QUALYS®

WHITE PAPER

SICHERHEITSAUDITS UND SCHWACHSTELLENMANAGEMENT ON DEMAND

Ein proaktives Verfahren zur Gewährleistung der Netzwerksicherheit

Inhalt

ON DEMAND SECURITY

“99% aller Netzwerkeinbrüche sind auf die Ausnutzung bekannter Sicherheitslücken oder Konfigurationsfehler zurückzuführen, für die Abhilfemaßnahmen verfügbar gewesen wären.”

Quelle: CERT, Carnegie Mellon University

I. KURZFASSUNG

Hacker beschränken ihre Angriffe heute nicht mehr auf stark exponierte Unternehmen und Organisationen wie Banken oder Regierungsbehörden. Durch automatisierte Tools ist es leichter geworden, Anfälligkeiten in Netzwerken zu finden und auszunutzen, was zu einem enormen Anstieg der Angriffe auf Netze geführt hat, die ans Internet angebunden sind. Gleichzeitig haben sich Viren, Würmer und Trojaner zu raffinierten Angriffswerkzeugen entwickelt, die sich selbstständig verbreiten und sehr schwer zu entdecken sind. Neuere Würmer führen globale Angriffszyklen durch und nutzen anfällige Hosts in Sekundenschnelle aus. Deshalb lassen sich Netzwerke nur schützen, wenn die Sicherheitslücken vorab gefunden und behoben werden.

Um ihre Netzwerke zu sichern, setzen IT-Teams vier Kerntechnologien ein: Virenschutzsysteme, Firewalls, Intrusion Detection-Systeme (IDS) und Schwachstellenmanagement. Jede dieser Technologien hat in einer umfassenden Sicherheitsstrategie ihren Platz. Jedoch bieten nur On-Demand-Lösungen für Sicherheitsaudits und Schwachstellenmanagement einen proaktiven Ansatz, da sie Schwachstellen in Netzwerken und Rechnern ermitteln, bevor Netzwerke kompromittiert werden.

Für das Schwachstellenmanagement stehen Unternehmen verschiedene Optionen zur Verfügung: manuelles Testen mit software-basierenden Produkten; Penetrationstests durch Consultants; und automatisierte Lösungen von Drittanbietern, die im Self-Service-Verfahren genutzt werden. Beim letzteren Verfahren – das als On-Demand-Sicherheitsaudits und -Schwachstellenmanagement bezeichnet wird – werden die Scans von Remote-Servern ausgeführt, die von einem vertrauenswürdigen externen Anbieter gehostet und unterhalten werden; die Kontrolle über die Sicherheitsaudits verbleibt jedoch beim Benutzer. Automatisierte Sicherheitsaudits bieten im Vergleich zu anderen Methoden der Schwachstellenanalyse klare Kosten- und Sicherheitsvorteile.

Dieses Whitepaper beschreibt den Nutzen der unterschiedlichen Ansätze zur Sicherung von Netzwerken. Es konzentriert sich dabei auf die einzigartige Rolle, die das Schwachstellenmanagement und insbesondere automatisierte Sicherheitsaudits spielen. Abschließend wird die Lösung QualysGuard vorgestellt.

II. HERAUSFORDERUNG NETZWERKSICHERHEIT

Vor noch nicht allzu langer Zeit hatten es die meisten Hacker auf Organisationen abgesehen, die stark im Rampenlicht stehen, wie etwa Banken und Regierungsbehörden. Doch die Zeiten haben sich geändert, und heute ist jedes ans Internet angebundene Unternehmen verwundbar, ob es nun Tausende von IP-Adressen hat oder nur eine.

Faktoren, die zum rapiden Anstieg der Risiken beitragen

Folgende Faktoren sind dafür verantwortlich, dass Unternehmen zunehmenden Risiken durch Netzwerkeinbrüche ausgesetzt sind:

• Immer mehr Netzwerke haben mehrere Zugangspunkte – zum Beispiel VPNs und Wireless Access Points, die von Remote-Mitarbeitern genutzt werden. Dies setzt die Netzwerke Bedrohungen durch unbekannte Software und ungeschützte Verbindungen aus.

Netzwerkeinbrüche unterbrechen den Geschäftsbetrieb, verursachen finanzielle Schäden und wirken sich negativ auf das Kundenvertrauen aus

Nachfolgend nur einige wenige Beispiele :

• SQL Slammer infizierte innerhalb von 10 Minuten 120.000 Hosts, setzte Geldautomaten außer Gefecht, löste Störungen in Notrufzentralen aus und verursachte weit reichende Unterbrechungen im Internetbetrieb (Associated Press, 27.01.03).

• Ein Hackerangriff führte zur vorübergehenden Schließung des größten japanischen Preisvergleichsportals. Wie Kakaku.com Inc. mitteilte, musste die Website aufgrund eines Einbruchs ins Computersystem vom Netz genommen werden. Schaden: Einnahmeverluste in Höhe von schätzungsweise 40 Mio. Yen (InfoSec News, 18.05.05).

• Ein mit einem Virus infizierter Computer in einem japanischen Kernkraftwerk führte dazu, dass streng vertrauliche Dokumente mit einem Umfang von rund 40 MB im Internet veröffentlicht wurden. Und noch eine weitere, ähnliche Panne ereignete sich im selben Jahr in der japanischen Energieindustrie: Ein PC mit Filesharing-Software soll dafür verantwortlich gewesen sein, dass sensible Infrastrukturdaten über das Internet verbreitet wurden (SecurityFocus 16.05.06).

• Einem Eindringling gelang es, durch Ausnutzung von Sicherheitslücken das Netzwerk des Dienstleisters CardSystems Solutions zu infiltrieren und sich Zugang zu den Daten von Karteninhabern zu verschaffen.

• Netzwerke und Anwendungen sind komplexer geworden und lassen sich schwer verwalten, zumal es an qualifiziertem Sicherheitspersonal fehlt und die IT-Etats schmaler geworden sind.

• Kurze Software-Entwicklungszyklen führen zu fehlerhaften oder schlecht getesteten Releases. Aufgrund dessen ist die Zahl der neu entdeckten und ausnutzbaren Schwachstellen in den letzten fünf Jahren um 1.149 Prozent gestiegen (vgl. Abb. 2: CERT Security Incident Reports).

• Hacker-Tools sind heute automatisiert und erfordern weniger Kenntnisse seitens ihrer Benutzer, was die Zahl der Hacker erhöht. Und da diese automatisierten Tools für großräumige Angriffe konzipiert sind, kann ein einziger Hacker innerhalb kurzer Zeit großen Schaden anrichten.

• Bösartige Würmer, Viren und Trojaner, die sich selbst vervielfältigen, treiben durch den Multiplikationseffekt die Schäden in die Höhe: Sie „rentieren“ sich noch lange, nachdem sie freigesetzt wurden.

• Der Lebenszyklus von Netzwerkattacken hat sich verkürzt (s. Abb. 1: Beschleunigung des Schwachstellen- und Exploit-Zyklus). Deshalb haben Unternehmen heute weniger Zeit, um Schwachstellen zu identifizieren und zu beheben, bevor diese von Hackern und Würmern ausgenutzt werden.

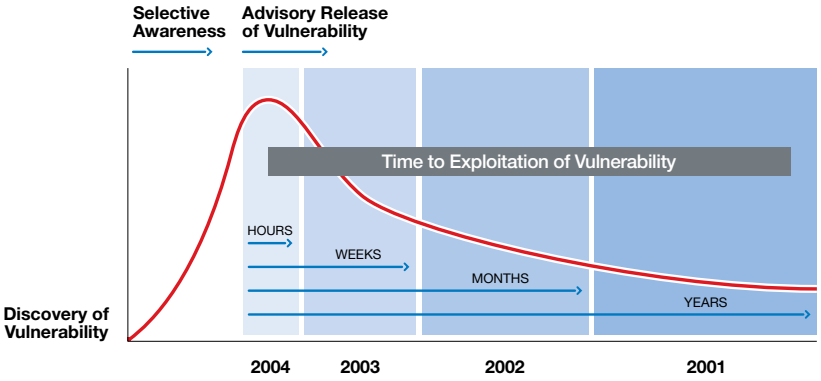

Abb. 1: Beschleunigung des Schwachstellen- und Exploit-Zyklus
Das Zeitfenster zwischen dem Auftauchen einer Schwachstelle und ihrer Ausnutzung verkürzt sich von mehreren Wochen auf wenige Stunden. Eine frühe Ermittlung von Schwachstellen ist die entscheidende Voraussetzung dafür, Einbrüche und die Kompromittierung wertvoller Daten zu verhindern.

Überhandnahme und Konsequenzen von Sicherheitsverletzungen

Im Rahmen der Computer Crime and Security Survey 2005, die vom Computer Security Institute (CSI) und der FBI Computer Intrusion Squad in San Francisco durchgeführt wurde, wurden 700 große Unternehmen und Regierungsbehörden befragt. Die Umfrage erbrachte folgende Ergebnisse:

• 56% der Befragten bestätigten, dass es im Lauf der vorausgegangenen 12 Monate Fälle von unbefugter Nutzung ihrer Computersysteme gegeben habe; 13% konnten nicht sagen, ob eine unbefugte Nutzung stattgefunden hat.

• 91% davon räumten finanzielle Verluste aufgrund von Einbrüchen in ihre Rechner ein und bezifferten auch deren Höhe: insgesamt 130.104.524 US$. Die größten Verluste waren auf Viren, unbefugte Zugriffe und Diebstahl von firmeneigenen Informationen zurückzuführen.

• 95% der Befragten gaben an, dass sich im vorausgegangenen Jahr mehr als 10 Website-Zwischenfälle ereignet hatten, verglichen mit nur 5% im Jahr 2004.

• Nur 20% der Betroffenen meldeten die Einbrüche bei den Strafverfolgungsbehörden. Die meisten unterließen dies, um negative Publicity zu vermeiden und zu verhindern, dass sich Wettbewerber die Information zunutze machen können.

Infolge dieser Trends müssen Unternehmen zunehmende Wachsamkeit walten lassen, um ihre Netzwerke vor der rapide ansteigenden Zahl von Sicherheitslücken zu schützen, die ausgenützt werden können, was finanzielle Verluste, negative Publicity und Wettbewerbsnachteile zur Folge haben kann.

Wachsende Kosten

Die Zahl der gemeldeten Sicherheitslücken wächst von Jahr zu Jahr. Allein 2005 wurden 5.990 neue Sicherheitslücken gemeldet. Von 1999 bis einschließlich 2. Quartal 2006 belief sich die Zahl der gemeldeten Schwachstellen auf insgesamt 26.713, was das Sicherheitsmanagement zu einer komplexen, ja geradezu beängstigenden Aufgabe macht. Historische Daten machen auch die wachsende Gefahr deutlich, die von Hackern ausgeht. Nach Angaben des Computer Emergency Response Teams (CERT) ist die Zahl der “Sicherheitsereignisse”, die im CERT-Koordinationszentrum an der Carnegie Mellon University erfasst wurden, von 1999 bis einschließlich 2003[1] um 1.149 Prozent gestiegen – eine durchschnittliche jährliche Wachstumsrate von 65,7 Prozent. (CERT definiert ein Sicherheitsereignis als den “entweder fehlgeschlagenen oder erfolgreichen Versuch, sich unbefugt Zugang zu einem System oder dessen Daten zu verschaffen”.) Jeder solche Versuch stellt eine potentielle Bedrohung für die Datenintegrität, Dienstverfügbarkeit und Vertraulichkeit der Informationen eines Unternehmenssystems dar.

