

Útoky vedené na počítačovou síť zevnitř, nejčastěji vlastními zaměstnanci nebo pomocí ukradených uživatelských identit/hesel, nejsou současnými technologiemi adekvátně řešitelné.

Stávající technologie pracují na principu zákazu. Princip zákazu není možné efektivně použít v otevřeném prostředí interní sítě LAN/WAN. Pomocí zákazu se totiž nelze bránit neznámým hrozbám. Proč? Nelze zakázat něco, co neznáme, jelikož už z principu nemůžeme vědět co konkrétního vlastně máme zakazovat.

Uveďme si několik příkladů z praxe.

Pan Jiří předpokládá, že ve firmě, kde je zaměstnán, brzy dojde na propouštění. Celková nejistota ho vede k tomu, že se začne zajímat, jak firmě, která by se k němu takto zachovala po 15 letech tvrdé práce, co nejvíce uškodit. Zaměří se na obchodní kontakty, unikátní firemní technologie a na výši odstupného, které dostali ostatní zaměstnanci. Jelikož má ze své pozice přístup k informacím o firemních technologiích a kontaktům na zákazníky, lehce zkopíruje tyto informace na svůj disk v notebooku a doma si je uloží na svůj osobní počítač.

Následně zjistí, že účetní má problémy s přístupem k Internetu. Zavolá tedy dané účetní, představí se jako člen IT oddělení a přesvědčí ji k vydání jejího hesla. Následně se již pod identitou účetní přihlásí k účetnímu a mzdovému systému a zjistí si informace o odstupném, které bylo vyplaceno dříve propuštěným zaměstnancům. Při té příležitosti si také pro všechny případy zkopíruje část firemního účetnictví.

Firma měla nasazena všechna moderní zařízení na ochranu sítě, ale neřešila ochranu před útoky zevnitř.

Tento případ byl zjištěn až když došlo na soudní řízení mezi panem Jiřím a nejmenovanou mezinárodní firmou.

Jak se tomu dalo předejít? Jednou z velmi efektivních možností je tzv. behaviorální analýza chování aplikací, uživatelů a zařízení. Pokud se podrobněji podíváme na výše uvedený příklad, je zřejmé, že analýza by odhalila několik anomálií. Uživatel přistupoval na server k nesrovnatelně více souborům a stáhl si mnohonásobně větší objem dat, než je u něj obvyklé. Působení osoby se zcizenou identitou lze v účetním systému odhalit díky nestandardnímu chování uživatele – přístupem z jiného počítače a neobvykle intenzivním prohlížením a stahováním účetních dat.

Podívejme se na jiný případ z praxe:

Administrátoři IT v jednom nejmenovaném bankovním ústavu měli pro potřeby výkonu své práce téměř úplný přístup ke všem systémům, včetně databáze zákazníků obsahující citlivá osobní data. Jeden z nich, pan J.K., byl jednoho dne osloven svým dlouholetým kamarádem z marketingové agentury, zda-li by mu za zajímavý finanční obnos

nepomohl. Bylo třeba získat seznam bonitních klientů pro marketingovou kampaň. Pan J.K. tedy data z databáze klientů postupně nahrál na DVD a předal svému příteli. Jelikož si byl vědom, že by se na to mohlo přijít, pečlivě smazal z auditovacího systému všechny údaje o svém přístupu k této databázi.

Banka pojala podezření teprve po delší době, poté co si část z klientů veřejně stěžovala na nepříjemnou reklamu na bankovní služby. Určité indicie ukazovaly na spojitost s panem J.K., ale nebylo možné jednoznačně prokázat jeho vinu, protože po sobě důkladně zametl stopy smazáním logů o přístupu k databázi.

Stejně jako v předchozím příkladu měla i banka nasazena veškeré moderní bezpečnostní systémy, ale bohužel opět příliš nehlídala své vlastní zaměstnance.

Dalo se i tomuto případu předejít? S behaviorální analýzou umožňující korelovat události na síti s aplikačními událostmi samozřejmě ano, neboť hlavním indikátorem tohoto úniku dat je fakt, že v síťovém provozu byl zaznamenán přístup k databázi klientů, ale v auditovacím systému databáze o tomto přístupu nebyla ani zmínka. Navíc neobvykle intenzivní přístup zaměstnance do databáze se výrazně odlišoval od jeho běžné práce a znamenal by evidentní anomálii, na kterou by systém behaviorální analýzy upozornil příslušné vnitřní kontrolní oddělení banky.

Na příkladech z praxe je vidět, že zaměstnanci vždy výrazně změnili své chování. Pro běžné bezpečnostní systémy je taková činnost zaměstnanců zcela legitimní, jelikož přistupovali k informacím dle svého oprávnění nebo pod zcizenou identitou.

