Schwachstellenmanagement: Eine Checkliste für Käufer

Wichtige Fragen vor dem Kauf einer Lösung für Schwachstellenmanagement

Schwachstellenmanagement ist die systematische Aufdeckung und Beseitigung von Schwachstellen in Netzwerken. Die Entscheidung für eine Schwachstellenmanagement-Lösung ist ein bedeutender Schritt zum Schutz Ihres Unternehmens und Ihrer Daten. Ohne bewährte, automatisierte Technologie zur präzisen Ermittlung und Korrektur von Schwachstellen kann kein Netzwerk der täglichen Flut neuer Schwachstellen, welche die Sicherheit ihrer Systeme bedrohen, widerstehen. Um Ihnen die Kaufentscheidung zu erleichtern, hat Qualys diese 12 Punkte umfassende Checkliste zusammengestellt, die Ihnen helfen wird festzustellen, welche Lösung für Ihr Unternehmen am besten geeignet ist.

12 Springende Punkte

☐Architektur

Wie wird die Schwachstellenmanagement-Lösung bereitgestellt?

Müssen Sie irgendwelche Software oder Hardware installieren und warten, oder wird die Software als Service (SaaS) bereitgestellt, sodass Sie sich einfach nur über einen Webbrowser in Ihr Konto einloggen müssen, um einen Scan zu starten? Eine Lösung, bei der Sie sich selbst um Installation, Updates, Hardware, Datenbanksicherheit etc. kümmern müssen, verursacht letztlich Kosten, die in der Regel weit über den reinen Kaufpreis der Software hinausgehen. Außerdem kann es sein, dass für den laufenden Betrieb zusätzliche Arbeitskraft benötigt wird.

☐ Bietet die Lösung eine grafische Benutzeroberfläche?

Einige Lösungen – insbesondere ältere, zweitklassige oder „kostenlose“ – bieten lediglich Kommandozeilenschnittstellen.Diese können schwer bedienbar sein , und bieten nur eingeschränkte Möglichkeiten zur Anpassung an spezifische Kundenwünsche (oder Zugangskontrollen). Informieren Sie sich, wie die Lösung bereitgestellt wird, und testen Sie sie vor dem Kauf.

☐ Müssen Sie auf allen Geräten in Ihrem Netzwerk Agenten ausführen?

Bei softwarebasierten Produkten für Schwachstellenmanagement kann es sein, dass Sie auf jedem zu scannenden System Agenten installieren und regelmäßig aktualisieren müssen. Suchen Sie nach einer Architektur, für deren Betrieb weder Agenten noch andere Software erforderlich sind, außer einem üblichen, SSL-fähigen Webbrowser für den Zugriff auf die Benutzeroberfläche.

☐ Müssen Sie für das Produkt eine Datenbank betreiben?

Bei softwarebasierten Schwachstellenmanagement-Produkten müssen Sie eventuell eine Datenbank installieren und betreiben, in der die Informationen für das Schwachstellenmanagement gespeichert werden. Bei einer SaaS-Architektur ist dies nicht notwendig.

☐ Warum sollten Sie für das Schwachstellenmanagement eine SaaS-Lösung in Erwägung ziehen?

Wenn es um eine Anwendung wie Schwachstellenmanagement geht, ist eine SaaS-Lösung für die meisten Unternehmen sinnvoller als ein Software-Produkt. Eine SaaS-Lösung ist einfacher zu implementieren und zu verwalten, kann veränderliche Geschäftsanforderungen flexibler unterstützen, und die Kosten sind niedriger und besser abschätzbar. Außerdem sind SaaS-Lösungen skalierbar, zwingen Sie nicht zum Abschluss eines langfristigen Lizenzvertrags und sind benutzerfreundlicher und zuverlässiger.

Sicherheit

☐ Welches Sicherheitsmodell wird angewandt, um die Lösung zu schützen?

Außerordentlich wichtig ist, dass die Schwachstellenmanagement-Lösung selbst sicher ist, insbesondere deswegen, weil sie kritische Daten über Netzwerk-Assets und mögliche Schwachstellen verwaltet. Bei softwarebasierten Lösungen sind Sie selbst für die Sicherheit verantwortlich – und der Schutz solcher Systeme und Informationen kann eine komplexe Aufgabe sein. Bei einer gehosteten SaaS-Lösung kümmert sich dagegen der SaaS-Anbieter um die Sicherheit. Vergewissern Sie sich, dass die SaaS-Lösung Ihre sensiblen Schwachstellendaten durchgehend schützt, und verschiedene proaktive Kontrollen, basierend auf anerkannten Standards einsetzt, um alle Ebenen der Anwendung zu schützen.

☐ Wie wird die Lösung physikalisch geschützt?

Stellen Sie sicher, dass Ihr Anbieter diese Frage beantwortet. Wie bereits erwähnt, müssen Sie bei herkömmlichen Software-Lösungen alle Aufgaben zur Sicherung der Lösung selbst übernehmen. Lösungen auf SaaS-Basis nehmen Ihnen diese Arbeit dagegen ab. So wird etwa der Service QualysGuard von Secure Operations Centern aus durchgeführt, die jährlich mit Erfolg nach dem Standard SAS70 Typ II zertifiziert werden. Die Rechner und Racks von QualysGuard sind in verschlossenen Sicherheitsräumen untergebracht, die ausschließlich Qualys vorbehalten sind und nur von Personen betreten werden können, die sich per Dienstmarke und biometrischer Authentifizierung ausweisen. Der physikalische Zugang ist dedizierten Mitarbeitern von Qualys vorbehalten, deren Referenzen und Hintergrund von einer unabhängigen Stelle überprüft wurden und die Vertraulichkeitserklärungen unterzeichnet haben. Die Systeme sind durch eine host-basierte Firewall, ein policy-basiertes Datei- und Integritätsprüfungssystem sowie eine IDS-Architektur geschützt. Das Personal überwacht ständig sämtliche Systeme und führt die geeigneten Korrekturen und Gegenmaßnahmen durch. Der Zugriff auf die Systeme ist nur dedizierten Mitarbeitern von Qualys möglich, die sich auf kritischen Servern per Zwei-Faktor-Authentifizierung einloggen müssen. Alle 24 Stunden werden vollständige Backups

auf einen Standby-Server sowie auf verschlüsselte Bänder geschrieben. Die Rotation der Backup-Bänder wird extern von einem Drittanbieter durchgeführt.

☐ Wie schützt die Schwachstellenmanagement-Lösung die Übertragung der Schwachstellendaten?

