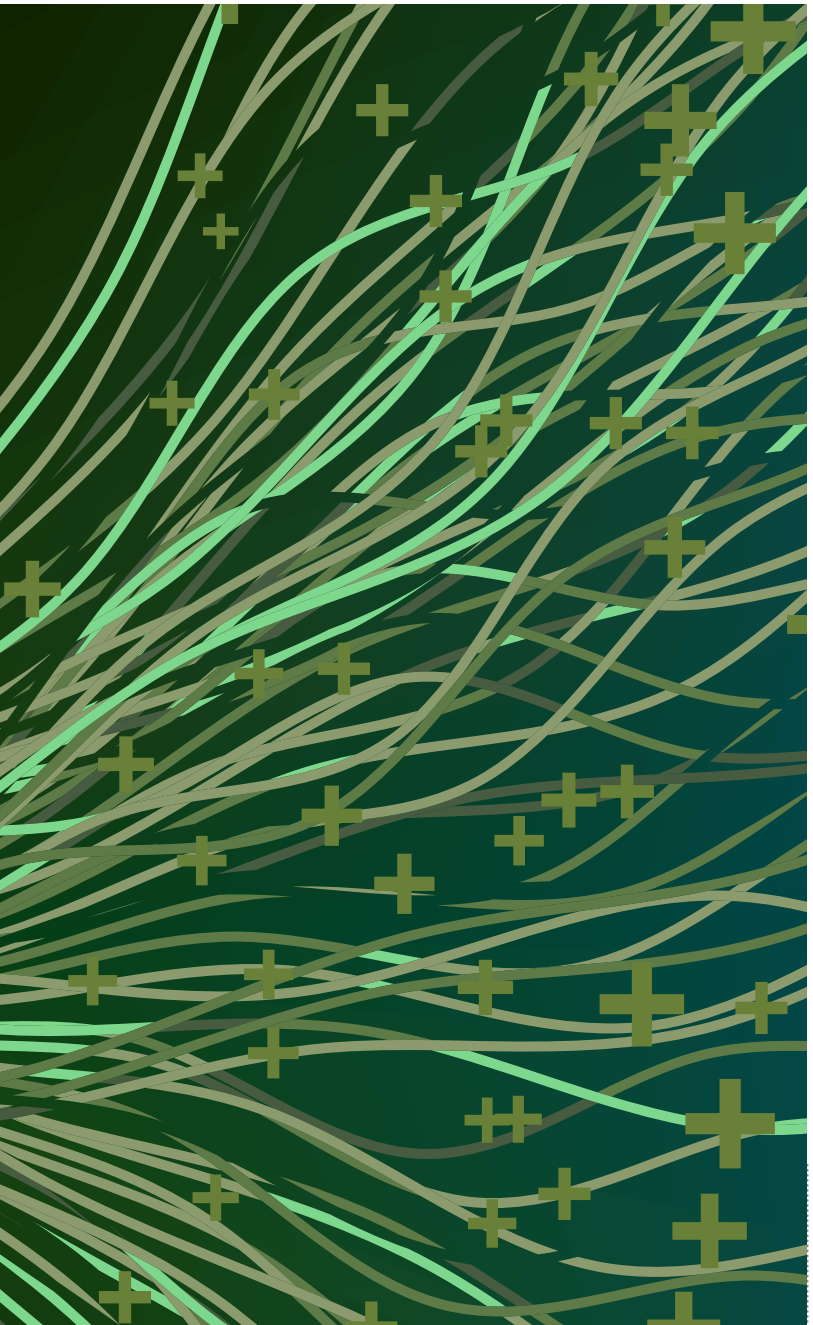
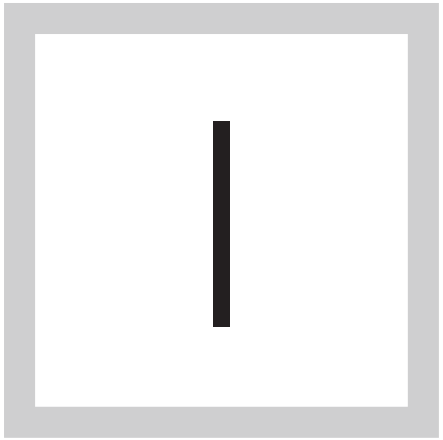


