baramundi

Whitepaper

Schwachstellenmanagement

Sicherheitslücken automatisiert erkennen und schnell schließen?

Empower your IT

INHALT

1 Mut zur Lücke – nein danke! 2
2 Von der Schwachstelle zur Cyber-Attacke 3
2.1 Begriffsklärung: Schwachstelle, Exploit und Co 3
2.2 Der Lebenslauf einer Schwachstelle 4
2.3 Angriffsvektoren: So umgehen Attacken Ihre Firewall 5
3 Schwachstellen identifizieren und schließen 7
3.1 Nicht praktikabel: Manuelles Schwachstellenmanagement 7
3.2 Sicherheitslücken automatisiert auf jedem Client aufspüren 7
3.3 Sicherheitslücken zentral und automatisiert schließen 9
4 Konfigurationsmanagement 10
4.1 Sichere Einstellungen durchsetzen 10
4.2 Ausnahmen bestätigen die Regel 11
5 Vom Schwachstellenmanagement zur Endpoint Security 13

© 2017 baramundi software AG

Aussagen über Ausstattung und technische Funktionalitäten sind unverbindlich und dienen nur der Information. Änderungen vorbehalten. DocID 170619

Vorstand: Dipl.-Ing. (FH) Uwe Beikirch | Dr. Lars Lippert
Aufsichtsratsvorsitzender: Dr. Dirk Haft
Sitz und Registergericht: Augsburg, HRB-NR. 2064 | Ust-IdNr. DE 210294111

1 Mut zur Lücke – nein danke!

Es war der 12. Mai 2017 an dem die bislang größte Ransomware-Attacke Großunternehmen, Behörden, Institutionen und Krankenhäuser in mehr als 150 Ländern weltweit heimsuchte: WannaCry. Nach Befall eines Computers verschlüsselt dieses Schadprogramm bestimmte Benutzerdateien des Rechners und fordert als Ransomware[1] den Nutzer auf, einen bestimmtem Betrag zu zahlen und nach ungenutztem Ablauf einer Frist droht das Programm mit Datenverlust. Außerdem versucht das Programm, als Computerwurm weitere Windows-Rechner zu infizieren und installiert die Backdoor „DoublePulsar".

Dieser und ähnliche spektakuläre und schlagzeilenträchtige Cyberangriffe, bei denen tausende Datensätze gestohlen oder gelöscht werden, sind keineswegs nur Geniestreiche von hochtalentierten Hackern. Vielmehr gehen sie immer öfter auf das Konto von Kriminellen, die ohne teures Equipment und ohne Profiprogrammierkenntnisse auskommen. Sie nutzen die im Internet kostenlos verfügbaren Exploits für die vielen tausend Schwachstellen, die potentiell auf jedem Windows-Client und -Server im Unternehmen vorhanden sind. Über jede dieser Lücken könnte ein erfolgreicher Angriff geführt werden. Firewalls und Virenscanner bieten bei derartigen Angriffen keinen effektiven Schutz und werden einfach umgangen. Gefährlich kann es auch werden, wenn ein Gerät nicht sicher konfiguriert ist: Ein schwaches Passwort, das seit Jahren nicht mehr geändert wurde, macht Angreifern ihr Treiben unnötig einfach.

Mut zur Lücke ist vor diesem Hintergrund für IT-Administratoren keine Tugend. Schließlich tragen sie die Verantwortung für die Sicherheit der Daten und einen störungsfreien Betrieb der Infrastruktur. Kundendaten, Geschäftszahlen, Entwicklungsunterlagen – die Konsequenzen eines erfolgreichen Cyberangriffs können den Betrieb lahmlegen und Firmeninterna offenlegen. Neben finanziellen Verlusten und einem Imageschaden für das Unternehmen drohen im ungünstigsten Fall sogar staatsanwaltschaftliche Ermittlungen, zum Beispiel, wenn der Verdacht auf einen Verstoß gegen Datenschutzregeln besteht oder gekaperte Firmenrechner in einem Botnet zusammengeschaltet und ferngesteuert für Cyberangriffe genutzt wurden – in diesem Fall führt die Spur der IP-Adresse in das eigene Unternehmen.

Angesichts der hohen und ständig weiter steigenden Zahl von Sicherheitslücken ist es für einen IT-Administrator allerdings de facto nicht möglich, ohne automatisierte Hilfsmittel den Überblick zu behalten und zuverlässig für größtmögliche Sicherheit auf allen Endgeräten zu sorgen. Gleiches gilt für die Konfiguration der zahlreichen Geräte im Unternehmen. Dieses Whitepaper beschreibt, welche Gefahren drohen und wie mit Hilfe einer Endpoint-Management-Software ein automatisiertes Schwachstellenmanagement aufgebaut wird, um gefährliche Lücken zuverlässig aufzuspüren und schnell zu schließen.

[1] https://de.wikipedia.org/wiki/Ransomware

2 Von der Schwachstelle zur Cyber-Attacke

2.1 Begriffsklärung: Schwachstelle, Exploit und Co

Eine Schwachstelle ähnelt einem vergessenen offenen Fenster im Haus: Sie stellt einen sicherheitsrelevanten Fehler in einem IT-System oder einer Institution dar. Es besteht also potentiell die Möglichkeit, dass ein Ganove einbricht – dies ist aber keine zwingende Folge. Dennoch wäre es fahrlässig, das Fenster unnötig lange offen stehen zu lassen.

