Systémy detekce a prevence průniků (IDS a IPS)
Penetrační testy v bezpečnostní analýze informačního systému

Penetrační testy tvoří důležitou součást bezpečnostní analýzy. Za použití různých nástrojů jsou prováděny pokusy proniknout do různých částí informačního systému zvenčí či zevnitř. Výsledkem těchto testů je odhalení slabých míst v ochraně informačního systému.

Penetrační testy jsou v podstatě napodobení útoku hackera. Útok může být směrován jak z vnější sítě (typicky z Internetu) na servery umístěné v DMZ (demilitarizované zóně) nebo na vnější rozhraní firewallu, tak i z vnitřku na síťovou infrastrukturu nebo zranitelné servery. Průnik z vnitřku do systému může být veden fyzicky přítomným hackerem, kterému se podařilo připojit vlastní počítač do interní sítě nebo získat fyzický přístup k počítači ve Vaší síti. Průnik ale může být veden i metodou tzv."sociálního inženýrství průniku", kdy hacker zneužije důvěřivosti uživatele či použije jinou netechnickou metodu a tím získá přístup, který mu samozřejmě nenáleží, nachytá běžného uživatele a podsune mu spustitelný kód, pomocí kterého převezme vládu nad jeho počítačem. Tento přístup pak může využít k získání citlivých dat či vedení dalšího útoku. Útoky pak mohou způsobit tyto škody:

1. Nedostupnost služby - tzv. DoS či DDoS útoky (Denial of Service či Distributed Denial of Service) - způsobí, že služba, na kterou byl útok veden, přestane obsluhovat legitimní požadavky uživatelů - může dojít i k "zatuhnutí", případně restartu serveru apod.
2. Neoprávněný přístup - výsledkem útoku může být situace, kdy útočník získá neoprávněný přístup k zařízení, serveru, službě či datům, a to mu následně umožní provádět neautorizované změny v konfiguraci, mazání nebo modifikaci souborů apod. Často bývá takto napadený server využíván jako základna pro provádění útoků na další zařízení.
3. Získání důvěrných informací - výsledkem útoku může být získání citlivých informací - např. seznam uživatelských jmen a hesel, účetnictví, ceníků, mezd apod.

Penetrační testy tvoří důležitou součást bezpečnostní analýzy. Za použití různých nástrojů jsou prováděny pokusy proniknout do různých částí informačního systému zvenčí či zevnitř. Výsledkem těchto testů je odhalení slabých míst v ochraně informačního systému, uložených dat a infrastruktury testovaného subjektu. Samozřejmě pak následuje definice existujících rizik. Penetrační testy ve své podstatě vyhledávají a aplikují metody pro napadení informačního systému tak, jak by k tomu mohlo potenciálně dojít při projevech počítačové kriminality. Tyto aktivity mají za účel prověřit zabezpečení informačního systému vůči napadení a současně ukázat analyzované organizaci, kde existují slabá místa a kudy může být informační systém napaden. Slabá místa v informačním systému jsou hackery trvale vyhledávána a používané systémy jsou testovány na možnosti napadení. Aby bylo možno čelit jejich útokům, je nutné velmi podrobně sledovat a testovat informační technologie podobným způsobem.

Při bezpečnostních testech infrastruktury je potřeba se zejména zaměřit na:

1. penetrační testy vnitřní i vnější (scanning, sniffing, redirecting)
2. zkušební útoky
3. analýzu zranitelnosti firewallů
4. kontrolu bezpečnostních pravidel mezi zónami firewallů
5. analýzu zranitelnosti aktivních prvků
6. analýzu zranitelnosti operačních systémů na serverech a stanicích
7. analýzu systému zálohování

Testy se provádějí na základě expertních zkušeností metodou "etického hackingu" a ve shodě s normami ČSN ISO/IEC TR 13335 a ČSN ISO/IEC 17799.

Při penetračních testech jsou především prováděny následující zkoušky:

1. firewally - Dos útoky, změny směrování, zranitelnost
2. Backdoory - programy umožňující získání kontroly nad počítačem
3. CGI scripty - získání plné kontroly www nad serverem
4. DNS systémy - předstíráním identity síťového zařízení
5. mailové systémy – spam
6. ftp systémy - neautorizovaný přístup k souborovému systému a převzetí kontroly nad serverem
7. LDAP systémy - zneužití adresářové služby LDAP (Lightweight Directory Access Protocol)
8. síťové odposlouchávání - špatná konfigurace aktivních prvků či nevhodný design infrastruktury umožní síťové odposlouchávání
9. NFS systémy - neautorizovaný přístup k souborovému systému a převzetí kontroly nad serverem (Network File System)
10. systémy založené na RPC -vzdálené volání procedur (Remote Procedure Call)
11. systémy se sdílením zdrojů - získání neautorizovaného přístupu (Samba, SMB)
12. SNMP systémy - bezpečnostních díry v implementaci Simple Network Management Protocolu v aktivních prvcích sítě

Získané znalosti mají další využití pro sledování, testování a výběr nástrojů ochranu před neoprávněným přístupem (Firewall) a pro automatizovanou detekci a zabránění pokusu o napadení informačního systému (Intrusion Prevention System).

