



Schwachstellenmanagement

Sicherheitslücken automatisiert erkennen und schnell schließen?

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	4
3	Schwachstellen identifizieren und schließen	6
3.1	Nicht praktikabel: Manuelles Schwachstellenmanagement	6
3.2	Sicherheitslücken automatisiert auf jedem Client aufspüren.....	6
3.3	Sicherheitslücken zentral und automatisiert schließen	8
4	Konfigurationsmanagement	9
4.1	Sichere Einstellungen durchsetzen	9
4.2	Ausnahmen bestätigen die Regel.....	10
5	Vom Schwachstellenmanagement zur Endpoint Security.....	11

© 2024 baramundi software GmbH

Aussagen über Ausstattung und technische Funktionalitäten sind unverbindlich und dienen nur der Information.
Änderungen vorbehalten. DocID 200916

1 Mut zur Lücke – nein danke!

Spektakuläre Cyberangriffe, bei denen unzählige Datensätze gestohlen oder gelöscht werden, sorgen immer häufiger für Schlagzeilen. Dabei sind diese Angriffe 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 Virens Scanner bieten bei derartigen Angriffen keinen effektiven Schutz und werden einfach umgangen. Gefährlich kann es auch werden, wenn ein Gerät nicht sicher konfiguriert ist: Ein Passwort, das seit Jahren für mehrere Accounts genutzt wird, macht Angreifern ihr Treiben unnötig einfach.

Mut zur Lücke ist vor diesem Hintergrund für IT-Admins 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 lahm- 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-Admin 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-Lösung ein automatisiertes Schwachstellenmanagement aufgebaut wird, um gefährliche Lücken zuverlässig aufzuspüren und schnell zu schließen.

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 dar. Es besteht also potentiell die Möglichkeit, dass ein Krimineller 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 Kriminelle die Leiter in der Hand, mit der er das offene Fenster erreichen kann. Doch während eine dunkel gekleidete Person 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.

Exploits werden verwendet, um die sogenannte Payload auf das angegriffene System einzuschleusen – ein beliebiges Schadprogramm, das Daten ausspäht, Dateien verschlüsselt oder den Client zum Teil eines Botnets macht.

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. Wem das immer noch zu kompliziert ist, der holt sich Unterstützung in Internetforen oder TikTok-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 bestand Windows 7 zum Beispiel aus rund 50 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 zu einem Problem für die IT-Sicherheit entwickeln können.

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.

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. 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.



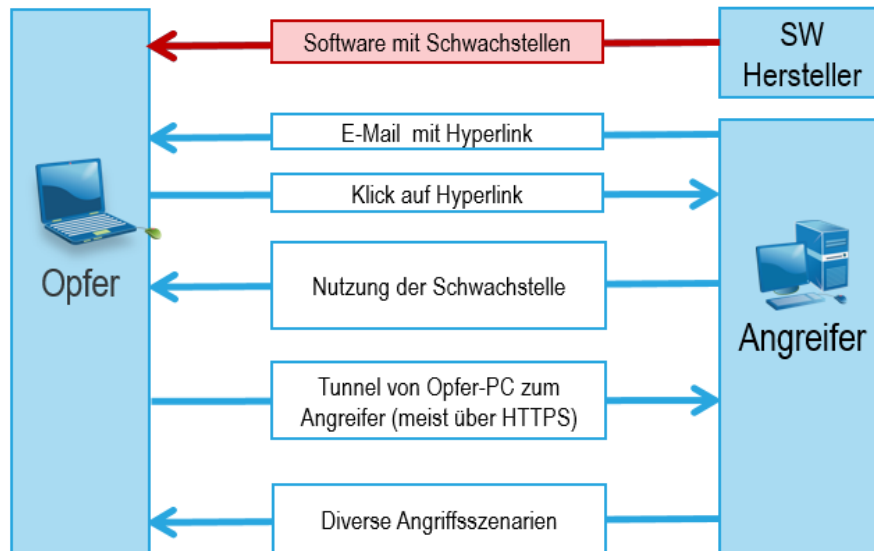
Gefährdung bis zum Schließen der Lücke auf allen Geräten

