

Víte, kde jsou díry ve vašem zabezpečení?

Qualys a McAfee ukazují cestu v testu automatizovaných nástrojů pro skenování a reportování zranitelností.

JOEL SNYDER

Všichni se bojíme, že na našich serverech je nějaký skrytý problém zabezpečení. Děláme, co můžeme, instalujeme opravy, používáme nejlepší postupy, udržujeme své znalosti aktuální pomocí školení a sledování novinek.

Nebylo by ale skvělé mít automatizovaný nástroj pro kontrolu naší práce? To je příslib analyzátorů zranitelností: jsou to produkty detekující problémy v konfiguracích, aplikacích a v oblasti instalace oprav.

Při správném používání může analyzátor zranitelností pomoci udržet na špičce stovky či tisíce serverů, síťových zařízení a vestavěných systémů. Budete vědět, na co zaměřit své síly při nápravě zabezpečení, a budete klidnější, že máte systém, který vám umožní zabránit, aby drobnosti unikly skulinami a způsobily velké problémy.

Naopak při nesprávném použití mohou analyzátoři vytvořit tisíce stran matoucích informací, frustrovat manažery zabezpečení a správce sítí, a nakonec z toho může vzniknout více problémů, než se vyřeší.

Otestovali jsme šest produktů předních dodavatelů z hlediska výsledků skenování zranitelností, schopnosti reportování, správy produktu, nástrojů pro pracovní procesy a interoperability s dalšími podnikovými produkty.

Dva produkty vyčnívaly: QualysGuard VM využívající technologii SaaS a McAfee Vulnerability Manager, který je nabízen v podobě softwaru a appliance.

Produktová řada SAINTmanager se umístila na třetím místě díky výkonnému skeneru, ale znevýhodněna byla slabým grafickým uživatelským rozhraním. Naš favoritovaný vyzvatel, eEye Retina CS, měl silný skener s nově vytvořeným grafickým uživatelským rozhraním. Zjistili jsme však mnoho chyb a nedostatků v designu, které je nutno odstranit předtím, než bude připraven pro nasazení v podnikovém prostředí.

Retina je relativně nový produkt, který je aktivně vyvíjen. Během tří měsíců našeho testu jsme u něj zaznamenali jeden upgrade a před předáním tohoto testu do tisku vydala společnost eEye další.

Produkt FusionVM společnosti Critical Watch je další nabídkou využívající technologii SaaS. Obsahuje určité skvělé nápady, ale provedení je nedostatečné. Lumension Scan odvedl dobrou práci

Prostředí produktu McAfee Vulnerability Manager (Zdroj: Comguard.cz)

v oblasti, pro kterou byl navržen, ale je to produkt s omezeným záběrem funkcí a nenabízí vlastnosti potřebné pro podnikovou sféru, na které jsme se zaměřovali.

Z různých důvodů se testu odmítly zúčastnit společnosti IBM, Nciracle, Trustwave, StillSecure, Rapid7, Beyond Security a Tenable.

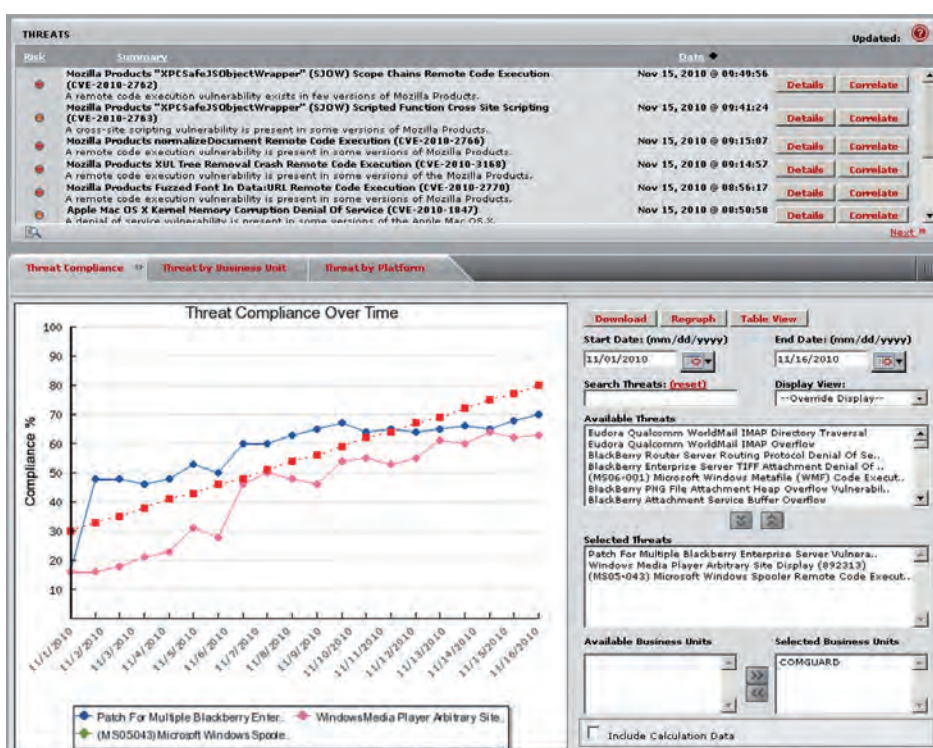
Skenování

Všechny analyzátoři zranitelností mají společné jádro: skener, který hledá zranitelnosti. Pokud byste prováděli síťový penetrační test, byl by skener jediným nástrojem, který byste potřebovali.

