Logmanager

Postupy pro minimalizaci hrozby a následku útoku

Ve stručnosti: Množství škodlivého software (malware) dnes a denně vzniká, využívá se a nakonec bohužel i úspěšně „monetizuje“. Jedním z nejpopulárnějších a “nejúspěšnějších” druhů malware mezi současnými typy hrozeb je ransomware. Šíří se překvapivě snadno a působí značné škody. Pro minimalizaci poškození způsobených vyděrači, navrhnul bezpečnostní tým Logmanageru soubor osvědčených postupů a protiopatření, která je vhodné dodržovat. Netvrdíme, že se jedná o úplný soubor pravidel a zásad, ale určitě poskytuje dobrý základ, kde začít. Pokud IT oddělení vaší společnosti přijme alespoň některá z nich, určitě tím připravíte tvrdý oříšek falešným hráčům při jejich další destruktivní misi.

Doporučené postupy pro síťovou infrastrukturu

1.	Implementujte pravidla na firewallu nejen pro příchozí provoz, ale nastavte pečlivě i pravidla pro odchozí provoz. Doporučujeme rovněž implementovat něco na způsob „whitelistu“, kam všude je povolen přístup. Logujte veškerý provoz na firewallu, krom zamítnutého příchozího provozu na perimetru sítě. Porovnejte efektivitu zónových pravidel pomocí analýzy počtu zásahů dle těchto pravidel v log managementu.	☐
Poznámky:		
2.	Oddělte interní sítě pomocí firewallu. Implementujte interní bezpečnostní zóny a vytvořte pravidla logiky nejmenších oprávnění pro limitování mezi-zónové komunikace. Pokud je to možné, logujte i veškerý provoz na firewallu, který se netýká perimetru.	☐
3.	Všude, kde je to možné, by měly být implementovány segmentované virtuální LAN (802.1Q) s režimem izolace portů nebo režimem privátních VLAN. Pokud se v komunikaci mezi jednotlivými VLAN používá ACL (namísto firewallů), logujte veškerá povolení/odmítnutí v rámci nastavených pravidel.	☐
4.	Implementujte Network Access Control dle 802.1X. Pokud dané zařízení připojené do sítě neumožňuje používat 802.1X „supplicanta“, použijte záložní autentizaci založenou na MAC. Logujte jak autentikátora (LAN, WLAN aktivní prvky), tak autentizační události na serveru. Nepovolujte připojení doménových počítačů do hostovské VLAN a použití doménových oprávnění pro 802.1X autentizaci (preferujte ověření přístupu na základě certifikátu pro systém).	☐
5.	Implementujte pravidla prevence průniků (Intrusion Prevention) alespoň na interním portu perimetru NG firewallu. Používejte profil optimalizovaný pro bezpečnost a logujte všechny události IPS, vytvořte upozornění na kritické.	☐
6.	Povinně „vždy zapnutá“ VPN se zakázaným split tunelem. Aby bylo zajištěno, že jsou vždy použita definovaná pravidla, měl by veškerý provoz vzdálených stanic procházet firewallem společnosti. Logujte veškerý VPN provoz, věnujte pozornost geolokaci příchozích VPN spojení a nadměrnému odchozímu provozu (možná exfiltrace dat).	☐
7.	Kontaktujte svého partnera pro síťovou infrastrukturu a znova ověřte, zda používáte osvědčené postupy pro detekci a prevenci „spoofingu“ (ARP inspekce, Port security a DHCP Snooping). Logujte všechny vzniklé události a varování.	☐
8.	Zálohujte a šifrujte zálohy aktivních prvků. Sledujte software aktivních prvků, pravidelně aktualizujte na poslední dostupné verze. Zvýšenou pozornost věnujte software Firewallu a VPN koncentrátoru. Pokud lze, přihlaste se k bezpečnostnímu newsletteru jejich výrobců.	☐