Special Report

WIE SIE FÜR OPTIMIERTES SCHWACHSTELLEN-MANAGEMENT SORGEN

TechTarget | SearchSecurity.de



N DEN LETZTEN Jahren hat es eine Reihe erfolgreicher Cyberangriffe auf Unternehmen gegeben und die Bedrohung wird auch in Zukunft sicher nicht nachlassen. Viele Führungskräfte sind davon überzeugt, dass Ihr Unternehmen niemals ins Visier von Cyberkriminellen geraten könnte – zu Recht? Dieser E-Guide erläutert, wie Sicherheitsrisiken, Schwachstellen und Bedrohungen gemessen werden und somit leichter in Angriff genommen werden können.

WIE KANN MAN SECURITY-RISIKEN, BEDROHUNGEN UND SCHWACHSTELLEN MESSEN?

Im Allgemeinen lassen sich Risiken nur schwer quantifizieren oder in Zahlen ausdrücken. Bevor ich nun Millionen an Dingen nenne, die sich messen lassen, sollten Sie etwas mehr zum Thema Risiko verstehen. Das gilt vor allen Dingen, wenn wir von Security sprechen. Bei TruSecure (nun Cyber Trust), hat CTO Peter Tippet Risiken mithilfe einer einfachen Gleichung definiert:

RISIKO = BEDROHUNG X VERWUNDBARKEIT (SCHWACHSTELLE) X KOSTEN

Bedrohung ist die Frequenz widriger Ereignisse. Verwundbarkeit ist die Wahrscheinlichkeit, dass ein bestimmter Angriff erfolgreich ist. Die Kosten sind die kompletten ökonomischen Auswirkungen eines erfolgreichen Angriffs. Anwender und Branchenkenner haben unterschiedliche Auffassungen, auf welche Weise man Risiken quantifiziert. Investoren, Versicherungs-Statistiker und Security-Profis sind bei diesem Thema unterschiedlicher Meinung. Allerdings ist diese Definition einfach und plausibel genug. Deswegen halten wir im Moment daran fest.

Sie müssen Ihre Security-Umgebung quantifizieren. Wir sprechen an dieser

Stelle von Bedrohungen und Schwachstellen. Im Anschluss kalkulieren Sie die Kosten anhand des Risiko-Niveaus. In der Realität könnten Sie Ihr restliches Leben damit verbringen, einen ausgeklügeltes Modell erschaffen zu wollen und dennoch falsch liegen. Genau genommen nehmen Sie etwas an, das auf Annahmen basiert, dem wiederum Annahmen zu Grunde liegen.

Ich schlage vor, dass man qualitativ an die Sache herangeht, um alles rund um das Thema Security zu quantifizieren. Sie finden viele Informationen dazu in meinem Buch The Pragmatic CSO. Nachfolgend stelle ich Ihnen die gekürzte Fassung zur Verfügung.

Konzentrieren Sie sich zu Beginn auf die relevanten Sachen und fokussieren Sie sich auf die Kosten. Welche Business-Systeme sind für Ihr Unternehmen am Wichtigsten? Wer benutzt diese? Wie viel ist ihre Zeit wert? Sobald Sie einen Überblick hinsichtlich der wichtigsten Systeme haben, finden Sie heraus, wodurch diese am ehesten bedroht sind. Sind sie anfällig für Cross-Site-Scripting-Angriffe? Könnte ihnen ein DDoS-Angriff Schaden zufügen? Benutzen Sie diese Informationen, um realistisch zu kalkulieren, wie wahrscheinlich so ein Angriff ist. Außerdem sollten Sie sich damit befassen, ob ein erfolgreiches Kompromittieren das System in einem unbrauchbaren Zustand hinterlassen könnte.

Unterm Strich sollten Sie herausfinden, ob es sich lohnt, einen neuen Prozess zu implementieren oder ein neues Produkt zu installieren. Versuchen Sie dabei herauszufinden, welche Komponenten das spezifische Produkt beeinflusst. Würde die Installation einer Web-Applikations-Firewall die Wahrscheinlichkeit eines XSS-Angriffs auf der wichtigen Plattform verringern? Wenn ja, zu welchem Grad? Versuchen Sie, das einzuschätzen. Würde es die Frequenz der Angriffe eindämmen? Natürlich nicht. Die einzige Methode, dies zu realisieren, würde ein Offline-Nehmen des Systems bedeuten. Diese Zahl bleibt in dem Fall eine Konstante. Gehen Sie wie oben beschrieben an die Geschichte heran, vergleichen Sie Äpfel mit Äpfel. Somit wissen Sie, welche verschiedenen Optionen am ehesten helfen, die Risiken so gut wie möglich einzudämmen.