V některých produktech, zejména Retina CS a produkt firmy SAINT, tj. SAINTscanner/SAINTmanager/SAINTwriter, je skener samostatným nástrojem, který lze spouštět bez nástrojů pro správu a reportování. (Viz box Možnost skenování webu.)

U ostatních produktů, jako jsou QualysGuard VM a Critical Watch FusionVM, je skener neoddělitelný od dalších součástí. Jste-li bezpečnostním konzultantem, který jen chce provádět skenování, potom se pro vaše potřeby nejlépe hodí produkty firm eEye a SAINT.

Abychom získali představu, jak dobře skenery pracují, proskenovali jsme tři produkční sítě ve třech společnostech a navíc speciálně postavenou laboratorní testovací síť. V té testovací jsme záměrně ponechali čtyři servery bez instalace oprav po dobu dvou měsíců: dva systémy Windows (Windows 2003 a 2008), linuxový systém a server OS X. Poté jsme zapnuli analyzátoři zranitelností a vyhodnotili výsledky.



Bezpečnost Vašeho digitálního světa



Hlavní bezpečnostní úskalí virtuálních technologií spočívají v nedořešeném propojení bezpečnosti virtuálních a fyzických serverů a ve zranitelnostech, které pramení ze složitosti patchování offline virtuálních serverů.

McAfee produkty splňují nejpřísnější požadavky na stoprocentní zabezpečení sítě integrací bezpečnostních prvků jak pro ochranu fyzických, tak virtuálních zařízení.

McAfee MOVE Anti-Virus for Virtual Desktops and Servers

Prověřené nástroje pro efektivní ochranu virtuálního prostředí

Management for Optimized Virtual Environments (MOVE) je řešení navržené pro organizace využívající virtuální prostředí, a to jak serverové, tak i desktopové. Díky architektuře MOVE ušetříte desítky procent výkonu Vašich strojů, jelikož AV neběží na každém stroji, ale zvláště na virtuální skenovací aplianaci.

McAfee MOVE-AV for Virtual Desktops

Součástí licence je nejnovější verze antivirového enginu s řadou pokročilých funkcí jako blokování infekce, portu a jména souboru, atd. Řešení je doplněno o McAfee SiteAdvisor enterprise plus pro bezpečné procházení webů a McAfee Host IPS, které zajistí ochranu před DoS útoky a útoky v čase nula.

McAfee MOVE Anti-Virus for Virtual Servers

Zajišťuje optimalizaci využívání výkonu virtuálních serverů tak, aby antivirový systém při skenování nepřetěžoval server a tím znemožnil poskytování serverových služeb. Lze jednoduše nastavit, aby ke skenování docházelo mimo pracovní hodiny a v případě přetížení serveru došlo k přerušení skenování.

Další balíčky pro ochranu virtuálních řešení:

VirusScan Enterprise for Offline Virtual Images

Automaticky skenuje, čistí a provádí updaty zabezpečení virtuálních serverů bez nutnosti jejich převedení do online režimu. **Servery jsou chráněny proti aktuálním hrozbám, které vznikly během jejich offline seance.**

McAfee Application Control for Servers

Aplikační audit serveru s vynucením možnosti spuštění jen autorizovaných aplikací, spolupracuje s update systémy Microsoft apod.

McAfee Change Control for Server

Hlídá neautorizované změny v konfiguracích, souborech, lozích a registrech včetně preventivní ochrany a blokování.

| VAD distribuce McAfee pro ČR a SR: COMGUARD a.s., www.comguard.cz.

◀ **Nejdříve varování:** skenery zranitelností mohou způsobit nestabilitu ve vaší síti a také ji pravděpodobně způsobí. Produkty SAINT a Critical Watch učinily v naší síti skutečnou škodu – uzamčení jednoho z našich produkčních unixových serverů – a dále vznikly potíže s úložištěm SAN, které vedly k přerušení služby pro několik klientů.

Prakticky všechny produkty zapříčinily restartování UPS jednotek společnosti APC, což (naštěstí) neovlivnilo nic kromě rozhraní pro správu. Dávejte tedy pozor, jaké IP adresy skenujete a jak skeny probíhají.

Možná byste si mysleli, že se naše síť za pouhé dva měsíce nedostala významněji mimo aktuální stav, ale testované skenery k tomu měly hodně co říci. Vítězem podle váhy byl produkt eEye, který vygeneroval 180stránkový report, ale produkt McAfee zvítězil počtem – sdělil nám 537 různých informací o těchto čtyřech systémech, přičemž 380 z nich nebyly specifické zranitelnosti, ale jen informační položky. Stále však zbývalo 84 kritických zranitelností, kde po nás produkt společnosti McAfee požadoval opravu.

Nástroje pro analýzu zranitelností a funkce pro dodržování směrnic

Dodržování směrnic je přirozeným rozšířením nástroje pro analýzu zranitelností. Normální skenování zranitelností zahrnuje vyhledávání nezáplatovaných systémů, nechráněných adresářů a dalších chyb v konfiguraci.

Kontrola dodržování směrnic obvykle přidá sadu namátkových kontrol, které jsou specifické pro konkrétní regulační režim. Zásady dodržování směrnic mohou například vyžadovat, aby mohly být jednotky DVD-ROM použitelné pouze lokálně přihlášenými uživateli. To skutečně není zranitelnost, je to jen něčí nápad pro konkrétní bezpečnostní zásadu.

