Compliance dank Client Lifecycle Management

Schwachstellen-Management als Prozess

29.09.14|Autor/Redakteur:ArminLeinfelder*/StephanAugsten

Die Zahl der Schwachstellen auf Windows-PCs nimmt stetig zu, sowohl auf Betriebssystem- als auch auf Anwendungsebene. Administratoren sollten dementsprechend zeitnah auf neue Gefahren reagieren. Am besten gelingt dies, wenn die wiederkehrenden Aufgaben im Sinne eines Lifecycle Managements abgebildet werden.

Große Software-Hersteller wie Microsoft verwenden viel Zeit und Mühe darauf, bei der Veröffentlichung ihrer Software Schwachstellen von vornherein zu vermeiden und vorhandene Lücken schnellstmöglich zu schließen. Auch Sicherheitswerkzeuge wie Firewalls, Virenscanner und Threat-Management-Lösungen sind heute hochgradig ausgereift.

Trotzdem wird die Situation für die IT-Abteilungen in den Unternehmen in puncto Sicherheit immer komplizierter: Früher hatte der Client-Administrator fast ausschließlich mit Windows-PCs und BlackBerrys zu tun. Heute kommen mit den beliebten Smartphones undTablets auch neue Betriebssysteme – allen voran Apples iOS sowie Googles Android – und Applikationen (oder Apps) ins Haus.

Natürlich müssen dabei auch weiter hin die vertrauten Windows-PCs und -Notebooks stets aktuell gehalten werden. Denn die drohenden Angriffe werden dank frei erhältlicher Toolkits nicht nur vielfältiger, sondern auch ausgefeilter – bis hin zu so genannten APTs (Advanced Persistent Threats), also über lange Zeiträume und mehrere Stufen laufende Angriffe.

Laut Berichten einschlägiger Security-Anbieter gab es 2013 einen neuen Höchststand bei den Zero-Day-Attacken. Aber auch längst bekannte Schwachstellen, für die es seit Monaten oder gar Jahren passende Patches gibt, bieten Angreifern immer wieder ein gern genommenes Einfallstor – all dies vor dem Hintergrund, dass Jahr für Jahr rund 4.000 bis 5.000 kritische Schwach stellen aufgedeckt werden. So wurden im Jahr 2013 pro Woche im Schnitt 100 neue Sicherheitslücken hoher Kritikalität bekannt.

Für den Administrator bedeutet dies vor allem Stress. Von ihm wird erwartet, dass er über die aktuelle Bedrohungslage informiert ist. Dazu müsste er die Warnmeldungen von CERTs (Computer Emergency Response Teams), namhaften Softwarehäusern und Security-Anbietern ebenso regelmäßig verfolgen wie die Berichterstattung einschlägiger Publikationen oder Blogs.

Zeitdruck bei der Schwachstellen-Behebung

Beim Auftreten neuer Risiken muss der Sicherheitsverantwortliche möglichst unverzüglich ermitteln, ob Geräte seines Unternehmens betroffen sind, und wenn ja, wie viele und welche Endgeräte. Sobald er über die benötigten Patches oder Workarounds verfügt, steigt sein Zeitdruck nochmals an. Denn auch Cyber-Kriminelle kennen mit Erscheinen des Patches die Sicherheitslücke.

Verfügbare Patches muss der Administrator zeitnah aufspielen. Häufen sich die neu Aktualisierungen, wie dies zum Beispiel bei Microsofts monatlichem Patchday der Fall ist, so muss er Prioritäten setzen: Soll er zu nächst sämtliche neu verfügbaren Patches auf die unternehmenskritischsten Geräte testen und aufspielen? Oder besser erst eine besonders gefährliche Lücke beheben, die den Großteil seiner Client-PCs betrifft?

Diese Bewertung muss ebenso rasch vonstattengehen wie das Beheben der Schwachstellen und das Reporting über den Patch-Status. In komplexen Umgebungen kann dabei eine Software helfen, die das Schwachstellen-Management weitgehend automatisiert – und dies im Sinne eines „Lifecycle Managements“:

- Informationen zu Schwachstellen einholen
- Sicherheitslücken bewerten und gewichten
- Beheben der Schwachstelle (Patches und Software-Updates einspielen, Workarounds, Scripting, Abschalten von Funktionen, Browser-Add-ons etc.)
- Unternehmensweites Reporting

Integrierte Lösungen laden regelmäßig und automatisch Daten über die neuesten Schwachstellen sowie täglich aktualisierte Regelwerke aus namhaften Internet-Quellen. So kann die Software auf der Basis der jeweils aktuellsten Regeln einen automatisierten Schwachstellen-Scan der Betriebssysteme und Applikationen aller verwalteten PCs durchführen.

Für den Echtzeit-Überblick sorgt in der Regel ein Dashboard, das den Sicherheits- und Compliance-Status visualisiert, beispielsweise per Tortendiagramm und Ampelfarben. Idealerweisel assen sich grafische Elemente anklicken, so dass ein Drill-down zu den jeweiligen Geräten und Patches möglichist.