Složitým rozhodnutím bývá správný okamžik pro penetrační testy. Řada společností penetrační testy odkládá pod záminkami, jako až bude nový firewall, máme webovou prezentaci hostovanou a do sítě nám přichází pouze emaily, máme čerstvě vybudovaný systém, a ten je přeci v pořádku, máme pravidelně aktualizovaný antivir. To jsou velmi naivní tvrzení, na penetrační testy je čas kdykoliv a je více než vhodné je pravidelně opakovat. Vždyť napadení počítačů a odepření jejich služby může nastat kdykoliv, třeba jen lavinovým rozšířením infikovaného emailu. Nebo třeba zprávou Skype s linkem na kliknutí. Ta přijde od známé a důvěryhodné osoby, a protože komunikace Skype je šifrována, tak nedojde k její kontrole antivirovým programem a hromadné nakažení počítačů je dílem okamžiku. Toto je však možné jen díky neexistenci, či flagrantnímu porušování bezpečnostní politiky. I takovéto situace lze technicky ošetřit, ale bohužel to není běžné.

V případě, že už máte nasazen systém IPS, udělali jste opravdu hodně pro zabezpečení sítě. I když není systém IPS samospasný, je to v dnešní době velmi účinný prostředek pro ochranu a prevenci v síti. Je důležité mít na paměti, že IPS je další částí zabezpečení Vaší sítě. Rozhodně nenahrazuje firewall, antivir či další prvky zabezpečení Vaší sítě. I v takovém případě je ale vhodné udělat penetrační test systému IPS.

Při testech IPS se sleduje především:

1. Zhodnocení nasazení IPS vzhledem k analýze rizik.
2. Zhodnocení procedur pro rekonfiguraci IPS, (false positives, filtry, změna závažnosti signatury).
3. Zhodnocení procedur pro aktualizaci signatur.
4. Zhodnocení znalostní báze incidentů a procedur pro reportování incidentů.
5. Zhodnocení nastavení korelace s ostatními systémy.
6. Zhodnocení, kde jsou v síti umístěny kritické prvky a kde chce organizace začít s detekcí.
7. Zhodnocení komplexního řešení incidentů.

8. Zkušební přenos infikovaného vzorku dat.
9. Odolnost na DDoS (Distributed Denial of Service – odepření služby). Tento test je velmi náročný na technické vybavení, útok musí být proveden dostatečným množstvím současně otevřených TCP session a k tomu je potřeba velké množství současně útočících počítačů.
10. Konfigurace a způsob vytvoření síťové karantény.

Výsledky penetračních testů musí být prezentovány ve srozumitelné formě jak pro technické, tak pro řídící pracovníky. Součástí zprávy musí být klasifikace problémů a samozřejmě i doporučení na odstranění zjištěných nedostatků.

Systémy prevence průniků (1) – jen detekovat nestačí

Donedávna se mělo za to, že firewally a systémy detekce průniků (Intrusion detection systems – IDS) dostatečně chrání síť před kompromitováním viry, červy, spywarem atd. Proč to neplatí a jak revolučně mění přístup systémy prevence průniků (Intrusion Prevention Systems - IPS) vám ukáže tento článek.

Dnes je velmi snadné dokázat, že firewally a to ani ty lepší (s integrovanou aplikační proxy) dostatečně neanalyzují data protokolů na aplikační vrstvě z hlediska známek útoků. Celkem nedávno jsem na setkání Windows User Group ukazoval, jak je snadné „hacknout" WinXP stanici, která je za hardwarovým stavovým firewallem s překladem adres. Ta stanice měla navíc skoro kompletní aktualizace a zapnutý svůj firewall integrovaný v operačním systému. Stačí jen emailem nebo přes ICQ poslat relativně důvěryhodný link, na který důvěřivý „běžný Franta uživatel" klikne a je Váš. Tedy spíše hackera, nebo jím distribuovaného robota. Ani jeden z firewallů totiž nebrání otevření spojení z vnitřní a bezpečné stanice do internetu a přijetí kompromitujícího kódu po tomto spojení zpět.

S IDS je to trošku jinak, ale ve finále to dopadne stejně. IDS analýzu sice provádějí a mohou zaznamenat i přenos kompromitujícího kódu, ale nepodnikají žádné kroky k zastavení zjištěného útoku, jen příznak logují. A kdo z nás čte pravidelně logy? Asi tolik, kolik čte manuály před instalací, že…

Tradičním doplňkovým řešením k firewallům a IDS bývá kontinuální záplatování serverů a pracovních stanic, což je časově náročný proces. Toto záplatování však přináší i další neplacenou práci, kterou si vyžádá testování vlivu každé záplaty na kritické systémy pokud možno ještě před vlastním nasazením záplaty. Příkladů z praxe, kdy nasazení neotestované záplaty či update aplikace, které spolu na první pohled nesouvisejí, způsobilo nefunkčnost kritického systému jistě znáte sami dost. Pro ilustraci například nedávno uvedený „.NET 3 Framework" si na neanglických Windows šeredně pohraje s ovladači některých tiskáren a neveselému uživateli se tiskne celá tisková úloha na jeden list. Přijde mi, že operační systémy i různé aplikace dnes nadmíru kontaktují každého uživatele a přesvědčují ho k instalaci záplaty. Ve všech případech zabírá proces záplatování čas a tím vzniká příležitost pro zneužití zranitelností u nechráněných hostů. Je možná načase rozhodnout se pro nové bezpečnostní řešení.

Instantní síťová prevence a rychlá a hlavně snadno nasaditelná karanténa!

Systémy prevence průniků (Intrusion Prevention Systems - IPS) zaplňují mezeru na trhu a revolučně mění přístup administrátorů k obraně sítě. IPS pracuje na cestě v síti a blokuje závadný provoz. Systém analyzuje aktivní spojení a zachycuje útoky při jejich průchodu, takže závadný útočný provoz nikdy nedosáhne svého cíle. Zařízení obvykle nemají MAC adresu ani IP adresu a jsou přitom "nárazníkem na síti" pro nekorektní provoz. Legitimnímu provozu nebrání v průchodu systémem při plné rychlosti sítě a měli by mít latenci v řádu desítek mikrosekund.