Všechny testované produkty kromě Lumension Scanu mají významnou komponentu pro kontrolu dodržování směrnic. U některých z nich je skenování dodržování směrnic k dispozici za příplatek nebo je tato možnost nabízena jako oddělená licence.

V analyzátorech zranitelností má „dodržování směrnic“ dvě hlavní části: jedna definuje zásady a kontrolu dodržování směrnic a druhá generuje reporty se specifickými kontrolami, které jsou vyžadovány regulačním režimem.

Protože je dodržování směrnic zcela separátní disciplínou analýzy zranitelností s velmi odlišnými požadavky, měli byste před výběrem analyzátoru zranitelností pečlivě zvažovat roli testování a reportování dodržování směrnic.

Požadavky na testování dodržování směrnic se budou měnit podle režimu, který se pokusíte podporovat, a tato sada funkcí je obvykle více zaměřena na auditování zásad a méně na zajišťování bezpečné konfigurace individuálních systémů.

Každý například ví, že instalace oprav v produkčních systémech neprobíhá během několika hodin po vydání nejnovější aktualizace společnosti Microsoft. Reportování dodržování směrnic se týká více reportování doby, kterou trvalo uvedení systémů zpět do stavu podle specifikace, než zjišťování, které systémy tyto opravy potřebují.

Je-li pro vás při pořízení analyzátoru zranitelností dodržování směrnic důležité, měli byste podrobněji zkoumat produkty eEye, McAfee, Qualys a SAINT. Při našem rychlém seznámení na nás nejvíce udělaly dojem nástroje pro vytváření zásad dodržování směrnic společnosti McAfee a schopnost produktů SAINT rychle importovat a upravovat standardizované zásady dodržování směrnic na základě tří standardních formátů.

Zřejmým závěrem bylo, že někteří dodavatelé neodvedli dobrou práci při redukci dat. Ano, je pravda, že oprava Adobe APSB10-14 pokrývá 28 různých zranitelností, ale jsou všechny opraveny jednou záplatou a zacházet s nimi jako s 28 separátními incidenty (jako to dělá McAfee) jednoduše podporuje zmatek.

Critical Watch měl podobný problém, zajištění všech částí jedné z kritických oprav od společnosti Microsoft jako separátních elementů, přestože úloha nápravy byla stejná: nainstalovat MS11-012 pro opravu pěti oddělených reportovaných zranitelností.

Pedantský bezpečnostní nadšenec by mohl trvat na reportování všech separátních problémů, ale to je účel detailních reportů. Ve výchozím stavu by tato informace měla být kombinována do stravitelnější podoby.

Některé výsledky byly velmi rutinní. Například při našem testu systémů Windows jsme měli seznam aktualizací zabezpečení a oprav, které nám sdělil systém Microsoft Update, a očekávali jsme zobrazení všech těchto oprav v seznamu zranitelností pro každý systém. Produkty McAfee, Qualys a eEye ve svých výsledcích skenování obsahovaly všechny položky z našich kontrolních seznamů. Produkty Critical Watch, Lumension a SAINT však některé z nich nezachytily.

Pokud by byl náš test tvořen pouze využitím kontrolního seznamu známých chybějících oprav zabezpečení, bylo by snadné produkty ohodnotit. Každý ze skenerů nám toho však sdělil hodně a bylo obtížné zjistit, zda tyto informace byly nebo nebyly relevantní či hodnotné.

Například Lumension uvedl, že v našich systémech Windows používáme zastaralou verzi produktu SecureCRT (to byla pravda), a ohodnotil tuto zranitelnost jako „vysoká“ (což je pravděpodobně přehnané). Toto však žádný jiný produkt neodhalil. Znamená to, že je Lumension lepší než ostatní skenery, které problém nezachytily?

Nu ano, kromě toho, že produkt eEye zjistil cca 1 999 různých nastavení ochrany v neznámém klíči registru, který by mohl být použit privilegovanými uživateli k dalšímu eskalování jejich práv během spouštění systému. Znamená to, že je eEye lepší než ostatní skenery, které problém v registru neodhalily? V tomto kruhu se můžete pohybovat stále dále, protože každý produkt oznámil problémy, většinou méně významné, které ostatní neohlásily.

Nesprávné detekce

Také jsme kontrolovali nesprávné detekce – místa, kde skenery reportovaly zranitelnost tam, kde žádná neexistovala. To je pro bezpečnostní „puristy“ citlivá oblast. Některé skenery jednoduše zpracovávají existenci konkrétního souboru jako zranitelnost systému.

Například Lumension označil unixový kernel na našem testovacím linuxovém systému jako zastaralý, protože viděl nainstalovaný Red Hat Package Manager se starým kernelem. My jsme ale tento kernel nepoužívali (byl jen uložen na disku), takže systém zranitelný nebyl.

Situaci však nebylo tak těžké posoudit u všech nesprávných detekcí. Například Critical Watch zjistil, že našemu systému Mac OS X chybí oprava Microsoft Windows, a produkt eEye požadoval opravy pro zranitelnosti VMware a Hyper-V v systémech, kde tyto virtualizační nástroje nebyly nainstalovány. Nesprávné detekce byly přítomné ve výsledcích všech skenerů kromě produktu Qualys.

