykonávanie forenznej analýzy. Umožňuje tak podporovať požiadavky **ZKB § 19 Povinnosti prevádzkovateľa základnej služby.**
- Riadiť bezpečnosť sietí a informačných systémov, prevádzky, prístupov, monitorovania a bezpečnostných auditov.
  LOGmanager sleduje kybernetické bezpečnostné udalosti a zaisťuje ochranu prístupu k vzniknutým záznamom. LOGmanager je nástroj podporujúci prevedenie jednorazového aj periodického auditu dodržiavania bezpečnostných politík a poskytuje platformu pre rolu audítora kybernetickej bezpečnosti. Umožňuje tak podporovať požiadavky **VKB § 10 Bezpečnostné opatrenia pre oblasť podľa § 20 ods. 3 písm. f) zákona.**
- Predchádzať a riešiť kybernetický bezpečnostný incident. Dosahovať súlad sietí a informačného systému s bezpečnostnými štandardmi v oblasti kybernetickej bezpečnosti.
  LOGmanager pomáha pri detekcii a vyhodnocovaní bezpečnostných udalostí a incidentov, zlepšuje možnosti koordinácie pri riešení IT incidentov všeobecne. Z hľadiska koordinácie – všetky dôležité strojové dáta sa nachádzajú v ľudsky zrozumiteľnom formáte v jednom štruktúrovanom úložisku, čím sa zrýchľuje prevedenie analýzy základných príčin incidentu (RCA – Root cause analysis) a následné prevedenie nápravy. Umožňuje tak podporovať požiadavky **ZKB § 24 Hlásenie kybernetických bezpečnostných incidentov prevádzkovateľom základnej služby.**
- Preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek stanovených týmto zákonom vykonaním auditu kybernetickej bezpečnosti.
  LOGmanager dopomáha súladu požadovaných opatrení tvorbou vhodných reportov a auditov. Umožňuje tak podporovať požiadavky **ZKB § 29 Audit.**
- Monitorovať bezpečnosti sietí a informačných systémov implementáciou centrálneho nástroja na zaznamenávanie činnosti sietí a informačných systémov a ich používateľov.
  LOGmanager je nástrojom na centrálny zber a analýzu činností všetkých systémov generujúcich strojové dáta. Umožňuje tak naplniť požiadavky **VKB § 15 Bezpečnostné opatrenia pre oblasť podľa § 20 ods. 3 písm. k) zákona.**

LOGmanagerom odporúčané technické opatrenia:

- Zaznamenávanie udalostí informačného a komunikačného systému, jeho užívateľov a administrátorov.

  Tu je hlavná doména LOGmanagera. LOGmanager vykonáva nespochybniteľné a dlhodobé uloženie zaznamenaných bezpečnostných a prevádzkových udalostí aktivít informačného a komunikačného systému. Spolupracuje pri jednorazovej sieťovej identifikácii zariadenia pôvodcu a zaznamenáva požadované informácie ako z hľadiska obsahu, štruktúry, tak aj činnosti. Podľa modelu LOGmanagera a množstva zbieraných strojových dát dokáže poskytnúť dostatočnú retenciu dát na naplnenie požiadaviek na nespochybniteľné ukladanie záznamov udalostí. A to bez nutnosti využívať externé dátové úložisko.

- Zber a vyhodnocovanie kybernetických bezpečnostných udalostí.

  LOGmanager je nástroj, ktorý zbiera a nepretržite vyhodnocuje kybernetické bezpečnostné udalosti na základe upozornení a korelácií. Poskytuje rýchle vyhľadávanie a zoskupovanie súvisiacich záznamov. Ďalej poskytuje informácie pre určené bezpečnostné role a umožňuje nastavenie pravidiel na včasné varovanie o vzniknutých bezpečnostných udalostiach.

- Kryptografické opatrenia.

  LOGmanager umožňuje upozorňovať na využívanie menej odolných algoritmov, kľúčov aj protokolov, ako je uvedené v odporučeniach vydaných Úradom.

Kybernetický bezpečnostný incident a LOGmanager:

LOGmanager pomáha splniť náležitosti hlásenia bezpečnostného incidentu. A to hlavne tým, že udalosti zaznamenáva v nespochybniteľnej podobe, s presnou identifikáciou informačného a komunikačného systému, dôveryhodnou časovou pečiatkou a poskytne potrebné informácie na vytvorenie podrobného popisu incidentu.

Minimálne požiadavky CSIRT.SK

V dôsledku nedostatkov presných technických požiadaviek na realizáciu Security Event Managementu je vhodné sa obrátiť na odporúčanie ďalších dôveryhodných inštitucií. Vládna jednotka pre riešenie počítačových incidentov v Slovenskej republike vo svojom dokumente: „**Metodika pre systematické zabezpečenie organizácií verejnej správy v oblasti informačnej bezpečnosti**“ sumarizuje minimálne opatrenia potrebné na zabezpečenie informačných systémov a infraštruktúry organizácie so zvýšenými požiadavkami na bezpečnosť. LOGmanager ako centrálna logovacia platforma je vhodným kandidátom na splnenie týchto požiadaviek. Zároveň môžu byť využité jeho rozsiahle reportovacie a alertovacie funkcionality, pomocou ktorých môžu byť rozosielané notifikácie a reporty zodpovedným osobám a administrátorom systémov.

Výber jednotlivých požiadaviek z uvedenej metodiky, ktoré je možné splniť pomocou LOGmanagera:

2.14 Musí byť implementované logovanie a logy by mali zaznamenávať minimálne:

a. (Úspešné aj neúspešné) Prihlásenie a odhlásenie.
b. (Úspešné aj neúspešné) Vytvorenie, modifikácia alebo zmazanie používateľa alebo skupiny.
c. (Úspešné aj neúspešné) Pokusy pristúpiť k citlivým údajom (údaje klasifikované hornými dvomi klasifikačnými stupňami v rámci organizácie).
d. (Úspešné aj neúspešné) Pokusy o kritické operácie.