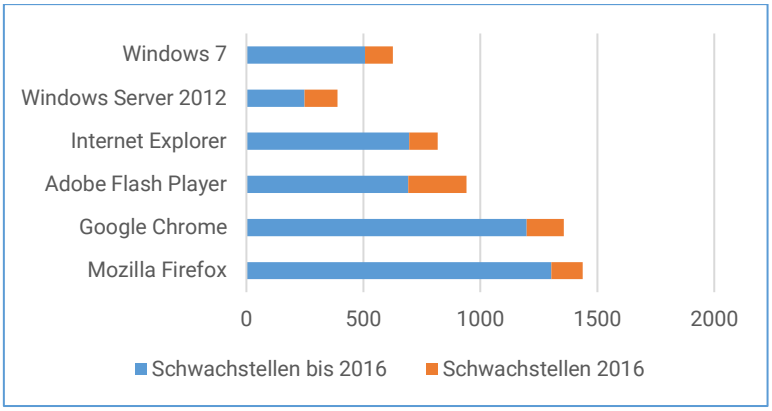
Gefährlich wird es, wenn ein Exploit zu der Schwachstelle existiert: ein passendes Werkzeug, um die Lücke auszunutzen. Denn nun hat der Ganove die Leiter in der Hand, mit der er das offene Fenster erreichen kann. Doch während ein dunkel gekleideter Mann mit Panzerknacker-Augenbinde und Aluleiter in der Nachbarschaft für Aufsehen sorgen könnte, lassen sich Exploits bequem und weitgehend anonym aus dem Internet herunterladen. Inzwischen hat sich eine ganze Schattenindustrie etabliert, die davon lebt, mit Exploits Geld zu verdienen. Die Bezahlung erfolgt einfach über Dienste wie PayPal. Daneben sind auch kostenlose Exploits verfügbar.

Exploits werden verwendet, um den sogenannten Payload auf das angegriffene System einzuschleusen – ein beliebiges Schadprogramm, das Daten ausspäht, Dateien löscht oder den Client zum Teil eines Botnets macht – sozusagen der Sack, in den der Einbrecher seine virtuelle Beute stopft und sie wegträgt.

Ein Framework wie Metasploit, das eigentlich als Tool zum Aufspüren von Sicherheitslücken gedacht ist, ermöglicht es auch wenig versierten Usern, Exploits einzusetzen und Angriffe auszuführen. Metasploit wird einfach unter Windows oder Linux installiert, steht menügesteuert oder mit grafischer Benutzeroberfläche zur Verfügung und ist auch als virtuelle Maschine verfügbar. Wem das immer noch zu kompliziert ist, der holt sich Unterstützung in Internetforen oder YouTube-Kurzanleitungen. Potenzielle Angreifer verfügen also über ein Tool, das ähnlich simpel zu bedienen ist wie eine Leiter, aber viel weniger auffällt.

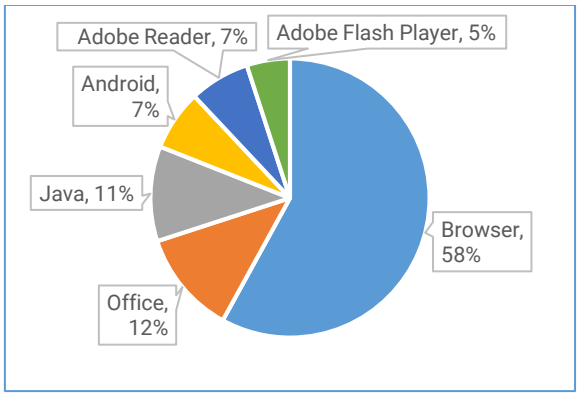
2.2 Der Lebenslauf einer Schwachstelle

Software ist ein hochkomplexes Produkt: Laut Microsoft besteht Windows 7 zum Beispiel aus rund 40 Millionen Zeilen Programmcode. Als Messlatte für eine gute Software gilt ein Wert von weniger als einem Fehler pro 1.000 Codezeilen. Auch bei der besten Qualitätskontrolle bleiben also genug Lücken offen, die sich alle zu einem Problem für die IT-Sicherheit entwickeln können.



Schwachstellenüberblick [2]verschiedener Software-Produkte

Solange die Schwachstelle im Verborgenen schlummert, sind die Risiken gering. Anders sieht es aus, wenn das offene Fenster jemand auffällt – einem Entwickler, einem Sicherheitsexperten oder einem Hobby-Programmierer. Diese Personen tauschen sich in Internetforen aus und dokumentieren entdeckte Schwachstellen in Datenbanken und melden sie an den Softwarehersteller. Große Unternehmen wie Microsoft oder Google zahlen Prämien für neu entdeckte Lücken, um diese schnell schließen zu können.