Vergewissern Sie sich bei der Auswahl einer SaaS-Lösung, dass alle Interaktionen https-(SSLv3) Verbindungen mit mindestens AES 128-bit-Verschlüsselung vom Webbrowser des Anwenders zu dem System erfordern, das den Scan ausführt. Achten Sie genau darauf, dass bei der Navigation auf der Benutzeroberfläche, beim Start von Scans oder der Erzeugung von Berichten keine Klartext-Kommunikation verwendet wird. Beim Login sollte das System die Authentifizierung mittels Benutzername/Passwort sowie optional eine Zwei-Faktor-Authentifizierung (SecureID oder Zertifikate) unterstützen. Außerdem sollten die Benutzerpasswörter auf keinen Servern gespeichert werden, und der Lösungsanbieter sollte keinen Zugang zu diesen Passwörtern haben.

☐ Welche Zugangskontrollen sind in die Lösung integriert?

Vergewissern Sie sich, dass die Schwachstellenmanagement-Lösung eine hierarchische Zugangskontrolle auf Basis von Benutzerrollen und Privilegstufen bietet. Ein Best-Practice-Ansatz sieht eine rollenbasierte Zugangskontrolle für fünf unterschiedliche Rollen vor: Manager (umfassende Kontrolle), Unit Manager (Kontrolle über einen Geschäftsbereich), Scanner (darf Assets scannen, sofern vom Unit Manager oder Manager gestattet), Reader (darf nur Berichte erstellen) und Contact (hat keinen Systemzugriff, darf nur Warnmeldungen per E-Mail versenden). Für jede Rolle sollten zusätzliche Konfigurationseinstellungen zur Vergabe granularer Berechtigungen möglich sein.

☐ Wie schützt die Lösung die Daten aus den Schwachstellen-Scans?

Achten Sie darauf, dass die Schwachstellendaten verschlüsselt und in einer separaten „Instanz“ einer geschützten Datenbank sicher gespeichert werden. Der Verschlüsselungsalgorithmus, die Schlüssel und der Entschlüsselungsprozess müssen robust sein – nichts davon darf in Klartext auf Platten geschrieben oder irgendwo gespeichert werden, außer vorübergehend im Systemspeicher während der Authentifizierungs-/Entschlüsselungsphase beim Login.

Skalierbarkeit / Benutzerfreundlichkeit

☐ Was bedeutet die Aussage, dass eine Schwachstellenmanagement-Lösung skalieren kann?

Bei einem Produkt auf Software-Basis wird die Skalierbarkeit durch die Infrastruktur begrenzt, die Sie erwerben, betreiben und pflegen, um das Produkt nutzen zu können. Stellen Sie sicher, dass Sie alle eventuellen Beschränkungen kennen. Eine SaaS-Lösung bietet unbegrenzte Skalierbarkeit. Sie kann selbst in den größten Netzwerkumgebungen externe Netzwerkerkennungen und Schwachstellenscans ausführen. Sie sollten die Möglichkeit haben, jedes Gerät mit einer IP-Adresse zu scannen – und das jeden Tag.

☐ Wie skaliert die Schwachstellenmanagement-Lösung, um sich an die Größe meines Netzwerks anzupassen?

Ohne intelligentes Scannen sind Netzwerkerkennung und Schwachstellenscans in großen Netzwerken nicht durchführbar. Vergewissern Sie sich, dass das System intelligentes Scannen ermöglicht, damit es in der Lage ist, die Karte, die es von Ihren Netzwerkgeräten und deren Betriebssystemen anlegt, mit allen bekannten Schwachstellen, die jedes einzelne System betreffen können, zu korrelieren. Das gewährleistet maximale Geschwindigkeit und Qualität bei der Schwachstellenanalyse in Ihrem Netzwerk und minimiert zugleich den Netzwerk-/Host-Traffic.

☐ Ist die Schwachstellenmanagement-Lösung vollautomatisiert?

Manuelle Netzwerkerkennung (oder Mapping) und manuelles Scannen sind zeitaufwändig und unpraktisch - deshalb ist Automatisierung ein Muss. Wählen Sie eine Lösung, mit der Sie Ihr gesamtes Netzwerk jederzeit auf Sicherheitsrisiken überprüfen und unverzüglich feststellen können, inwieweit Sie externe Standards und Kontrollen einhalten. Produkte für Schwachstellenmanagement, die zu viel manuelle Intervention benötigen, sind anfällig für menschliches Versagen, erbringen oft ungenaue Ergebnisse und verschwenden Zeit und Ressourcen.

☐ Wie viel Support steht für die Lösung zur Verfügung?

Probleme mit Schwachstellen können zu jeder Tages- und Nachtzeit auftreten – vergewissern Sie sich deshalb, dass die Lösung 24x7x365-Support bietet. Der Support sollte Hilfe per Telefon und E-Mail sowie eine umfassende Online-Dokumentation, technische Hinweise und häufig gestellte Fragen (FAQs) einschließen. Achten Sie darauf, dass die Versprechen, die der Anbieter hinsichtlich des Supports abgibt, in einem Service Level Agreement (SLA) festgeschrieben sind.

☐ Schließt der Support auch Schulungen ein?

Vergewissern Sie sich, dass Sie zu Ihrer Schwachstellenmanagement-Lösung alle erforderlichen Informationen erhalten und dass der Lösungsanbieter Schulungs- und Zertifizierungsprogramme bietet (live und auf Video). Im Idealfall sollte all dies im Abonnement eingeschlossen sein.

☐ Wie ist die Lösung mit anderen Anwendungen integriert?

Interoperabilität mit Ihren anderen IT-Sicherheitsanwendungen ist unerlässlich. Die Lösung sollte einen integrierten, spezifisch angepassten Scan- und Korrektur-Workflow mit bestehenden Callcenter-/Helpdesk-Systemen wie z.B. Remedy AR System unterstützen. Ebenso sollte sie führende SIM-/SEM-Lösungen wie Symantec SESA V2 und Patch-Management-Systeme wie McAfee Remediation Manager sowie das Cisco Security Monitoring, Analysis and Response System unterstützen.

Genauigkeit / Leistung

☐ Wie präzise ist die Schwachstellenmanagement-Lösung?

Wenn die Lösung eine Schwachstelle übersieht, die Hacker ausnutzen um Ihr Netzwerk zu kompromittieren, dann lautet die Antwort auf diese Frage: „Nicht genau genug“. Wenn die Lösung fälschlicherweise Probleme meldet, die gar keine sind (d.h. „False Positives” meldet), dann werden Sie mit ungültigen Daten überhäuft und verlieren wertvolle Zeit. Viele Anbieter behaupten, dass ihre Produkte überragende Genauigkeit bieten; fordern Sie Nachweise für solche Behauptungen.