2.15 Logy musia byť centrálne ukladané a archivované minimálne 6 mesiacov.

2.16 Riešenie musí podporovať aj logovanie vo formáte syslog a musí podporovať preposielanie týchto logov na externý syslog server.

3.65 Na serveri musí byť aktívne logovanie:

d. Logy musia byť uchovávané na separátnom zariadení, resp. na separátnej logickej partícii.
f. Logy by mali byť archivované na čas stanovený pravidlami organizácie, minimálne však 6 mesiacov.

4.34 V prípade neobvyklej udalosti by mal byť notifikovaný systémový administrátor, a to minimálne v týchto prípadoch:

a. Blížiace sa zaplnenie kapacity úložného priestoru.
b. Neštandardne vysoká záťaž systému (load).
c. Detekovaná neobvyklá bezpečnostná udalosť.

4.35 Odporúča sa implementovať unifikovaný centrálny monitorovací systém s nastavenými metrikami pre každé monitorované zariadenie/systém. Príklady nastavenia metrík: upozornenie e-mailom pri 80 % zaplnenia diskovej partície, SMS alert pri 95 % zaplnení diskovej partície, upozornenie pri 50 % využití CPU počas 5 minút, SMS alert pri nedostupnosti kritickej služby viac ako 5 minút.

4.39 Odporúča sa nastaviť monitorovací systém tak, aby v prípade vážnych udalostí produkoval aj upozornenie cez „out-of-band" kanál (napríklad e-mail a SMS).

4.40 Logy musia obsahovať korektné informácie o dátume, čase a použitej časovej zóne. Na korektné nastavenie času sa odporúča nastaviť synchornizáciu s dôveryhodným NTP serverom. Odporúča sa využiť autentifikovanú NTP synchronizáciu.

4.42 Logovanie musí byť nastavené tak, aby prípadné zaplnenie logovacieho miesta neovplyvnilo stabilitu OS. Možné opatrenia: samostatná disková partícia, rotovanie logov a maximálna veľkosť logov.

4.43 Logy z kritických služieb a serverov musia byť synchronizované na samostatné logovacie zariadenie.

4.44 Logovacie súbory by mali byť zabezpečené aspoň takýmto spôsobom:

a. Mali by byť čitateľné pre administrátora.
b. Nemali by byť prepisovateľné a vymazateľné (mal by byť možný len zápis na koniec súboru).
c. Odporúča sa komprimovať a šifrovať archivované logovacie súbory. Pri ručnej archivácii sa odporúča aj podpisovať logovacie súbory.

7.6 Bezpečnostné logy z pracovných staníc by mali byť odosielané na centrálny server a ukladané minimálne 6 mesiacov.

Linka pre záujemcov o podrobné preštudovanie spomínanej metodiky. Táto je v úplnom znení k dispozícii na webovej adrese: https://www.csirt.gov.sk/informacna-bezpecnost/osvedcene-postupy/metodika-zabezpecenia-ikt-8a6.html

LOGmanager – zhodnotenie nákladov na riešenie a prínosov pre organizáciu

Pred realizáciou zákonom požadovaných opatrení je vhodné spraviť analýzu rizík a zhodnotiť celkové náklady na rôzne varianty riešenia, a to pri maximálnom zachovaní súladu s reguláciami. LOGmanager poskytuje vyvážený pomer na vynaložené náklady na riešenie pri dostatočnom plnení bezpečnostných a technických opatrení vyžadovaných ZKB/VKB.

Hlavné výhody riešenia LOGmanager pre organizácie hľadajúce optimálny pomer medzi dosiahnutou bezpečnosťou a rozumnými nákladmi:

- Rýchla implementácia. Na dosiahnutie súladu s reguláciami postačuje implementácia v priebehu niekoľkých dní.
- Obsahuje základné SIEM funkcie a vzorové alerty aj korelácie pre typické užívateľské príklady použitia.
- Jednoduché zaškolenie obsluhy. Užívateľsky prehľadné a intuitívne ovládanie v češtine/angličtine.
- Detailná dokumentácia v češtine aj angličtine. Návody na vhodné nastavenie zdrojov udalostí.
- Nízke a hlavne presne definované náklady na prevádzku riešenia. Hardvér, softvér, služby v cene.
- Žiadne skryté licenčné náklady, LOGmanager neobsahuje licenčné obmedzenia.
- Súlad s normou STN EN ISO/IEC 27001:2013, splnenie požiadaviek regulácií.

Na záver: Aj keď vaša organizácia zatiaľ nepatrí medzi povinné subjekty podľa ZKB, môže preukázať zodpovedný prístup („due diligence" and „due care") k bezpečnosti informácií a IT systémov realizáciou opatrení uvedených v odporučeniach ZKB.

Dňa 3.6.2019 LOGmanager security solution architect Peter Dömény. Email: peter.domeny@logmanager.sk

INFORMÁCIE O VÝROBCOVI A REFERENCIE

LOGmanager je vyvíjaný od roku 2014 ako nosný produkt firmy Sirwisa a.s., ktorá sídli v Prahe. Doteraz našiel LOGmanager viac ako 150 spokojných zákazníkov a na stránkach www.logmanager.sk nájdete vybrané referencie. Medzi našich zákazníkov patrí nielen štátna správa, ale aj priemyslové podniky všetkých veľkostí a oborov, obchodné spoločnosti, banky, poisťovne a ďalšie. Pre ďalšie referencie priamo z oblasti, ktorá Vás zaujíma nás neváhajte kontaktovať.