Überblick [3]Security-Angriffe nach Häufigkeit im Jahr 2016

[2] Quelle: https://www.cvedetails.com
[3] Quelle: https://securelist.com

In der Regel dauert es auch nicht lange, bis ein entsprechender Patch bereitsteht, der die Lücke schließt. Doch damit ist die Gefahr noch nicht ausgeräumt – im Gegenteil: Denn auch Exploit-Entwickler lesen Schwachstellendatenbanken und erfahren so von Lücken. Und sie analysieren die vom Hersteller bereitgestellten Patches und können daraus Rückschlüsse ziehen, wie sich die Lücke ausnutzen lässt. Solange der Patch nicht auf allen von der Lücke betroffenen Geräten eingespielt wurde, sind unter Ausnutzung der bekannten Schwachstelle wirkungsvoll Angriffe möglich.

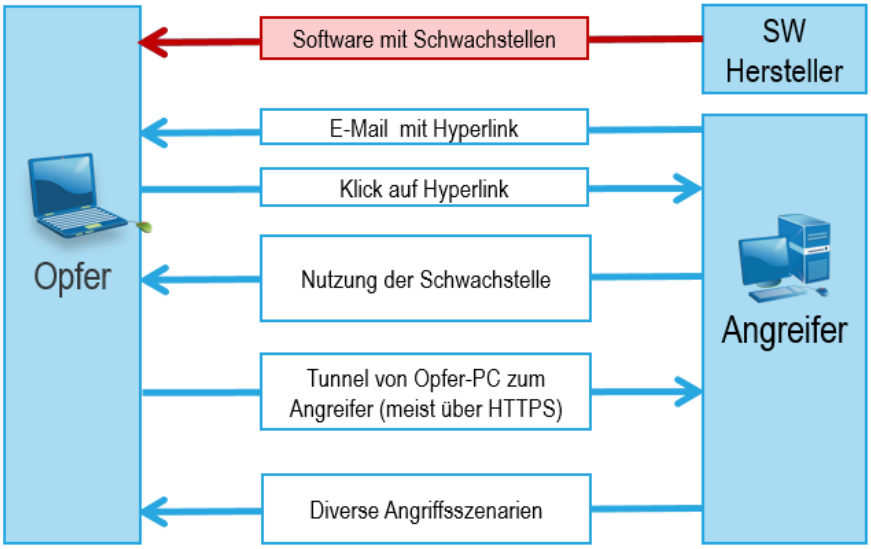
Gefährdung bis zum Schließen der Lücke auf allen Geräten

2.3 Angriffsvektoren: So umgehen Attacken Ihre Firewall

In der Vergangenheit versuchten Cyberkriminelle in der Regel, die Firewall auszuhebeln und verschafften sich so Zugriff auf das Netzwerk dahinter. Doch mittlerweile sind die Sicherheitsvorkehrungen derart ausgefeilt und wirkungsvoll, dass dieser Weg kaum noch Erfolg verspricht.

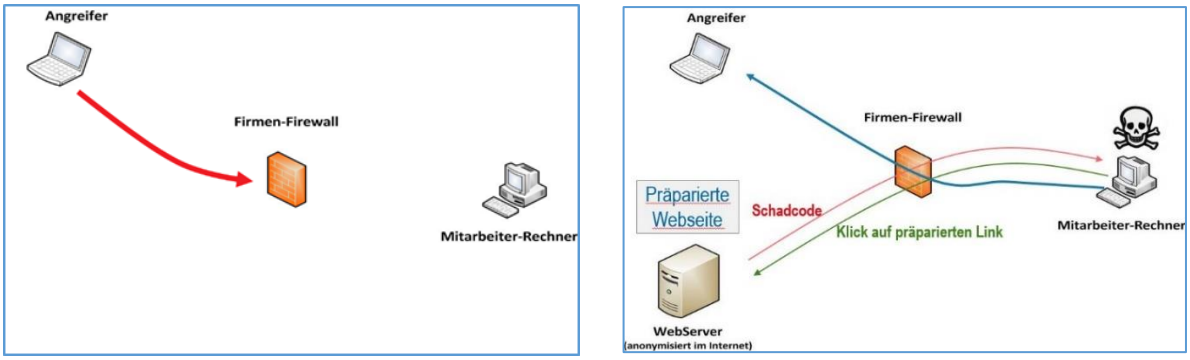
Die Online-Ganoven von heute wählen daher subtilere Methoden: Teilweise erfolgen Angriffe über Anzeigen auf eigentlich harmlosen Webseiten. Oder die Angreifer locken ihr Opfer auf präparierte Webseiten, die Schadcode verteilen. Zum Einsatz kommen auch manipulierte Dateien, die Schwachstellen im Anzeigeprogramm ausnutzen (DOC, PDF, …), die Anwendern zugespielt werden. Dabei verwenden die Angreifer Informationen aus sozialen Netzwerken und ähnlichen Quellen, um die Zielpersonen in die Falle zu locken.

Ein klassisches Beispiel: Eine E-Mail an die Mitarbeiter eines großen Unternehmens mit einer Betreffzeile, die sensationelle Rabatte für ein beliebtes Produkt verspricht. Mit an Sicherheit grenzender Wahrscheinlichkeit wird ein gewisser Prozentsatz der Empfängerinnen und Empfänger den Link in der E-Mail anklicken. Doch was sich dann öffnet, ist ein Fake-Webshop, der auf eine Schwachstelle im Browser oder Flashplayer zielt. Der Nutzer ärgert sich kurz über die Seite, die nicht mal wieder nicht richtig lädt, schließt das Fenster – wird aber sicher nicht den Administrator informieren, da privates Surfen am Arbeitsplatz eigentlich verboten ist.