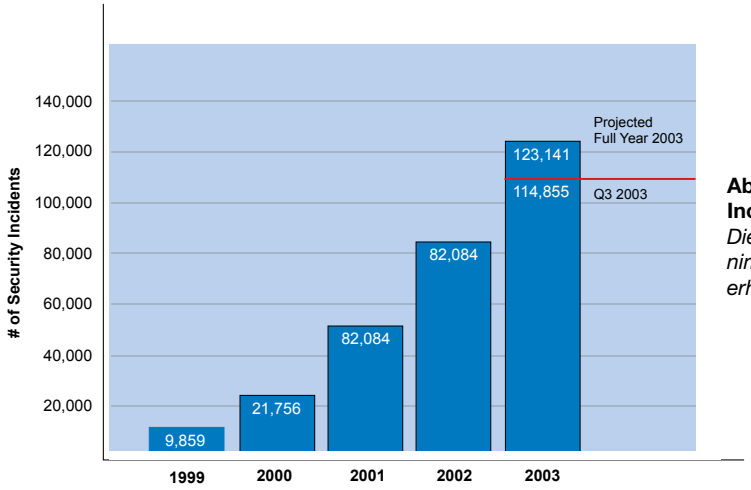

Abb. 2: CERT Security Incident Reports
Die Zahl der Einbrüche nimmt von Jahr zu Jahr erheblich zu.

Sicherheitsverletzungen verursachen Kosten in Milliardenhöhe: Kosten für Ausfallzeiten, Reparaturen, Abzug von IT-Ressourcen und unkalkulierbare Schäden aufgrund verlorenen Kundenvertrauens. Im schlimmsten Fall können Netzwerk-Sicherheitspannen sogar das Aus für ein Unternehmen bedeuten. Der Online-Händler Egghead.com musste seinen Betrieb einstellen, kaum ein Jahr, nachdem das Unternehmen einen erfolgreichen Hackerangriff entdeckt hatte und die Namen von 3,7 Mio. Kreditkarteninhabern, deren Daten möglicherweise kompromittiert worden waren, den Ausstellerbanken melden musste. Und Einbrüche in Netzwerke sind alles andere als ungewöhnlich.

III. DIE “VIER SÄULEN” DER SICHERHEIT

Unternehmen können eine Kombination aus verschiedenen Strategien einsetzen, um die Sicherheit ihrer Netzwerke zu gewährleisten: Virenschutz, Firewalls, Intrusion Detection-Systeme (IDS) und Schwachstellenanalysen. Jede dieser vier Strategien erfüllt eine eigene und wichtige Aufgabe.

Die meisten Unternehmen haben Firewalls installiert, die unautorisierten Netzwerkverkehr unterbinden. In manchen

[1] Für die noch nicht vorliegenden Daten für das 4. Quartal wurde eine Wachstumsrate von 50 Prozent auf Basis der Zahlen von 2002 bis einschließlich 2003 hochgerechnet; das Wachstum im 3. Quartal betrug 40 Prozent.

Auch Gartner empfiehlt Schwachstellenmanagement
Sicherheitsanforderungen treiben den Trend zum Schwachstellenmanagement voran

"Unternehmen, die solides Schwachstellenmanagement betreiben, statt sich lediglich auf Intrusion Detection zu verlassen, erleben weniger Cyberangriffe und tragen weniger Schaden durch solche Angriffe davon."

M. Nicolett, J. Pescatore
(19/11/2003)

Schwachstellenmanagement ist die Grundlage jeder Sicherheits-Policy und muss deshalb kontinuierlich durchgeführt werden.

"Da ans Internet angebundene Systeme am anfälligsten für Remote-Angriffe sind, sollten Unternehmen diese Systeme ständig überprüfen, um Sicherheitslücken zu finden, zu analysieren und zu beheben."

Quelle: Security Threats and Attack Trends, IBM
August 2004

Unternehmen sind auch Intrusion Detection-Systeme implementiert. Und praktisch jedes Unternehmen setzt eine Virenschutzlösung ein. Wie kann es angesichts all dieser Sicherheitstechnologien nun sein, dass Angreifer weiterhin erfolgreich in Netzwerke einbrechen und dort immense Schäden anrichten? Die Antwort lautet: Sie nützen die Schwachstellen in den Anwendungen aus, mit deren Hilfe die Unternehmen ihr Geschäft betreiben. Es ist somit eine betriebliche Notwendigkeit, diese Schwachstellen zu finden und zu beheben, bevor sie ausgenützt werden können.
Die nachstehende Tabelle gibt einen Überblick über die vier Hauptstrategien der Netzwerksicherheit, ihre Funktionen und ihre Grenzen bei isoliertem Einsatz.

Sicherheitsstrategie	Beschreibung	Grenzen bei isoliertem Einsatz
Virenschutz	Überwacht die Dateisysteme und Speicher von Desktops und Servern sowie die Mailserver auf Viren; hindert Viren effektiv daran, in ein Netzwerk oder System einzudringen	Schließt oder behebt keine offenen Sicherheitslöcher, die von Hackern, Script-Kiddies, Würmern und automatisierten Angriffen ausgenützt werden können.
Firewall	Gewährleistet, dass die Kommunikation zwischen den Servern eines Unternehmens und der Außenwelt bestimmten Sicherheitsregeln entspricht. Dient zudem als Authentifizierungsstelle für Benutzer und oft als VPN-Endpunkt zwischen Netzwerken oder für Remote-Benutzer.	Wird im Allgemeinen so konfiguriert, dass der http-, ftp- und smtp-Netzwerkverkehr passieren kann – womit oft ein optimaler Pfad für die Ausnutzung von Sicherheitslücken gegeben ist. Außerdem können Änderungen der Firewall-Policy verborgene Schwachstellen freilegen.
Intrusion Detection-System (IDS)	Warnt den Administrator bei ungewöhnlichen Aktivitäten vor einem möglichen Hacking-Versuch.	Informiert den Netzwerkadministrator nicht über Sicherheitslücken, bevor sie ausgenutzt wurden, also dann, wenn ein Eingreifen am meisten nützen würde. Ist anfällig für False Positives und False Negatives und erfordert komplexe Konfiguration.
Schwachstellenanalyse	Versetzt Unternehmen in die Lage, Sicherheitslücken zu identifizieren und zu beheben, bevor sie ausgenützt werden: Testet die Netzwerkgeräte und -systeme auf Sicherheitslücken, ermittelt, wo diese sich befinden, und nennt empfohlene Abhilfemaßnahmen für eine effiziente Beseitigung.	Informiert Netzwerk- und Systemadministratoren über Sicherheitslücken und Abhilfemaßnahmen. Informiert die Administratoren nicht, wenn Einbrüche im Gang sind, und säubert keine infizierten Dateien, sondern überlässt diese Aufgaben dem IDS und den Virenschutz-Tools.

Tab. 1: Vier Säulen der Sicherheit
Virenschutz, Firewalls, IDS und Schwachstellenanalyse stellen vier eigenständige Technologien zur Sicherung von Netzwerken dar. Jede von ihnen ist nützlich, keine von ihnen jedoch eine vollständige Lösung

Virenschutz

Virenschutz-Software läuft auf File-Servern und Desktops, um die Dateisysteme und Speicher auf Muster zu überwachen, die auf das Vorhandensein eines Virus hindeuten. Außerdem überwacht Virenschutz-Software auch die Mailserver, über die fast 90 Prozent aller Viren eingeschleust werden. Um genau arbeiten zu können, muss Virenschutz-Software häufig bzw. mittels automatischer Updates aktualisiert werden. Neue mehrteilige Würmer – bestehend aus einer sich selbst vervielfältigenden äußeren Schicht, die Schwachstellen ausnützt, um die Sicherheitssysteme zu umgehen, und einer inneren Schicht mit einer Payload-Schadensfunktion (wie z.B. Code Red) – überlisten jedoch die Virenschutztechnologien, indem sie Schwachstellen in Anwendungen ausnützen. Kurz nachdem die Virenschutz-Tools aktualisiert worden waren, um Code Red aus Systemen und Netzwerken entfernen zu können, nützte Nimda die gleiche Schwachstelle aus, die sich schon Code Red zunutze gemacht hatte – es wurde also zweimal dasselbe Einfallstor verwendet. Wenn man Schwachstellen identifizieren und beheben will, ist eindeutig eine andere Technologie als Virenschutz-Tools notwendig.

CERT empfiehlt Schwachstellenanalysen

Laut CERT verbessern Schwachstellenanalysen die Computersicherheit, weil dabei unautorisierte Systeme gefunden werden und das Netzwerk auf neue Zugangspunkte überprüft wird.

"Scannen Sie regelmäßig sämtliche Systeme mithilfe entsprechender Tools auf bekannte Schwachstellen … und beseitigen Sie alle Schwachstellen, die von diesen Tools gefunden werden."

"Setzen Sie regelmäßig Tools für Netzwerk-Mapping und -Scanning ein, damit Sie wissen, was Eindringlinge, die solche Tools verwenden, über Ihre Netzwerke und Systeme in Erfahrung bringen können."

Firewalls

Firewalls dienen sozusagen als Brückenköpfe, die das Netzwerk-Perimeter definieren, also den Übergang zwischen Unternehmensnetz und Internet. Da Firewalls bestimmen, welche Daten aus dem Internet ins Unternehmensnetz gelangen können, sind sie die entscheidende erste Verteidigungslinie gegen Hacker. Eine Firewall, die einer durchgängigen Ziegelmauer gleicht und keinerlei Daten von außen passieren lässt, schützt ein Unternehmen perfekt. Allerdings wäre sie alles andere als praktikabel, weil sie das Unternehmen von seinen Kunden und Geschäftspartnern isoliert. Stattdessen muss die Firewall Datenverkehr selektiv auf Basis der Regeln passieren lassen, die das Unternehmen definiert. Damit ist potenziellen Eindringlingen die Tür geöffnet. Und mehr noch: Wann immer das Unternehmen seine Firewall-Regeln verändert – zum Beispiel, um neuen Diensten oder Geräten die Möglichkeit zu geben, auf das Internet zuzugreifen, oder um die Regeln zu aktualisieren –, können unabsichtlich neue Sicherheitslücken geschaffen werden.

Intrusion Detection-Systeme

Intrusion Detection-Systeme (IDS) überwachen und analysieren System- und Netzwerkereignisse, um versuchte unautorisierte Zugriffe auf Systemressourcen zu erkennen und die Netzwerkadministratoren davor zu warnen. Mit einem IDS kann ein Unternehmen Hacking-Versuche oder tatsächliche Einbrüche erkennen, indem es seine Netzwerke oder Hosts auf verdächtige Daten oder andere anomale Aktivitäten untersucht.

Für IDS-Lösungen gibt es zwei verschiedene Ansätze:

• Hostbasierte IDS überwachen Hosts auf verdächtige Aktivitäten. Die Überwachung findet oft auf Datei- oder Betriebssystem-Ebene statt, normalerweise mithilfe einer zusätzlichen Software, die auf dem überwachten Host läuft. Dabei werden beispielsweise System-Logs, Dateien oder andere Ressourcen auf unerwartete Veränderungen analysiert. Werden ungewöhnliche Aktivitäten entdeckt, löst das IDS einen Alarm aus oder verständigt den Administrator anderweitig. Hostbasierte IDS werden auf das Betriebssystem des zu überwachenden Hosts installiert; sie fangen Software- und Benutzeraufrufe an das Betriebssystem und den Kernel ab und validieren sie.