Jak vypadá optimální IPS?

Optimální IPS by v sobě měli mít automaticky nastaveny tisíce filtrů pro blokování nekorektní komunikace v tom, čemu se říká "doporučená" konfigurace. Tyto filtry rozpoznají provoz, který je pokládán za škodlivý kdykoliv, za jakýchkoliv podmínek a v jakémkoliv prostředí. V optimálním případě administrátor tento systém pouze zapne, nakonfiguruje uživatelské jméno a heslo pro administrativní rozhraní a připojí datové kabely. Od tohoto okamžiku by měl být systém plně funkční, blokovat útoky a chránit zranitelné systémy před kompromitováním. Žádné „Walk before Run", či jinak nazývané používání v IDS režimu před přepnutím do IPS režimu, které je spojené s náročným hledáním false positiv. Před uvedením rozumného IPS do plnohodnotného provozu by nemělo být třeba žádné konfigurace, korelace, integrace nebo ladění čehokoliv. Pokud je to možné, měl by IPS systém poskytovat i karanténní činnost. Pod karanténní činností myslím schopnost nejen zablokovat šíření škodlivého kódu, ale i aktivně pracovat se stanicí, která šíření tohoto kódu realizuje. Například vhodnou formou informovat uživatele lokální sítě, jehož stanice je nakažena, zablokovat port příslušné stanice na přepínači, přepnout port přepínače do karanténní virtuální sítě a také se postarat o doručení příslušných „léčebných" procedur. To vše pokud možno bez zásahu administrátora, automaticky. Dále by měl mít optimální IPS efektivní systém aktualizace svých filtrů, které by se měli okamžitě, tím myslím zase bez ladění, nasazovat do činnosti.

No a v neposlední řadě by měl být systém certifikovaný, že opravdu provádí to, co se od něho očekává. Papír obchodníka, který Vám IPS prodává, totiž snese všechno. Základní certifikační autoritou je v případě IPS stejně jako firewallů ICSA Labs. Dnes jsou na stránkách ICSA Labs uvedeny čtyři výrobci s certifikovanými IPS.

Tabulka ICSA Labs certifikovaných výrobců IPS systémů k 18.březnu 2007:

Výrobce	Dosažený výkon	Průměrné zpoždění
3Com (TippingPoint)	3000 Mbit/s	81 mikrosekund
IBM (ISS)	350 Mbit/s	398 mikrosekund
Fortinet	75 Mbit/s	305 mikrosekund
BroadWeb	100 Mbit/s	441 mikrosekund

Vícesegmentový IPS 3Com TippingPoint 5000E

Nyní něco blíže k filtrům psaným pro IPS

Tvůrce IPS filtrů navrhuje filtry tak, aby neměly falešná pozitiva, nezhoršovaly výkon a byly odolnější vůči útočníkům, kteří se speciálně zaměřují na vyhnutí se detekci. Tento úkol přinesl velkou změnu ve filozofii přístupu, která byla tradičně přijímána v oblasti IDS. Navíc tento úkol vyžaduje nebývalý výkon a flexibilitu u prevenčního zařízení i filtrovacího jazyka.

Nejprve je nutno definovat některé pojmy. Slovo signatura se používá pro popis logiky detekcí; to znamená shromažďování testovacích kritérií používaných k oddělení útočného provozu od normálního. Obecně je signatura spíše abstraktní pojem, který

popisuje klasifikační algoritmus, ale nic neříká o způsobu, jakým bude reagováno na kladnou identifikaci útoku. Protože IDS pouze identifikují útoky, ale nijak na ně nereagují, používá se slovo signatura pouze v souvislosti s IDS.

Na druhou stranu slovo filtr se používá v souvislosti s logikou detekce v kombinaci s předpokládanou blokovací akcí. Filtry obsahují „pruning", neboli odstraňování něčeho z toku provozu. Výraz filtrování se obecně používá v souvislosti s firewally, protože firewally aktivně odstraňují vybrané typy paketů z celkového toku. Nicméně "inteligence" stojící za filtrováním firewally je tradičně základní, založená z větší části na číslech portů a typech protokolů. Proto nemá příliš smysl diskutovat o "logice detekce" nebo "signaturách", které používá určitý filtr firewallu.

Vstup systémů prevence průniků na scénu promíchal vody terminologie a způsobil mnoho zmatku každému, kdo se zabývá bezpečností sítí. Ani jeden z existujících termínů – signatura a filtr – nepopisuje adekvátně schopnosti IPS, pokud byly interpretovány jako tradiční výbava IDS nebo firewallu. IPS dokáže, s podobnou inteligencí jako systém detekce průniků, velmi přesně odlišit útočný provoz od neškodného. Testovací kritéria IPS používaná k detekci každého útoku si jistě zaslouží název "signatura" ve významu flexibility a výkonnosti klasifikace. Navíc IPS aktivně odděluje závadný provoz z toku paketů, čímž okamžitě činí použitelným slovo "filtr". Nicméně zákazníci jsou z toho v rozpacích. Slovo signatura použité v popisu IPS si nikdo v duchu nespojí s blokovací schopností zařízení. Na druhou stranu ze slova filtr mohou lidé odvodit, že "inteligence" tohoto zařízení se omezuje na jednoduchá pravidla používaná firewally. Navíc je zde ještě další faktor, který zhoršuje tento zmatek. Během let své existence měly IDS produkty tolik závažných problémů s falešnou pozitivitou, že dospěly k bodu, kdy IDS a falešná pozitiva jsou považovány za dvě strany téže mince. Navíc, IDS jsou historicky neoddělitelně spjatá s terminologií signatur. Proto kdykoliv se slovo signatura použije v kontextu IPS, lidé okamžitě pomyslí na falešné detekce a hned se obávají blokování legitimního provozu. Ale nebojte se, naštěstí tomu tak u certifikovaných výrobců IPS není.