Mögliches Angriffsszenario durch eine Software-Schwachstelle

Existierte auf dem PC, auf dem der präparierte Link aufgerufen wurde, die Sicherheitslücke, ist es bereits zu spät: Der Angriff war erfolgreich. Auf dem Rechner befindet sich nun Schadsoftware, die mit dem Angreifer Kontakt aufnimmt. Da diese Verbindung aus dem Unternehmensnetzwerk heraus aufgebaut wird, ist die Attacke aus Sicht der Firewall nicht zu erkennen.



Verbindungsaufbau zum Angreifer

Eine gute Firewall, wirkungsvolle Antivirensoftware und ein Management der Benutzerrechte sind daher zwar weiter essentiell. Sie müssen aber durch weitere Maßnahmen ergänzt werden: durch die Sensibilisierung aller User. Und vor allem durch ein konsequentes und schnellstmögliches Schließen aller Sicherheitslücken auf allen Geräten.

3 Schwachstellen identifizieren und schließen

3.1 Nicht praktikabel: Manuelles Schwachstellenmanagement

Von Hand ist es für einen Administrator in der Praxis nahezu unmöglich, alle PCs, Notebooks und Server in seiner Umgebung auf alle bekannten Schwachstellen abzuklopfen: In den letzten 3 Jahren[4] wurden in der National Vulnerability Database[5] über 24.000 neue Sicherheitslücken registriert – rund 150 pro Woche. Hinzu kommen bereits länger bekannte Lücken in noch genutzten Programmen, kombiniert mit verschiedenen Sprachversionen sowie gegebenenfalls Betriebssystemen und Prozessorarchitekturen.

Der Administrator müsste laufend Datenbanken und Blogs auf Meldungen über Schwachstellen durchsuchen, diese bewerten, die eigenen Rechner prüfen, Updates paketieren, testen, verteilen und erfassen, ob die Verteilung erfolgreich war. In größeren Netzwerken und bei verteilten Standorten sowie Außendienstmitarbeitern ist dieser Ansatz zum Scheitern verurteilt. Gleichzeitig muss der IT-Verantwortliche aber die Compliance der Umgebung garantieren, gegebenenfalls den Patch-Status reporten können und im Extremfall für Probleme geradestehen.

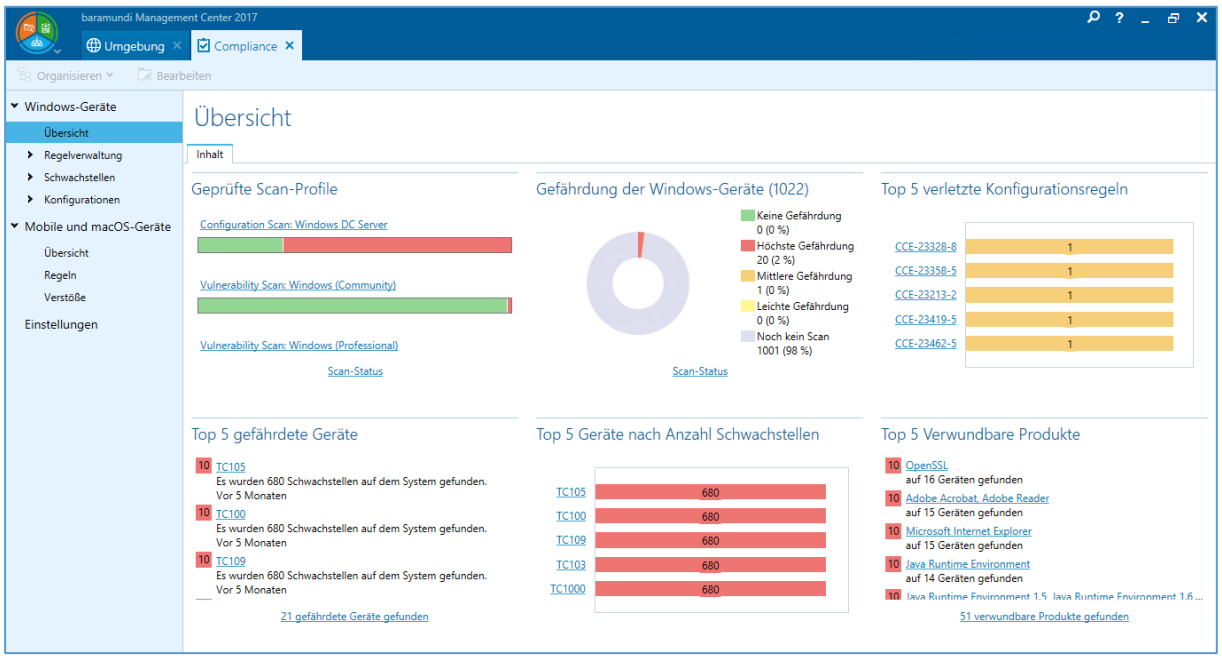
3.2 Sicherheitslücken automatisiert auf jedem Client aufspüren

Es bietet sich daher an, Tools zur Automatisierung einzusetzen, wie zum Beispiel die Endpoint-Management-Software baramundi Management Suite. Eine solche Lösung scannt die Clients und Server in der Umgebung laufend auf Schwachstellen und bietet die Möglichkeit, Lücken zentral und schnell zu schließen. Dabei werden sowohl Geräte berücksichtigt, die im Unternehmens-Hauptstandort verbunden sind, als auch Endgeräte in Außenstandorten oder von Außendienstmitarbeitern (bspw. im Homeoffice).