• Netzwerkbasierte IDS überwachen die Netzwerkpakete, die das Netzwerk passieren. Diese Art von Lösung kann in Form von Hardware oder Software implementiert werden. Netzwerk-basierte IDS erkennen auch, wenn Würmer das System kompromittieren, da sie "sehen" können, wie sich der Wurm vom Host aus fortzupflanzen versucht.

IDS-Lösungen spielen eine wichtige Rolle als "Nachhut" in der Systemverteidigung. Das heißt, sie schlagen Alarm, wenn ein potenzieller Angriff im Gang ist. Die Sicherheits-Manager eines Unternehmens würden aber natürlich lieber Angriffe verhindern als zu erfahren, dass bereits ein Angriff stattgefunden hat. Darüber hinaus haben IDS noch in anderer Hinsicht Grenzen :

• Unzureichende Daten – Die Daten in den Netzwerkpaketen oder Systemaufrufen reichen oft nicht aus, um zuverlässig erkennen zu können, ob ein Angriff stattfindet.

• Verarbeitung auf Basis falscher Annahmen – Wenn sich ein Netzwerk-IDS in

einer demilitarisierten Zone (DMZ) oder in Netzwerken befindet, auf die von außen zugegriffen werden kann, interpretiert es möglicherweise Vorgänge als Angriff, die für die internen, geschützten Netzwerke keine Gefahr bedeuten. Zum Beispiel: Ein fehlerhaft aufgebautes Paket, das von einem externen Netzwerk empfangen wird, ist nicht unbedingt in der Lage, geschützten Netzwerken Schaden zuzufügen.

• Durchsatzprobleme – Sowohl hostbasierte als auch netzwerkbasierte IDS müssen große Datenmengen filtern oder analysieren. Die heutigen Rechner in Netzwerken laufen oft mit Geschwindigkeiten von 100 Mbps oder mehr und können damit die Leistungsfähigkeit von IDS-Produkten überfordern, deren Bandbreite häufig nicht hoch genug ist, um alle Daten untersuchen zu können.

• Das IDS kann ausgehebelt werden – Hacker führen solche Angriffe zumeist durch, indem sie Datenpakete subtil verändern, um das IDS zu verwirren. Zu den Techniken, die Hacker in diesem Zusammenhang anwenden, gehören Denial-of-Service-Angriffe, so genannte “Insertion”-Attacken, die im IDS Fehlalarme erzeugen und “Evasion”-Angriffe, die dem IDS entgehen und dann das Zielsystem schädigen.

Schwachstellenmanagement
IDS sind reaktive Lösungen, die Angriffe erkennen, während sie im Gang sind oder nachdem sie bereits stattgefunden haben. Schwachstellenmanagement ist dagegen proaktiv: Es stellt fest, für welche Angriffe ein Netzwerk anfällig ist, bevor es korrumpiert wird. Die Schwachstellen werden frühzeitig entdeckt, sodass ein Unternehmen sie beheben kann, bevor Netzwerkangriffe Schaden anrichten. Früher wurde Schwachstellenmanagement mit Techniken wie etwa jährlichen oder vierteljährlichen Penetrationstests betrieben, die von Security-Consultants durchgeführt wurden. Heute jedoch können Unternehmen dank On-Demand-Lösungen für Sicherheitsaudits und Schwachstellenmanagement Anfälligkeiten wesentlich häufiger ermitteln und beseitigen, dabei Kosten sparen und das “Fenster der Gefährdung” in ihrem Netzwerk schließen.

Beim Schwachstellenmanagement werden Sicherheitslücken auf methodische Weise ermittelt und priorisiert. Das Verfahren versetzt IT-Teams in die Lage, ihre Netzwerke ohne Eingriffe in die Systeme aus der “Perspektive eines Hackers” zu analysieren und automatisch:

• Sicherheitslücken und Fehlkonfigurationen im Netzwerk zu identifizieren
• nicht autorisierte Geräte zu identifizieren, einschließlich Wireless und VPN Access Points
• Anfälligkeiten zu entdecken und zu priorisieren
• Patches und Fixes für bekannte Sicherheitslücken zu installieren
• Firewall- und IDS-Konfigurationen zu validieren

Unternehmen, die Schwachstellenmanagement betreiben, scannen typischerweise Systeme, wenn diese erstmals an das Netzwerk angeschlossen werden, wenn Software installiert oder neu konfiguriert wurde und darüber hinaus auch turnusmäßig. Wenn eine Schwachstellen entdeckt wird, behebt das Unternehmen sie und führt dann einen weiteren Scan durch, um sich zu vergewissern, dass sie tatsächlich beseitigt wurde.

Das Schwachstellenmanagement arbeitet Hand in Hand mit dem Virenschutzsystem, der Firewall und dem IDS. Es findet potenzielle Sicherheitslücken, bevor sie ausgenutzt werden können, während das IDS das Unternehmen alarmiert, wenn sich eine ungewöhnliche Aktivität ereignet hat. Die beiden Ansätze ergänzen einander: Das Schwachstellenmanagement versetzt das IT-Team in die Lage, offensichtliche Sicherheitslücken zu finden und zu schließen, damit die Zahl der IDS-Alarme überschaubar bleibt.

Gleichzeitig arbeitet das Schwachstellenmanagement auch mit den Firewalls zusammen und überprüft das Netzwerk kontinuierlich und nahtlos auf eventuelle Schwachstellen, die bei Veränderungen der Firewall-Policy unabsichtlich herbeigeführt wurden.

On-Demand-Sicherheitsaudits können teure Penetrationstests ergänzen oder gar ersetzen

Penetrationstest ist die Bezeichnung für einen Netzwerk-Sicherheitsaudit, der von externen Consultants durchgeführt wird. Für einige wenige solche Tests pro Jahr werden 100.000 US$ bis 1.000.000 US$ in Rechnung gestellt. Ein Penetrationstest liefert umfassende Informationen über die Schwachstellen, die zu einem ganz bestimmten Zeitpunkt bestehen. Sein „Verfallsdatum" ist schnell erreicht: Die Resultate sind nur so lange gültig, bis sich die IT-Umgebung ändert oder neue Bedrohungen auftauchen. Um es auf einen Nenner zu bringen – die Ergebnisse von Penetrationstests sind nur wenige Stunden gültig. Da Netzwerkadministratoren Tag für Tag Netze und Geräte neu konfigurieren und pro Woche 25+ neue Schwachstellen bekannt werden, lässt sich Netzwerksicherheit nur durch häufige, kontinuierliche Tests gewährleisten. On-Demand-Sicherheitsaudits sind somit die ideale Ergänzung – oder gar der Ersatz – für Penetrationstests. Das On-Demand-Modell ermöglicht die Durchführung unbegrenzt vieler Audits – täglich, wenn nötig – zu einem Bruchteil der Kosten eines einzigen Penetrationstests. Außerdem ermöglicht es eine vergleichende Berichterstattung und Trendanalysen.

Gartner empfiehlt nahezu fortlaufende Scans

"Um neue Schwachstellen schnell zu finden, muss nahezu fortlaufend gescannt werden, weil Veränderungen an Anwendungen, Netzwerken und Systemen unweigerlich Konfigurationsfehler mit sich bringen und die System- und Applikationshersteller ständig neue Sicherheitslücken bekannt geben. Da Cyber-Angreifer laufend nach Einfallstoren scannen, müssen Unternehmen diese finden, bevor es die Angreifer tun."

M. Nicolett, J. Pescatore
(19/11/2003)

IV. VERFAHREN FÜR SCHWACHSTELLENMANAGEMENT IM VERGLEICH

Unternehmen können unter verschiedenen Verfahren für Schwachstellenmanagement wählen : manuelle Tests mit Produkten auf Software-Basis; von Consultants durchgeführte Penetrationstests; und extern gehostete, automatisierte Lösungen, die im Selbstbedienungsverfahren genutzt werden können. Bei der letzteren Methode, die auch als On-Demand-Sicherheitsauditing bezeichnet wird, werden die Scans remote durch einen externen Dienstleister durchgeführt, während die Kontrolle beim Benutzer verbleibt. Einen externen Dienst zu nutzen ist die einzige Möglichkeit, objektive Third-Party-Audits zu erhalten – mit denen sowohl die tatsächlich bestehenden Schwachstellen gefunden und behoben werden können als auch die Einhaltung der gesetzlichen Sicherheitsvorschriften dokumentiert werden kann.

Produktbasierte und servicebasierte Lösungen

Es gibt zwei verschiedene Kategorien von Lösungen für Schwachstellenmanagement: produktbasierte und servicebasierte.

Produktbasierte Lösungen

Produktbasierte Lösungen werden im internen Netzwerk des Unternehmens installiert und im Allgemeinen manuell betrieben. Schwachstellenmanagement auf Produktbasis hat jedoch den Nachteil, dass es keine Außensicht auf die Schwachstellen im Netzwerk liefert. Das Produkt muss entweder im nicht routbaren, privaten Teil des Unternehmensnetzwerks installiert werden oder im offenen, über das Internet adressierbaren Teil. Beide Installationsoptionen werfen Probleme auf. Wird das Produkt im privaten Teil installiert – also hinter der Firewall – dann ist es nicht immer in der Lage, die vielen verschiedenen Formen von externen Angriffen zu entdecken, bei denen explizit verformte Pakete an das Unternehmensnetz geschickt werden. Die Firewall selbst, gleich, ob proxy- oder paketbasiert, verzerrt die Genauigkeit des Tests, und False Positives und False Negatives treten in Hülle und Fülle auf.

Wird das Produkt dagegen in einem öffentlichen, über das Internet adressierbaren Netzwerk installiert, dann wird die Sicherheit des Knotens zu einem großen Problem, auf dem die Schwachstellenmanagement-Software läuft. Was, wenn der Rechner, der die Schwachstellenmanagement-Tests ausführt, selbst angegriffen oder von einem Angreifer überwacht wird? Wie können die Resultate auf sichere Weise vom externen Host an sichere Knoten übertragen werden? Das Unternehmen riskiert nicht nur einen verfälschten Test, sondern auch, dass entscheidende Informationen über die internen Netzwerke Hackern preisgegeben werden.

Ein weiterer Nachteil des produktbasierten Schwachstellenmanagements tritt zutage, wenn große Netzwerke getestet werden. In großen Netzwerken muss die Schwachstellenmanagement-Software auf mehreren Knoten laufen. Somit sind natürlich auch die Analyse-Resultate auf mehrere Rechner verteilt. Um eine unternehmensübergreifende Sicht zu ermöglichen, müssen die Administratoren die Daten typischerweise zusammenstellen und Ergebnisberichte manuell erstellen – womit den ohnehin schon überlasteten Sicherheitsadministratoren noch mehr Arbeit aufgebürdet wird.

Und schließlich ist auch an die Pflege der Software zu denken. Die Software muss aktualisiert werden, damit stets auf die aktuellsten Schwachstellen getestet wird. Bei 25+ neu entdeckten Schwachstellen pro Woche ist es

Denken wie ein Hacker
QualysGuard ahmt den Workflow eines Hackers nach. Jeder Scan umfasst folgende Schritte :

- *Sammlung von Informationen — Es wird so viel wie möglich über einen Host herausgefunden, ohne einzudringen oder sich mit dem Host zu verbinden. Dabei werden Techniken wie Whois, DNS-Abfragen und Scannen von IP-Adressen genutzt.*
- *Erkennung – Identifizierung der Hosts im Ziel-Subnetz (Topologie, Firewalls und andere Geräte).*
- *Scannen – Netzwerk- und Port-Scanning zur Ermittlung der potenziellen Ziele, der Schwachstellen in der Hardware und Software und der jeweiligen offenen Ports.*
- *Korrelation – Bestätigung der Schwachstellen, um das gewünschte Ziel zu erreichen.*

schwer, stets auf dem neuesten Stand zu bleiben – eine weitere Bürde für die Administratoren.