2.3 Angriffsvektoren: So umgehen Attacken Ihre Firewall

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

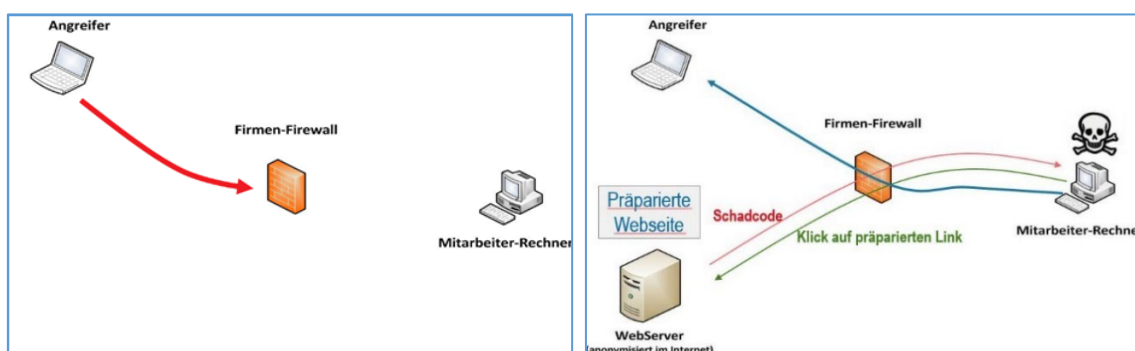
Die Online-Ganoven von heute wählen daher subtilere Methoden: Teilweise erfolgen Angriffe über Links auf eigentlich harmlosen Webseiten. Oder die Angreifer locken ihr Opfer auf präparierte Webseiten, die Schadcode verteilen. Zum Einsatz kommen auch manipulierte Dateien, die Schwachstellen im Anzeigeprogramm ausnutzen (DOCX, PDF, ...), welche den 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 den Anwender zu einem angeblich wichtigen Dokument leiten. Mit an Sicherheit grenzender Wahrscheinlichkeit wird ein gewisser Prozentsatz der Empfängerinnen und Empfänger das Dokument öffnen. Das reicht, um den Exploit auszuführen. Der User bekommt nur mit, dass der Anhang anscheinend fehlerhaft ist.



Mögliches Angriffsszenario durch eine Software-Schwachstelle

Existierte auf dem PC, auf dem der präparierte Link aufgerufen wurde, die Sicherheitslücke, ist es jetzt 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 zusätzliche Maßnahmen ergänzt werden, wie durch die Sensibilisierung aller User. Vor allem aber durch ein konsequentes und schnellstmögliches Schließen bekannter Sicherheitslücken auf allen Geräten.