Doporučené postupy pro MS AD

1.	Rozdělte role AD administrátorů. Doménový administrátor by se měl připojovat svým účtem pouze k DC serverům. Pokud by se s daným účtem připojil kamkoliv jinam, považujte tento účet za kompromitovaný a změňte co nejdříve jeho heslo. Totéž platí pro servery. Administrátoři serverů mohou používat své účty pouze pro připojení k AD serverům a nikam jinam, ani k pracovním stanicím a/nebo DC. Logujte veškeré aktivity administrátorů.	☐
Poznámky:		
2.	Mininalizujte počet uživatelů s vysokým oprávněním. Vytvořte speciálního uživatele s delegovanými právy k přidávání počítačů do domény. Logujte přidávání nových uživatelů do domény. Pravidelně kontrolujte seznam privilegovaných účtů.	☐
3.	V MS AD prostředí přepněte na autentizaci pouze přes Kerberos. Nejdříve proveďte audit NTLM a po dobu jednoho týdne logujte veškerý NTLM audit. Na základě výsledků potom vytvořte výjimky a omezte NTLM autentizaci v Group Policies ("Deny all" - nejlepší přístup; "Deny for Domain Servers" – minimálně). Odkaz.	☐
4.	Zakažte lokální administrátory. Nikdo z uživatelů pracovních stanic by neměl být lokálním administrátorem. Používejte pouze účty helpdesku/supportu. Administrátor helpdesku/supportu by neměl být současně serverovým administrátorem. Logujte všechny aktivity lokálního administrátora na stanicích a nastavte zasílání upozornění.	☐
5.	Zvažte používání „whitelistů" a globální využití AppLockeru a jeho schopnosti omezit seznam spustitelných souborů z jiných než programových složek. Logujte veškeré aktivity AppLockeru. Odkaz1. Odkaz2. Odkaz3.	☐
6.	Nainstalujte a upravte si „Administrative Template" soubory pro O365 a Office. Omezte všem uživatelům otevírání dokumentů obsahujících makra pouze na takové soubory, kde jsou makra podepsána lokální certifikační autoritou (nejlepší postup) nebo blokujte spouštění maker v souborech Office z Internetu (minimálně). Odkaz.	☐
7.	Zkontrolujte, zda je doméně zakázáno používání LLMNR (Local-link Multicast Name Resolution) a NBT-NS (NETBIOS).	☐
8.	Používejte Microsoft PKI, zejména striktně pak pro RDP přístupy na servery i stanice. Zvažte, kde dále je možné nasadit ověřování prostřednictvím certifikátů nebo vícefázového ověření.	☐
9.	Dbejte na řádný patch management. Logujte aktivity „windows update" a nastavte zasílání upozornění na nezdařené aktualizace na serverech hostujících aplikace. Věnujte pozornost zejména serverům, které jsou v zónám zabezpečení internetu/DMZ (mají povolenu komunikaci se zdrojem spojení v internetu).	☐
10.	Zbavte se staré verze SMB protokolu. Vytvořte v GPO politiku pro podepisování komunikace SMBv2 a SMBv3. Pravidelně prověřujte přístupová práva k SMB a logujte veškeré SMB aktivity – Advanced Audit Policy – Detailed File Share.	☐
11.	Používejte a správně nastavte pokročilé auditní politiky prostřednictvím GPO. Pokud používáte Logmanager, v on-line dokumentaci naleznete podrobný návod, jak nastavit „Advanced Audit Policy" pro rozdílné skupiny systémů.	☐

Doporučené postupy pro zálohování

100% ochranu před nevratnou katastrofou způsobenou ransomwarem Vám poskytne jedině zálohování! Pouze pokud máte správně uložené zálohy (on site, offsite, offline), můžete svá data alespoň obnovit zpět! Pravidelně ověřujte, zda dokážete obnovit data ze záloh.

1.	Pravidelně zálohujte veškerá důležitá data, kontrolujte/monitorujte správné zálohování, nastavte zasílání upozornění. Logujte všechny změny konfigurace zálohovacího serveru a veškeré zálohovací operace. Nastavte zasílání upozornění s velkou prioritou na nezdařená zálohování.	☐
Poznámky:		
2.	Zálohovací server by neměl být součástí domény a uživatelské jméno/heslo na zálohovací server by mělo být silné a odlišné od všech ostatních administrátorských účtů používaných v AD. Logujte všechny přístupy k zálohovacímu serveru. Logujte síťové aktivity zálohovacího serveru.	☐
3.	Omezte síťový přístup k zálohovacímu serveru tak, aby byl byly povoleny pouze ty TCP/UDP porty, které server potřebuje skutečně využívat. Logujte firewall pravidla omezující přístup na zálohovací server. Umístěte zálohovací server do speciální VLAN a aplikujte do této VLAN přístupové restrikce.	☐