Servicebasierte Lösungen
Externe Firmen bieten servicebasierte Lösungen an. Einige dieser Third-Party-Lösungen werden im Netzwerk gehostet, andere dagegen extern. Bei der letzteren Variante wird die Perspektive eines Hackers eingenommen und das Netzwerk am Perimeter gescannt. Das heißt, die Schwachstellenanalyse wird aus der Sicht eines Hackers durchgeführt, der von außen nach innen blickt. Lösungen auf Servicebasis werden sowohl von Consultants durchgeführt als auch von Anbietern automatisierter Sicherheitsaudits, wie etwa Qualys (s. Randspalte: Denken wie ein Hacker). Third-Party-Audits sollten auch über Funktionen verfügen, die es ermöglichen, die Sicherheit der internen Netzwerke innerhalb des Firewall-Perimeters zu analysieren.

Baumbasierte und inferenzbasierte Analyse
Gleich, ob Schwachstellenmanagement-Tools produkt- oder servicebasiert sind, sie setzten immer entweder eine baumbasierte oder eine inferenzbasierte Analysetechnologie ein.

Baumbasierte Technologie
Frühe Technologien für Schwachstellenanalysen testeten Server oder sonstige Geräte anhand von Listen – oder Bäumen – mit Schwachstellen. Die Administratoren lieferten dabei die Informationen, indem sie die passenden Bäume für den jeweiligen Rechner auswählten – zum Beispiel die Bäume für einen Server, auf dem Windows, Webservices und eine Datenbank liefen.

Bei diesem Ansatz hängt die Schwachstellenanalyse also davon ab, dass die Administratoren zunächst Informationen bereitstellen; anschließend läuft der Scan blind weiter, ohne irgendwelche Informationen zu berücksichtigen, die während des Scans selbst ermittelt werden. Außerdem werden sämtliche Tests in einem gegebenen Baum durchgeführt, ganz gleich, ob sie zur Konfiguration der getesteten Geräte passen oder nicht. Deshalb dauert die Schwachstellenanalyse länger und die getesteten Hosts werden unnötigerweise zusätzlich belastet.

Inferenzbasierte Technologie
Inferenzbasierte Technologie zur Schwachstellenanalyse basiert auf einem Ansatz, der sich vom oben beschriebenen baumbasierten Ansatz erheblich unterscheidet. Bei der inferenzbasierten Analyse beginnt der Scan-Prozess damit, dass Informationen mittels verschiedener Erkennungsmethoden gesammelt werden. Dazu zählen etwa Host-Identifikation, Ermittlung von Betriebssystemen/OS-Fingerprinting, Port-Scanning und Protokollerkennung. Mithilfe der auf diese Weise gewonnenen Informationen kann die Scanning-Engine feststellen, welche Ports von bestimmten Diensten genutzt werden, wie etwa Webservern, Datenbanken und Mailservern. Nach der Phase der Informationsgewinnung wählt die Scanning Engine auf intelligente Weise die geeigneten Schwachstellen-Checks für den Scan aus und führt diese durch. Es wird nur nach denjenigen Schwachstellen gesucht, die angesichts der spezifischen Konfiguration der einzelnen Rechner tatsächlich vorhanden sein könnten.

Inferenzbasiertes Scannen ist ein Expertensystem-Ansatz, bei dem die

Informationen über ein Netzwerk mit genau denselben Mitteln gewonnen werden, die auch ein Hacker einsetzen würde. Inferenzbasierte Analysesysteme integrieren neue Informationen, sobald sie zur Verfügung stehen. Auf diese Weise werden die Kenntnisse über den Rechner in Echtzeit erweitert und genau diejenigen Tests ausgeführt, die Resultate erbringen könnten. Deshalb ist dieser Ansatz effizienter, belastet den Rechner weniger und maximiert den Erfolg der Schwachstellenerkennung, während False Positives und False Negatives minimiert werden.

Kriterien für eine effektive Lösung für Schwachstellenanalyse
Die effektivste Lösung für Schwachstellenanalyse erfüllt folgende Kriterien :

• Analyse aus der Perspektive eines Hackers – "von außen nach innen" – , jedoch durch einen objektiven, vertrauenswürdigen Dritten.

• Scannt automatisch auf Basis einer laufend aktualisierten, umfassenden Datenbank für bekannte Angriffsmethoden.

• Äußerst präzise Ermittlung von Schwachstellen und Eliminierung von Fehlalarmen mit Methoden, die nicht in die Systeme eingreifen.

• Inferenzbasierte Scanning Engine, die selektiv auf relevante Schwachstellen testet. Diese intelligente Methode der Schwachstellenanalyse sorgt dafür, dass bei jedem Scan nur auf tatsächlich mögliche Schwachstellen getestet wird.

• Nützt das Internet zur Bereitstellung. Dies hat folgende Vorteile:

- Audits 24x7, sowohl vorab geplant als auch on demand
- Zugriff über jeden Webbrowser
- Skalierbar, wenn das Netzwerk wächst
- Auto-Provisioning für leichtes Hinzufügen/Entfernen von Geräten und Benutzern
- Keine Installation oder Pflege von Software erforderlich

• Erzeugt prägnante, praktisch nutzbare, anpassbare Berichte, einschließlich Priorisierung der Schwachstellen nach Fehlerklasse und Trendanalyse.

• Empfiehlt getestete Fixes und Workarounds zur Beseitigung von Schwachstellen.

• Unterstützt heterogene Netzwerke.

• Nur QualysGuard erfüllt alle genannten Kriterien auf kostengünstige Weise.

V. QUALYSGUARD – ON-DEMAND-LÖSUNG FÜR SICHERHEITSAUDITS UND SCHWACHSTELLENMANAGEMENT

QualysGuard steht für die nächste Generation der inferenzbasierten Scan-Technologie. Als Webservice, der durch den Benutzer gesteuert, aber remote gehostet und verwaltet wird, automatisiert QualysGuard Sicherheitsaudits und Schwachstellenmanagement in Netzwerken – und sorgt so dafür, dass die Sicherheitsadministratoren um ein Vielfaches effektiver und effizienter arbeiten können. Der Webservice ahmt die Perspektive eines Hackers nach – "von außen nach innen" – und überprüft das Netzwerk innerhalb und außerhalb der Firewall.

QualysGuard ist ein Service auf Subskriptionsbasis, mit dem die Kunden eine unbegrenzte Anzahl von Scans durchführen können, sowohl turnusmäßig als auch on demand und von jedem Webbrowser aus. Da sich der Subskriptionspreis nach der Anzahl der zu scannenden IP-Adressen richtet, können die Netzwerk-Administratoren so oft wie nötig scannen, um Sicherheitslücken zu finden und zu prüfen, ob sie erfolgreich beseitigt wurden.

Unternehmen, die den Service QualysGuard abonnieren, profitieren von der objektiven Perspektive eines unabhängigen Dritten. Dadurch ermitteln sie automatisch Schwachstellen, auf die sie selbst möglicherweise nicht getestet hätten,

Vorteile einer Subskription von QualysGuard – Highlights

QualysGuard ist der erste skalierbare, kostengünstige Webservice für proaktive On-Demand-Sicherheitsaudits innerhalb und außerhalb der Firewall und lässt sich in heterogenen Netzwerken jeder Größe effektiv einsetzen. Die Lösung gibt dem Anwender vollständige Kontrolle über den gesamten Prozess der Sicherheitsanalyse und des Schwachstellenmanagements und bietet dabei insbesondere folgende Vorteile:

- Skalierbares Management auf Basis der Webservice-Architektur von Qualys
- Komplett automatisierte Lösung ersetzt traditionell arbeitsaufwändige Verfahren, spart Zeit und vereinfacht das Schwachstellenmanagement in großen Netzwerken erheblich
- Schnelle Identifizierung und Visualisierung von Netzwerk-Assets
- Präzise Ermittlung von Schwachstellen macht zeitaufwändige manuelle Überprüfung von Resultaten und Konsolidierung von Daten überflüssig
- Zugriff durch autorisierte Benutzer von jedem Ort der Welt aus

und erfüllen gleichzeitig die branchenspezifischen Vorschriften für Netzwerksicherheit und Corporate Governance. Dazu zählen etwa der U.S. Healthcare Insurance Portability and Accountability Act (HIPAA), der Gramm-Leach-Bliley Act (GLBA), der für US-Finanzdienstleister maßgeblich ist, der Sarbanes-Oxley Act, California SB 1386, der Turnbull Report, der interne Kontrollen für börsennotierte Unternehmen in Großbritannien vorschreibt, und der britischen Data Protection Act.

Qualys bietet einen vertrauenswürdigen, objektiven Third-Party-Service. QualysGuard erfordert keine Installation, keinen Setup, keine Anschaffung oder Pflege von Hardware oder Software, kein spezifisches Sicherheits-Know-how im Unternehmen und keine Schulungen. Die Lösung automatisiert den gesamten Prozess des Schwachstellenmanagements (s. Abb. 3: QualysGuard ermöglicht Sicherheitsaudits und Schwachstellenmanagement on demand). Da die Zahl der Scans unbegrenzt ist, können die Administratoren beliebig viele Netzwerk-Audits durchführen und Geräte auf Schwachstellen testen, so oft irgendwelche Änderungen vorgenommen wurden.

Die folgenden Abschnitte geben einen Überblick über die verschiedenen Elemente des Security Audit Services QualysGuard. Alle diese Elemente sind im Abonnement enthalten.

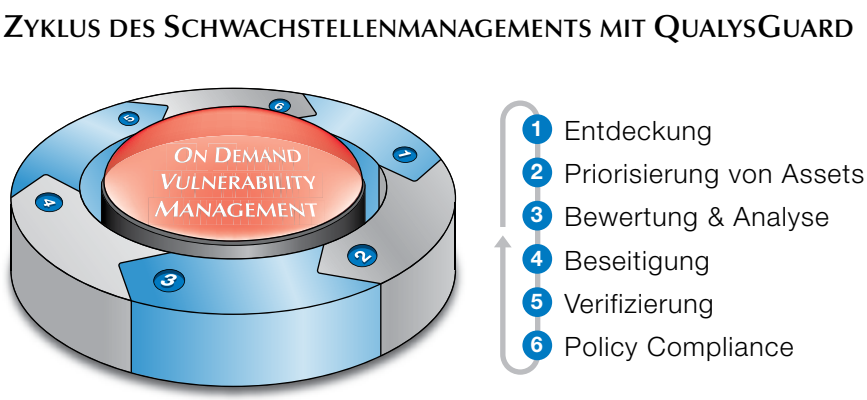

Abb. 3: QualysGuard ermöglicht Sicherheitsaudits und Schwachstellenmanagement on demand
Bei jedem Scan erkennt QualysGuard alle Geräte im Netzwerk, stellt sie dar und analysiert sie im Abgleich mit der branchenweit umfassendsten und aktuellsten Datenbank für Sicherheitslücken. Dabei wird ein inferenzbasiertes Verfahren angewandt. Zudem bietet QualysGuard klar verständliche, unlöschbare Audit-Reports mit Links zu bewährten Reparaturmaßnahmen und Workarounds.

