

Vulnerability Management: Das Exekutivorgan für IT-Security

Die hohe Komplexität und Heterogenität der IT-Infrastrukturen, nicht rechtzeitig erkennbare Schwachstellen und technische Bedrohungen wie Viren, Würmer, Spam, Trojaner, Spyware oder durchlässige WLAN Access Points und damit zusammenhängend mögliche Imageverluste zeichnen ein breites Gefährdungsspektrum, dem sich Unternehmen heute stellen müssen. Mit einem gezielten Vulnerability Management kann die Verwundbarkeit des Unternehmensrückgrats – sprich der IT-Infrastruktur – nachhaltig minimiert werden.

Die Mehrzahl der Unternehmen im deutschsprachigen Raum tut sich bei der Identifizierung und Priorisierung von erforderlichen Sicherheitsmassnahmen einer Studie der Experton Group zufolge heute mangels Risikomanagement noch ziemlich schwer. Etliche Vorhaben konzentrieren sich auf das operative IT Risk Management mit dem Ziel, die Effizienz der Sicherheitsmassnahmen zu überprüfen und eventuell Compliance-Prozesse zu unterstützen. Was aber häufig völlig fehlt, ist eine Verknüpfung mit den letztendlich zu schützenden Geschäftsprozessen und Informationen und damit ein effizientes Vulnerability Management.

Angesichts ständig neuer Bedrohungen müssen Unternehmen systematisch die verwundbaren Punkte ihrer IT-Infrastruktur absichern. Andererseits sind die Hersteller dazu gezwungen, beinahe täglich Sicherheitslücken ihrer Produkte bekannt zu geben. Diese und andere Faktoren tragen dazu bei, dass es immer schwieriger wird einzuschätzen, wie gut Infrastrukturen tatsächlich geschützt sind.

Auch wenn Firewalls, Virenschutz, Intrusion Detection und andere Sicherheitsmassnahmen längst State-of-the-Art sind – das Problem ist, wie werden die Sicherheits- und Konfigurationseinstellungen kontrolliert und wer entscheidet, was bei der entstehenden Flut an Log-Daten wirklich relevant ist.

Schwachstellen in der IT-Infrastruktur können viele Ursachen haben: Durch Fehler im Softwaredesign, falsche Konfigurationen sowie ungepatchte oder unautorisierte Systeme entstehen Sicherheitslücken. Aber auch fehlgerichtete Security-Richtlinien oder mangelndes Sicherheitsbewusstsein der Mitarbeiter erhöhen deren Anfälligkeit. Schwachstellen können demnach nicht nur auf technischer, sondern auch auf prozessualer wie organisatorischer Ebene auftreten.

Umfragen bei verschiedensten IT-Organisationen betreffend Vulnerability Management zeigen ein ständig wiederkehrendes Bild: Die technischen Aspekte von Virenschutz, zu denen auch die Bereitstellung von Spezialisten für Virensupport und Evaluierung von Virenschutzlösungen gehört, schneiden recht gut ab. Management-Aspekte dagegen kommen durchwegs schlecht davon. Zu solchen Management-Aufgaben gehört es beispielsweise, Virenschutzrichtlinien festzulegen und Notfall-Prozeduren zu etablieren.

Durch die Einführung von Sicherheitsrichtlinien erhoffen sich die Unternehmen, den Sicherheitsstandard ihrer Infrastrukturen zu erhöhen. In den seltensten Fällen jedoch kann die Einhaltung dieser Richtlinien auch tatsächlich kontrolliert werden. Vorgaben vom Gesetzesgeber oder von dritter Seite (Basel II, Sarbanes-Oxley etc.), welche eine solche Kontrolle voraussetzen, können in der Praxis folglich nur schwer umgesetzt werden.

Zunahme der Komplexität

Der Umgang mit schützenswerten Daten gehört längst zum täglichen Geschäft aller Organisationen und muss präventiv geregelt sein. Andererseits nehmen Grösse und Komplexität von Unternehmensnetzwerken laufend dazu, und damit auch die Vielfalt der eingesetzten Produkte.

Da solcherart die IT-Umgebung in einem Betrieb immer neuen Bedrohungen ausgesetzt ist, rückt auch ein entsprechendes Vulnerability Management immer mehr in den Mittelpunkt effizienter Präventionsszenarien. Da die Angriffe von innen und aussen immer ausgeklügelter werden, sind Firmen dazu gezwungen, technisch immer auf dem aktuellen Stand zu bleiben. Um heute potenzielle Schwachstellen jedoch vorsorglich beurteilen zu können, ist ein mehr an Zeit, Sorgfalt und Fachwissen erforderlich, als je zuvor. Mit jedem neuen Sicherheitsalarm oder -update rückt Vulnerability- und Berechtigungsmanagement für die Sicherheit eines Unternehmens immer mehr in den Mittelpunkt.

Nach Ansicht vieler Industrieexperten soll eine Vulnerability-Management-Lösung konkret folgende Möglichkeiten bieten:

- Benachrichtigung und Beratung
- Verfahrensregeln
- Einschätzung von Schwachstellen
- Sanierungsmanagement

Aus zeitlichen wie wirtschaftlichen Gründen ist heute eine Risikoanalyse notwendig, um die Systeme und die darin ermittelten Schwachstellen nach ihrem Wert für den Geschäftsgang beziehungsweise ihren Auswirkungen auf wesentliche Geschäftsprozesse ordnen zu können. Es muss sichergestellt sein, dass die vorhandenen IT-Systeme die neusten Standards und Regeln erfüllen. Es muss klar sein, wo die begrenzten IT- und Personal-Ressourcen am sinnvollsten eingesetzt werden und welche Geschäftsprozesse am dringendsten gesichert werden müssen.

