

Security Lifecycle Review

Skutečně víte, co se děje ve vaší síti? Většina společností postrádá ucelený přehled o aktivitách a zařízeních ve svých sítích, takže jsou v naprosté nevědomosti o bezpečnostních rizicích. Služba Security Lifecycle Review (SLR) poskytuje individuální bezpečnostní posouzení aplikací, IoT zařízení (internetu věcí), bezpečnostních slabin, hrozeb a rizik ve vašem prostředí. Jakmile máte představu o tom, kde jsou největší rizika, můžete určit, na co se soustředit, vypracovat akční plán a upevnit svou bezpečnostní pozici.

Přínosy služby SLR

- **Ucelený přehled:** Uvidíte, jak se protivníci snaží narušit vaši obranu, jaké různé aplikace se ve vaší síti používají a jaká všechna zařízení jsou k síti připojena.
- **Kvantifikované riziko:** Můžete s jistotou dělat rozhodnutí podložená daty, priorizovat a na základě získaných poznatků implementovat patřičné zásady nebo provést technologické kroky.
- **Úspora času:** Jediná sestava shrnuje klíčová rizika a doporučení, aby se vaše bezpečnostní týmy mohly soustředit na hlavní priority.

Co je SLR?

Cílené, bezplatné posouzení bezpečnostních rizik. Výsledkem SLR je zpráva, která shrnuje objem a typy hrozeb, jimž je síť vystavena, a slabin identifikovaných v síti za určené časové období. Zahnuje taky doporučení, jak omezit celkovou rizikovou expozici a zlepšit bezpečnostní pozici.

Přehled o IoT zařízeních a souvisejících rizicích	Rizika související s SaaS a dalšími aplikacemi	DNS Analýza zabezpečení	URL Analýza aktivity	Hrozby podle cílové země
Slabiny aplikací	Analýza hrozeb	Analýza přenosů souborů	Analýza malwaru	Spotřebovaná šířka pásma

Obrázek 1: Zjištění ve vaší zprávě SLR¹

SLR se dá provést při prvotním posouzení nebo v rámci pravidelné bezpečnostní kontroly. Zjištění vycházejí z dat shromážděných za sledované období (obvykle sedm dnů), přičemž data se shromažďují neintruzivně.

Proč provést SLR?

Pro účinnou správu zabezpečení sítě a robustní systém prevence narušení (IPS) potřebujete hluboký vhled do prostředí své organizace. Všechny hrozby by se měly pravidelně vyhodnocovat a měla by se jim přiřazovat relativní rizika. Pak budete moci s ohledem na tato rizika efektivně spravovat priority a zdroje, vytvořit pevnou bezpečnostní pozici a účinně bránit narušením provozu a útokům.

SLR je rychlý a jednoduchý způsob, jak si udělat představu o aplikacích, hrozbách a slabinách v síti. Zpráva uvádí podrobnosti o softwaru používaném jako služba (SaaS) a dalších aplikacích, o provozu vzhledem k URL, o typech obsahu, IoT zařízeních (viz obrázek 3) a o známých i neznámých hrozbách vstupujících do vaší sítě (viz obrázek 4). Nechybí ani doporučení ohledně největších rizik a oblastí, na které je potřeba se prioritně zaměřit (viz obrázek 5).

Stručné shrnutí pro ACME

HLAVNÍ ZJIŠTĚNÍ		
664 POUŽÍVANÝCH APLIKACÍ Používá se celkem 664 aplikací, které s sebou nesou potenciální provozní i bezpečnostní vývoj. Když se kritické funkce dostávají mimo kontrolu organizace, zaměstnanci používají aplikace, jež nesouvisí s prací, a kybernetičtí špióni mohou jejich prostřednictvím doručovat hrozby a krást data.	130 VYSOCE RIZIKOVÝCH APLIKACÍ Bylo zaznamenáno 130 vysoce rizikových aplikací včetně těch, které mohou do sítě vnášet nebo skryvat škodlivé aktivity, vynášet soubory mimo síť nebo navazovat neoprávněná komunikační spojení.	211 SAAS APLIKACÍ Ve vaší síti bylo zaznamenáno 211 SaaS aplikací. V zájmu udržení administrativní kontroly doporučujeme používat ty SaaS aplikace, které může váš IT tým spravovat.
121 744 ZNEUŽITÍ SLABIN Ve vaší organizaci bylo zaznamenáno celkem 121 744 zneužití slabin včetně úniků informací, spouštění kódu a útoků hrubou silou.	123 285 HROZEB CELKEM Ve vaší síti bylo nalezeno celkem 123 285 hrozeb, výskytů známého a neznámého malwaru a případů odchylek řídicích povelů.	74 VÝSKYTŮ MALWARU Ve vaší organizaci bylo zaznamenáno 60 výskytů známého malwaru a 14 výskytů neznámého malwaru.