3 Schwachstellen identifizieren und schließen

3.1 Nicht praktikabel: Manuelles Schwachstellenmanagement

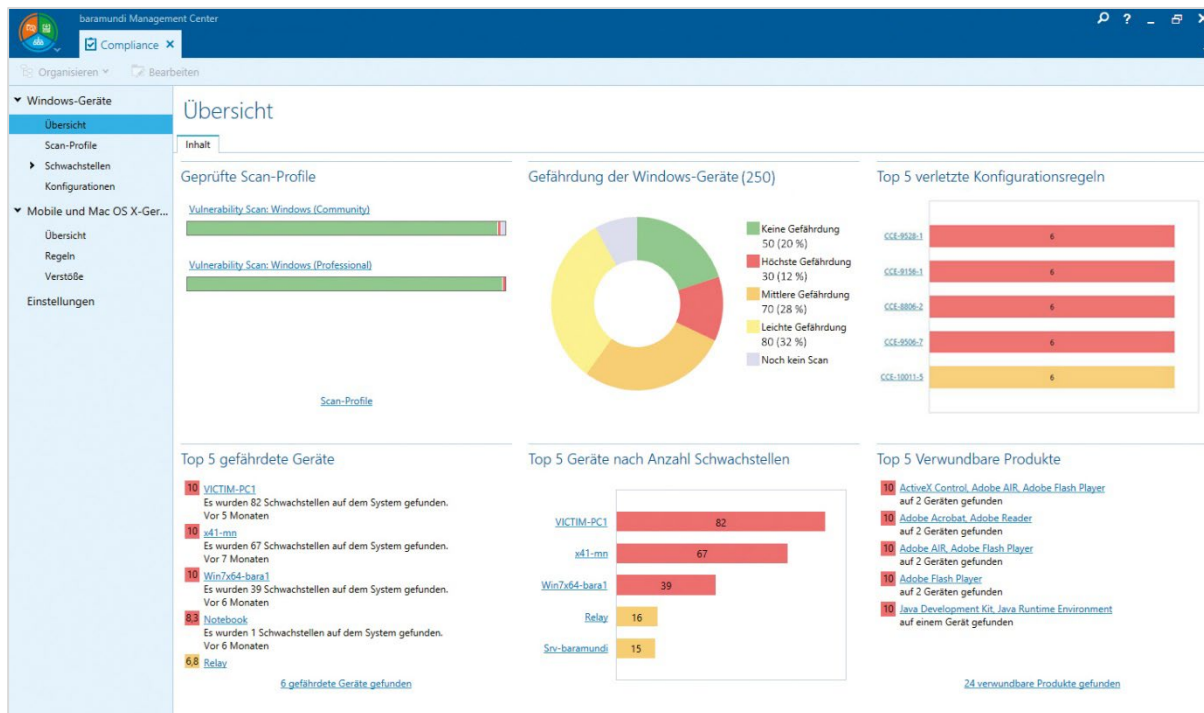
Von Hand ist es für einen Administrator in der Praxis nahezu unmöglich, alle PCs, Notebooks und Server in seiner Umgebung auf alle bekannten Schwachstellen abzuklopfen

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 Patchstatus reporten 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 Lösung 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 sind, als auch Endgeräte in Außenstandorten oder von Außendienstmitarbeitern (bspw. im Home-Office) genutzt werden.

Dazu greift das System auf die ständig aktualisierten Schwachstellendatenbanken anerkannter Organisationen zu. Der Schwachstellenscanner in der baramundi Management Suite nutzt bspw. einen Katalog von bekannten Schwachstellen, um Sicherheitslücken in der IT-Umgebung aufzudecken. Ein übersichtliches Dashboard zeigt den Admins den Zustand ihrer 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.



baramundi Management Suite: Übersicht über Gefährdung der Umgebung

Dieser Schwachstellenscan nimmt potentiellen Angreifern den Vorsprung: Der Administrator erhält die nötigen Informationen, um bestehende Lücken schnellstmöglich zu schließen, ehe sie für Attacken genutzt werden können.



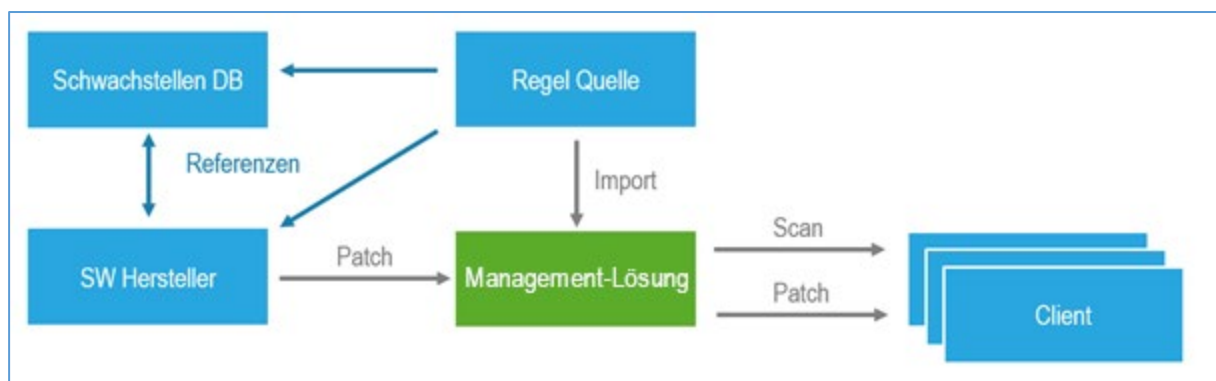
Schnelle Installation des Patches verringert die rot markierte Zeitspanne, in der Angriffe wahrscheinlich sind