Ermittlung und Management von Schwachstellen innerhalb und außerhalb der Firewall

Mit QualysGuard können Unternehmen die Sicherheit ihres Netzwerks aus der Perspektive eines Außenstehenden überprüfen. Dank der Webservice-Architektur von QualysGuard (s. Anhang 1) betrachten die Qualys Remote-Scanner das Unternehmensnetz von außerhalb der Firewall. QualysGuard überprüft automatisch alle Hosts des Unternehmens, die mit dem Internet verbunden sind. Geräte-Versionen der Qualys Remote-Scanner ermöglichen Audits in internen Netzen. Diese Geräte, die Qualys Intranet Scanner, integrieren sich problemlos in das Unternehmensnetz und versetzen QualysGuard in die Lage, auf sichere Weise nach internen Schwachstellen zu scannen. Die Intranet Scanner arbeiten vollautomatisch unter Einsatz der aktuellsten Schwachstellensignaturen, erfordern keine Wartung und gewährleisten sichere Kommunikation mit SSL-Verschlüsselung.

Wie QualysGuard Hosts findet

Qualys verwendet folgende Methoden, um Hosts zu ermitteln:

AXFR: QualysGuard ermittelt den Nameserver (NS), der für die Domain zuständig ist, und fordert eine Liste aller Hosts an, die dieser Server verwaltet. Eine solche Anfrage ist jedoch nicht immer zulässig. Tatsächlich sollten Administratoren ihre Systeme so konfigurieren – und tun es in der Regel auch –, dass derartige Anfragen abgewiesen werden.

FQDN Brute Force: QualysGuard verwendet eine eigene Liste mit rund 100 gängigen Hostnamen (zum Beispiel www, ftp etc.) und bildet daraus eine Liste mit Fully Qualified Domain Names (FQDNs). Dann schickt QualysGuard eine Anfrage an den NS und lässt ihn die IP-Adressen finden, die den FQDNs zugeordnet sind.

Ping-Scan: QualysGuard führt in den Adressbereichen, die der Administrator angibt, einen Ping-Scan durch, um Ziel-Hosts zu finden.

Erkennung: Dynamische Ermittlung aller Netzwerkgeräte

QualysGuard erstellt ein zugreifbares Inventar sämtlicher Geräte und Systeme im Netzwerk und erzeugt eine visuelle Topologie aller Netzwerkgeräte des Unternehmens, die vom Internet aus „zu sehen“ sind (s. Abb. 4: Netzwerkerkennung). Durch Senden von Pings an alle IP-Adressen (Ping Sweep) und Fingerprinting von Hosts kann QualysGuard Folgendes präzise erkennen und darstellen:

- Access-Gateways, Router, Betriebssysteme und ISP-Identifikation für jeden Host
- Umfang des Kundennetzwerks
- Zugangspunkte zu den erkannten Netzwerken
- Rechnernamen
- Private Netzwerke und Intranets
- Offene TCP-Ports
- Betriebssysteme aller erfassten Hosts

Manchmal identifiziert QualysGuard Geräte, von denen der Netzwerkadministrator gar nicht wusste, dass sie sich im Netzwerk befinden: Das können Hosts sein, die zu böswilligen Zwecken oder versehentlich im Netzwerk platziert wurden.

Alle Resultate der Netzwerkübersicht werden verschlüsselt und gespeichert, sodass sie später ausgelesen und für eine vergleichende Berichterstattung genutzt werden können. Wenn also die Baseline-Architektur erst einmal erfasst ist, kann vergleichendes Netzwerk-Mapping dazu beitragen, unautorisierte Systeme zu finden. Die Abonnenten können eine unbegrenzte Zahl von Mappings durchführen, sowohl turnusmäßig als auch on demand. Auf diese Weise können sie die Netzwerk-Architektur ständig überwachen und die Konfigurationen über längere Zeiträume hinweg miteinander vergleichen.

Um ein Netzwerk-Mapping zu starten, gibt der Kunde einen oder mehrere Internet-Domain-Namen und die gewünschten Netzwerk-IP-Adressbereiche in QualysGuard ein. QualysGuard verwendet diese Informationen, um die Computer innerhalb dieser Domain und dieses Adressraums zu finden, auf die vom Internet aus zugegriffen werden kann. Auf diese Weise können die Administratoren Geräte finden, die nicht im DNS-Record eingetragen sind, und ihre Firewall- und IDS-Konfigurationen validieren (s. Randspalte: „Wie QualysGuard Hosts findet“). Berichte über die Netzwerk-Topologie werden in drei Formaten zur Verfügung gestellt: grafisch, XML und tabellarisch in HTML.

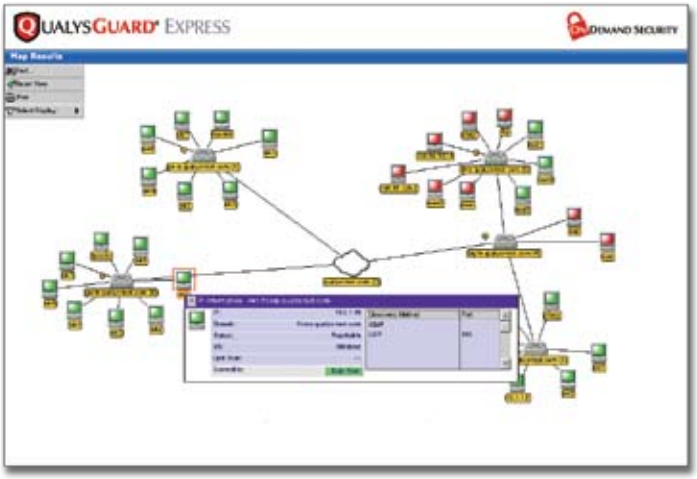

Abb. 4: Netzwerkerkennung
QualysGuard erkennt unverzüglich sämtliche Geräte am Internet-Perimeter und innerhalb der Firewall und stellt ihre Topologie dar. Vergleichende Netzwerkübersichten können on demand erstellt werden, sodass die Netzwerk-Administratoren unautorisierte Systeme finden können.

Geräte und Anwendungen, die von QualysGuard gescannt werden

Betriebssysteme:
Windows NT, 2000, 2003, XP und CE, Linux, BSD, MacOS X, Solaris, HP-UX, Irix, AIX, SCO, Novell

Webserver:
Apache, Microsoft IIS, iPlanet, Lotus Domino, IpSwitch, Zeus; und umfassende Unterstützung für virtuelles Hosting

SMTP/POP-Server:
Sendmail, Microsoft Exchange, Lotus Domino, Netscape Messaging Server, QMail

FTP-Server:
IIS FTP Server, WuFTPd, WarFTPd

Firewalls:
Check Point VPN1/FireWall-1 und NG, Cisco PIX, NetScreen, Gauntlet, CyberGuard, Raptor

Datenbanken:
Oracle, Sybase, MS SQL, PostgreSQL, MySQL

eCommerce:
Icat, EZShopper, Shopping Cart, PDGSoft, Hassan Consulting Shopping, Perlshop

LDAP-Server:
Netscape, IIS, Domino, Open LDAP

Load-Balancing-Server:
Cisco CSS, Alteon, F5 BIG IP, IBM Network Dispatcher, Intel Router, Administrable

Switches und Hubs:
Cisco, 3Com, Nortel Networks, Cabletron, Lucent, Alcatel

Wireless Access Points:
Cisco, 3COM, Symbol, Linksys, D-Link, Netgear, Avaya, Apple Airport, Nokia, Siemens

Analyse: Inferenzbasierte Schwachstellen-Scans

QualysGuard analysiert jedes mit dem Netzwerk verbundene Gerät und System auf mögliche Sicherheitslücken und setzt dazu ein proprietäres, inferenzbasiertes Verfahren ein. Die Expertensystem-Analytik ist in der Lage, die Topografie des gescannten Netzwerks "zu erlernen". Sie trifft keine Annahmen und schließt nichts aus, ohne jedes zu testende System genau zu verstehen – so ist eine präzise und vollständige Erkennung gewährleistet. Zu den Analysen, die durchgeführt werden, gehören aktive Tests, Protokoll- und Daemon-Fingerprinting, Brute Forcing und Passwort-Raten sowie Tests auf der Netzwerk- und Anwendungsschicht (s. Abb. 5: Die inferenzbasierte Scanning Engine von QualysGuard). Um die Analyse zu starten, wählt der Administrator einen oder mehrere Hosts aus – nach Typ des Betriebssystems, Ort, funktionaler Gruppe, Netzwerk-Administrator etc. –, die dann von der QualysGuard-Webseite aus gescannt werden. Die Abonnenten können unbegrenzt viele Scans durchführen, wahlweise vorab geplant oder on demand.

Abb. 5: Die inferenzbasierte Scanning-Engine von QualysGuard
QualysGuard setzt bei den Audits ein lernfähiges, intelligentes Verfahren ein, das aus einer Bibliothek mit Hunderten von proprietären Testmodulen nur diejenigen Tests auswählt und durchführt, die für den gescannten Host relevant sind. Dies optimiert den Scan-Prozess und beschränkt die Datenbelastung der Kundennetzwerke auf ein Minimum.

Die Scans wirken sich kaum auf die Netzlast aus, weil die inferenzbasierte Scanning Engine von QualysGuard nur Exploits testet, die der Konfiguration des Netzwerks entsprechen. So wird QualysGuard beispielsweise einen Linux-Rechner nicht auf Windows-NT-Sicherheitslücken testen. Um die Effizienz zusätzlich zu erhöhen, überprüft QualysGuard laufend die verfügbare Bandbreite und verwendet nur den vom Netzwerk-Administrator festgesetzten Prozentsatz.

Die umfassende Scanning Engine von QualysGuard greift auf eine laufend aktualisierte Vulnerability KnowledgeBase (Wissensbank) zurück, die mehr als 5.000 Netzwerkschwachstellen verzeichnet. Die KnowledgeBase bildet die Basis für die "Hacker-Perspektive", aus der Netzwerk, Systeme, Anwendungen und kommerzielle sowie Open-Source-Betriebssysteme gescannt werden. Wenn neue Sicherheitslücken auftauchen – was im Schnitt 25 mal pro Woche der Fall ist –, werden entsprechende Signaturen erstellt und sofort in die Wissensbank aufgenommen. So testen die Abonnenten von QualysGuard ihre Netzwerke stets automatisch auf die neuesten bekannten Schwachstellen. Den aktuellen Schwachstellen-Counter sowie eine Beschreibung neuer Schwachstellen finden Sie unter http://www.qualys.com/research/rnd/knowledge/vulncount/

Eine Lösung für Schwachstellenanalyse ist nur so leistungsfähig wie die Exploit-Datenbank, auf die sich ihre Tests stützen. Qualys hält es für unzureichend, die Daten zu Schwachstellen und Exploits nur aus einer einzigen Quelle zu beziehen. Vielmehr enthält die Qualys KnowledgeBase Schwachstellen- und

Schwachstellen-Kategorien, die von QualysGuard abgedeckt werden

Backdoors und Trojaner

Brute Force-Angriffe

CGI

Datenbanken

DNS und Bind

eCommerce-Anwendungen

File Transfer Protocol

Firewalls

Allgemeine Remote-Services

Hardware und Netzwerkgeräte

Information/Directory Services

SMB/Netbios Windows

File-Sharing

SMTP und Mail-Anwendungen

SNMP

TCP/IP

Webserver

X-Windows

Wireless Access Points

VoIP

Fingerprint-Daten aus zahlreichen Quellen. Dazu zählen die Qualys-Partner Security Focus (Bugtraq) und Vigilinx; weitere Informationen stammen von CERT, aus der CVE-Liste, von Hacker-Websites im Internet, aus Mailing-Listen, die im Untergrund kursieren, und vielen anderen Quellen.