Obrázek 2: Stručné shrnutí SLR

Stručné shrnutí poskytuje vysokoúrovňový přehled o aplikacích a hrozbách zaznamenaných v síti.

1. Vyžaduje určitá předplatná.

Zabezpečení IoT

Středa 1. ledna 2020 – pondělí 23. března 2020

Podnikové síť už se neskládá jenom z tradičních IT aplikací a zařízení. Používají se v nich i specializovaná zařízení připojená k internetu, která pomáhají s optimalizací každodenních činností – zařízení operační technologie (OT) a zařízení široce označovaná jako internet věcí (IIoT). Tato IIoT zařízení často bývají nespolehlivá a představují pro organizace ohromné bezpečnostní riziko, protože nespědí pod obvyklou správou životního cyklu (IT) od nasazení přes průběžnou údržbu až po vyřazení. Řešení Palo Alto Networks IoT Security tato zařízení patentovanými algoritmy strojového učení vyhledává, zjišťuje rizika a doporučuje vhodné zásady pro zlepšení bezpečnostní pozice a koordinovanou správu životního cyklu.

HLAVNÍ ZJIŠTĚNÍ

574 NALEZENÝCH IIoT ZAŘÍZENÍ	4 ZAZNAMENANÁ UPOZORNĚNÍ IIoT	12 ZAZNAMENANÝCH SLABIN IIoT
Ve vaší síti bylo nalezeno 574 IIoT zařízení. 110 z nich představuje kritické riziko, 130 je vysoce rizikových a 140 představuje střední riziko. Největší riziko představují následující profily zařízení: Polycam IP Phone (153), Aruba Instant AccessPoint (107), Polycam Device (106), Polycam Video Conferencing Device (81) a Avaya IP Phone (33).	Ve vaší síti byla zaznamenána 4 upozornění. 1 upozornění je kritické, 1 upozornění vysoce vážné a 1 středně vážné. Nejčastější typy upozornění: anomální chování (4).	Ve vaší síti bylo zaznamenáno 12 slabín. 3 jsou potvrzené slabiny – 2 kriticky vážné a 1 středně vážná. 9 je potenciálních slabín – 4 kriticky vážných, 1 vysoce vážná a 2 středně vážné.

Obrázek 3: Část „Zabezpečení IoT“

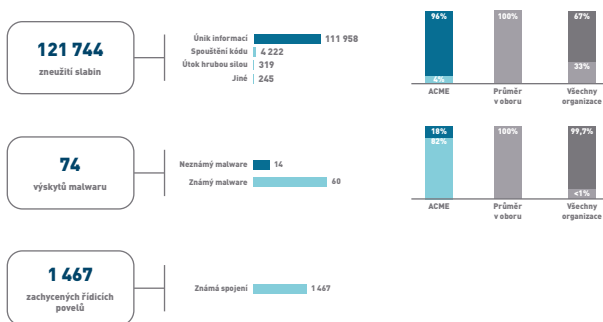
Část „Zabezpečení IoT“ poskytuje špičkový přehled a prioritizaci rizik souvisejících s IIoT zařízeními, abyste mohli lépe spravovat zabezpečení IIoT v průběhu celého životního cyklu zařízení.

Přehled hrozeb

Pro pochopení rizikové expozice a nutných úprav bezpečnostní pozice kvůli prevenci útoků jsou nutné poznatky o typu a objemu hrozeb namířených proti vaší organizaci. Tato část popisuje zaznamenané slabiny aplikací, známý a neznámý malware a aktivity řídících povět zachycené ve vaší síti.

HLAVNÍ ZJIŠTĚNÍ

- Ve vaší organizaci bylo zaznamenáno celkem 121 744 zneužití slabín včetně úniků informací, spouštění kódu a útoků hrubou silou.
- Bylo zaznamenáno 74 případů výskytu malwaru. Průměr mezi firmami ve vašem oboru je 0.
- Bylo identifikováno celkem 1 467 požadavků řídících povět, které svědčí o pokusech malwaru komunikovat s útočníky, stahovat další malware, dostávat pokyny a vynášet data.



Obrázek 4: Část „Přehled hrozeb“

Část Přehled hrozeb uvádí typy a objem hrozeb namířených proti vaší organizaci včetně známého a neznámého malwaru, neoprávněných řídících povětů a slabín aplikací.