☐ Woher bezieht die Schwachstellenmanagement-Lösung ihre Informationen über Schwachstellen?

Ihre Scan-Lösung sollte auf die umfassendste Schwachstellen-Datenbank der Branche zurückgreifen und die darin enthaltenen Informationen mit CERT, Symantec DeepSight, Security Focus, Secunia, Mitre und Seclists korrelieren. Außerdem sollte die Lösung auch die Security Bulletins von Microsoft und anderen führenden Software-Anbietern einbeziehen.

☐ Wie aktualisiert die Lösung ihre Datenbank um die neuesten Schwachstelleninformationen?

Bevor Signaturen zur Erkennung von Schwachstellen freigegeben und Ihnen als Kunde zur Verfügung gestellt werden, müssen sie gründlich getestet werden. Bei Open-Source-Lösungen gibt es oft kein formales Test- und Abnahmeverfahren, und so kann es vorkommen, dass Sie fehlerhafte Signaturen verwenden. Außerdem müssen Signaturen zu hoch riskanten Schwachstellen innerhalb von Stunden nach der Veröffentlichung der Schwachstellen aktualisiert und freigegeben werden. Vergewissern Sie sich, dass der Anbieter über eine zuverlässige Wissensdatenbank verfügt, die mehrmals täglich um neue Schwachstellen-Checks sowie Erweiterungen für bereits bestehende Signaturen aktualisiert wird. Entscheidend ist, dass der gesamte Update-Prozess vollautomatisch und für Sie als Kunden komplett transparent abläuft.

☐ Können Ihre Scan-Policies neue Schwachstellensignaturen automatisch mit einbeziehen?

Es ist sehr wichtig, dass die Schwachstellensignaturen automatisch aktualisiert werden – nicht nur, um Ihr Netzwerk vor den neuesten Bedrohungen zu schützen, sondern auch, um zu gewährleisten, dass die unternehmenseigenen Policies für Sicherheitsscans kontinuierlich durchgesetzt werden. Vergewissern Sie sich, dass die Lösung dies ohne manuelle Intervention erledigt.

☐ Wie zeigt die Lösung Schwachstellen an?

Sie sollten sicherstellen, dass Sie laufend über neue Schwachstellen informiert werden, von denen Ihr Netzwerk betroffen sein kann. Die Lösung sollte eine Liste der neuesten Schwachstellen anzeigen, die in die Wissensdatenbank aufgenommen wurden. Zu jeder Schwachstelle sollten eine detaillierte Beschreibung sowie Informationen zur Beseitigung gegeben werden. Im Idealfall sollte die Liste interaktiv sein und den Benutzern die Möglichkeit geben, sie nach CVE ID, Stichwort oder Titel, Anbieterverweis etc. zu durchzusuchen.

Netzwerkerkennung / Mapping

☐ Ist Netzwerkerkennung / Mapping Bestandteil der Lösung?

Bevor ein Netzwerk auf Schwachstellen gescannt wird, muss man wissen, wonach überhaupt gesucht werden soll. Schwachstellen sind spezifischer und nicht allgemeiner Natur – sie betreffen eine bestimmte Plattform, ein bestimmtes Betriebssystem und Service-Pack, eine bestimmte Applikation und Versionsnummer, eine bestimmte Patch-Version usw. Stellen Sie sicher, dass die Lösung sämtliche Systeme in Ihrem Netzwerk abbilden und diese Mapping-Informationen mit den Schwachstellen korrelieren kann, um so den Scan-Prozess zu verbessern und zu beschleunigen. Ein genaues Inventar ermöglicht es, Korrekturen zu priorisieren, und gewährleistet, dass die richtigen Patches ausgewählt und installiert werden. Außerdem gewährleistet der Erkennungs-/Mapping-Prozess auch, dass wirklich alle Geräte in Ihrem Netzwerk abgedeckt werden.

☐ Können mit der Lösung alle Geräte in meinem Netzwerk leicht identifiziert werden? .

Manuell durchgeführt, könnte diese Aufgabe äußerst mühselig werden. Stellen Sie sicher, dass die Lösung, für die Sie sich entscheiden, den gesamten Prozess automatisiert. Sie sollten einfach nur eine IP-Adresse oder einen Adressbereich eingeben müssen, und das System sollte dann alle Geräte in Ihrem Netzwerk schnell identifizieren.

☐ Welche Informationen liefert Mapping über das Netzwerk?

Die automatisierte Mapping-Funktionalität der Lösung sollte alle mit ihrem Netzwerk verbundenen Geräte finden. Ein kleiner Footprint-Scan muss das Betriebssystem des Geräts und den Gerätetyp (z. B. Router, Switch, Zugangspunkt etc.) genau identifizieren. Im Idealfall wird die Netzwerkerkennung noch weitere Informationen liefern, so etwa den DNS-Namen, den NetBIOS-Namen und den Zeitpunkt, zu dem das Gerät zuletzt gescannt wurde.

☐ Kann das System „Rogue“-Geräte entdecken?

Die beim Mapping erstellte Netzwerkübersicht sollte alle „neuen” Geräte anzeigen, ob sie nun autorisiert oder nicht autorisiert („rogue“) sind. Auf diese Weise gewinnen Sie ein umfassendes Bild von Ihrem Netzwerk.

☐ Kann die Lösung die Mapping-Daten mit Ihren Geschäftsbereichen korrelieren?

Mapping-Daten sollten nicht in einem technischen Vakuum existieren. Vielmehr sollte Ihnen die Lösung erlauben, das Netzwerkinventar nach logischen Gruppen oder nach Geschäftsbereichen aufzuteilen – mit granularen Informationen über die Hardware, Software, Applikationen, Dienste und Konfigurationen. Zugangskontrollen geben einem Geschäftsbereich die Möglichkeit, nur die eigenen Geräte zu inventarisieren, auf Schwachstellen zu scannen und entsprechende Berichte zu erzeugen. Außerdem trägt die Verknüpfung von Mapping-Daten mit Geschäftsbereichen dazu bei, die Resultate praktisch verwertbar zu machen.

Scannen

☐ Worauf sollten Sie bei einem Schwachstellen-Scanner besonders achten?