Při porovnávání skenerů jsme měli další problémy. Databáze CVE (Common Vulnerabilities and Exposures) podporovaná ministerstvem USA pro národní bezpečnost je nejbližší referencí se standardem běžných jmen. Očekávali bychom, že dodavatelé zajistí, že jejich zranitelnosti budou řádně odpovídat záznamům databáze CVE, ale když jsme se pokoušeli porovnávat výsledky, zjistili jsme chyby a opomenutí u většiny skenerů.

Například jsme si mysleli, že produkt McAfee jako jediný odhalil problém (záznam CVE-2010-3886), dokud jsme nezjistili, že je skrytý v eEye jako Retina Audit 13156, bez čísla CVE.

Také jsme sledovali dvě další důležitá kritéria: reportování důkazů zranitelnosti a podporu více platformem.

Kde jsou důkazy?

Zda jsme našli důkazy nebo jestli nám chybí – to je velký rozdíl. Když skener hlásí zranitelnost, je důležité mít pohotově dostupné podpůrné důkazy. Například když na našich serverech Windows jeden ze skenerů ohlásil zranitelnost „uživatel se nikdy nepřihlásil“, aniž jsme se ale dozvěděli, o jakého uživatele se jedná. Jak je to užitečné? (Odpověď zní, že moc ne.)

McAfee, Qualys a SAINT poskytly skvělé podpůrné důkazy a produkt Critical Watch nabídl některé důkazy, ale ne v rozsahu, jak bychom si přáli. Lumension a eEye byly v tomto směru skoupé, i když eEye skryl některé z důkazů v reportech, jež nebyly vidět pomocí webového rozhraní.

Skenování různých platform operačních systémů bylo dalším rozlišovacím faktorem, který nemusí být důležitý pro každého správce sítě. Všechny produkty podporovaly Windows, ale zjistili jsme různé úrovně zvládnutí ostatních systémů, jako jsou Mac a Unix, stejně jako u infrastrukturních zařízení, jako jsou prepínače či směrovače. SAINT a v menším rozsahu také eEye měly ve srovnání s ostatními produkty silnější zaměření na unixové systémy.

Celkově jsme zjistili, že produkty firem Qualys a SAINT měly nejsilnější skenery a produkt společnosti McAfee byl téměř na stejné úrovni. Lumension, eEye a Critical Watch měly vyšší počty nesprávných detekcí (falešně pozitivních i falešně negativních) a také slabou prezentaci důkazů při dokumentaci zranitelností.

Reportování

Skrutí informací o zranitelnosti uvnitř produktu správcům sítě nijak nepomůže. Očekáváme, že produkt pro vyhodnocení zranitelnosti bude schopen reportovat zjištěné informace způsobem, který maximalizuje pochopení a minimalizuje ztracený čas.

Správci sítě budou pravděpodobně chtít používat pro reporty grafická uživatelská rozhraní, protože budou chtít zjišťovat podrobnosti o jednotlivých systémech a zranitelnostech a zaměřovat se na úlohy, jako jsou náprava a instalace oprav.

Auditoři a správci mohou chtít tištěné reporty, které shrnují informace a poskytují celkový obraz toho, kde existuje riziko pro celý podnik a tam, kde se budou potřebovat zaměřit. Sledovali jsme

všechny typy výstupů v rámci obecné kategorie „reportování“, abychom vyhodnotili srozumitelnost, transparentnost, konfigurovatelnost a užitečnost.

Zjistili jsme, že zde skutečně existují dva typy analyzátorů zranitelnosti: založené na skenování a založené na vybavení. Ten první jmenovaný je ten, kde jsou všechny reporty a data zaměřeny na skenovací činnosti. Jinými slovy, takový analyzátor provádí skenování a potom z této činnosti můžete získat report.

Protože skener zranitelnosti pracuje tak, že sleduje seznam cílů a spouští některé vybrané skeny a vytváří výstup, je vytvoření analyzátoru zranitelnosti založeného na skenování velmi přirozené.

Vezmete skener, na kterém jste tak těžce pracovali, a přilepíte k němu vyšperkované grafické uživatelské rozhraní. Takový skener může sledovat informace, jako jsou trendy, ale nejedná se o udržování podrobné historie pro každý skenovaný systém.

Alternativou je analyzátor založený na vybavení. („Vybavením“ může být server, pracovní stanice, směrovač a kdovíco ještě.) Zaměření není tak silné na činnost skenování, ale na shromažďované informace, které jsou sbírány o příslušném vybavení. Skener postupem doby nasbírá informace o prvcích ve vašich sítích a vytvoří obrázek zranitelnosti, konfigurací a dokonce historie instalace oprav. Někteří dodavatelé začali tento přístup nazývat ve své literatuře pojmem „jedno skenování a více reportů“.

Pokud potřebujete provést skenování pro PCI audit nebo penetrační test, budete spokojeni s analyzátory zranitelnosti založenými na skenování. Pokud se však pokoušíte zahrnout správu zranitelností do pokračujícího procesu zaměřeného na pochopení stavu zabezpečení v rámci celé podnikové sítě v průběhu času, budete spíše potřebovat analyzátor založený na vybavení.

S tímto přístupem vám možná zabere konfigurace skenování delší dobu, ale budete ji spouštět pravidelně a opakovaně, a přispívat tím do souboru znalostí o vaší síti.

Analyzátor založený na vybavení se vždy může chovat jako analyzátor založený na skenování jednoduše tak, že vytvoří report pro naposledy provedené skenování. Každý z testovaných produktů to dělal perfektně. Přesto jsme však zaznamenali různé výsledky při snaze získat od produktů obraz většího celku pomocí reportů pro více skenů za určitou dobu.