Ich bin kein Fan davon, einfach Dinge zu zählen. Mit der hier beschriebenen Methode können Sie bestimmte Entscheidungen gegen andere abwägen, indem Sie die einzig wichtige Metrik zu Rate ziehen: Das Risiko für das jeweilige Business-System.

SCHWACHSTELLEN-MANAGEMENT IST MEHR ALS PATCH-MANAGEMENT

Unter dem klassischen Patch-Management versteht man die Notwendigkeit, neue Updates und Hotfixes des jeweiligen Software-Anbieters einzuspielen. Natürlich gibt es schon lange Zeit Anbieter, die diese mühsame Aufgabe übernehmen und permanent sicherstellen, dass Unternehmen up-to-date bleiben.

Andere Softwareapplikationen updaten sich selbstständig oder die Signaturen werden zum Kunden „gepusht“. Reines Patch-Management ist heute jedoch eine Standardroutine, die kostengünstig und automatisiert vonstattengehen sollte.

Im Gegensatz dazu geht Schwachstellen-Management (Vulnerability Management) einige Schritte weiter und analysiert die eigene Umgebung permanent auf die tatsächliche Tauglichkeit der Aktivitäten sowie auf bekannte Verwundbarkeiten, wodurch die Uhr der Zero-Day-Threats zu ticken beginnt.

Unter anderem überprüft klassisches Vulnerability-Management (VN) nicht nur, ob Patches geladen und eingespielt wurden, sondern auch tatsächlich aktiv sind. Darüber hinaus ist ein wesentlich höherer Automatisierungsgrad gegeben,

auch Veränderungen von Devices im Netzwerk werden gescannt.

Eine Interaktion mit anderen Security-Tools wie mit einer SIEM-Lösung ist ebenso notwendig. Dadurch erhöht sich das Sicherheitslevel dramatisch. Da diese VN-Lösungen zudem ständig Tests in der eigenen IT-Umgebung laufen lassen, senken sie auch den Aufwand für Audits und erfreuen die Compliance-Verantwortlichen.

SIEM INTEGRIERT VULNERABILITY MANAGEMENT

Wenn man sich auf dem IT-Markt umsieht, gibt es viele Anbieter für Nischenprodukte sowie die Massenmärkte namhafter Security-Anbieter, die auch übergreifende Querschnittsthemen „mitnehmen“. Auf dem nächsthöheren Schutzlevel befinden sich Schwachstellen-Management, SIEM-Lösungen und Log-Management.

Sieht man von den Anbietern ab, die diese Themen streifen – wie manche Firewall-Hersteller oder klassische Security-Universalanbieter – verbleiben die jeweiligen Top-Anbieter der einzelnen Fachgebiete, an die man sich zum Aufbau eines wirksamen Schutzes wenden kann.

Aufgrund der Komplexität und der bisherigen Erfahrungen des letzten Jahrzehnts ist es anzuraten, von der Komponente Security Information and Event Management auszugehen. Diese „Engine“ sammelt und korreliert alle relevanten

Ereignisse und integriert somit auch den Aspekt der Schwachstellenanalyse.

Auch eine allfällige Alarmierungskette, Logs aus Firewall-Systemen und anderen Softwaretools können in der zentralen SIEM-Datenbank ausgewertet werden. Meist sind Schwachstellen-Scanner out-of-the-box integriert oder Fremdprodukte lassen sich einfach einbinden. Umfassende Reports nach internationalen Standardvorgaben sind genauso möglich wie ein regelbasiertes Filtern von Logs und bessere Abwehrmöglichkeiten bekannter und komplexer Gefahren, wo signaturbasierte Verfahren nicht mehr helfen.