Dazu greift das System auf die ständig aktualisierten Schwachstellendatenbanken anerkannter Organisationen zu. Der Schwachstellenscanner in der baramundi Management Suite nutzt bspw. inzwischen einen Katalog von über 20.000 bekannten Schwachstellen, um Sicherheitslücken in der IT-Umgebung aufzudecken. Ein übersichtliches Dashboard zeigt dem Administrator den Zustand seiner Umgebung an. Listendarstellungen erlauben einen Drill-down nach Rechner, Schwachstelle oder Gefährdungsgrad: So können gezielt die Geräte mit den meisten Sicherheitslücken, die häufigsten Schwachstellen in der Umgebung oder die gefährlichsten Lücken identifiziert werden, um sie schnellstmöglich zu beseitigen.

---

[4] April 2014 bis April 2017
[5] https://nvd.nist.gov



baramundi Management Suite: Übersicht über Gefährdung der Umgebung

Dieser Schwachstellenscan findet bei minimiertem Ressourcenverbrauch im Hintergrund statt und beeinträchtigt den angemeldeten Nutzer am Client nicht bei der Arbeit. Gleichzeitig nimmt er potentiellen Angreifern den Vorsprung: Der Administrator erhält alle nötigen Informationen, um bestehende Lücken schnellstmöglich zu schließen, ehe sie für Attacken genutzt werden können.

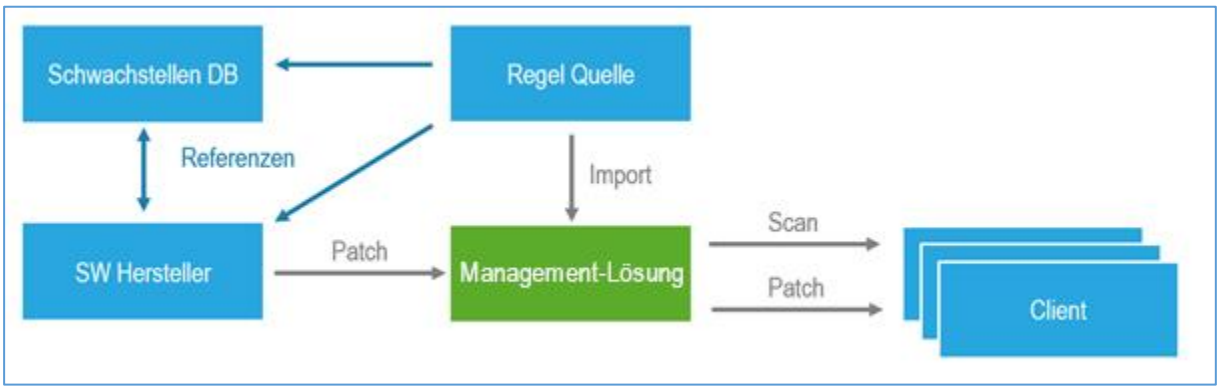
Schnelle Installation des Patches verringert die rot markierte Zeitspanne, in der Angriffe wahrscheinlich sind

3.3 Sicherheitslücken zentral und automatisiert schließen

Um die nötigen Updates und Patches zu verteilen, bietet die Endpoint-Management-Software ebenfalls automatisierte Lösungen an. Updates für Microsoft-Produkte werden über ein Patch-Management-Modul bereitgestellt, das die Rechner regelbasiert mit allen erforderlichen Updates versorgt. Die Installationen laufen im Hintergrund ab und nötige Reboots werden zusammengefasst, um die Installationsdauer so kurz wie möglich zu halten. Da Patches von mehreren Datei-Servern installiert werden können, bleibt auch die Netzwerklast gering. Der Administrator gibt Patches automatisch oder manuell frei und definiert verschiedene Regeln für unterschiedliche Gruppen. Nach Einführung der kumulativen Patches von Microsoft, ist es möglich, die funktionalen und sicherheitsrelevanten Updates auch gebündelt auf die Clients und Server auszurollen.

Programm-Updates von Nicht-Microsoft-Produkten werden ebenfalls von anderen Software-Herstellern (z. B. Adobe, Mozilla) als verteilfertige Softwarepakete bereitgestellt, die auch zur Erst- oder Deinstallation genutzt werden können. Die automatisierte Verteilung übernimmt ebenfalls die Endpoint-Management-Software – auch an Außenstandorten, die nur über das Internet angebunden sind, oder auf den Notebooks von Außendienstlern.

Da alle Prozesse in die Endpoint Management Suite eingebunden sind, erhält der IT-Administrator eine aussagekräftige Rückmeldung zu allen Abläufen: Erfolgreiche Installation, laufende Installation, aufgetretene Fehler – so ist sichergestellt, dass der Sicherheitspatch nicht nur auf die Reise geschickt wurde, sondern auch sein Ziel erreicht und die Lücke geschlossen hat.