Systémy prevence průniku (2) – pravidla pro tvorbu IPS filtrů

Tvůrce IPS filtrů navrhuje filtry tak, aby neměly falešná pozitiva, nezhoršovaly výkon a byly odolnější vůči útočníkům, kteří se speciálně zaměřují na vyhnutí se detekci. Tento úkol vyžaduje nebývalý výkon a flexibilitu u prevenčního zařízení i filtrovacího jazyka.

Při psaní filtrů pro blokování musí být dodržena dvě pravidla:

1. Žádná falešná pozitiva. Nikdy, za žádných okolností nesmí IPS blokovat legitimní provoz. Toto pravidlo má vždy nejvyšší prioritu.
2. Žádná falešná negativa. Nenechte projít útok, ani když se útočník intenzivně snaží vyhnout detekci. Toto má vysokou prioritu.

Tvůrce filtrů musí mít stále na paměti tato dvě pravidla a jejich relativní prioritu. Klíčový rozdíl v přístupu k psaní signatur mezi IPS a IDS spočívá ve vzájemném pořadí těchto dvou cílů. Umění tvorby filtrů pro blokovací zařízení spočívá v co největším zobecnění logiky detekce tak, aby bylo dosaženo pravidla 2, bez porušení pravidla 1.

Derivování Zero False Negative Filtru

Při provádění výzkumu technických zranitelností musí technik nejprve pátrat po všech okolnostech, které jsou nezbytné pro úspěšný útok. Výzkumník začíná vytvořením programu, který na dálku spustí zranitelnost. Tento program se používá k obměňování všech "zajímavě vypadajících" částí útoku. Změny jsou prováděny postupně jedna po druhé a jsou pečlivě zaznamenávány. (Řetězce, příznaky, doby trvání, bannery, čísla verzí, kódování znaků, bílá místa... tento seznam pokračuje dál. Je dobré vyzkoušet všechno.) Pokud útok uspěje i v případě, že určitá proměnná má náhodnou hodnotu, pak tato proměnná není pro prevenční systém důležitá. Výzkumník může případně určit kompletní soubor proměnných, které jsou důležité pro úspěch útoku, a dojít k souboru kritérií, která musí být souhrnně splněna, aby byl jakýkoliv útok úspěšný. Pokud je možné vést útok z různých směrů, výzkumník musí uplatnit tuto analýzu na každý z nich zvlášť. Pro úspěšnost IPS mají tyto podmínky zásadní význam.

Zadáním souboru kritérií, která musí být splněna, aby útok uspěl, je možno popsat logiku filtrů, které mají nulová falešná negativa (zero false negatives). To znamená, že útok jednoduše nemůže uspět, jestliže jeho provoz na síti nemá přesně ty charakteristiky, které filtr vyhledává.

Derivování Zero False Positive Filtru

Po zadání zero false negativ filtru, jak bylo popsáno výše, musí výzkumník také zhodnotit přesnost vakcíny z hlediska falešných pozitiv. V tomto stádiu se výzkumník pokouší určit nejméně jednu charakteristiku, která by nikdy nenastala v normálním provozu. Pokud existuje taková charakteristika, která je současně abnormální ve srovnání s normálním provozem a kritická pro úspěch útoku, pak je taková zero false negativ signatura současně i zero false positive signaturou.

Pro tvorbu tohoto typu filtrů se nabízí mnoho typů útoků. Například:

- SQL Injection Attacks: ve specifickém webovém požadavku jsou na místo určité hodnoty dosazeny speciální znaky jako ´ a %27.
- PHP Remote File Include Attacks: ve specifickém webovém požadavku je na místo určité hodnoty dosazena hodnota obsahující vzdálenou URL.
- Buffer Overflow: při jistém typu konverzace je zaměněna jistá zpráva obsahující určitou proměnnou za jinou, která obsahuje nadměrné množství určitého druhu dat.
- Integer Overflows and Signedness Problems: namísto určité hodnoty, která by měla být vždy (relativně) nízké kladné číslo, je dosazeno extrémně velké nebo záporné číslo.
- Format String Attacks: během určité změny protokolu je odeslána specifická zpráva, která obsahuje hodnotu se znaky formátu string.

Jak výše uvedené příklady naznačily, množství práce na detekční logice často spočívá v souvislostech nezbytných pro položení klíčové otázky, zda je hodnota příliš velká nebo příliš malá nebo zda hodnota obsahuje určité znaky či řetězce. To, jestli IPS zařízení je či není schopno využít příležitosti logické dokonalosti teoretické signatury, závisí na tom, za A) zda je jazyk filtrování dostatečně flexibilní k vyjádření nezbytné logiky, a za B) zda je zařízení dostatečně výkonné pro správnou aplikaci různých testů síťového provozu probíhajících in-line při plné rychlosti.

Souhrnně o filtrech v IPS zařízeních

Nejprve si povězme, že znalosti a pečlivost výzkumníka zranitelností mají zásadní význam. Výzkumník musí dostatečně porozumět zranitelnosti, aby mohl předpovědět směry útoků a aby vytvořil filtry odolné proti falešným negativům i falešným pozitivům. Rovněž víte, že detekce anomálií protokolů je často velmi užitečná, ale jistě není vždy tím pravým. Další a možná nejdůležitější zjištění je, že falešná pozitiva i falešná negativa jsou problémem těch IPS/IDS produktů, které nejsou schopny precizně implementovat detekční logiku. Pro podporu efektivních filtrů zranitelností je zapotřebí výkonného zařízení, které dokáže fungovat ve vysokorychlostním prostředí, kde aktivně běží zranitelné protokoly.