Die zentralisierte QualysGuard KnowledgeBase wird laufend aktualisiert, oft mehrmals täglich. Die Updates werden automatisch allen Abonnenten gleichzeitig zugänglich gemacht. Die KnowledgeBase speist die neuesten Schwachstellen-Informationen laufend in die Scanning-Server von Qualys ein und gewährleistet damit, dass die Benutzer der Lösung QualysGuard ihre Netzwerke stets auf die neuesten Sicherheitslücken testen.

Genau wie die Topologie-Karten werden auch alle Scan-Resultate verschlüsselt und gespeichert, sodass sie später für dynamisches Reporting einschließlich Trendanalysen genutzt werden können.

Zusammengefasst zeichnet sich die einzigartige Scanning Engine von QualysGuard durch folgende Eigenschaften aus:

• Greift nicht in die Systeme ein, beeinträchtigt weder die Verfügbarkeit noch die Integrität der Hosts, die gescannt werden.

• Da die inferenzbasierte Scanning Engine modular aufgebaut ist, werden nur relevante Schwachstellen getestet, basierend auf intelligenter Informationsgewinnung während des Scan-Prozesses. Angewandt werden Techniken zur Host-Erkennung, Port-Scanning, Betriebssystem-Erkennung/ OS-Fingerprinting und Methoden zur Protokoll-Erkennung.

• Präzise und vollständig, führt folgende Analysen durch:
  - Banner-Identifizierung und aktive Tests.
  - Protokoll- und Daemon-Fingerprinting.
  - Brute Forcing und Passwort-Raten.
  - Tests und Analysen auf der Netzwerk- und Anwendungsschicht.

• Hochleistungsfähig und skalierbar; nutzt die globale Webservice-Architektur von Qualys, die umfassendes Scannen ermöglicht, ohne dass den Benutzern Kosten für Infrastruktur und Software-Pflege entstehen.

Reporting: Ausführliche technische oder Übersichtsdaten und Trendanalysen

QualysGuard liefert sowohl technische Daten als auch Übersichtsdaten, wahlweise in kundenspezifisch anpassbaren oder vordefinierten Formaten. Grafische Reports können über die QualysGuard Web-Benutzeroberfläche in HTML erzeugt werden (s. Abb. 6: QualysGuard Schwachstellen-Report). Die Berichte geben einen Überblick über den Sicherheitsstatus jedes Netzwerkgeräts: Dazu gehören Informationen über den Scan, spezifische Informationen über den Host sowie eine Auflistung der entdeckten Sicherheitslücken. Zu jedem ermittelten Sicherheitsrisiko liefern die Berichte eine Beschreibung, geben die Problemschwere an (Fehlerklassen von 1 bis 5 gemäß Branchenstandard), nennen die potenziellen Auswirkungen, geben Compliance-Informationen und führen Links zu bewährten Patches und Fixes auf (s. Randspalte: “Fehlerklassen”). Mit diesen Informationen ausgerüstet, können Security-Manager die richtigen Prioritäten setzen, wenn es um die Entscheidung geht, welche Schwachstellen wann und auf welche Weise

Fehlerklassen

Die QualysGuard Scanning Engine weist jeder entdeckten Schwachstellen eine Fehlerklasse zu:

- *Level 1 (niedrig): Informationen können gesammelt werden.*
- *Level 2 (mittel): Sensible Informationen können gesammelt werden, z.B. die genauen Versions- und Release-Nummern von Software, die auf der Zielmaschine läuft.*
- *Level 3 (hoch): Anzeichen für Bedrohungen wurden entdeckt, z.B. Directory-Browsing, Denial of Service oder teilweise Lesbarkeit bestimmter Dateien.*
- *Level 4 (kritisch): Alarmierende Hinweise auf Dateidiebstahl, potenzielle Backdoors oder lesbare Benutzerlisten auf Zielrechnern wurden entdeckt.*
- *Level 5 (gravierend): Lese- und Schreibzugriff auf Dateien, Remote-Ausführung oder Backdoor-Software wurde entdeckt, oder sonstige Aktivitäten sind im Gang.*

behoben werden sollen.
Zudem generiert QualysGuard auf Basis der Scan-History Trendanalysen und vergleichende Reports zur Security Policy Compliance. Führungskräfte können diese Informationen als Grundlage nutzen, um finanzielle Mittel zuzuweisen und Versicherungsgesellschaften, Geschäftspartner, Aktionäre und Vorstände über den Sicherheitszustand auf dem Laufenden zu halten.

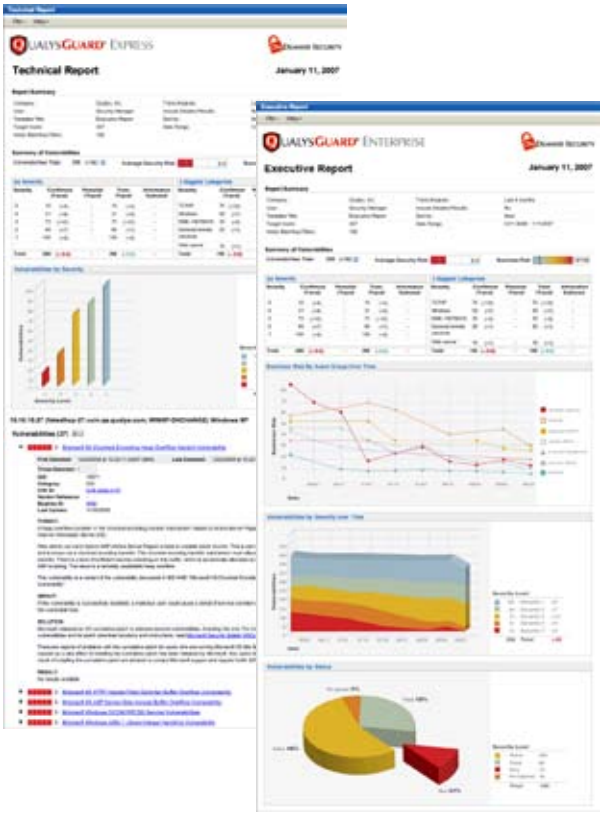

Abb. 6: QualysGuard-Schwachstellen-Report *QualysGuard priorisiert die Schwachstellen nach der Problemschwere und versetzt damit die IT-Teams in die Lage, die Sicherheitsressourcen vorrangig da einzusetzen, wo sie am dringendsten benötigt werden*

Darüber hinaus sammelt und veröffentlicht Qualys anonymisierte Berichtsdaten, um Unternehmen die Erkennung häufig vorkommender Angriffe zu erleichtern und ihnen ein Verständnis dafür zu vermitteln, wie ihre eigenen Netzwerke im Vergleich zu denen anderer Unternehmen mit ähnlichem Anfälligkeitsprofil abschneiden. Die Management-Funktionalitäten zur Durchführung von Sicherheitsaudits, Einsichtnahme in die Berichte und Behebung von Schwachstellen können an zuständige Sicherheitsmitarbeiter im gesamten Unternehmen verteilt werden. Alle Informationen, die sich auf spezifische Unternehmen beziehen, werden komplett vertraulich behandelt.

Das dynamische Reporting von QualysGuard bringt den Benutzern folgende Vorteile:

- Maßgeschneiderte Berichterstattung – Die Benutzer können maßgeschneiderte Berichte erstellen lassen und Berichte als Templates speichern.
- Trend-Analysen zu Schwachstellen – Die Benutzer können Scan-Resultate vergleichen: über längere Zeiträume hinweg oder von einem Scan zum nächsten.
- Grafische Berichte – Die Benutzer können grafische HTML-Reports über die entdeckten Schwachstellen sowie Tabellen einsehen.
- Sortierung und Filterung – Die Benutzer können Daten aus Scan-Resultaten sortieren und filtern.
- Überblicksberichte – QualysGuard ermöglicht die Erzeugung von High-Level-Reports, die einen Gesamtüberblick über die Netzwerksicherheit vermitteln.

Für Unternehmen, die die Informationen von QualysGuard in Reporting-Tools von Drittanbietern integrieren möchten, liefert Qualys vollständige Scan- und Map-Details in XML.

Schwachstellenbeseitigung: Links zu geprüften Fixes

Zu jeder entdeckten Sicherheitslücke empfiehlt QualysGuard verifizierte Gegenmaßnahmen, Patches und Workarounds und liefert Links zu Websites, auf denen Dokumentationen oder Patches zu finden sind. Die Sicherheitsexperten im Qualys Vulnerability Laboratory testen und validieren die Abhilfemaßnahmen und geben die geschätzte Zeit für die Beseitigung behebbarer Schwachstellen an.

Abb. 7: QualysGuards One-Click-Links zu verifizierten Fehlerbeseitigungsmaßnahmen
Empfehlungen zu sofortigen Gegenmaßnahmen, Patches und Workarounds für jede entdeckte Sicherheitslücke sowie Time-to-Fix-Schätzungen werden von QualysGuard validiert und den Kunden zur Verfügung gestellt.

Manche Lösungen für Schwachstellen-Auditing informieren die Administratoren typischerweise nur dann über Sicherheitslücken, wenn sie verfügbare Fixes kennen. Das stellt die Administratoren vor eine schwierige Wahl: Entweder bleiben sie anfällig für Angriffe oder sie schalten wichtige Informationsdienste ab. QualysGuard dagegen meldet alle entdeckten Sicherheitslücken, ganz gleich, ob ein Patch verfügbar ist oder nicht. Ist kein Patch verfügbar, schlägt QualysGuard Workarounds vor, die den Administratoren die Möglichkeit geben, ihre Netzwerkdienste weiter zu betreiben, während die Hersteller einen Patch entwickeln.

Mithilfe der IP-Grouping-Funktion von QualysGuard können Netzwerk-Sicherheitsmanager QualysGuard als Workflow-Ticketing-Lösung einsetzen und Reparaturaufgaben automatisch bestimmten Administratoren zuweisen.

On-Demand-Sicherheits-Audits sind ein iterativer Prozess

On-Demand-Sicherheitsaudits sind ein Prozess, der sich ständig wiederholt: QualysGuard entdeckt, analysiert und meldet Schwachstellen und die Unternehmen wenden die empfohlenen Lösungsmaßnahmen an. Dann wiederholen die Benutzer das Verfahren, um sich zu vergewissern, dass die Sicherheitslücken wirklich beseitigt wurden. Wenn ein Unternehmen den Service zum ersten Mal abonniert, wird es diesen Prozess typischerweise mehrfach durchlaufen, bis nur noch wenige Schwachstellen und keine mit hoher Risikostufe verblieben sind. Danach werden die Scans in regelmäßigen Abständen durchgeführt sowie immer dann, wenn ein Rechner- oder Netzwerk-Setting geändert wurde.

VI. SCHLUSS

QualysGuard bietet Unternehmen eine einfache, effektive, effiziente und erschwingliche Möglichkeit, ihre Netzwerke zu sichern. Die Benutzer können unverzüglich, in Echtzeit und on demand auf Übersichten über die Netzwerk-Topologie, detaillierte Reports zu den Sicherheitslücken und validierte Lösungsmaßnahmen zugreifen.

Als Pionier für proaktives Online-Security-Auditing und vertrauenswürdiger Anbieter kann Qualys den Kunden auf einzigartige Weise helfen, umfassende Sicherheit am Netzwerk-Perimeter und innerhalb des Unternehmensnetzwerks zu gewährleisten. Durch seine nicht intrusiven, dem neuesten Stand der Technik entsprechenden Scans und seine fortschrittlichen Reporting-Techniken unterstützt Qualys die Kunden dabei, ihre Netzwerk zu schützen sowie

Branchenrichtlinien und gesetzliche Vorschriften bezüglich Sicherheit und Datenschutz einzuhalten. So verhilft Qualys den Kunden zu der beruhigenden Gewissheit, dass ihre Netzwerke sicher sind.