Aus dieser Sicht muss eine Vulnerability-Lösung eine agile Plattform verkörpern, die garantiert, dass alle relevanten Mechanismen eingebunden werden können. Eine Plattform, die die Policies verwaltet und den Beurteilungs- und Sanierungsprozess automatisiert.

Schutz gegen Daten-Missbrauch

Mit zunehmendem Einsatz unterschiedlichster Security-Vorrichtungen und -Systeme und einem immer komplexer werdenden Netzwerk klettern Zeit- und Kostenaufwand für die Beobachtung und Analyse von Sicherheitsvorfällen in nicht mehr tolerierbare Höhen. Gefragt sind daher kosteneffiziente und einfache Systeme, welche browser-gestützt bedienbar sind, zeitunabhängige Automatisierungsfunktionen beinhalten, ein grafisch übersichtliches Reporting liefern und die Fehlalarme reduzieren. Solche Systeme sollen es ermöglichen, die Sicherheitsrichtlinien durchzusetzen und zu kontrollieren. Risikoanalysen der Infrastruktur im Zusammenhang mit neu entdeckten Sicherheitslücken sollen schnell und verlässlich durchgeführt werden können.

Skalierbarkeit, stufengerechte Top-Down-Aufbereitung der Security Daten, ein inkludiertes Ticketing-System sowie ein entsprechendes OS-Fingerprinting zur Überwachung der Betriebssystemstände zählen zu den weiteren Funktionsanforderungen. Mit integrierten Vulntrak-Technologien können Sicherheitslücken von der Identifikation bis zur Behebung verfolgt werden. Und durch stufengerechte Aufbereitung der Scann-Daten werden die Informationen zum Sicherheitsstatus empfängergerecht zur Verfügung gestellt.

Vulnerability Management ist als eigenständiger, fortwährender Prozess zu verstehen – angefangen bei der Ermittlung von Schwachstellen über die Bewertung der Verwundbarkeiten bis hin zu ihrer schnellen und nachhaltigen Behebung.

Vorgehen und Projektziele

Es ist empfehlenswert, die Infrastruktur in verschiedene Risikozonen einzuteilen. Eine zentrale und übersichtliche Applikation, welche verschiedenste Infrastrukturkomponenten einbinden kann, sollte eingerichtet werden. Per Vergabe entsprechender Rechte wird die Applikation den verschiedenen Abteilungen (Sicherheit, Betrieb, Entwicklung) zur Verfügung gestellt. Es wird damit eine zentrale Quelle für Informationen über bestehende und neue Sicherheitsrisiken geschaffen.

Darüber hinaus werden Sicherheitsrichtlinien, Hardening-Bestimmungen sowie Patch- und Prüfkonzpte erstellt. Die Infrastruktur wird durch eine Einteilung in verschiedene Risikozonen differenziert. Die installierten Applikationen werden inventarisiert. Das Inventar wird gezielt mit Filtern hinsichtlich bekannter und neuer Sicherheitslücken abgeglichen. Ein Überwachungstool wird eingesetzt, welches das Netzwerk regelmässig entlang der Richtlinien scannt und die Patches überprüft.

Fazit

Security-Experten erachten einen Vulnerability-Management-Zyklus nur dann als sinnvoll, wenn er in nicht allzu grossen Intervallen wiederholt wird. Eine jährliche oder vierteljährliche Bewertung stellt dabei lediglich eine Momentaufnahme der Sicherheitssituation zu einem bestimmten Zeitpunkt dar und liefert keine Übersicht über die sich rapide verändernde Sicherheitslage eines Unternehmens. Ohne Unterstützung spezialisierter Werkzeuge sind die mit dem Schwachstellen-Management verbundenen Aufgaben jedoch kaum zu stemmen. Viele Firmen sind allerdings gar nicht in der Lage, ein umfassendes Vulnerability Management ohne fremde Hilfe einzuführen, da sie ihre internen Prozesse noch nicht darauf vorbereitet haben. Einer der häufigsten Fehler dabei ist es, zu versuchen, die Organisation einem Vulnerability Management-Tool anzupassen.

Autor: Stefan Näpflin, Head Consulting & Projects, Inhaber.

Effiziente Projekte dank Partnerschaft mit Visonys AG

IT-Security Infrastrukturen mit Web Entry Security und IAM. Weitere Informationen unter www.ispin.ch oder markus.kaegi@ispin.ch

Über Ispin AG (1999 – AK: CHF 300'000, eigenfinanziert): Schutz vertraulicher Daten – in Swiss made Qualität. Informations- und Informatiksicherheit sowie Datenschutz in Bezug auf Technologie, Organisation und Mensch. Information- & IT-Security, Authentisierungs-Plattformen mit Identity & Access Management und sicheren Web Entry Lösungen. Awareness-Programme, Sicherheitshandbücher, Security Frameworks, Security Officer Services. Business Continuity Management, DMZ-, Firewall-, VPN-, und Netz-Infrastrukturen. Datenschutz und lebbare Risiko-Kultur sichern. Operation, Betrieb, Support von Sicherheitsplattformen. Wissens- und Kompetenzvermittlung mit Kursen, Ausbildungen und persönliche Trainings für Lösungen, Technologien, Normen und Zertifizierungen sowie Methoden. Enge Zusammenarbeit mit Technologieherstellern und Projektpartnern sowie Engagement in öffentlichen Organisationen und Fachverbänden (ISSA, Infosurance, ISACA, ISSS (ehemals FGSec) Datenschutzforum etc.). Hohe Fachkompetenz. Eigene Marken und individuelle Softwareentwicklung.