DOPORUČENÍ

- Implementujte zásady bezpečných aplikací, které povolí jenom aplikace nutné pro chod firmy a budou detailně kontrolovat všechny ostatní.
- Zaměřte se na vysoce rizikové aplikace s potenciálem zneužití, mezi které patří vzdálený přístup, sdílení souborů nebo šifrované tunely.
- Zaměřte se na komunikaci řídících povětů provedením síť nebo zdrojového hostitele. To, k čemu skutečně došlo, může naznačit detekce a odezva nebo protokolovací řešení.
- Nasadte bezpečnostní řešení, které dokáže zjišťovat a blokovat známé i neznámé hrozby, zmiřovat tak riziko ze strany útočníků.
- Používejte řešení, která dokážou automaticky přeprogramovat sebe sama i jiné bezpečnostní produkty, vytvářet a koordinovat ochranu před novými hrozbami a vycházet přitom z poznatků od globální komunity podnikových uživatelů.
- Implementujte spravované zásady hostitelů, které omezí vektory útoků bez použití souborů a sníží riziko zneužití řídících povětů sdílením poznatků o hrozbách mezi bezpečnostními produkty téměř v reálném čase.
- V případě zjištění riskantních IIoT zařízení zvažte následující opatření:
 - Posouzení rizik souvisejících s těmito zařízeními.
 - Podchycení nebo zmírnění známých problémů úpravou konfigurací zařízení, upgradem jejich softwaru nebo instalací bezpečnostních oprav.
 - Omezení prostoru pro útok zavedením doporučených zásad.
 - Rozdělení zařízení do segmentů, které případné útoky zablokují, omezí nebo zpomalí.

Obrázek 5: Část „Doporučení“

Poslední část zprávy SLR shrnuje klíčová zjištění a poskytuje doporučení, jak může vaše organizace zareagovat na největší zjištěná rizika.

Nejčastější otázky (FAQ)

Jak můžu SLR spustit?

K samoobslužnému spuštění SLR se dostanete na [Portálu zákaznické podpory](#). Pokud potřebujete pomoc, obraťte se na svého obchodního zástupce. SLR je rovněž k dispozici jako [aplikace poskytovaná v cloudu](#).

Nejsem zákazník Palo Alto Networks. Můžu spustit SLR?

Ano! Obráťte se na místního obchodního zástupce nebo si [vyžádejte SLR online](#).

Zprávu SLR pro vaši organizaci vypracujeme spuštěním SLR ve vašem prostředí. Jedná se o neintruzivní proces. SLR se dá spustit na virtuálním i fyzickém firewallu.

Jak často mám SLR spouštět?

Zákazníci Palo Alto Networks můžou spouštět SLR na vyžádání tak často, jak potřebují. Doporučujeme pravidelně vyhodnocovat bezpečnostní rizika spuštěním SLR přinejmenším každých 90 dní nebo vždycky, kdy ve vaší síti došlo k podstatné změně.

Můžu získat jednu zprávu SLR pro několik zařízení?

Ano, funkce multi-statsdump merge umožňuje nahrát soubory statsdump z několika zařízení a vygenerovat souhrnnou zprávu SLR.

Další zdroje

- Další otázky? Navštivte náš [Portál zákaznické podpory](#).
- Chcete začít? Navštivte nás online a vyžádejte si SLR <https://start.paloaltonetworks.com/security-lifecycle-review-risk-assessment.html>
- Spouštíte SLR sami? Přečtěte si náš stručný návod [SLR QuickStart Guide](#).
- Potřebujete s aplikací SLR poradit? Přečtěte si [technickou dokumentaci](#).

Předplatná, která jsou nutná pro SLR

Pro nejucelenější přehled o svém prostředí budete potřebovat:

- Obecně: Předplatná WildFire, URL Filtering, Threat Prevention
- Část IIoT: Předplatné Cortex™ Data Lake a aktivní instance IIoT Security
- Část DNS: Předplatné DNS Security

O společnosti Palo Alto Networks

Palo Alto Networks, globální lídr na poli kybernetického zabezpečení, utváří budoucnost postavenou na cloudech technologiemi, které proměňují způsob fungování lidí a organizací. Naším posláním je coby preferovaný partner pro kybernetické zabezpečení chránit náš způsob života v digitálním věku. Pomáháme řešit největší bezpečnostní výzvy světa inovacemi, které staví na nejnovějších objevch v oblasti umělé inteligence, analytiky, automatizace a koordinace. Poskytováním integrovaných platformy a podporou rostoucího ekosystému partnerů jsme v popředí ochrany cloudů, sítí a mobilních zařízení tisíců organizací. Jde nám o to, aby den ode dne bylo na světě bezpečněji. Další informace najdete na webu www.paloaltonetworks.com.



3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

© 2020 Palo Alto Networks, Inc. Palo Alto Networks je registrovaná ochranná známka společnosti Palo Alto Networks. Seznam našich ochranných známek najdete na <https://www.paloaltonetworks.com/company/trademarks.html>. Všechny ostatní zmíněné značky mohou být ochrannými známkami příslušných společností.
security-lifecycle-ds-072420