Systémy prevence průniku (3) – režim karantény

Nyní již víte, jak pracuje IPS systém na detekci a zastavení útoku. To však není vše, co je třeba od IPS očekávat. Můžete se totiž spolehnout, že dříve nebo později se objeví „útočník" i na vnitřní síti. Třeba notebook se síťovým červem, chyceným v hotelové bezdrátové síti.

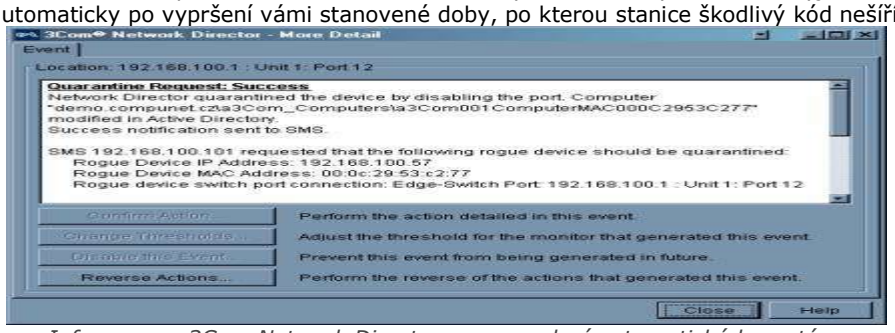
V tomto případě již nestačí jen zablokovat na IPS šíření škodlivého kódu, ale také provést karanténu stanice. Dnes v této oblasti není zcela jednotný přístup. Na jedné straně je silně marketingově propagován Network Access Control (NAC), který za použití software klienta hlídá zda na stanici je nainstalován poslední servisní balíček, zapnutý firewall, aktualizovaný antivirus a podobně. NAC software se postará o limitování přístupu neaktualizované stanice do lokální sítě ať již přepojením do karanténní virtuální sítě, nebo zablokováním příslušné stanice úplně. Ovšem v případě, že veškeré podmínky NAC software jsou splněny, ale i přes to se na stanici nachází škodlivý program, je tento přístup marný.

Řešení firmy 3Com

Dále již budu hovořit o přínosu firmy 3Com k této problematice. Firma 3Com karanténní činnost neváže na existenci NAC software, který musíte mít nainstalovaný na všech stanicích sítě (což znamená další koupený, licencovaný a spravovaný kus software na klientech). Řešení je založeno na inteligenci IPS a její schopnosti identifikovat „nakaženou" stanici v L2/L3 síti a provést karanténu nezávisle. K dispozici jsou tři možnosti nasazení.

První možnost využívá pouze kombinaci blokování provozu v IPS ve volitelné kombinaci s privátními virtuálními sítěmi. Předpokladem je nasazení IPS segmentu mezi stoh přepínačů serverové farmy a centrální přepínače sítě. Tento způsob nasazení karantény je velmi snadný a přitom neuvěřitelně účinný. Jakmile IPS detekuje šíření škodlivého kódu ze stanice, zabrání jeho šíření a zablokuje přístup stanice na internet. Ve chvíli, kdy si uživatel ze stanice, šířící škodlivý kód otevře webový prohlížeč na libovolný server na intranetu nebo internetu, je mu namísto očekávaného obsahu předložena stránka s karanténními informacemi. Mimo to je samozřejmě notifikován administrátor sítě. Privátní virtuální sítě zamezí možnosti šíření škodlivého kódu mezi uživateli a tak je zdroj útoku izolován. Výhodou tohoto typu 3Com karanténního řešení je snadnost rychlost nasazení a velká flexibilita řešení. Nemusí se navíc jednat pouze o karanténu pro šíření škodlivého kódu, ale třeba i karanténu v případě provozování aplikací, které jsou v rozporu s firemní politikou. Představte si, že uživateli podnikové sítě, který si spustí P2P aplikaci nebo nepovolený typ messangeru se zobrazí v prohlížeči informace, že jeho porušení firemní politiky je logováno a přístup k internetu mu bude obnoven po 10 minutách od ukončení porušování firemních politik. Vše automaticky, bez zásahu administrátora. Jak říkám: „Čistá práce".

Druhou možností je přizvání nástroje na správu sítě k součinnosti s IPS . Zde také není třeba ověřování přístupu do sítě ani existence privátních virtuálních sítí. Stačí jen používat efektivní nástroj na správu sítě (Network Management Station – NMS), který dokáže korektně pracovat s TRAP notifikací z IPS systémů. Princip tohoto typu karantény spočívá právě ve schopnosti software na správu sítě určit pozici stanice která šíří škodlivý kód v síti a provést manipulaci s příslušným portem stanice na přepínači. Celé to funguje taktéž překvapivě jednoduše. Stačí na NMS reagovat na přesně formátovanou TRAP notifikaci z IPS a provést korelaci z TRAPem dodané IP/MAC adresy na zdrojový port přepínače. V 3Com nástrojích na správu sítě jsou tyto nástroje běžnou součástí, tudíž není třeba nic dolaďovat, stačí pouze karanténní činnost povolit. Průběh karantény je poté následující: IPS systém detekuje šíření škodlivého kódu, posílá TRAP na NMS, NMS provede korelaci z IP/MAC adresy na přepínač/příslušné číslo portu, kde je stanice připojena a přes SNMP provede zablokování portu, případně zařazení portu do karanténní VLAN. Celá karanténní operace netrvá déle než 3 vteřiny. Z karantény lze stanici vyjmout manuálně, případně automaticky po vypršení vámi stanovené doby, po kterou stanice škodlivý kód nešíří.