Ziel des Scannens ist es, Schwachstellen im Netzwerk aufzudecken und zu korrigieren. Ein Scanner prüft die Wirksamkeit der Sicherheitsrichtlinien und -kontrollen in Ihrer Infrastruktur. Zu diesem Zweck muss er die IP-Geräte, -Dienste und -Applikationen systematisch auf bekannte Sicherheitslücken testen und analysieren. Außerdem muss er einen Bericht über die gefundenen echten Schwachstellen liefern und angeben, was Sie in welcher Reihenfolge korrigieren müssen, ohne dabei die Stabilität der Geräte zu gefährden.

☐ Müssen Sie jeden Scan manuell starten?

Neben manueller Steuerung sollte Ihnen die Lösung auch die Möglichkeit geben, Scans vorab zu planen, die dann automatisch ohne manuelle Intervention ausgeführt werden.

☐ Unterstützt die Lösung externes und internes Scannen ... und das so, dass alle Daten an einem Ort zu finden sind und Ihre Firewall nicht durchlöchert wird?

Diese Optionen beziehen sich auf Scan-Geräte, die sich außerhalb der Firewall befinden, im Gegensatz zur Konfiguration innerhalb der Firewall. Die Lösung muss über eine sichere Methode zur Durchführung von Perimeter-Scans für extern erreichbare IPs verfügen. Sie muss das gesamte Netzwerk „verstehen“ und sollte in der Lage sein, Domänen abzubilden und IPs hinter der Firewall zu scannen. Die für interne Scans benötigten Geräte müssen angriffssicher sein: Sie müssen über einen gehärteten Betriebssystemkern verfügen und dürfen keine Hintergrunddienste oder Daemons ausführen, die zum Netzwerk hin exponiert sind. Die internen Geräte sollten automatisch Software-Updates und neue Schwachstellensignaturen herunterladen und Job-Requests verarbeiten – all das auf sichere und zuverlässige Weise.

☐ Ermöglicht die Lösung Scannen in „Turbogeschwindigkeit“?

Große Unternehmen können von einer Schwachstellenmanagement-Lösung profitieren, die die Scan-Geschwindigkeit optimiert, ohne das Netzwerk zu überlasten. So verfügt beispielsweise QualysGuard über eine Funktionalität zur Scanner-Parallelisierung, dank derer die Scan-Geschwindigkeit bis auf das Vierfache gesteigert werden kann, ohne dass dadurch die Genauigkeit der Scans abnimmt. Diese Funktionalität verteilt einen Scanvorgang auf mehrere Scanner-Appliances in einer bestimmten Asset-Gruppe. Nach Abschluss werden die Ergebnisse in einem einzigen Bericht zusammengefasst.

☐ Was, wenn Sie Netzwerke Ihrer Geschäftspartner scannen wollen?

Elektronische Geschäftsprozesse sind häufig mit denen von Geschäftspartnern verflochten. Leider können die Netzwerke von Partnern jedoch ein Kanal für Schwachstellen-Exploits sein. Deswegen ist es wichtig, alle diese Netzwerke zu scannen. Einige Regularien für Security-Compliance schreiben vor, dass die Partner Scans nachweisen müssen – oder Ihr Unternehmen muss dies für sie tun. Ihre Lösung sollte so flexibel sein, dass Sie alle aus dem Internet erreichbaren IP-Adressen oder IP-Bereiche

schnell scannen und die Lösung somit in den Netzwerken Ihrer Partner genauso einsetzen können wie in Ihren eigenen.

☐ Unterstützt der Scanner „Trusted Scanning“?

Die Authentifizierungsfunktionalität von Windows ermöglicht Windows Trusted Scanning. Deshalb muss Ihre Schwachstellenmanagement-Lösung Trusted Scanning für Windows voll unterstützen, ebenso wie für UNIX, Oracle und SNMP-Systeme. Auf diese Weise können Sie mehr Informationen über die Systeme , was wiederum dem Scanner die Möglichkeit gibt, mehr Schwachstellen zu finden. Für Compliance-Scans zur Richtlinienüberprüfung ist Trusted Scanning obligatorisch.

Reporting

☐ Welche Arten von Berichten bietet die Lösung?

Die Berichterstattung ist bei Schwachstellenmanagement-Lösungen eine ausgesprochen wichtige Funktionalität, weil sie die Grundlage für die Maßnahmen zur Schwachstellenbeseitigung bildet. Netzwerkscanner nützen wenig, wenn Ihnen die Reports nicht helfen, Ihre Sicherheits- und Compliance-Ziele zeitgerecht und kosteneffektiv zu erreichen. Die Reporting-Funktionalität muss sowohl flexibel als auch umfassend sein. Die Berichte sollten folgende Bestandteile enthalten: Netzwerk-Assets (IPs und/oder Asset-Gruppen), Diagramme und Tabellen, die einen Gesamtüberblick vermitteln und den Sicherheitsstatus des Netzwerks anzeigen, Trendanalysen, detaillierte Informationen über entdeckte Schwachstellen sowie Filter- und Sortierungsoptionen für spezifisch angepasste Sichten auf die Daten.

☐ Welche vorgefertigten Out-of-the-Box-Berichte liefert die Lösung?

Die Lösung sollte Default-Berichte bieten, die den typischen Anforderungen der meisten Unternehmen entsprechen. Wichtig sind auch Scorecard-Reports, weil diese Ihnen helfen können, z.B. Schwachstellen innerhalb von Asset-Gruppen, ignorierte Schwachstellen, die meist verbreiteten Schwachstellen und die anfälligsten Hosts rasch zu isolieren, und Ihnen einen Patch-Report liefern. Halten Sie Ausschau nach Lösungen, die Executive-Level-Reports, technische Reports, Risikomatrix- und SANS20-Reports bieten. Wenn Sie spezifische Compliance-Anforderungen erfüllen müssen (z.B. PCI DSS), fragen Sie nach vorgefertigten Berichten, die diesen Anforderungen gerecht werden.

☐ Welche Optionen für Templates und spezifisch angepasste Berichte bietet die Lösung?

Die Schwachstellenmanagement-Lösung darf nicht nur Default-Berichte bieten, sondern muss flexibel genug sein, um Schwachstellendaten in jeder von Ihnen gewünschten Form darstellen zu können. Sie sollten den Detailgrad der Berichte an die Bedürfnisse unterschiedlicher Adressaten anpassen können. Typischerweise verwendete Optionen sind: Schweregrad der Schwachstelle, Art oder spezifische ID (oder CVE), Asset-Gruppe (z.B. geografischer Ort, Systemfunktion, Stelle im Netzwerk), IP-Adresse, Dienst oder Port, Status (z.B. neu, aktiv, korrigiert, wieder eröffnet), Kategorie (z.B. webbasiert, Datenbank, DNS, RPC, SMB, TCP/IP usw.) sowie unterstützende Grafiken, um die gewählten Datensätze darzustellen.