Automatisiertes Client Lifecycle Management

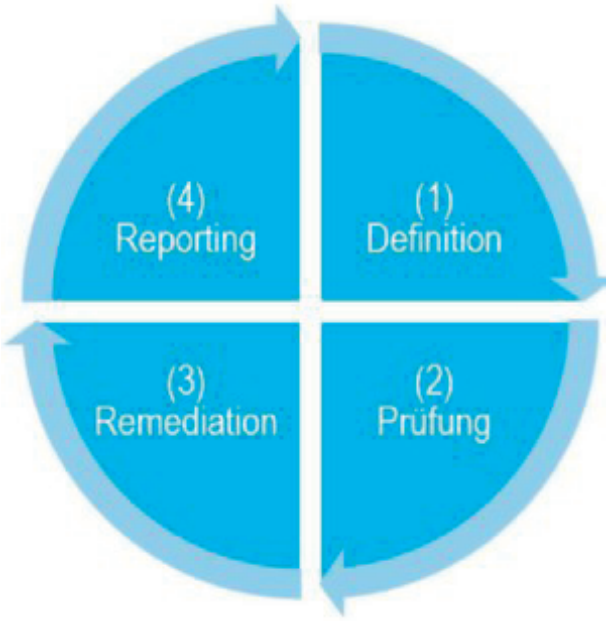
Die Maßnahmen, um Sicherheits lücken zu beseitigen, sind sehr vielfältig: Sie reichen vom einfachen Schließen eines Ports an der Firewall über Betriebssystem-Upgrades (etwa die letzthin viel diskutierte Migration weg von WindowsXP) bis hin zur forensischen Analyse einzelner von Schadsoftware befallener Endgeräte.

Der häufigste Fall im IT-Alltag dürftej edoch sein, dass der Administrator gefährdete Rechner ermittelt und die Schwachstellen dann durch gezielte Verteilung von Software-Updates oder Patches beseitigt. Moderne Lösungen für das Client Lifecycle Management (CLM) kombinieren zu diesem Zweck Standardfunktionen wie eine Inventarisierung, das Aufspielen von Betriebssystemen, Softwareverteilung, Patch

Management und Mobile-Device-Management zusammen mit einem integrierten Schwachstellenmanagement.

Die Kernaufgabe einer CLM-Lösung ist die strukturierte Umsetzung jener Aufgaben, die im Laufe eines Software-Lebenszyklus ständig wiederkehren. Diese Aufgaben folgen dem immer gleichen Muster:

Auf die Definition eines Sollzustands (1) folgt die Prüfung zum Abgleich des Client-Bestands mit diesen Vorgaben (2), daraufhin die Behebung (3) festgesteller Abweichungen („Remediation“ genannt) sowie schließlich ein Reporting über den nun erzielten Zustand (4). Letztere Informationen bilden dann wiederum die



Auf die Definition eines Sollzustands (1) folgt die Prüfung zum Abgleich des Client-Bestands mit diesen Vorgaben (2), darauf hin die Behebung (3) festgesteller Abweichungen („Remediation“ genannt) sowie schließlich ein Reporting über den nun erzielten Zustand (4). Letztere Informationen bilden dann wiederum die Informationsbasis für die nächste Runde im ununterbrochenen Aktualisierungskreislauf.

Aus CLM-Sicht ist das Auftreten von Schwachstellen schlicht eine (wenn auch sicherheits-, zeit- und geschäftskritische) Abweichung vom gewünschten Sollzustand. Die Integration von Funktionen zur Behebung von Schwachstellen in eine umfassende Client-Lifecycle-Management-Suite erleichtert dem Systemverantwortlichen die Arbeit erheblich. Und sie verschafft ihm einen wichtigen Zeitvorsprung – ein Vorteil, der beim Auftreten kritischer Sicherheitslücken für sein Unternehmen entscheidend sein kann.

*Armin Leinfelder ist Produktmanager bei der baramundisoftware AG in Augsburg.

▸ Die baramundi Management Suite 2014

Mit der baramundi ManagementSuite (bMS) 2014 bietet der deutsche Sicherheitsanbieter baramundi eine integrierte Lösungen für das Schwachstellenmanagement. Sie kombiniert Standardfunktionen wie Inventarisierung, Softwareverteilung und Mobilgeräteverwaltung mit einem integrierten Schwachstellenmanagement.

Das neue Modul baramundi Compliance Management dient in bMS2014 als integrierte Managementumgebung für Schwachstellen-Scans. Hierzu werden regelmäßig neue Regelwerke von namhaften Quellen über einen baramundi-Dienst heruntergeladen. Anhand dieser Regeln steuert die Lösung die Schwachstellen-Scans auf allen zu verwaltenden Rechnern. Dies ermöglicht die kontinuierliche Überprüfung auf bekannte Sicherheitslücken.

Copyright © 2014 – Vogel Business Media

Dieser Beitrag ist urheberrechtlich geschützt.
Sie wollen ihn für Ihre Zwecke verwenden?
Infos finden Sie unter www.mycontentfactory.de.

Dieses PDF wurde Ihnen bereitgestellt von http://www.security-insider.de