Informace v 3Com Network Directoru o provedení automatické karantény

Třetí možnost je již za využití ověřování přístupu do sítě. Pokud používáte 802.1X Network Login nebo na RADA (RADIUS Authenticated Device Access), je k dispozici karanténní řešení založené na manipulaci s atributy RADIUS serveru. Celé je to založeno na schopnosti 3Com TippingPoint SMS (dohledová konzole pro IPS) pracovat jako RADIUS proxy. SMS naslouchá všem ověřovacím procesům a zná umístnění všech ověřených stanic na síti. Jakmile IPS detekuje narušení pravidel, informuje SMS, která provede karanténu čistým řezem. Na přepínač, kde je „útočník" připojen pošle SNMP příkaz na vypnutí a zapnutí portu. To vyvolá nové ověřování stanice, které je za běžných okolností realizováno přes PROXY RADIUS integrovaný v SMS. Nicméně pro tento konkrétní případ SMS nezapracuje jako PROXY, ale jako běžný RADIUS server a v odpovědi zda je stanice oprávněná přistupovat k síti odešle Vámi nadefinovanou odpověď. Ta může být buď negativní nebo může stanici na síť pustit, ale jako atribut je zasláno modifikované členství portu tak, aby byl zařazen do karanténní virtuální sítě.

Závěr

Výkonný systém prevence průniků může fungovat jako virtuální softwarová záplata a chránit tak zranitelné počítače před kompromitováním v síti, kde nemusely být aplikovány host-by-host záplaty, nebo i záplatovaný systém není zcela odolný vůči průniku škodlivého kódu. Schopnost virtuálního záplatování na IPS vychází přímo ze schopnosti identifikovat a blokovat přenos závadného provozu před tím, než útok dosáhne svého cíle. Technologie, která umožňuje toto virtuální záplatování, spočívá ve vysoce přesných filtrech zranitelností. Tyto filtry jsou navrhované profesionály tak, aby zajistily optimální pokrytí prostoru pro útoky a maximální odolnost proti obcházení. Tím je zajištěno vyřazení škodlivého provozu ze sítě. Dále je třeba zajistit, aby škodlivý kód nezasáhl další účastníky provozu. To lze realizovat prostřednictvím nasazení karantény. Většina výrobců IPS dnes karanténu nabízí, rozdíl je však ve složitosti nasazení. Poslední rada na závěr. Pokud se rozhodnete nasadit IPS, což vřele doporučuji, nespoléhejte se jen na papír obchodníka. Vybraná zařízení si před nákupem pečlivě otestujte a zvažte, zda pro vás opravdu budu přínosem nebo spíš zátěží. V jednoduchosti je síla. Mnoho zdaru.

Zabezpečení sítě proti neoprávněnému přístupu pomocí funkce NetworkLogin 802.1x

S přechodem většiny důležitých vnitropodnikových dat na elektronickou formu může získání přístupu neautorizovanou osobou k počítačové síti znamenat pro firmu potencionální nebezpečí. Z tohoto důvodu je nutné podobnému jednání zamezit.

To neznamená zabezpečit fyzický přístup k aktivním prvkům či počítačové kabeláži, ale zejména znemožnit k počítačové síti v libovolném místě připojit donesený notebook, bezdrátový přístupový bod či analyzátor sítě. Řízením přístupu k síti lze v aktivních prvcích přesně vyspecifikovat skupinu zařízení či uživatelů, kteří se mohou přes tento aktivní prvek připojit. Ostatní zařízení/uživatelé potom nebudou do sítě vpuštěni dočasným či trvalým zablokováním fyzického portu, skrz který se pokoušeli neoprávněně do sítě připojit.

NetworkLogin 802.1x

Zabezpečení počítačové sítě pomocí funkce NetworkLogin 802.1x umožňuje aktivnímu prvku bezpečně ověřit uživatele na základě uživatelského jména a hesla a teprve po ověření jej připustit ke zdrojům sítě. Aktivním prvkem může být v tomto případě přepínač, přístupový server, bezdrátový přístupový bod (AP). Ověřovací autoritou není aktivní prvek sám, ale centrální databáze uživatelů, se kterou jako její klient komunikuje. Tato databáze se nazývá RADIUS (Remote Authentication Dial In User Service – RFC 2865). RADIUS server je možné provozovat jako službu integrovanou v Microsoft ActiveDirectory.

Ověření pomocí funkce NetworkLogin 802.1x

Celý proces ověření probíhá tak, že stanice (v terminologii 802.1x Suplicant) se připojí k portu zabezpečenému 802.1x. Svoji existenci přepínači dá najevo libovolným paketem, například požadavkem o přidělení IP adresy. Přepínač však přijatý DHCP požadavek nepřeposílá dál, ale obratem posílá žádost o identifikaci zpět na stanici. Stanice odpovídá svým uživatelským jménem a heslem. Přepínač přijaté informace zašifruje do paketu a pošle na ověřovací autoritu. RADIUS server provede vyhodnocení přijatých informací a zpět přepínači odešle potvrzení či odmítnutí uživatele. Přepínač na základě této informace vpustí či odmítne stanici přístup do takto zabezpečené sítě.

Metody ověřování

Stanice může být ověřena na základě uživatelského jména a hesla nebo digitálního certifikátu. Ověřování pomocí digitálního certifikátu vyžaduje, aby v síti byla instalována Certifikační autorita a stanice měly přidělené digitální certifikáty.