MÖGLICHE MEHRWERTE EINES SIEM- UND LOG-MANAGEMENT-PROJEKTES

In der Praxis sieht man immer wieder, dass unterschiedliche Anforderungen zu einem SIEM-Projekt führen. Aus der Sicht der Compliance-Verantwortlichen, die oftmals auch Aspekte der IT-Forensik zu berücksichtigen haben, steht der Gesichtspunkt der Log-Datensammlung an erster Stelle. Im Vordergrund stehen somit Fragen des Datenschutzes, des Speicherbedarfs und der Suchoptionen.

Auf der anderen Seite wollen Projektmanager auch bisher unbekannte Trojaner- und Bot-Systeme aufspüren, verstärkte Regeln und Prozesse durchsetzen oder letztlich sogar ein Security Operation Center (SOC) aufbauen. Diese Features

sind klassische SIEM-Funktionen, die eine sehr erfahrene Security-Mannschaft erfordern – ebenso wie eine Rund-um-die-Uhr-Betreuung, was für verschiedene Varianten aus dem Angebot der Managed-Security-Services sprechen würde.

Möchte man bei Vorfällen auch noch Security-Spezialisten vor Ort zur Unterstützung wissen und kurzfristig auf notwendige Tools (Advanced Threat Protection) und Hersteller zugreifen, wird die Luft schon sehr dünn. Gleichzeitig kann aber auch der Schutzlevel so erhöht werden, dass Eindringlinge schnell erkannt und überführt werden oder der Aufwand eines Angriffs schlicht zu hoch wird.

Wenn nun auch Schwachstellen-Management und möglicherweise Honeypot-Systeme integriert werden, kommt eine externe Betreuung durch einen spezialisierten IT-Dienstleister in Frage. Die besten Ergebnisse werden mit den Software-Herstellern selbst und deren Partnern erzielt, wobei aber vertrauliche Daten weder das Land verlassen noch ungeschützt in die Cloud „entgleiten“ sollten.

KOSTENLOSE ONLINE-RESSOURCEN FÜR IT-EXPERTEN

TechTarget publiziert qualifizierte Medieninhalte im IT-Bereich, die Ihren Informationsbedarf bei der Suche nach neuen IT-Produkten und Technologien abdeckt, und Ihr Unternehmen somit gezielt in der Strategieentwicklung unterstützt. Es ist unser Ziel, Ihnen durch die Bereitstellung von Online-Ressourcen über die aktuellsten Themen die Kaufentscheidungen für IT-Produkte zu erleichtern und kostengünstiger zu gestalten.

Unser Netzwerk an Technologie-Webseiten gibt Ihnen die Möglichkeit, auf eine der weltweit größten Online-Bibliotheken zum Thema IT zuzugreifen, und anhand von unabhängigen Expertenmeinungen und Analysen, sowie auch zahlreichen Whitepapern, Webcasts, Podcasts, Videos, virtuellen Messen und Forschungsberichten zu einer ausgewogenen Kaufentscheidung zu gelangen.

Unsere Online-Ressourcen berufen sich auf die umfangreichen Forschungs- und Entwicklungskompetenzen führender Technologieanbieter, und ermöglichen es Ihnen somit, Ihr Unternehmen für künftige Marktentwicklungen und Herausforderungen zu rüsten. Unsere Live-Informationsevents und virtuelle Seminare geben Ihnen die Möglichkeit, Ihre täglichen individuellen Herausforderungen im Bereich IT mit den Experten der Branche zu diskutieren.

Außerdem können Sie in unserem Social Network, dem IT Knowledge Exchange, praxisnahe Erfahrungsberichte mit Fachkollegen und Experten in Echtzeit austauschen.

WAS MACHT TECHTARGET SO EINZIGARTIG?

Bei TechTarget steht die Unternehmens-IT im Mittelpunkt. Unsere Autoren und das Redaktions-Team sowie auch unser großes Netzwerk an Industrieexperten bietet Ihnen Zugriff auf die neuesten Entwicklungen und relevantesten Themen der Branche.

TechTarget liefert klare und überzeugende Inhalte und umsetzbare Informationen für die Profis und Entscheidungsträger der IT-Branche. Wir nutzen die Schnelligkeit und Unmittelbarkeit des Internets, um Ihnen in realen und virtuellen Kommunikationsräumen hervorragende Networking-Möglichkeiten mit Fachkollegen zu ermöglichen.