Ovšem pro systém, který sleduje chování dlouhodobě je tato neobvyklá aktivita odhalena a nahlášena jako bezpečnostní incident.



Komplexní řešení MyNetScope® zahrnuje monitorování sítě, dlouhodobé uložení statistik o provozu na síti, centrální zpracování statistik, behaviorální analýzu, nástroje pro dohled nad provozní infrastrukturou a administrativně-organizační zázemí bezpečnostního týmu. Jako první komerční řešení implementuje standard Bidirectional flows a metody detekce útoků na síťové služby na úrovni sítě (network-based metody) bez nutnosti zpracování obsahu přenášených dat.

Monitorování toků v síti

- Vysoce výkonné autonomní řešení NetFlow v5/v9 monitoringu v reálném čase
- Podpora linek od 10Mbps do 10Gbps
- Podpora pro IPv4, IPv6, VLAN a MPLS
- Neviditelné na L2 a L3 vrstvě
- Poskytuje primární data pro další aplikace:
 - Analýza síťového provozu
 - Sledování uživatelů a služeb
 - Dohled nad přístupem k Internetu
 - Plánování kapacity sítě a datových linek
 - Kontroly peeringu a SLA
 - Dodržování zákona o elektronických komunikacích a souvisejících předpisů
 - Detekce nežádoucích vzorů chování
 - Detekce anomálií
 - Průzkum bezpečnostních incidentů

Centrální uložení statistik o provozu na síti

- Vysoce výkonný kolektor pro sběr NetFlow statistik z libovolného počtu monitorovaných bodů v síti
- Dostupná kapacita od 1TB do 50TB
- Centrální databáze pro dlouhodobé uchování statistik o provozu na síti
- Platforma pro analýzu a další vyhodnocování statistik
- Platforma pro dohled nad dostupností a výkonností síťových prostředků

Centrální vyhodnocování statistik o provozu na síti

- Implementace standardu Bidirectional Flows
- Předdefinovaná sada nežádoucích vzorů chování
- Předdefinovaná sada pravidel detekce anomálií
- Připraveno na rozšíření o další vzory nežádoucího chování a pravidla detekce anomálií
- Zvýšení bezpečnosti sítě a možnost odhalení vnějších i vnitřních útoků
- Detekce slovníkových útoků
- Budování dlouhodobých profilů chování zařízení
- Odhalování skrytých/nejádoucích služeb v síti
- Klasifikace bezpečnostních incidentů dle druhů a závažnosti
- Historie bezpečnostních incidentů

Behaviorální analýza

- Vysoce výkonná analýza chování v reálném čase:
 - uživatelů
 - síťových zařízení
 - jednotlivých aplikací
 - síť jako celku

- Detekce nežádoucích vzorů chování
- Monitorování aktivit uživatelů a využívání služeb
- Korelace událostí na úrovni sítě s aplikačními logy

Dohled nad provozem na síti a prvky síťové infrastruktury

- Přehled o dění v síti v reálném čase
- Monitoring provozního stavu síťových prvků (SNMP)
- Pravidelný a souhrnný reporting
- Analýza dlouhodobých statistik s rozlišením na jednotlivé počítače a uživatele, aplikace a konverzace

Pokročilá analýza provozu na síti

- Automatická integrace s DNS s inteligentní cache
- Filtrování dle různých kritérií
- Překlad čísel portů na názvy odpovídajících služeb. Doplnkové informace o službách, informace o známých hrozbách.
- Integrace nástrojů síťové diagnostiky (ping, tracer, nmap) a dalších informací (WHOIS)
- Průzkum bezpečnostních incidentů
- Rychlé a přesné řešení problémů na síti
- Detailní průzkum chování vybraného zařízení nebo uživatele na síti
- Pohled na celkovou situaci na síti

Administrativně-organizační zázemí bezpečnostního týmu

- Ukládání textů ve standardu dokuwiki
- Přístup ke změnám ve formátu RSS
- Ticketovací systém, automatický mailing změn
- Centralizace bezpečnostního know-how v organizaci
- Evidence bezpečnostních incidentů/úkolů
- Sledování postupu řešení bezpečnostních incidentů
- Metodiky a pracovní postupy bezpečnostních týmů

Technická podpora a aktualizace SW

- Telefonická a e-mailová podpora 8x5
- Vzdálená asistence a konfigurace zařízení
- Bezpečnostní konzultace
- Aktualizace software a firmware zařízení
- Nové vzory chování/aktualizace vzorů chování

Řešení MyNetScope® na rozdíl od běžných produktů roste se zákazníkem, zejména je připraveno na rozšíření počtu monitorovaných bodů v síti a zvýšení zátěže sítě. MyNetScope® vykazuje vynikající poměr cena/výkon a nízké náklady na správu. Průměrná náročnost implementace řešení je v řádu hodin a běžný provoz nevyžaduje specializované odborníky.