RADA

Radius Authenticated Device Access - rozšíření technologie Network Login, která umožní přihlášení do sítě a rozšíření na všechna zařízení, bez ohledu na klienta, tedy například i síťové tiskárny, IP telefony, bezdrátové přístupové body, terminály a podobně. RADA navíc umožňuje definovat řízený přístup k síti pro dočasné uživatele, které začlení do definované hostitelské oblasti, například s přístupem pouze do Internetu. RADA používá k ověření fyzickou adresu, ale lze ji kombinovat i s ověřením přes uživatelské jméno a heslo. Síť potom rozlišuje, zda je připojeno povolené zařízení nebo neznámý počítač, případně v kombinaci s přihlášením rozlišuje i práva uživatele. Tyto způsoby ověření podporují i automatické zařazení uživatele ke skupině (AutoVLAN) nebo automatické nastavení kvality služby (AutoQoS).

AutoVLAN

Funkce, která doplňuje ověřování uživatele a umožňuje automatizovat nastavení virtuální sítě. Uživatel/stanice má na ověřovacím serveru uveden rovněž příznak skupiny (vedle jména a hesla). Po úspěšném ověření uživatele je port přístupového přepínače nastaven do příslušné virtuální sítě. Uživatelé a stanice jsou potom nezávislí na místě připojení, vždy dostanou stejné prostředí.

GuestVLAN

Funkce umožňují automatické zařazení neautorizovaných uživatelů do zvláštní VLAN, která má nastavená přístupová pravidla třena jen pro přístup k Internetu.

AutoQoS

Funkce, která doplňuje ověřování uživatele a umožňuje automatizovat nastavení QoS parametrů. Uživatel/stanice má na ověřovacím serveru uveden příznak QoS, vedle jména a hesla. Po úspěšném ověření uživatele je na port přístupového přepínače nastavena příslušná kvalita služby. Uživatelé a stanice jsou potom nezávislí na místě připojení, vždy dostanou stejné prostředí.

Voice VLAN

Funkce, která usnadní konfiguraci uživatelům IP telefonie. Podporuje IP telefony hlavních dodavatelů a automaticky umístí telefon do definované hlasové VLAN.

DHCP Tracker

Zajímavá funkce přepínačů, které směrují IP provoz. L3 přepínač sleduje, zda stanice používá adresu, kterou získala korektní DHCP žádostí. Funkce umožní komunikovat mimo svoji VLAN pouze klientům, kteří přijali svoji IP adresu z DHCP serveru. Pokud uživatel manuálně nastaví jiné parametry, přepínač komunikaci zablokuje.

PVLAN

Privátní virtuální síť sice není přímo součástí NetworkLogin, ale je výborným rozšířením zabezpečení sítě. PVLAN zajistí, že stanice/uživatelé v jedné VLAN nemohou vzájemně sdílet prostředky. Můžou komunikovat pouze směrem na L3 interface. Zde můžou být aplikována další přístupová pravidla.

Funkce síťové karantény v systémech IPS a IDS

Funkce síťové karantény představuje prevenci šíření nákazy z nakažené stanice na ostatní uživatele. Je to vlastně automatická izolace stanice, která je nakažena virem nebo je zdrojem nevhodné komunikace. Pokud IPS zjistí na síti nevhodná data, vyvolá definovanou činnost.

Výhodou je, když řešení nevyžaduje instalaci žádného softwaru na koncovou stanici a umožňuje chránit libovolné zařízení či operační systém. Karanténa využívá systémů IPS nebo IDS, které dokážou identifikovat nejen působení virů a červů, ale i reagovat například na průzkumné utility a další nástroje.

Pokud IPS zjistí na síti nevhodná data, vyvolá definovanou činnost. Akce karantény nemusí být nutně izolace stanice, ale může to být například:

- blokování dat a zobrazení výstražné a informační web stránky
- umístění klienta do izolace
- zapnutí filtrů pro přístup do některých oblastí

Pro seznam speciálních zařízení nebo stanic lze stanovit výjimku z akce karantény, bezpečnostní správce dostane upozornění, že nastala událost, která vyžaduje karanténu, ale blokovací akce na zařízení ze seznamu spuštěna není. To se týká například serverů s kritickými aplikacemi, směrovačů, přepínačů.

Výhody síťově založené karantény:

- automaticky provádí ochranu sítě
- nevyžaduje instalaci a správu klientského softwaru
- je univerzální, podporuje všechny typy operačních systémů
- dokáže kontrolovat všechny typy zařízení (IP telefony, PDA)
- hostitelské systémy nemusejí bezpodmínečně splňovat nějaké bezpečnostní parametry, blokuje či limituje nevhodné nebo nepovolené aktivity uživatelů sítě
- centrální správa
- spolupracuje s MS NAP

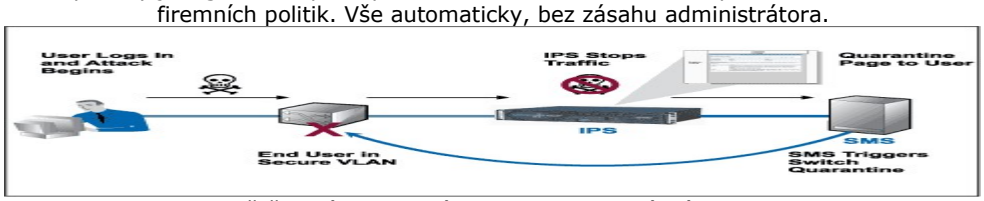
Srovnání síťové karantény a NAC

Network Access Control (NAC), za použití software klienta hlídá, zda na stanici je nainstalován poslední servisní balíček, zapnutý firewall, aktualizovaný antivirus a podobně. NAC software se postará o limitování přístupu neaktualizované stanice do lokální sítě ať již přepojením do karanténní virtuální sítě, nebo zablokováním příslušné stanice úplně. Ovšem v případě, že veškeré podmínky NAC software jsou splněny, ale i přes to se na stanici nachází škodlivý program, zůstává infikovaná a škodící stanice připojená v síti.