☐ Wie werden die Schwachstellen in den Berichten klassifiziert?

Die Lösung sollte Schweregradwerte zuweisen, die auf Industriestandards wie CVE und NIST basieren. Die Schwachstellen sollten klassifiziert werden, um die unterschiedlichen Schweregrade kenntlich zu machen. Zum Beispiel: Stufe 1 = niedrig, Stufe 2 = mittel, Stufe 3 = hoch, Stufe 4 = kritisch und Stufe 5 = dringend. Zusätzlich sollte die Lösung eine Bewertung anhand des Standards Common Vulnerability Scoring System (CVSS) ermöglichen.

☐ Kann die Lösung die Berichte an alle zuständigen Personen verteilen?

Um Doppelarbeit zu vermeiden, sollte die Lösung eine Funktionalität zur Berichtsverteilung bieten. Diese Funktionalität sollte die Zusammenarbeit von Mitarbeitern und die Verteilung von Berichten zum Schwachstellenstatus unterstützen. Halten Sie nach Lösungen Ausschau, bei denen es möglich ist, Berichte je nach der zugewiesenen Benutzerrolle zu verteilen und einzusehen. Die Lösung sollte auch die Möglichkeit zur Erstellung und Verteilung von verschlüsselten Berichten beinhalten, insbesondere wenn Berichte an externe Personen verteilt werden müssen.

☐ Welche Formate bietet die Lösung für externe Berichtsanwendungen?

Die Schwachstellenmanagement-Lösung sollte über flexible Ausgabeoptionen verfügen, die eine individuell angepasste Nutzung ermöglichen. Sie sollte es erlauben, die Berichtsdaten in den Formaten PDF, Compressed HTML (gezippt), Web Archive (MHT, nur für Internet Explorer), CSV und XML in externe Anwendungen zu exportieren.

☐ Sind Funktionalitäten für Trendanalysen und vergleichende Berichterstattung vorhanden?

Um strategisches Schwachstellenmanagement zu ermöglichen, muss es die Lösung erlauben, Trends zu analysieren und Scan-Ergebnisdaten über längere Zeiträume hinweg zu vergleichen. So sollten beispielsweise Trenddaten für eine bestimmte Anzahl von Tagen, Wochen oder Monaten vorgelegt werden. In einem vergleichenden Bericht könnten etwa die Resultate der letzten beiden Scans für eine spezifischen Gruppe von Assets einander gegenübergestellt werden. Da Sie die Entwicklung der Ergebnisse über längere Zeiträume hinweg beobachten können müssen, sollten Sie die Möglichkeit haben, Sätze von Scans von jedem beliebigen Zeitpunkt auswählen und zu vergleichen.

☐ Gibt es Berichte, die Sie bei der Einhaltung von PCI, HIPAA, SOX und anderen Vorschriften unterstützen?

Compliance kann IT-Abteilungen vor immense Probleme stellen: Sie müssen Nachweise dafür erbringen, dass ein Unternehmen angemessene und effektive Sicherheitskontrollen implementiert hat, wie sie von unterschiedlichen Gesetzen und Unternehmensregularien vorgeschrieben werden. Halten Sie Ausschau nach Lösungen, die über diese Compliance-Berichtsfunktionen und benutzerfreundliche Templates verfügen, mit deren Hilfe Sie Daten zu Schwachstellen und Systemkonfigurationen extrahieren können, um Ihren spezifischen Berichtsanforderungen gerecht zu werden.

☐ Kann die Lösung mit anderen Technologien für Security Information Management zusammenarbeiten?

Viele große Unternehmen setzen bereits SIM-/SEM-Lösungen ein. Suchen Sie nach Lösungen, die diesbezüglichzahlreiche Integrationen unterstützen, einschließlich ArcSight, Guardednet, NetForensics, RSA [Network Intelligence], Open Systems, Symantec SIM 4.0, NetIQ, Cisco MARS/Protego, Intellitactics und eSecurity.

Schwachstellenbeseitigung

☐ Warum sollte die Schwachstellenbeseitigung mit dem Schwachstellen-Scanner integriert sein?

Asset-Erkennung, Schwachstellenscans und Reporting sind wichtige Teile des Schwachstellenmanagements, doch das Endziel ist die Korrektur und Beseitigung der Schwachstellen. Sie sollten eine Lösung wählen, in die ein automatisiertes Ticketing/Trackingsystem für die Schwachstellenbehebung integriert ist. Dieses System verfolgt automatisch die Änderungen, die sich durch Maßnahmen zur Schwachstellenbeseitigung ergeben, um so einen erfolgreichen Abschluss des Workflow-Prozesses zu gewährleisten.

☐ Wie implementiert die Lösung Richtlinien für die Schwachstellenbeseitigung?

Für alle Workflows zur Schwachstellenbeseitigung muss es autorisierte Richtlinien geben. Die Lösung sollte Menüs bieten, mit deren Hilfe Sie unkompliziert Policies erstellen können, die festlegen, wie und wann Tickets generiert werden und wem sie zugewiesen werden. Stellen Sie sicher, dass das System Regeln und Berechtigungen auf Basis von Benutzerrollen unterstützt.

☐ Plant das System Korrekturmaßnahmen in einer bestimmten Reihenfolge ein?

Es ist sinnvoll, Schwachstellen in der Reihenfolge ihres Schweregrads zu beheben. Jedoch müssen Sie auch über ein System verfügen, das es ermöglicht, die Bedeutung der Assets zu berücksichtigen, die gepatcht werden müssen. Die Lösung muss über intelligente Funktionen verfügen, um die Schwachstellenbeseitigung anhand von Richtlinien zu priorisieren, die von den Security Managern festgelegt werden. Mithilfe dieser Richtlinien können Sie die Korrekturmaßnahmen automatisch priorisieren, indem Sie den Schweregrad einer Schwachstelle zu den geschäftlichen Auswirkungen in Beziehung setzen – indem Sie also berücksichtigen, wie sehr die Ausnutzung der Schwachstelle den Betrieb eines bestimmten Geräts, einer Geschäftseinheit oder gar des gesamten Unternehmens beeinträchtigen würde.

☐ Was passiert, wenn ein Ticket generiert wird?