Nejvíce se našemu ideálu, jak by mělo fungovat perfektní reportování analyzátoru zranitelnosti, přiblížil produkt firmy Qualys, při-

INZERCE



Pod záštitou ministra vnitra



Odborní partneři:



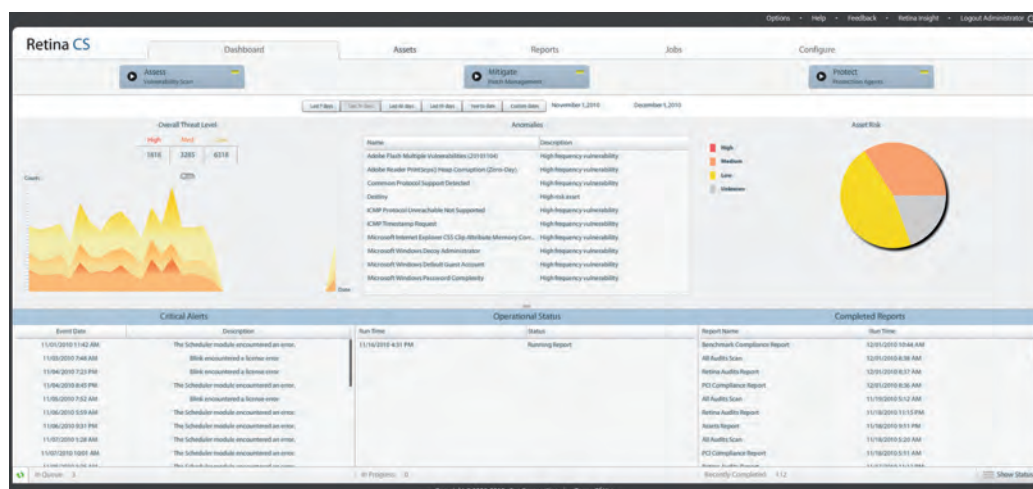
čemž produkt společnosti McAfee byl téměř na stejné úrovni. Oba umožňují vytvářet snadno čitelné a přehledné reporty, a to založené na skenování i na vybavení. U obou je také intuitivní rozhraní pro reportování; důrazně preferujeme, aby reportování bylo zcela odděleno od skenování.

Žádný z produktů však nebyl perfektní. Qualys nám neumožnil spouštět automatizované reporty. Je to vedlejší efekt jeho silného modelu zabezpečení SaaS. Protože Qualys udržuje ve svých databázích extrémně citlivé informace o vaší síti a systémech včetně přihlašovacíh údajů, které jste zadali pro účely skenování, bere zabezpečení velmi vážně.

V tomto případě možná až příliš vážně. Jeho šifrovací model brání komukoli vidět vaše podniková data, dokud nejste aktuálně přihlášení do webového uživatelského rozhraní. Bohužel slovo „komukoli“ v tomto případě zahrnuje také generátor reportů Qualys. Nespustí se, pokud nejste přihlášení, což znamená, že donutit Qualys k vytvoření reportů a k jejich zaslání na pravidelném základě je 100× těžší, než by mělo být. Pokud na tom však trváte, můžete to provést.

Tým Qualysu nám poskytl informace o rozhraní QualysGuard API, což je nástroj, který by mohl umožnit vzdáleně spouštět reporty, možná v rámci dávkové úlohy. Není to však to, co jsme hledali. Společnost Qualys je hrdá na to, jak vážně přistupuje k zabezpečení citlivých dat, ale toto je jeden z případů, kde potřebuje vymyslet lehčí způsob k provedení jednoduché úlohy.

Společnost McAfee také odvedla dobrou práci při poskytování pohledů na informace o zranitelnostech, a to jak pohledů založených na vybavení, tak i na skenování. Například MVM byl jeden ze dvou produktů (QualysGuard VM byl druhý), které úspěšně vytvořily rozdílový report ukazující změny ve zranitelnostech mezi jednotlivými skeny.



Dashboard řešení RetinaCS od společnosti eEye.

Produkt společnosti McAfee však neumožnil dostatečně jednoduchou navigaci ve vybavení a zranitelnostech v grafickém uživatelském rozhraní. Reporty lze snadno vytvořit a jsou přehledné – to je výhoda vůči většině ostatních produktů.

Pokud však chcete zobrazit stejné informace pomocí webového grafického uživatelského rozhraní, jste více omezeni v možnostech procházet zranitelnosti a získat dobré pochopení stavu vašeho zabezpečení. Chtěli jsme vidět reporty, které by měly stejnou úroveň informací nezávisle na tom, zda byly čteny prostřednictvím formátu PDF nebo přes webové grafické uživatelské rozhraní.

I když firmy Qualys a McAfee odvedly velmi dobrou práci, našli jsme velký příslib u produktů společností SAINT a eEye. Oba produkty mají ke svým solidním skenerům přidané bezplatné generátory reportů. SAINTWriter a Insight jsou pro tyto dva dodavatele cestou pro přesun z původních produktů schopných jen skenovat do

řešení určená pro podniky. Naše testování však ukázalo, že oba mají určité výrazné slabiny.

SAINT obsahuje v produktu SAINTWriter 16 předdefinovaných typů reportů. Pokud těchto 16 typů (včetně reportů založených na vybavení a na zranitelnostech) splňuje vaše potřeby, budete s řešením mnohem spokojenější, než když budete muset použít jeho vlastní rozhraní k definování reportů.