Import von Regeln und Patches, Scan der Clients auf Lücken und zentrale Patch-Verteilung

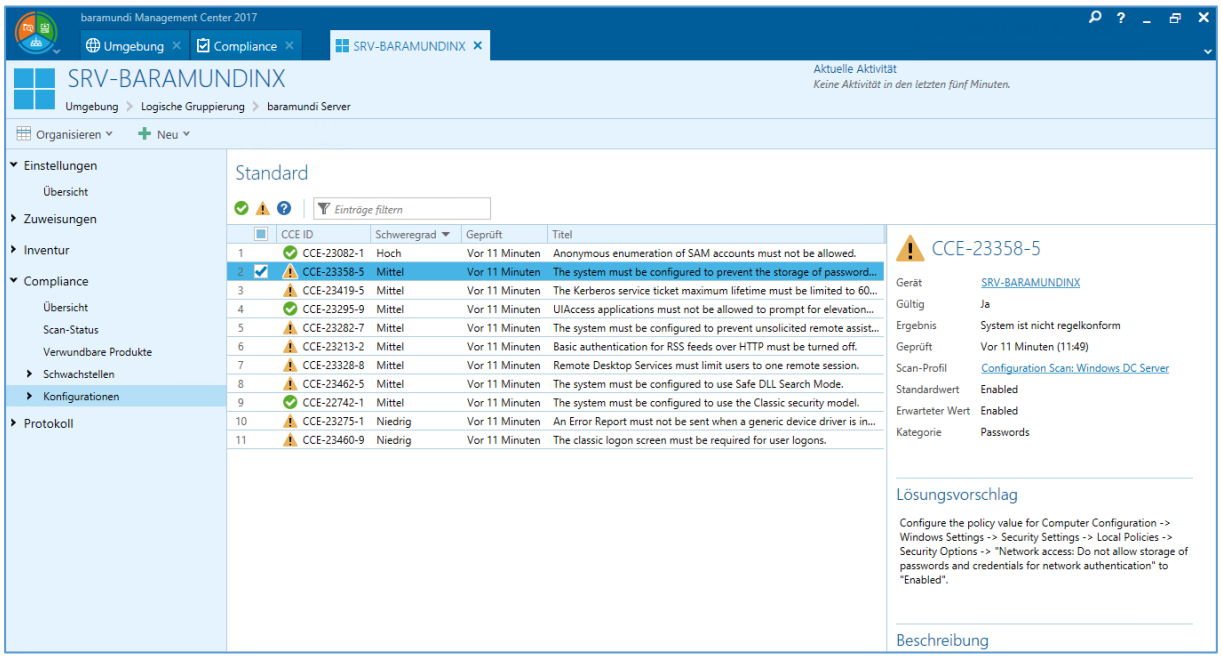
4 Konfigurationsmanagement

4.1 Sichere Einstellungen durchsetzen

Passwortlänge und Ablaufdatum oder die Passwortabfrage nach dem Standby – derartige Einstellungen sind essentiell für das Sicherheitsniveau eines Gerätes. Ebenso wichtig ist es, zu erfahren, ob Autoplay für alle Laufwerke deaktiviert ist, welche Arten von Remote-Zugriffen auf entfernte Rechner möglich sind oder ob eine reversible Passwort-Verschlüsselung zugelassen ist.

Derartige Einstellungen werden zwar in der Regel über Gruppenrichtlinien verteilt und vorgegeben. Um ein hohes Sicherheitsniveau durchzusetzen, muss jedoch auch geprüft werden, dass sie auf allen Clients angekommen sind. Zudem ist es denkbar, dass die Konfiguration im Rahmen von Supportmaßnahmen oder unbefugt durch den Endanwender verändert wurde.

Genauso wie bei der Suche nach Schwachstellen in Anwendungen und Betriebssystemen ist es für einen IT-Administrator aber in größeren Umgebungen praktisch unmöglich, ohne automatisierte Hilfsmittel die Konfiguration aller Rechner im Auge zu behalten. Abhilfe schafft eine Lösung für Konfigurationsmanagement. Diese prüft auf den Clients einen Regelsatz, der die unternehmensinternen Anforderungen an die Konfiguration widerspiegelt. Derartige Lösungen werden – häufig gebündelt mit Lösungen für das Schwachstellenmanagement – integriert in Endpoint-Management-Systeme angeboten.



Ergebnis eines Konfigurations-Scans auf einem Windows-Endgerät

Sie zeigen dem IT-Administrator übersichtlich auf, auf welchen Geräten welche Verstöße bestehen. Die Ergebnisse des Scans können für den einzelnen Client oder aber aggregiert auf Ebene von Gruppen bzw. Organisationseinheiten angezeigt werden. Dabei werden auch Lösungsvorschläge gegeben, um eventuelle Verstöße gezielt beseitigen zu können.