Wenn Sie das Trouble-Ticketingsystem und die Ticketing-Workflows Ihrer Schwachstellenmanagement-Lösung nutzen, achten Sie darauf, dass die Lösung automatisch ein Ticket generieren kann, wenn bei einem Scan eine Schwachstelle gefunden wird. Auf Basis vorgegebener Richtlinien sollte das Ticket einer Person (bzw. mehreren Personen) zugewiesen werden, die für die Beseitigung der Schwachstelle verantwortlich ist. Das Ticket sollte so lange als „offen" klassifiziert werden, bis die Schwachstelle behoben ist. Sobald ein nachfolgender Scan die Beseitigung der Schwachstelle verifiziert hat, wird das Ticket als „geschlossen" klassifiziert.

☐ Kann die Ticketing-Funktionalität der Lösung an externe Systeme angebunden werden?

In großen Unternehmen werden die Helpdesks bereits ein Trouble-Ticketing-System verwenden. Stellen Sie daher sicher, dass die Schwachstellenmanagement-Lösung über eine dedizierte „Ticketing-API" – eine XML-basierte Programmierschnittstelle zur Ticket-Extraktion und -Bearbeitung – an Ticketing-Systeme von Drittanbietern angebunden werden kann. So bietet etwa QualysGuard integrierte Anbindung an Remedy Help Desk sowie eine spezielle „Ticketing-API" zur Anbindung an andere Trouble-Ticketing-Lösungen.

☐ Wie handhabt die Lösung Maßnahmen zur Schwachstellenbeseitigung?

In vielen großen Netzwerken sind ständig zahlreiche Tickets zur Schwachstellenbeseitigung offen. Um zu wissen, welche Fortschritte gemacht werden und ob die Korrekturmaßnahmen mit den Richtlinien im Einklang stehen, benötigen die Security Manager einen entsprechenden Bericht. Stellen Sie sicher, dass Ihre Schwachstellenmanagement-Lösung Executive Reports zu Tickets, Tickets-pro-Schwachstelle, Tickets-pro-Benutzer und Tickets-pro-Asset-Gruppe erzeugen kann. Die Benutzer und Manager sollten auch Trendanalysen zu offenen Tickets durchführen können, um so die Fortschritte zu überprüfen. Halten Sie außerdem nach Lösungen Ausschau, bei denen Sie täglich E-Mail-Updates zu den Tickets erhalten können.

Policy Einhaltung

☐ Warum sollte Policy Compliance mit der Schwachstellenmanagement-Lösung integrierbar sein?

Die Policy Compliance-Funktionen setzen das Schwachstellenmanagement zu unternehmensinternen Sicherheitsrichtlinien sowie Gesetzen und Verordnungen in Beziehung. Insbesondere geben Sie Ihnen die Möglichkeit, die Einhaltung von Vorschriften automatisch zu prüfen und gegenüber internen und externen Auditoren zu dokumentieren – und somit Zeit, Geld und eine Menge manueller Arbeit zu sparen. Wenn dies für Sie wichtig ist, suchen Sie nach Lösungen, die solche Funktionen umfassen.

☐ Wie wird die Lösung von Auditoren eingesetzt?

Um ihre Aufgaben zu erfüllen, müssen interne und externe Auditoren auf Schwachstellendaten zugreifen können. Halten Sie nach Lösungen Ausschau, bei denen Sie die Möglichkeit haben, Auditoren den Zugriff auf Compliance-Management-Funktionalitäten zu gewähren.

☐ Kann die Lösung Assets zu Compliance-Zwecken von anderen trennen?

Die meisten Gesetze und Vorschriften zur Netzwerksicherheit beziehen sich auf Teilmengen von Assets. So schreibt etwa Sarbanes-Oxley nur den Schutz von Systemen zur Finanzberichterstattung vor oder PCI DSS nur den Schutz der Systeme, die zur Verarbeitung und Übertragung der Daten von Kreditkarteninhabern dienen. Achten Sie darauf, dass Sie mit Ihrer Schwachstellenmanagement-Lösung bestimmte Assets Gruppen zuweisen können, die mit spezifischen Policy-Anforderungen verbunden sind.

☐ Welche Policies und Kontrollen unterstützt die Lösung?

Kontrollen werden auf Basis der CIS- und NIST-Standards erstellt und auf Frameworks und Vorschriften wie COBIT, ISO und ITIL angewandt. Kontrollen sind die Bausteine für Compliance-Policies, welche wiederum Sammlungen von Kontrollen für eine oder mehrere Technologien in Ihrer Systemumgebung sind. Jede Kontrolle in den Richtlinien umfasst eine Anweisung, wie das technologiespezifische Element implementiert werden muss, sowie einen oder mehrere Tests, um die Kontrolle zu validieren. Suchen Sie nach einer Lösung, die alle diese Faktoren unterstützt.

☐ Kann die Lösung bereits bestehende Policies unterstützen?

Prüfen Sie, ob die von Ihnen gewählte Schwachstellenmanagement-Lösung eine Policy Library für Kontrollen umfasst, die Sie direkt in Ihr Konto importieren und zur Compliance-Berichterstattung verwenden können. Die Kontrollen sollten nach Technologie, Compliance-Framework oder -Vorschrift und Art des Compliance-Checks klassifiziert werden. Nach dem Importieren sollten Sie die Kontrollen bearbeiten können, um die Parameter undTechnologien der einzelnen Kontrollen optimal an die Bedürfnisse Ihres Unternehmens anpassen zu können.

☐ Inwieweit liefert die Lösung einen geschützten Audit Trail?

Rechnungsprüfer werden Schwachstellendaten mit Misstrauen betrachten (und vermutlich nicht akzeptieren), die von Ihrem Unternehmen manipuliert werden können. Stellen Sie sicher, dass die Lösung den Benutzern keinen direkten Zugriff auf die Schwachstellendaten, sondern nur „Read only“-Zugriff erlaubt. Außerdem müssen Sie unbedingt überprüfen, ob die Schwachstellendaten vor Manipulationen jeglicher Art vollständig geschützt – und somit revisionsicher – sind.

Management

☐ Welche Möglichkeiten bietet die Lösung zur Verwaltung von Assets?

Asset-Gruppierung ermöglicht es, Assets nach Gruppen und Geschäftsbereichen einzuteilen, und diesen eine Wichtigkeit auf Ihre Geschäftsprozesse zuzuweisen. Die Lösung, für die Sie sich entscheiden, sollte unbedingt über diese Funktionalität verfügen. Achten Sie darauf, dass die Lösung große Flexibilität und höchste Genauigkeit bei den Schwachstellenscans, der Schwachstellenbeseitigung und beim Reporting bietet.

☐ Wie kann ich mit der Lösung Benutzer verwalten?