Možnosti realizace síťové karantény jsou v zásadě tři:

Karanténa realizovaná pouze IPS

První možnost využívá pouze kombinaci blokování provozu v IPS ve volitelné kombinaci s privátními virtuálními sítěmi. Předpokladem je nasazení IPS segmentu na výstup do internetu. Tento způsob nasazení karantény je velmi snadný a přitom neuvěřitelně účinný. Jakmile IPS detekuje šíření škodlivého kódu ze stanice, zabrání jeho šíření a zablokuje přístup stanice na internet. Ve chvíli, kdy si uživatel ze stanice, šířící škodlivý kód otevře webový prohlížeč na libovolný server na internetu, je mu namísto očekávaného obsahu předložena stránka s karanténními informacemi. Mimo to je samozřejmě notifikován administrátor sítě. Privátní virtuální sítě zamezí možnosti šíření škodlivého kódu mezi uživateli a tak je zdroj útoku izolován. Výhodou tohoto typu karanténního řešení je snadnost rychlost nasazení a velká flexibilita řešení. Nemusí se navíc jednat pouze o karanténu pro šíření škodlivého kódu, ale třeba i karanténu v případě provozování aplikací, které jsou v rozporu s firemní politikou. Představte si, že uživateli podnikové sítě, který si spustí P2P aplikaci nebo nepovolený typ messangeru se zobrazí v prohlížeči informace, že jeho porušení firemní politiky je logováno a přístup k internetu mu bude obnoven po 10 minutách od ukončení porušování firemních politik. Vše automaticky, bez zásahu administrátora.



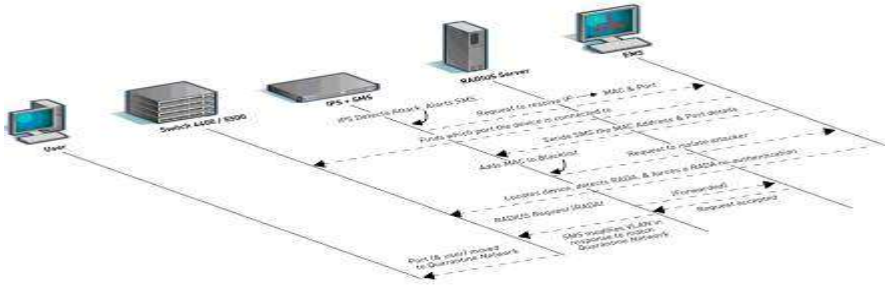
Přeřazení infikované stanice do karanténní VLAN

Karanténa realizovaná IPS + NMS

Druhou možností je přizvání nástroje na správu sítě k součinnosti s IPS. Zde také není třeba ověřování přístupu do sítě ani existence privátních virtuálních sítí. Stačí jen používat efektivní nástroj na správu sítě (Network Management Station – NMS), který dokáže korektně pracovat s TRAP notifikací z IPS systémů. Princip tohoto typu karantény spočívá právě ve schopnosti software na správu sítě určit pozici stanice, která šíří škodlivý kód v síti a provést manipulaci s příslušným portem stanice na přepínači. Celé to funguje překvapivě jednoduše. Stačí na NMS reagovat na přesně formátovanou TRAP notifikaci z IPS a provést korelaci z TRAPem dodané IP/MAC adresy na zdrojový port přepínače. Průběh karantény je poté následující: IPS systém detekuje šíření škodlivého kódu, posílá TRAP na NMS, NMS provede korelaci z IP/MAC adresy na přepínač/příslušné číslo portu, kde je stanice připojena a přes SNMP provede zablokování portu, případně zařazení portu do karanténní VLAN. Celá karanténní operace netrvá déle než 3 vteřiny. Z karantény lze stanici vyjmout manuálně, případně automaticky po vypršení stanovené doby, po kterou stanice škodlivý kód nešíří.

Karanténa realizovaná IPS + NetworkLogin

Třetí možnost využívá ověřování přístupu do sítě. Pokud používáte 802.1X Network Login nebo na RADA (RADIUS Authenticated Device Access), je k dispozici karanténní řešení založené na manipulaci s atributy RADIUS serveru. Celé je to založeno na schopnosti SMS (dohledová konzole pro IPS) pracovat jako RADIUS proxy. SMS naslouchá všem ověřovacím procesům a zná umístnění všech ověřených stanic na síti. Jakmile IPS detekuje narušení pravidel, informuje SMS, která provede karanténu čistým řezem. Na přepínač, kde je „útočník" připojen pošle SNMP příkaz na vypnutí a zapnutí portu. To vyvolá nové ověřování stanice, které je za běžných okolností realizováno přes PROXY RADIUS integrovaný v SMS. Nicméně pro tento konkrétní případ SMS nezapracuje jako PROXY, ale jako běžný RADIUS server a v odpovědi, zda je stanice oprávněná přistupovat k síti, odešle Vámi nadefinovanou odpověď. Ta může být negativní nebo může stanici na síť pustit, ale jako atribut je zasláno modifikované členství portu tak, aby byl zařazen do karanténní virtuální sítě.



Průběh činností v automatické karanténě realizované IPS + NetworkLogin
(klepnutím na obrázek jej zobrazíte v plném rozlišení)