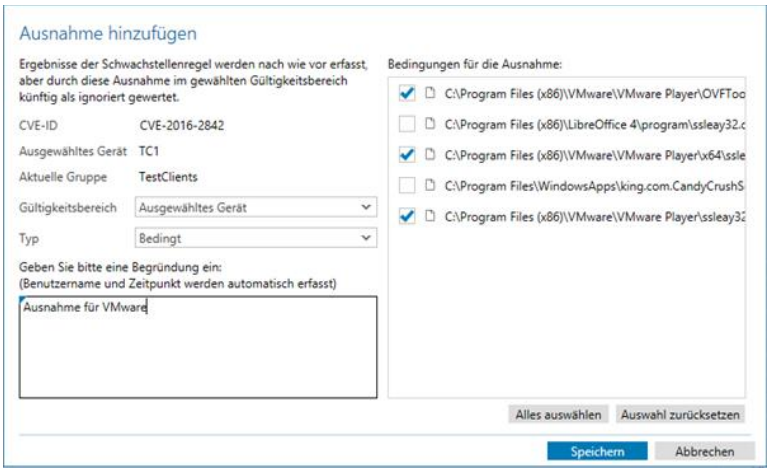
4.2 Ausnahmen bestätigen die Regel

In einer komplexen IT-Umgebung ist in den meisten Fällen auch die Softwarevielfalt sehr groß. Unterschiedlichste Anwendungen von Standardsoftware, spezieller Individualsoftware und/oder verschiedene Betriebssystemkomponenten-Software befinden sich auf den Endgeräten im Unternehmen. Diese Software beinhaltet wiederum vereinzelt Komponenten (z.B. SSL-Bibliotheken), die Schwachstellen enthalten können.

Als Anwender kann man diese Bibliotheken meist nicht isoliert austauschen, ohne ein Update des Programmherstellers zu bekommen. Sind davon betroffene Programme für das Unternehmen entbehrlich, so mag deren Deinstallation das Mittel der Wahl sein. Andernfalls kann eine Nutzen-Risiko-Abwägung auch zur Entscheidung für die Weiternutzung des Programms führen und die OpenSLL-Bibliotheken im dortigen Programmverzeichnis werden entsprechend als Ausnahmen deklariert.

Für ein gutes Schwachstellenmanagement einer Endpoint-Management-Lösung ist es in diesem Fall wichtig, zum einen für Transparenz zu sorgen, dass eine potentielle Sicherheitslücke besteht und zum anderen die Möglichkeit bieten, Ausnahmen zu definieren, dass diese Schwachstellen bewusste und tolerierte Ausnahmen im Unternehmen darstellen.

Im folgenden Beispiel in der baramundi Management Suite wird die gefährdete Bibliothek im Kontext des VMware-Players per Ausnahmeregelung toleriert, wohingegen die gleiche Datei für LibreOffice oder andere Apps nicht akzeptiert wird.