Die Benutzerverwaltung bei einer Schwachstellenmanagement-Lösung basiert im Wesentlichen darin, dass den Benutzern unterschiedliche, rollenbasierte Berechtigungsstufen zugewiesen werden können, um z.B. Erkennungs- und Schwachstellenscans auszuführen, Policies zu erstellen, Schwachstellen zu beseitigen,oder die Einhaltung von Policies zu steuern. Achten Sie darauf, dass die Lösung ein rollenbasiertes Benutzerkonzept enthält und Ihnen die Möglichkeit gibt, Benutzer und deren Rechte effektiv zu verwalten.

☐ Wie arbeitet die Lösung bei komplexen Netzwerk-Konfigurationen?

Im IT-Bereich führt Komplexität oft zu verlangsamter Verarbeitung von Operationen, die eigentlich unkompliziert sind, und verzögert deren Abschluss. Prüfen Sie die Funktionen zur Asset- und Benutzerverwaltung, die die Lösung bietet. Vergewissern Sie sich, dass Sie Ihr Netzwerk mit der Lösung leicht segmentieren können, um effizientes und präzises Schwachstellenmanagement zu gewährleisten.

☐ Ist irgendeine Form von Systemwartung erforderlich, zum Beispiel Patching der Scanner-Software?

Ihre Schwachstellenmanagement-Lösung könnte die Belastung, die Ihnen durch die Notwendigkeit laufender Software-Patchings ohnehin entsteht, noch zusätzlich vergrößern – oder auch nicht. Suchen Sie nach SaaS-basierten Lösungen, weil diese auf einer On-Demand-Plattform aufbauen und alle Patching-Prozesse und System-Updates automatisch für Sie durchführen. Stellen Sie sicher, dass Sie selbst nichts herunterladen, installieren, aktualisieren oder warten müssen … nicht einmal in Bezug auf interne Scanner-Appliances. Jedes Mal, wenn Sie Ihre Schwachstellenmanagement-Lösung nutzen, sollte Ihnen eine Lösung zur Verfügung stehen, die auf dem allerneuesten Stand ist.

☐ Welche Aktionen sind notwendig, um die Aktivitäten von Auditoren zu verwalten?

Die von Auditoren gestellten Anforderungen können, gelinde gesagt, eine Herausforderung sein. Die Schwachstellenmanagement-Lösung sollte einem Manager oder Unit Manager die Möglichkeit geben, auf einfache Weise Auditoren-Benutzerkonten für autorisierte Personen, die Audits durchführen, zu erstellen. Sie werden Auditoren vermutlich nicht die Berechtigung zur Durchführung von Compliance-Scans geben wollen, doch sollten sie Policies definieren und Berichte auf Basis der Daten aus den Compliance-Scans generieren können.

Kosten

☐ Welche Kosten verursacht Schwachstellenmanagement mit herkömmlichen Software-Lösungen?

Verschaffen Sie sich einen Überblick über sämtliche Kosten, die die verschiedenen Schwachstellenmanagement-Lösungen verursachen, die Sie prüfen. Kalkulieren Sie unbedingt die tatsächlichen Gesamtunterhaltungskosten mit ein. Die Nutzung einer softwarebasierten Schwachstellenmanagement-Lösung bringt viele Kosten mit sich: Die Software selbst erfordert den Erwerb einer Lizenz und ist mit jährlichen Support- und Wartungskosten verbunden. Benutzer und Administratoren müssen geschult werden. In einem personalaufwändigen Prozess müssen Genehmigungen der einzelnen Abteilungen eingeholt und die Anwendungen konfiguriert und im Detail angepasst werden. Pflege und Partionierung einer Datenbank sind erforderlich, ebenso wie Verschlüsselung zum Schutz der Daten. Zur Unterstützung und Pflege der Anwendungen müssen Mitarbeiter Updates und neue Signaturen überprüfen und installieren, Scans ausführen und die entdeckten Schwachstellen beseitigen. Und schließlich sind auch die Kosten zu bedenken, die Server, Appliances, Speicher-Infrastruktur und Disaster Recovery verursachen.

☐ Ist es nicht billiger, einen Consultant zu engagieren?

Consultants können eine große Hilfe sein, doch konzentriert sich ihre Arbeit normalerweise auf einen Penetrationstest, der nur die Schwachstellen aufdeckt, die zu einem ganz bestimmten Zeitpunkt existieren. Wenn man Consultants für die Durchführung regelmäßiger, laufender Schwachstellenanalysen bezahlt, wird dies im Vergleich zu anderen Lösungen schnell zu teuer. Consultants setzen Sie am besten dazu ein, das Know-how Ihrer Sicherheitsabteilung zu erweitern und bei der Beseitigung von Problemen zu helfen, die im Verlauf des Schwachstellenmanagements entdeckt werden.

☐ Können Sie Geld sparen, indem Sie gratis verfügbare Open-Source-Software verwenden?

Gratis verfügbare Open-Source-Software kann verlockend wirken, doch auf lange Sicht müssen Sie die realen Kosten und die allgemeine Effektivität einer solchen Lösung mit einkalkulieren. Die offensichtlichen Nachteile, wie etwa fragwürdige Qualität des Codes, potenzielle Einschleusung von Schwachstellen über ungetestete Open-Source-Module und dürftige Schulungs- und Supportleistungen sollten wesentlichen Einfluss auf Ihre Entscheidung haben. Und natürlich müssen Sie immer noch die oben erwähnten Kosten tragen, die herkömmlicherweise bei der Nutzung einer Software-Lösung anfallen.

☐ Ist kommerziell verfügbare Schwachstellenmanagement-Software eine kostengünstigere Option?

Kommerziell verfügbare Software ist oft von besserer Qualität als Open-Source-Software; auch die Schulungs- und Supportangebote sind besser. Sie verursacht jedoch zusätzliche jährliche Kosten für die Lizenz, den Support und die Pflege. Daneben müssen Sie die Kosten für alle üblichen Anforderungen tragen, die, wie bereits beschrieben, mit der Verwendung von Software verbunden sind.

☐ Inwiefern senkt Software-as-a-Service die Kosten des Schwachstellenmanagements?

SaaS ist die kostengünstigste Form des Schwachstellenmanagements. Bei SaaS-Lösungen stellt ein externer Anbieter, wie etwa QualysGuard, auf einem sicheren Webserver die Anwendung zur Verfügung, die die Benutzer dann über einen Webbrowser nach Bedarf einsetzen und steuern. Sie sparen Geld, indem Sie periodisch eine Subskriptionsgebühr zahlen, anstatt die Kosten für Software, regelmäßige Updates und laufende Wartung tragen zu müssen.