Um den On-Demand Security Audit Service QualysGuard kostenlos zu testen, besuchen Sie bitte http://www.qualys.com/forms/?lsid=6468.

Für einen kostenlosen Scan besuchen Sie bitte https://freescan.qualys.com.

Für eine Guided Tour besuchen Sie bitte http://qualys.com/products/qgent/seetrybuy/guided/.

VII. ANHANG A : Die Webservice-Architektur von QualysGuard

Die Webservice-Architektur von QualysGuard besteht aus sechs Elementen.
Das nachstehende Schaubild zeigt, wie die Webservice-Architektur von QualysGuard aufgebaut ist und wie der Dienst mit den Internet-Systemen des Kunden kommuniziert.

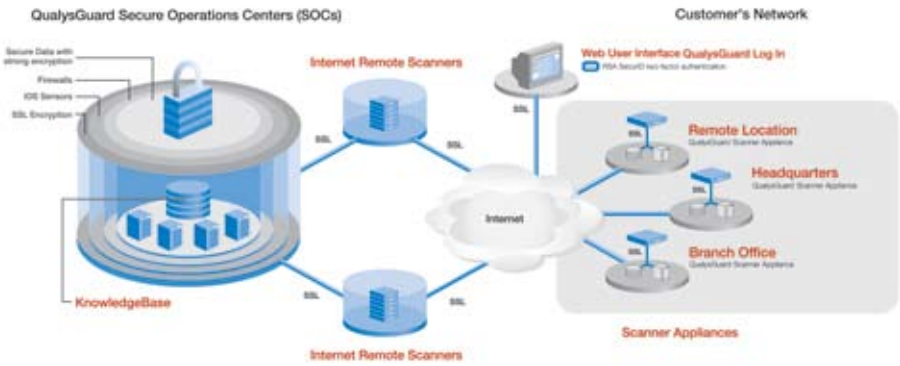

Abb. 8: Die Webservice-Architektur von QualysGuard
Die Architektur von QualysGuard umfasst sechs Elemente: sichere, redundante Qualys Datacenter, Sicherung von Systemen & Kommunikation, mehr als fünf Dutzend QualysGuard Remote-Scanner, QualysGuard Intranet Scanner Appliances, die Qualys KnowledgeBase und die QualysGuard Web-Benutzeroberfläche.

Die QualysGuard Secure Operations Center

Die QualysQuard Secure Operations Center (SOCs) ermöglichen die sichere Speicherung und Verarbeitung der Schwachstellen-Daten und setzen dazu eine n-tier-Architektur aus Anwendungsservern mit Lastverteilung ein. Zu den redundanten SOCs gehört das primäre Operations Center in Santa Clara, Kalifornien, das in einem sicheren Rechenzentrum von Cable & Wireless untergebracht ist und über redundante Systeme und Netzwerkzugang verfügt. Alle Rechner und Racks sind von den anderen Systemen isoliert und in verschlossenen, ausschließlich Qualys vorbehaltenen Sicherheitsäumen untergebracht. Diese können nur von Mitarbeitern von Qualys betreten werden, die sich per Dienstmarke und biometrischer Authentifizierung ausweisen. Qualifizierte Sicherheitstechniker von Qualys überwachen den Betrieb 24x7x365. Im Rahmen des Einstellungsprozesses werden die Referenzen und der Hintergrund aller Mitarbeiter von einer unabhängigen Stelle überprüft; zudem müssen die Mitarbeiter Vertraulichkeitserklärungen unterzeichnen.

Sicherung von Systemen & Kommunikation

Die Sicherheit der Qualys Secure Operations Center wird durch einen erfolgreichen SAS-70-Audit der von Qualys eingesetzten Verfahren und Kontrollen für Datenspeicherung und Datenzugriff dokumentiert. Ein von @stake durchgeführter Audit dokumentiert außerdem die erfolgreiche Prüfung der Qualys-Sicherheitsarchitektur und einen erfolgreichen Penetrationstest. Die Systeme sind mit einer hostbasierten “multi-homed”-Firewall, einem policy-gesteuerten Dateisystem, einem Integritätsprüfungssystem und einem Intrusion Detection-System konfiguriert. Die Server von QualysGuard verbinden sich mit der Report-Datenbank über private (nicht routbare) IP-Adressen. Um sich einloggen zu können, ist Zwei-Faktor-Authentifizierung erforderlich. VeriSign, Inc. stellt digitale Zertifikate sowie ein internes Ticketing-System zur Verfügung, das sicherstellt, dass alle Zertifikate rechtzeitig erneuert werden. Sämtliche Abläufe sind redundant und werden mit Lastverteilung durchgeführt, um die Systemleistung zu optimieren.
Für die gesamte Kommunikation mit den Benutzern setzt QualysGuard https (SSLv3) und starke Kryptographie ein. Klartextkommunikation wird bei keinem Aspekt von QualysGuard unterstützt, einschließlich der Navigation auf der

Datenportabilität, APIs und Integration in Lösungen von Drittanbietern

Die offene, XML-basierte API-Plattform von Qualys ist in der Sicherheitsindustrie einzigartig. Die APIs ermöglichen anderen Programmen den Zugriff auf Kernfunktionen von QualysGuard, einschließlich Scan, Map, Scheduler und Einstellungen. So können die Kunden die Schwachstellen-Audits ihren spezifischen Bedürfnissen anpassen und sie eng in ihre eigenen Sicherheitsprozesse integrieren.

Die Kunden können die Berichte nicht nur über die webbasierte Qualys-Benutzeroberfläche einsehen, sondern ihre Schwachstellen-Daten und Scan-Resultate/-Reports mithilfe der offenen, veröffentlichten API-Spezifikationen von QualysGuard auch manuell oder über ein anderes Programm in XML-Format exportieren.

Diese Leistungsmerkmale werden in einer Reihe aktueller und in der Entwicklung befindlicher Third-Party-Integrationen genutzt. So unterstützt QualysGuard etwa die Produkte der führenden Firewall- und IDS-Hersteller. Die Firewall-Integrationen von QualysGuard überwachen Firewall-Management-Konsolen laufend auf Schwachstellen, die möglicherweise durch Veränderungen der Firewall-Policy unbeabsichtigt verursacht werden. Die IDS-Integrationen von QualysGuard versetzen Unternehmen in die Lage, stattfindende Angriffe automatisch mit tatsächlich bestehenden Schwachstellen im Ziel-Host zu korrelieren, um so die Zahl der Fehlalarme zu reduzieren.

Außerdem integriert sich QualysGuard auch in Vulnerability Remediation-Systeme, um zu gewährleisten, dass Software-Patches, Hotfixes, Konfigurationsänderungen und sonstige Daten zur Schwachstellenbeseitigung automatisch auf die anfälligen Rechner aufgespielt werden. Weitere Informationen zur QualysGuard API finden Sie unter : http://www.qualys.com/docs/APIuser_10282003a.pdf

Benutzeroberfläche, des Starts von Scans oder der Erzeugung von Reports. Für den Login durch Windows- oder Unix-Clients verwendet QualysGuard SSH- (Secure Shell) Software statt unsicherer Alternativen wie telnet und FTP. QualysGuard unterstützt Zwei-Faktor-Authentifizierung mit SecurID und Authentifizierung per Client-Zertifikat.

Auf den QualysGuard-Servern werden keine Benutzerpasswörter gespeichert, und Qualys hat auf Benutzerpasswörter keinerlei Zugriff. Die KnowledgeBase speichert den MD5 Hash des Benutzerpassworts, das bei der Einrichtung des Kontos erzeugt und zur Benutzerauthentifizierung verwendet wird. Wenn ein Benutzer sein Benutzerpasswort für QualysGuard vergisst, kann es nicht wiederhergestellt werden, und es ist kein Zugriff auf die Daten zu früheren Sicherheitsaudits des Kunden mehr möglich. Die Kundendaten werden mit Blowfish-CBC ohne IV verschlüsselt. Der Schlüssel für den Schwachstellen-Report ist 96 Bit lang und wird für jedes Kundenkonto nach dem Zufallsprinzip erzeugt. QualysGuard schreibt diesen Schlüssel niemals in Klartext auf Festplatten und hält ihn nirgends vor, außer im Speicher. Die Audit-Daten werden auf Pro-Kunde-Basis verschlüsselt und gespeichert, sodass niemand die Audit-Daten von Kunden lesen kann – nicht einmal ein Qualys-Administrator, der über vollständige Zugriffsrechte auf die Systeme verfügt.

Die QualysGuard Internet Remote-Scanner

Die Internet Remote-Scanner ermöglichen die schnellsten und effizientesten Perimeter-Scans, die branchenweit verfügbar sind. Fünf Dutzend dieser Scanner sind weltweit an zentralen Stellen stationiert. Die Internet Remote-Scanner sind die Basis für ein verteiltes, inferenzbasiertes Scan-Verfahren, das die Datenerfassung und -verarbeitung bei Sicherheitsaudits beschleunigt. Die Architektur unterstützt drei Elemente:

• Sammlung von Informationen

• Automatisierte, nicht-destruktive Testmechanismen für intelligente Scans, gekoppelt mit einer detaillierten Wissensbank

• Einen Verarbeitungs- und Evaluierungsprozess, der den Vorgehensweisen von Sicherheitsexperten nachempfunden ist

Die Remote-Scanner bestehen aus skriptfähigen Modulen, die das Scan-Verfahren als Multithreaded-Prozess auf der n-tier-Architektur von QualysGuard implementieren, die sich aus Anwendungsservern mit Load-Balancing zusammensetzt. Auf diese Weise kann QualysGuard parallel scannen und Sicherheitsaudits verarbeiten, um optimale Betriebsgeschwindigkeit zu gewährleisten. Das inferenzbasierte Scan-Verfahren von QualysGuard ist ein “Expertensystem”-Ansatz, bei dem Informationen über ein System mit genau den gleichen Methoden gewonnen werden, die auch ein Hacker einsetzen würde. Bei der inferenzbasierten Analyse erstellen die Remote-Scanner zunächst ein Inventar der Protokolle, die auf dem zu prüfenden Rechner zu finden sind. Nach der Erkennung der Protokolle ermittelt der Scan, welche Ports von welchen Diensten genutzt werden, etwa Webservern, Datenbanken oder Mailservern. Sobald feststeht, welche Dienste auf dem Rechner laufen, werden die Schwachstellen ausgewählt, die gemäß der genauen Konfiguration dieses Rechners vorhanden sein könnten, und dementsprechend werden nur die relevanten Tests ausgeführt.

Die Scanner setzen sowohl aktive Techniken zur Erkennung von Betriebssystemen ein (z.B. Banner Grabbing und Binary Grabbing, Ermittlung betriebssystemspezifischer Protokolle, TCP/IP Stack-Fingerprinting) als auch passive Techniken wie etwa Paket-Spoofing. Zum Fingerprinting gehört eine gründliche Prüfung auf subtile Veränderungen bei der Implementierung der RFC-Standards. Eine Service Discovery Engine entdeckt Backdoors, Trojaner und Würmer durch Prüfung von mehr als 120 TCP- und UDP-Diensten, einschließlich solcher, die Non-Default-Ports verwenden oder deren Banner editiert wurden. Ein ähnliches Fingerprinting-Verfahren wird angewandt, um http-Anwendungen zu erkennen, einschließlich Versions-ID, Service-Pack-ID und installierten Patches. QualysGuard korreliert OS- and http-Fingerprinting, um die tatsächlich existierenden Schwachstellen schnell zu finden und False Positives zu minimieren.