Ve srovnání například s návrhem reportů systému firmy eEye je přidávání reportů k produktu SAINT bolestné a obtížné. SAINT má také určitá výrazná omezení. V nástroji pro definici reportů například nelze vytvořit dynamické dotazy typu „zobraz všechny zranitelnosti s vysokou závažností“ nebo „zobraz všechny opravy společnosti Microsoft“.

SAINT má také obtížnou navigaci pomocí grafického uživatelského rozhraní ve výsledcích skenování. Nalezení jednoho systému v síti vyžaduje značné manévrování, a pokud vaše síť obsahuje stovky systémů v databázi skeneru zranitelností, je v produktu SAINT téměř nemožné udržet kontrolu.

Na druhou stranu, jakmile naleznete systém, který chcete, jsou k dispozici dobré nástroje pro zkoumání a správu zranitelností, jako jsou funkce na jedno kliknutí „ignoruj tuto zranitelnost u tohoto systému“ a podobně hezká možnost „ignoruj tuto zranitelnost u všech systémů“.

Přestože vývojáři společnosti eEye vestavili do produktu Retina pro reportování a navigaci ve zranitelnostech velmi atraktivní grafické uživatelské rozhraní založené na technologii Shockwave Flash, zjistili jsme několik funkčních problémů, které způsobují frustrace při používání a překážejí efektivní správě zranitelností.

Situaci nezlepšil ani nedostatek dokumentace, zejména pro důležité funkce. Retina je poměrně novým produktem, který je přibližně rok starý a je postaven na vrcholu váženého a velmi respektovaného skeneru firmy eEye.

Během tří měsíců našeho testu jsme zaznamenali jeden upgrade produktu Retina a před předáním tohoto testu do tisku vydala společnost eEye další, který řešil dvě z našich hlavních námitek: neschopnost ignorovat zranitelnosti pro určité systémy a neschopnost vytvářet rozdílové reporty.

Ve srovnání se všemi ostatními testovanými nástroji je definice nových reportů v produktu Retina pohádková.

Grafické uživatelské rozhraní produktu Retina je zcela podřízeno reportům: Určíte, co potřebujete získat za report, a Retina provede skenování za účelem získat data (nebo použije stará data, pokud chcete jen jiný formát reportu pro stejná stará data).

Jakmile definujete report a spustíte ho, potom přejeme hodně štěstí: Všechny se totiž zobrazují s obecným titulkem – nelze pojmenovat specifické spuštění například podle lokality, aniž vytvoříte zcela novou šablonu reportu. To způsobuje vyšší náročnost při hledání výsledků – musíte reporty proklikat, abyste zjistili, který je který.

Celkově mají reportovací a analytické schopnosti produktu Retina potenciál velkého pokroku a produkt se tak může stát skvělým nástrojem. V současné době však reportovací sada nástrojů Retina nenabízí použitelnost a funkcionalitu potřebnou v podnicích pro vyhodnocení zranitelností v rámci velkého rozsahu. To se však může velmi rychle změnit.

Produkt	McAfee Vulnerability Manager (MVM) 7	QualysGuard Vulnerability Management	SAINTmanager	Retina CS 2.0	FusionVM	Lumension Scan 6.4
Dodavatel	McAfee	Qualys	SAINT	eEye	Critical Watch	Lumension
Cena	16 820 dolarů v prvním roce (včetně appliance 1U), 9 020 dolarů v roce druhém	17 495 dolarů	19 000 dolarů první rok, 4 750 dolarů druhý rok	28 000 dolarů první rok, 7 000 dolarů druhý rok	18 500 dolarů (první rok včetně podpory 1 000 IP adres)	6 500 dolarů
Výhody	Solidní, spolehlivý, hodně funkcí	Vynikající sada funkcí, silné reportování	Propracované penetrační testy	Snadno definovatelné reporty, ekosféra pro produkty dalších dodavatelů	Nabídka SaaS, silná sada funkcí pro kontrolu dodržování směrnic, vestavěné skenování webu	Základní funkce a nízká cena
Nevýhody	Komplikované workflow	Obtížné spuštění automatizovaných reportů	Slabé rozhraní správy	Relativně nový produkt s drobnými chybami	Webové grafické uživatelské rozhraní potřebuje aktualizaci	Omezené funkce

Podle našeho názoru funkce reportování v produktech Critical Watch a Lumension nedosahovaly standardů ostatních účastníků testu.

Rozhraní Critical Watch nespĺňuje nejzákladnější hlediska návrhu – má trojnásobně vnořené posuvníky, nedostatek možností přizpůsobení obrazovky zobrazení a slabou integraci s vlastním systémem správy zásad. Když například vidíte zranitelnost, kterou chcete v příštích reportech odfiltrovat (například jako falešně pozitivní), vyžaduje grafické uživatelské rozhraní osm či více kliknutí a poté ztratíte místo, kde jste se v reportu nacházeli.

I když v produktu FusionVM existují informace o obecném trendu a další dobře navržené reporty včetně odlišnosti od očekávání, není možné provést rozdílové reportování. U produktu FusionVM jsme zjistili další problémy s interoperabilitou při reportování, jako jsou PDF reporty, které jsou nekompatibilní s některými prohlížeči (možná protože jsou šifrované), a reporty pro Excel, které nelze do této aplikace importovat.