☐ Von der betrieblichen Perspektive aus betrachtet: In welcher Weise senkt SaaS sonst noch die Kosten?

Eine SaaS-Lösung wie QualysGuard ist bereits „voll in Betrieb“ und kann deshalb unverzüglich bereitgestellt werden, ganz gleich, wie groß und komplex eine Infrastruktur auch sein mag. Es ist nicht notwendig, an irgendeiner Stelle der Infrastruktur Agenten oder sonstige Software zu installieren. Zudem bietet QualysGuard eine Programmierschnittstelle zur einfachen, schnellen Anbindung an Plattformen für das Enterprise Network Management.

☐ Wenn man von den Ersparnissen beim Deployment einmal absieht, ist SaaS dann nicht genauso teuer wie der Einsatz von Software?

Eine SaaS-Lösung, wie beispielsweise QualysGuard, ist kostengünstiger als Software, weil es sich um eine gehostete Lösung handelt. Updates für die Software und die Schwachstellensignaturen werden unverzüglich und automatisch für das ganze Unternehmen bereitgestellt. Der Abgleich von Schwachstellendaten erfolgt automatisch, sodass Sie jeweils sofort einen unternehmensweiten Überblick über Ihre Sicherheitsaufstellung erhalten.

☐ Welche „weichen Kosten“ reduziert SaaS?

Es gibt viele Bereiche, in denen weitere Ersparnisse erzielt werden. Software-Deployment in Geschäftseinheiten, die auf verschiedene nationale oder internationale Standorte verteilt sind, erfordert häufig Vor-Ort-Unterstützung oder den Einsatz professioneller Dienstleister; SaaS-Deployment kann unverzüglich erfolgen. Um Software zu skalieren, muss die Hardware-Infrastruktur aufgestockt werden; SaaS ist sofort und unbegrenzt skalierbar, ohne dass die Anwender mehr Hardware einsetzen müssen. Die Einhaltung der Verschlüsselungsrichtlinien eines Unternehmens kann beim Einsatz von Software eine komplexe Aufgabe sein; bei QualysGuard erfolgt die Verschlüsselung automatisch. Um Interoperabilität zu ermöglichen, müssen Software-Lösungen oft stark angepasst

werden; die integrierte XML-basierte Programmierschnittstelle von QualysGuard lässt sich sofort mit jeder Anwendung verbinden, die diesen universellen Standard nutzt.

Lösungsanbieter

☐ Wie sieht die Geschäftsentwicklung und Marktstärke des Lösungsanbieters aus?

Achten Sie darauf, einen Marktführer zu wählen, der auf Schwachstellenmanagement spezialisiert ist. Ziehen Sie Ressourcen von Analysten wie Gartner und Forrester heran, um festzustellen, was diese über den Anbieter und seine Lösung zu sagen haben. Lesen Sie Fallstudien und überprüfen Sie die Referenzen. Das Unternehmen sollte einen soliden Ruf haben und über eine nachweisliche Erfolgsbilanz verfügen.

☐ Wie sieht die Schwachstellenmanagement-Produktlinie des Lösungsanbieters aus?

Ein Anbieter, der auf Schwachstellenmanagement-Lösungen spezialisiert ist, kann für gewöhnlich eine ebenso breite wie spezifische Produktpalette vorweisen. Achten Sie darauf, dass die Lösung Ihren spezifischen Bedürfnisse entspricht. Oder anders ausgedrückt: Achten Sie darauf, dass die Lösung skalierbar, ausreichend robust, benutzerfreundlich und kostengünstig ist.

☐ Welche Kunden hat der Lösungsanbieter?

Stellen Sie fest, wie viele Kunden die Lösung einsetzen, und was diese darüber zu sagen haben. Stellt der Anbieter öffentlich Fallstudien und Testimonials von etablierten, marktführenden Unternehmen zur Verfügung, die die Lösung nutzen? Nutzen diese Unternehmen die Schwachstellenmanagement-Lösung auch tatsächlich? Überprüfen Sie die Referenzen und fragen Sie, ob Sie mit Kunden sprechen können, die in Ihrer eigenen Branche tätig sind.

☐ Welche Partner hat der Lösungsanbieter?

Mit wem arbeitet der Anbieter zusammen? Mit welchen Produkten sind seine Lösungen integrierbar? Stellen Sie fest, ob die Lösung mit führenden Sicherheitsprodukten und Technologien in folgenden Bereichen integrierbar ist: *Security Information & Event Management* (ArcSight, Cisco, netForensics, RSA [Network Intelligence], Novell, StillSecure, 1Labs, Symantec); *Patch-Management* (Citadel), *Helpdesk-Ticketing-Systeme* (CA Service Center, BMC Magic Service Desk, HP Service Desk, Bugzilla und andere); *Risikomanagement* (Redseal, Skybox); *Network Access Control* (MetaInfo); *IDS/IPS* (Neon Software, ForeScout); *Network Patching* (BlueLane); *Netzwerk-Verhaltensanalyse* (Mazu Networks); *Security Policy Management* (Archer Technologies, McAfee); *Penetrationstests* (Core Security Technologies).

☐ Welche Auszeichnungen hat der Anbieter in jüngster Zeit für seine Lösung erhalten?

In jüngster Zeit vergebene Auszeichnungen sind ein weiterer starker Indikator für hohe Produktqualität und starke Marktdurchdringung. So konnte etwa Qualys in jüngster Zeit unter anderem folgende Auszeichnungen verbuchen: Gewinner bei den SC Magazine Awards 2008 (US), Information Security Readers Choice 2008, Frost & Sullivan Best Practices Award 2008, Information Security Decisions Best in Show 2007, Gewinner bei den SC Magazine Awards 2007 (Europa) und Network World Clear Choice Award.

☐ Können Sie die Schwachstellenmanagement-Lösung kostenlos evaluieren?

Kaufen Sie nichts, was Sie nicht ausprobieren können. Sie müssen die Möglichkeit haben, selbst festzustellen, wie die Lösung in Ihrer IT-Umgebung arbeiten würde, und sie gründlich zu testen. Es ist wichtig zu wissen, wie einfach (oder schwierig) die Lösung zu installieren, zu pflegen und anzuwenden ist – in Ihrem gesamten Unternehmen.

Qualys bietet Ihnen die Möglichkeit, die Lösung QualysGuard in ihrem vollen Umfang 14 Tage lang kostenlos zu evaluieren. Beginnen Sie jetzt mit der Evaluierung, indem Sie sich auf http://www.qualys.com/products/trials/ einloggen.