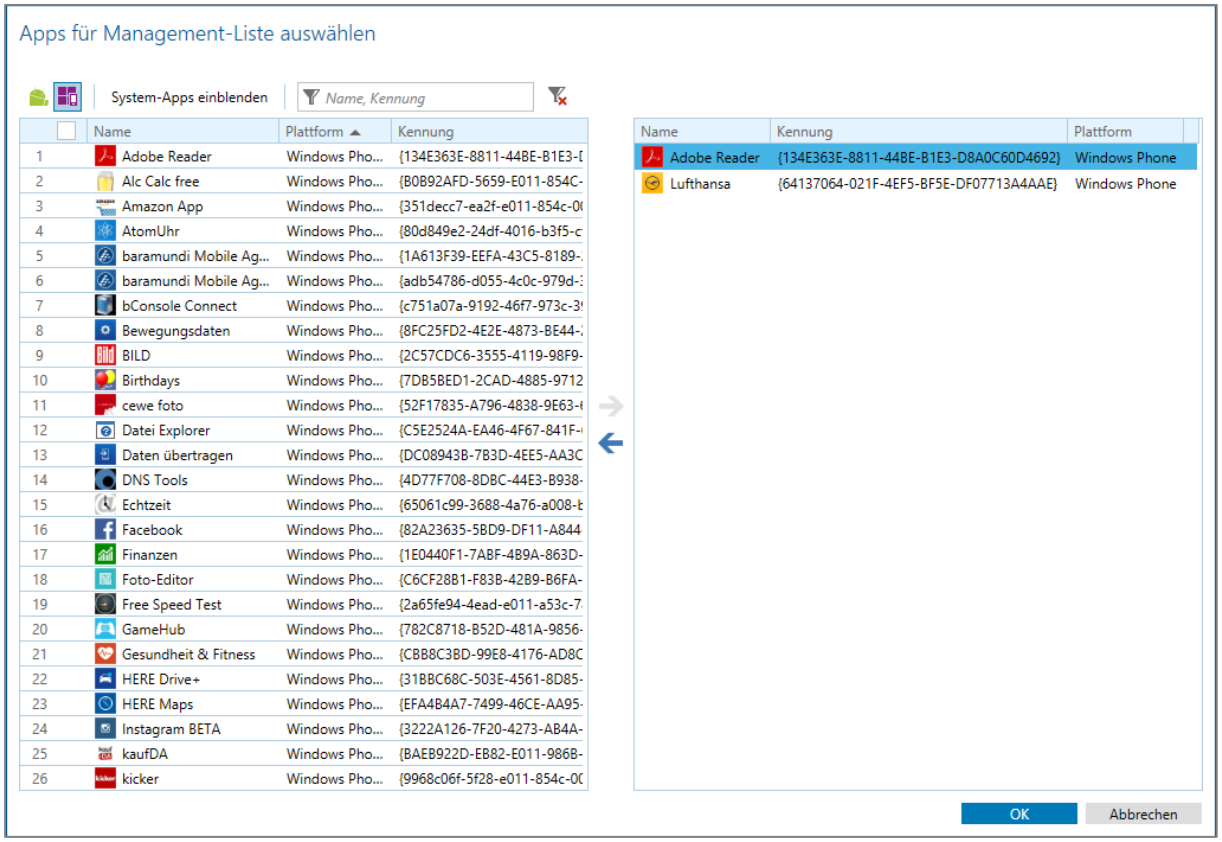
Ausnahmen für Schwachstellen definieren

5 Vom Schwachstellenmanagement zur Endpoint Security

Ein automatisiertes Schwachstellen- und Konfigurationsmanagement ist ein wirkungsvoller Baustein einer erfolgreichen Sicherheitsstrategie. Für hohe Endpoint Security und Datensicherheit müssen jedoch noch weitere Aspekte berücksichtigt werden.

So müssen Sicherheitslücken auch auf Smartphones und Tablets, die inzwischen in nahezu jedem größeren Netzwerk zu finden sind, erkannt werden, um schnell Gegenmaßnahmen einzuleiten. Bei den Mobilgeräten ist ein derartiger Scan mindestens ebenso wichtig wie auf PC-Clients, da die Consumer-orientierten Mobilgeräte in der Regel keine Administratorenrolle vorsehen, über die eine Softwareinstallation durch den Endbenutzer unterbunden werden könnte. Auch hierfür sind automatisierte Tools verfügbar, zum Beispiel das in die baramundi Management Suite integrierte baramundi Mobile Devices. Es prüft frei definierbare Regeln auf den verwalteten Mobilgeräten und erkennt zum Beispiel Jailbreaks bzw. Root-Zugriffe oder unerwünschte Apps.

Weitere Lösungen der Client-Management-Software ermöglichen ein zentrales und automatisiertes Backup von Daten und Benutzereinstellungen, verschlüsseln mobile Datenträger (z. B. USB-Sticks), verhindern unzulässige Kopien auf mobile Speichermedien oder blockieren – mit Hilfe von App Black- und Whitelisting - den Start unbekannter, nicht autorisierter Anwendungen im Unternehmensnetzwerk und unterstützen den Administrator wirkungsvoll dabei, für bestmögliche Sicherheit zu sorgen.



App-Auswahl für Black- oder Whitelisting

Über die baramundi software AG

Die baramundi software AG ermöglicht Unternehmen und Organisationen das effiziente, sichere und plattformübergreifende Management von Arbeitsplatzumgebungen. Mehr als 2.500 Kunden aller Branchen und Größen profitieren weltweit von der langjährigen Erfahrung und den ausgezeichneten Produkten des deutschen Herstellers. Diese sind in der baramundi Management Suite nach einem ganzheitlichen, zukunftsorientierten Unified-Endpoint-Management-Ansatz zusammengefasst: Client-Management, Mobile-Device-Management und Endpoint Security erfolgen über eine gemeinsame Oberfläche, in einer einzigen Datenbank und nach einheitlichen Standards.

Durch die Automatisierung von Routinearbeiten und eine umfassende Übersicht über den Zustand aller Endgeräte optimiert die baramundi Management Suite Prozesse des IT-Managements. Sie entlastet die IT-Administratoren und sorgt dafür, dass Anwendern jederzeit und überall die benötigten Rechte und Anwendungen auf allen Plattformen und Formfaktoren zur Verfügung stehen – auf PCs, Notebooks, Mobilgeräten oder in virtuellen Umgebungen.

Der Firmensitz der baramundi software AG befindet sich in Augsburg. Die Produkte und Services des im Jahr 2000 gegründeten Unternehmens sind komplett Made in Germany. Beim Vertrieb, der Beratung und Betreuung von Anwendern arbeitet baramundi weltweit erfolgreich mit Partnerunternehmen zusammen.

Mehr Informationen zu baramundi: www.baramundi.de

Sie möchten sich die baramundi Management Suite ansehen? Melden Sie sich zum Live-Webinar an

Erleben Sie im kostenfreien Webinar, wie Sie mit der baramundi Management Suite Ihre PC-Clients, Server, Mobilgeräte und Macs automatisiert verwalten und absichern: www.baramundi.de/webinar

baramundi

Wir freuen uns Sie kennenzulernen!

Kontaktieren Sie uns!

baramundi software AG
Beim Glaspalast 1
86153 Augsburg, Germany

+49 821 5 67 08 - 380
request@baramundi.de
www.baramundi.de

+44 2071 93 28 77
request@baramundi.co.uk
www.baramundi.co.uk

+48 735 91 44 54
request@baramundi.pl
www.baramundi.pl

+49 821 5 67 08 - 390
request@baramundi.com
www.baramundi.com

baramundi software USA, Inc.
550 Cochituate Road, Suite 25
Framingham, MA 01701, USA

+1 508 861 75 61
requestUSA@baramundi.com
www.baramundi.com

baramundi software Austria GmbH
Landstraßer Hauptstraße 71/2
1030 Wien, Austria

+43 1 7 17 28 - 545
request@baramundi.at
www.baramundi.at

Empower your IT