Byli jsme také frustrováni reportovacími funkcemi produktu Lumension. Automatické generování reportů podle plánu není možné a reportování krátkodobých trendů mělo 2 800 stran pro dva skeny vzdálené od sebe méně než 24 hodin.

Protože je produkt Lumension založen na skenování, zjistili jsme, že pokus prohlížet data jinak než pro celý sken (například podmnožinu skenovaných systémů, která je z určitého důvodu zajímavá) byl v podstatě nemožný bez opětovného skenování a opakovaného generování reportu.

Lumension má jednodušší analytické rozhraní a reportování než ostatní produkty. To usnadňuje začátek práce a orientaci, ale jakmile narazíte na zeď omezených funkcí, neexistuje moc prostoru pro kreativní konfigurace.

Snadnost správy a pracovní procesy

Se stovkami a tisíci skenovaných systémů nevyhnutelně během času roste komplikovanost správy konfigurací. Zařízení budou mít pravidla pro „ignorování“ (například konkrétní zranitelnost by již neměla být reportována) a výjimky ze zásad a konfigurací budou stále více upravovány.

Cílem správců sítě je mít týdenní report zranitelností co nejkratší se zvýrazněním pouze důležitých a nových problémů, které je nutno zohlednit. Jediným způsobem, jak to udělat, je nakonfigurovat analyzátor zranitelností tak, aby pečlivě sledoval síť.

Čím méně času je věnováno správě analyzátoru zranitelností, tím více času je k dispozici pro jejich skutečné odstraňování, takže snadné použití a dobře promyšlené grafické uživatelské rozhraní jsou velmi důležité. Jedním z našich základních hodnotících kritérií bylo, jak dobře se tyto produkty hodí pro nepřetržitý cyklus správy stavu zabezpečení namísto provedení jednorázového skenování.

Jsmo přesvědčeni, že McAfee nabízí nejlepší úroveň snadné správy ze všech testovaných produktů. Dobrým příkladem je konfigurace přihlašovacích údajů. Ty bývají slabinou skenování zranitelností –

musíte poskytnout skeneru oprávnění pro přihlášení do každého systému, ale použití těchto uživatelských jmen a hesel vytváří ohrožení zabezpečení.

Navíc pro systém Windows nemůže jít o přihlašovací údaje jen tak nějakého uživatele, protože pro plné vyhodnocení úrovně oprav a nastavení registru jsou vyžadována některá zvýšená oprávnění.

McAfee má nejlepší systém správy přihlašovacích údajů ze všech produktů. Přihlašovací údaje jsou spravovány a ukládány odděleně, takže je snadné je přinést v případě potřeby pro libovolné skenování.

Srovnáme to například s produktem eEye, kde jsou přihlašovací údaje připojeny ke konkrétním úlohám skenování namísto k vybavení, což znamená, že je nutno je vkládat stále dokola, jak jsou spouštěny různé úlohy v rámci sítě.

Další částí systému správy McAfee velmi pomáhají správci sítě rychle a snadno získat kontrolu nad skenováním a jeho zásadami. Zranitelnosti jsou například seskupeny intuitivním způsobem podle kategorií a operačního systému. Můžete si vybrat odpovídající seskupení a použít ho pro úlohu skenování, takže snadno omezíte činnost na sadu bezpečnou pro vaši síť.

To je důležitá schopnost. Každý dodavatel skeneru zranitelností, který tvrdí, že vždy zjišťuje operační systémy a provádí jen bezpečná skenování, nejedná čestně nebo nezná dobře svůj produkt. McAfee není jediným dodavatelem, který tuto funkci poskytuje, ale někteří dodavatelé nabízejí dělení na téměř absurdní segmenty, jako například Lumension, který umožňuje rozlišovat mezi systémy Windows 2003, Windows 2008 a Windows 2008 SP2.

V ostatních oblastech jsme zjistili podobné funkce, ale v některých produktech byly implementovány lépe. Například delegovaná správa je důležitá, protože umožňuje správcům sítě rozdělit síť a změřit reportování na jednotlivce zodpovědné v každé oblasti.

Tuto funkci měli všichni, ale Qualys a CriticalWatch ji měli lépe navrženou – zahrnovala efektivní oddělení skenování a funkce reportování. To zajišťuje, že dva jednotlivci sledující stejnou sadu výsledků mohou vidět dvě různá zobrazení v závislosti na svých zodpovědnostech.

Nejvíce problémů jsme měli s delegovanou správou společnosti eEye, která je skvělá v oblasti skenování, ale nikoli ve sféře reportování. Ve skutečnosti má Retina nepochopitelně dva zcela separátní systémy autentizace – jeden pro reportování a jeden pro vše ostatní.

Zcela základní úlohou pro analyzátor zranitelností je zpracování zranitelností: jejich přiřazení někomu, aby je odstranil, označit je, aby byly ignorovány, nebo je jen na několik týdnů ignorovat, než se objeví jejich oprava. V našem testu jsme toto vše uvedli do kategorie pracovní procesy.

Při posuzování produktu Critical Watch jsme byli různě úspěšní. Produkt má integrovaný ticketový systém nazývaný Remediation Manager, ale nepracoval s prohlížečem Firefox, Safari ani Internet Explorer, což jej v našem testu tak trochu odsoudilo k nezdaru. Na druhou stranu má fantastický Filter Manager, který lze velmi snadno použít k selektivnímu maskování zranitelností na různých úrovních.