Další doporučené postupy

1.	Zbavte se všech aplikací používajících vzdálenou plochu, které umožňují neomezený přístup ke zdrojům společnosti (jako teamview). Logujte použití a monitorujte využívání povolených aplikací používajících vzdálenou plochu. Nastavte zasílání upozornění na nové aplikace s povolením vzdáleného přístupu.	☐
Poznámky:		
2.	Používejte důvěryhodné antivirové řešení optimálně s EDR/XDR funkcionalitou a s centrálním managementem. Logujte všechny aktivity antiviru přes jeho centrální management, nastavte zasílání upozornění na deaktivované AV a přidané výjimky z AV ochrany ze všech pracovních stanic i serverů.	☐
3.	Implementujte NG-IPS funkcionalitu se zabudovaným SSL proxy pro odchozí provoz. Logujte všechny aktivity NG-IPS.	☐
4.	Implementujte „sandbox“ inspekci příchozích souborů pro webový a emailový provoz. Logujte všechny aktivity „sandboxu“ a nastavte zasílání upozornění při detekci hrozby. Integrujte zpětnou vazbu detekce ze „sandboxu“ na NGFW nebo IPS.	☐
5.	Logujte všechny DNS dotazy a analyzujte možné DNS skryté kanály. (covert channels)	☐
6.	Zajistěte pro uživatele alespoň jednou ročně online školení základní IT bezpečnosti a odolnosti proti phishingu.	☐

Další vylepšení bezpečnosti ke zvážení

1.	Prostřednictvím log managementu objevte používání nezabezpečených protokolů a nahraďte je zabezpečenými. Věnujte pozornost zejména Telnetu, SNMPv1/v2c s povolením přístupu pro zápis, FTP a zranitelnému SMBv1.	☐
Poznámky:		
2.	Implementujte automatizované a pravidelné skenování zranitelností všech serverů a aplikací (nejlepší řešení), nebo alespoň systémů v DMZ/Internet bezpečnostní zóně. Pokud si to můžete dovolit, provádějte zde i penetrační testy.	☐
3.	Logujte aktivity Linux administrátora včetně příkazů vydaných v CLI. Nastavte zasílání upozornění na atypické nebo nebezpečné příkazy. Příklad příkazů, na které je třeba upozorňovat: *history; cat /home/*/.ssh/id_rsa; python -m SimpleHTTPServer; python -m http.server; nc -e /bin/sh; nc -l -p;… Odkaz.	☐
4.	Prostřednictvím log managementu monitorujte všechny páry spojení Internal-IP <—> External-DNS-PTR (IP adresa interní sítě - zpětného překladu IP adresy na doménové jméno systému v internetu) a kontrolujte páry s nadměrným počtem spojení nebo přílišnou celkovou délkou spojení. Používejte ASN čísla nebo jména k vyloučení důvěryhodných externích sítí z tohoto seznamu.	☐
5.	Logujte a nastavte zasílání upozornění na jakoukoliv změnu času/data, která není řízena NTP, a na operace zastavení logování (stop syslog).	☐
6.	Poučte uživatele o zásadách pro hesla. (Zdůrazněte zejména zákaz používání firemních emailů k registraci soukromých účtů a nutnost používat rozdílná hesla pro použití na internetu.) Používejte systém centralizovaného bezpečného ukládání hesel (například www.secureanybox.com) a dejte tento systém k dispozici i svým zaměstnancům pro soukromé účely.	☐

Závěr: Používání alespoň některých z těchto doporučení rozhodně pomůže zlepšit zabezpečení prostředí vaší sítě. Ale s tím, jak se hrozby vyvíjejí, měla by se vyvíjet i vaše obrana. Zabezpečení je vždy průběžný proces a je důležité pravidelně kontrolovat, zda jsou vaše systémy v dobrém stavu a jsou chráněné i proti nejnovějším vektorům útoků. Pokaždé, když přidáte nový software nebo hardware, nebo provedete jiné významné změny ve své infrastruktuře, řešte, jak tyto změny zahrnete do svých bezpečnostních zásad a auditujte je ve svém log managementu. **Nejdůležitější rada - plánujte a mějte připravený aktuální, alespoň teoreticky otestovaný Disaster Recovery Plán.**

Poskytněte nám prosím zpětnou vazbu a návrhy k tomuto dokumentu na email: security-team@logmanager.com.

INFORMACE O VÝROBCI A DALŠÍ REFERENCE

Logmanager je vyvíjen od roku 2014 jako nosný produkt firmy Sirwisa a.s., která sídlí v Praze. Na stránkách www.logmanager.cz naleznete vybrané reference. Mezi naše zákazníky patří nejen státní správa, ale i průmyslové podniky všech velikostí a oborů, obchodní společnosti, společnosti z oblasti bankovnictví a další. Pro podrobnější list referencí přímo z oblasti Vaší činnosti nás neváhejte poptat. Příslušné kontakty na stávající zákazníky, kteří souhlasí s uváděním na referenčním listu, rádi předáme.