Die QualysGuard Intranet Scanner Appliances
Der Intranet Scanner ist ein clientseitiges Plug-In-Gerät, das Sicherheitsaudit-Daten innerhalb der Firewall erhebt und auf sichere Weise mit den QualysGuard Remote-Scannern kommuniziert. Er ist mit einem speziell gehärteten Betriebssystem-Kernel ausgerüstet, um Shell-Code- und Buffer-Overflow-Angriffe zu verhindern. Auf dem Intranet Scanner laufen keine zum Netzwerk hin exponierten Dienste oder Daemons. Der Setup dauert nur wenige Minuten: Über ein LCD-Panel und eine Tastatur werden einfach der Benutzername, die IP-Adresse und die DNS- und Proxy-Daten eingegeben. Das Gerät wird von Qualys virtuell über das Internet verwaltet. Zur Kommunikation wird starke Verschlüsselung und SSLv3 via Port 443 verwendet. Das Gerät kommuniziert mit QualysGuard, um automatisch Software-Updates und neue Schwachstellensignaturen herunterzuladen und Job Requests für Netzwerkerkennung und Scans zu verarbeiten.

Der Intranet Scanner speichert keine Scan-Resultate, vielmehr werden sämtliche Daten sicher verschlüsselt, an die redundanten Rechenzentren von Qualys übertragen und dort gespeichert.

Die QualysGuard KnowledgeBase
Die KnowledgeBase ist das Kronjuwel der Architektur von QualysGuard. Sie enthält die Informationen, die die Grundlage für die umfassenden On-Demand-Audits der Netzwerksicherheit, das Schwachstellenmanagement und die Schwachstellenbeseitigung bilden. Qualys aktualisiert die KnowledgeBase täglich mit Signaturen für neue Sicherheitslücken, validierten Patches, Fixes für False Positives und sonstigen Daten, um die Effektivität seines Webservices für Sicherheitsaudits laufend zu optimieren. Im September 2006 umfasste die KnowledgeBase Signaturen für mehr als 5.100 Sicherheitslücken.

Alle Abonnenten von QualysGuard profitieren automatisch von den Updates der KnowledgeBase, da die Qualys Remote-Scanner und Intranet Scanner stets die neueste Version der KnowledgeBase nutzen. Die Anwender des Webservices QualysGuard testen ihre Systeme also stets auf die allerneuesten Sicherheitslücken.

Die Web-Benutzeroberfläche von QualysGuard
Die Web-Benutzeroberfläche gewährleistet, dass sich der Webservice QualysGuard leicht bedienen lässt. Mit jedem Standard-Webbrowser können Sie durch die Benutzeroberfläche von QualysGuard navigieren, Scans starten und die Audit-Daten in den Berichten prüfen. Für Kommunikationssicherheit sorgt https-Verschlüsselung (SSLv3). Für den Login durch Windows- oder Unix-Clients setzt QualysGuard SSH- (Secure Shell) Software ein, anstelle von unsicheren Optionen wie telnet und FTP. QualysGuard unterstützt Zwei-Faktor-Authentifizierung via SecurID sowie Authentifizierung mit Client-Zertifikat. Über einen Webbrowser steuern die Benutzer den vierstufigen Prozess des Webservices QualysGuard:

• Erkennung – dynamische Identifizierung von Netzwerkgeräten

• Audit – automatische Analyse der Sicherheitsanfälligkeit

• Reporting – praktisch nutzbare Berichterstattung mit Trendanalysen

• Reparatur – Verfolgung der Schwachstellen und Installation von Patches

VIII. ANHANG B: Glossar

DHCP Dynamic Host Configuration Protocol – ein Kommunikationsprotokoll, mit dessen Hilfe Netzwerkadministratoren die Zuweisung von IP-Adressen (Internet-Protocol-Adressen) im Unternehmensnetzwerk zentral vornehmen und automatisieren können.

Exploit Ein Angriff auf eine Netzwerkschwachstelle, die potenziell zur Kompromittierung der Netzwerksicherheit führt.

Exhaustive Search (erschöpfende Suche) Ein Algorithmus, der eine Lösung für ein Problem findet, indem er jede Möglichkeit erschöpfend ausprobiert.

Fully Qualified Domain Name Ein Fully Qualified Domain Name (FQDN) ist derjenige Teil eines Internet Uniform Resource Locators (URL), der das Serverprogramm, an das eine Internet-Anfrage adressiert ist, vollständig identifiziert. Zum FQDN gehören der Second Level Domain Name (wie etwa „meinefirma.com“) sowie alle anderen Level („www.meinefirma.com“ oder „www1.meinefirma.com“).

IP Das Internet Protocol (IP) ist das Verfahren bzw. Protokoll, mit dessen Hilfe Daten im Internet von einem Rechner an einen anderen geschickt werden können. Jeder Computer (manchmal auch als Host bezeichnet) im Internet hat mindestens eine IP-Adresse, die ihn unter allen anderen Rechnern im Internet eindeutig identifiziert.

IP-Adresse In der heute am meisten verbreiteten Version des Internet Protocol – Version 4 – ist eine IP-Adresse eine 32-Bit-Zahl, die jeden Sender oder Empfänger von Informationen identifiziert, die in Form von Paketen über das Internet übertragen werden. Eine IP-Adresse wird normalerweise dezimal in vier Blöcken geschrieben, die jeweils acht Bit repräsentieren und durch Punkte voneinander getrennt sind (z.B. 210.29.32.112). Jede IP-Adresse setzt sich aus zwei Teilen zusammen: Der eine Teil bezeichnet ein bestimmtes Netzwerk im Internet; der andere, “lokale” Teil bezeichnet den jeweiligen Rechner in diesem Netzwerk (dabei kann es sich um einen Server, eine Workstation oder ein anderes Gerät handeln). Im Internet selbst – d.h. zwischen den Routern, die die Pakete auf ihrem Weg durchs Internet von einem Punkt an den nächsten schicken – wird nur der Netzwerkteil der Adresse registriert. Bei IP-Adressen der Klasse A bilden die lokalen und die Netzwerkzahlen eine IP-Adresse der Form “network.local.local.local”. Bei einer IP Adresse der Klasse C bilden sie eine Adresse der Form “network.network.network.local”. Die Zahlenversion der IP-Adresse kann von einem oder mehreren Namen repräsentiert werden (und wird es in der Regel auch); diese Namen werden als Fully Qualified Domain Names bezeichnet.

Internet Remote-Scanner Ein Software-Tool, das schnelles, effizientes externes Scannen (Perimeter-Scannen) ermöglicht. Internet Remote-Scanner sind auf Qualys-Servern in Qualys Secure Operations Centern implementiert. Ihre inferenzbasierte Scanning-Engine gewährleistet eine äußerst präzise Erkennung von Sicherheitslücken und Eliminierung von Fehlalarmen.

Intranet Scanner Appliance Geräteversion des Internet Scanners, die das Auditing interner Netzwerke ermöglicht. Die Scanner Appliance arbeitet vollautomatisch und nutzt dabei jeweils die aktuellsten Schwachstellensignaturen. SSL gewährleistet sichere Kommunikation.

Intrusion Detection Analyse der Netzwerksicherheit “von innen” mittels Software- oder Hardware-Tools. Diese Tools untersuchen entweder Low-Level-Daten von Netzwerkpaketen (“netzwerkbasiertes IDS”) oder Betriebssystem- bzw. Dateisystemaufrufe (hostbasiertes IDS) auf ungewöhnliche Datenmuster oder andere unautorisierte Aktivitäten.
Netzwerk-Sicherheitsanalyse Verfahren, mit dem geprüft wird, ob ein Unternehmensnetzwerk vor Angriffen geschützt ist, die von innerhalb oder außerhalb des Unternehmens gestartet werden.

Netzwerkschwachstelle Eine Schwachstelle in einem Rechner, Netzwerkgerät, einer Software-Anwendung oder einer anderen Komponente, die es ermöglicht, diese Komponente zu anderen Zwecken als den vorgesehenen zu nutzen.

Port-Nummer In TCP/IP-basierten Netzwerken ein Endpunkt einer logischen Verbindung zwischen zwei IP-adressierbaren Geräten. Eine Port-Nummer identifiziert oft den speziellen TCP-basierten Dienst, der über die Verbindung läuft. Z.B. wird Port 80 typischerweise für http-Verkehr verwendet.

TCP Da IP ein kommunikationsloses Protokoll ist, gibt es keine kontinuierliche Verbindung zwischen den miteinander kommunizierenden Endpunkten, und jedes Paket, das im Internet unterwegs ist, wird als unabhängige Dateneinheit betrachtet, die keine Beziehung zu irgendeiner anderen Dateneinheit hat. Das Transmission Control Protocol sorgt bei der Übertragung im Internet für den korrekten Transport der Datenpakete, sodass diese in der richtigen Reihenfolge ankommen.

Schwachstellen-Analyse Analyse der Netzwerksicherheit “von außen” mithilfe bewusster Versuche, Sicherheitslücken zu identifizieren. Dabei werden bekannte Angriffe auf kontrollierte Weise eingesetzt.

Schwachstellen-Scanner Ein Software-Tool, das die Ermittlung der Schwachstellen im Zielnetzwerk auslöst.

IX. ÜBER QUALYS

Qualys, Inc. ist der führende Anbieter von On-Demand-Lösungen für das Management von Sicherheitslösungen und Compliance-Anforderungen. Qualys ist das einzige Security-Unternehmen, das diese Lösungen über eine umfassende Software-as-a-Service-Plattform bereitstellt. Mit QualysGuard® können Unternehmen die Sicherheit ihrer Netzwerke erhöhen und automatisierte Sicherheits-Audits durchführen, um die Einhaltung von Richtlinien und Vorschriften zu gewährleisten. Als skalierbare, offene Plattform gibt QualysGuard den Partnern die Möglichkeit, ihre eigenen Managed Security Services auszubauen und ihre Consulting-Dienste zu erweitern. Die On-Demand-Lösungen von Qualys können innerhalb von Stunden an jedem Ort der Welt bereitgestellt werden und geben den Kunden einen sofortigen Überblick über ihren Sicherheits- und Compliance-Status. QualysGuard ist die meistgenutzte On-Demand-Sicherheitslösung der Welt und führt pro Jahr mehr als 150 Mio. IP-Audits durch.

Für weitere Informationen besuchen Sie bitte www.qualys.com.

QUALYS®
www.qualys.com

USA – Qualys, Inc. • 1600 Bridge Parkway, Redwood Shores, CA 94065 • T: 1 (650) 801 6100 • sales@qualys.com
UK – Qualys, Ltd. • 224 Berwick Avenue, Slough, Berkshire, SL1 4QT • T: +44 (0) 1753 872101
Germany – Qualys GmbH • München Airport, Terminalstrasse Mitte 18, 85356 München • T: +49 (0) 89 97007 146
France – Qualys Technologies • Maison de la Défense, 7 Place de la Défense, 92400 Courbevoie • T: +33 (0) 1 41 97 35 70
Japan – Qualys Japan K.K. • Pacific Century Place 8F, 1-11-1 Marunouchi, Chiyoda-ku, 100-6208 Tokyo • T: +81 3 6860 8296
Hong Kong – Qualys • 2/F, Shui On Centre, 6-8 Harbour Road, Wanchai, Hong Kong • T: +852 3163 2888

ON DEMAND SECURITY