Firma eEye zvolila jinou cestu – vytvořením partnerství s dalšími dodavateli zabezpečení včetně produktů pro trouble tickety (elektronické lístky doprovázející problém v celém jeho životním cyklu) a také produktů SIM (správa zabezpečení informací). Získání tiketů z Retiny je snadné, pokud máte pro jejich správu další produkt.

Jednou ze silných stránek řešení Retina je její velmi úzká integrace s produktem pro zabezpečení koncových bodů, eEye Blink. Jejich kombinace dohromady vytváří holističtější pohled na zabezpečení koncových bodů integrací zásad ochrany (jako jsou konfigurace firewallů koncových bodů) a skenování zranitelností.

To nabízí schopnosti zmírnit známé útoky ještě dříve, než jsou opravy dostupné či nainstalované. Retina CS také získává první cenu za skvěle vypadající systém správy, i když některé z nových objektů rozhraní AJAX jednoznačně nefungují nebo jsou špatně vymyšleny.

Lumension Scan pracuje podobně jako Retina nejlépe při integraci s vlastními nástroji tohoto výrobce pro koncové body. Správa oprav Lumension dobře ladí s produktem Lumension Scan, a vytváří tak lépe integrované řešení pro servery i pracovní stanice.

Analyzátoři zranitelností nabízejí i možnost skenování webu

Skenování webu se liší od skenování zranitelností, protože vyhledává chyby v samotných webových aplikacích namísto v softwaru nainstalovaném na webovém serveru. Skenery zranitelností nás například všechny informovaly o starém vestavěném systému v naší síti, který byl zranitelný útokem skriptování mezi weby (cross-site scripting) z důvodu staré verze PHP.

To je jen normální skenování zranitelnosti a v závislosti na konfiguraci vašich webových aplikací a webového serveru může skener vygenerovat velké množství falešně pozitivních detekcí. Skutečné nalezení zneužitelného skriptu na webové stránce však vyžaduje intenzivnější vyhledávání z vnějšího prostředí a také specializovanější skener.

Skenování webu obvykle zahrnuje nějaký typ funkcí DLP (při hledání informací o identitě na webových stránkách), skenování vyrazování informací (hledání dostupnosti celých databází), detekci cross-site scriptingu a SQL injection, a samozřejmě skenování na známé zranitelnosti v běžných webových aplikacích.

Produkty FusionVM, McAfee MVM a QualysGuard VM obsahují možnost skenování webu ve svých skenerech (někdy v rámci oddělené licence), zatímco eEye nabízí separátní produkt, Retina Web, který je na tento úkon přímo zaměřen.

Při hodnocení různých analyzátorů zranitelností jsme pátrali po podpoře protokolu IPv6. Většina jich ani nezmínila a jedinou výjimkou byla firma SAINT. SAINT sice zatím nepodporuje protokol IPv6 všude, ale v rámci testované skupiny je to produkt, který se nejvíce blíží připravenosti na IPv6.

Bez správy oprav má produkt Lumension Scan obzvláště primitivní pracovní proces. Chcete-li ignorovat zjištěnou zranitelnost, musíte si opsat informace z reportu a poté překonfigurovat úlohu tak, aby tuto zranitelnost nezahrnovala.

Na druhou stranu měl Lumension Scan některé skvělé nástroje správy. Například jakmile byla zranitelnost opravena, bylo možné ji jen otestovat v konkrétním systému pomocí jednoho kliknutí, což bylo velmi praktické. Pokud Lumension Scan zjistil zranitelnost v nějakém parametru konfigurace, byla informace, jak a proč opravu provést, vestavěna přímo v rozhraní správy, což šetří čas a energii.

Pracovní proces byl u produktu McAfee zbytečně komplikovaný. Zranitelnosti mohou téci přímo do integrovaného systému trouble ticketů (nebo externě přes SMTP či SNMP) a mohou být přiřazeny uživatelům na základě různých pravidel. V tomto místě je snadné ignorovat zjištěnou zranitelnost nebo ji označit jako opravenou či jako falešně pozitivní.

Při práci s pracovními procesy jsme však zjistili, že je navigace nekonzistentní. Například v některých případech můžete nastavit ignorování nějaké položky, ale na jiných místech, kde by to mohlo být stejně tak vhodné, to možné není.

Tato nekonzistence platila také u produktu QualysGuard. Zjistili jsme, že některá zobrazení v rámci grafického uživatelského rozhraní umožňují změnit chování systému, ale jiné ne, často bez souvislosti či bez příčiny.

Celkově trpí QualysGuard VM ve svém rozhraní správy zastaralým designem. V nabídkách je příliš mnoho informací a pro stejné pojmy je používáno často vyjádření pomocí různých slov. Jakmile překonáte křivku učení, není těžké s produktem pracovat, ale sem a tam se vyskytnou matoucí části, které nedávají smysl.

Pokud nějaký produkt potřebuje přepracovat grafické uživatelské rozhraní a pracovní procesy, je to SAINT. Rychle jsme se však naučili neodsuzovat produkt podle jeho grafického uživatelského rozhraní.

I když z designu obrazovek číší devadesátá léta minulého století, nabízí produkt pod povrchem hodně skrytých schopností. Integrovaný systém trouble ticketů lze například překvapivě snadno používat a má dobře navrženou základnu pravidel, kterou lze použít k automatickému přiřazování trouble ticketů odpovídající skupině.

INZERCE

ESET NOD32 ANTIVIRUS 5



chrání redakci
Security World