3.3 Sicherheitslücken zentral und automatisiert schließen

Um die nötigen Updates und Patches zu verteilen, bietet das Endpoint Management ebenfalls automatisierte Lösungen an. Updates für Microsoft-Produkte werden über ein Update 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. Updates werden automatisch installiert, können aber ggf. vom Admin verzögert oder gesperrt werden.

Programm-Updates von Nicht-Microsoft-Produkten werden ebenfalls von anderen Software-Herstellern (z. B. Adobe, Mozilla) als verteilte Softwarepakete bereitgestellt, die auch zur Erst- oder Deinstallation genutzt werden können. Die automatisierte Verteilung übernimmt ebenfalls das Endpoint Management – 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 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 Remotezugriffe auf Rechner möglich sind oder ob eine angreifbare Passwortverschlüsselung zugelassen ist.

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

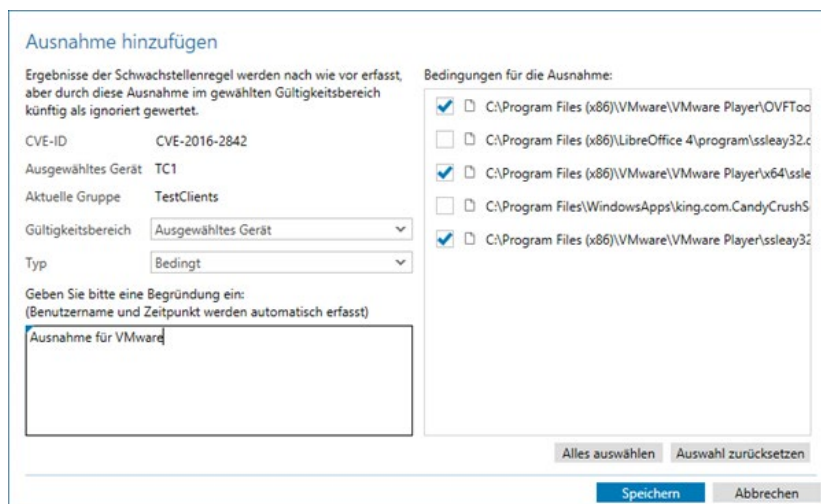
4.2 Ausnahmen bestätigen die Regel

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, wie 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 OpenSSL-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 potenzielle 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.



Ausnahme hinzufügen

Ergebnisse der Schwachstellenregel werden nach wie vor erfasst, aber durch diese Ausnahme im gewählten Gültigkeitsbereich künftig als ignoriert gewertet.

CVE-ID: CVE-2016-2842

Ausgewähltes Gerät: TC1

Aktuelle Gruppe: TestClients

Gültigkeitsbereich: Ausgewähltes Gerät

Typ: Bedingt

Geben Sie bitte eine Begründung ein:
(Benutzername und Zeitpunkt werden automatisch erfasst)

Ausnahme für VMware

Bedingungen für die Ausnahme:

- ☒ C:\Program Files (x86)\VMware\VMware Player\OVFTool.exe
- ☐ C:\Program Files (x86)\LibreOffice 4\program\ssleay32.dll
- ☒ C:\Program Files (x86)\VMware\VMware Player\x64\ssleay32.dll
- ☐ C:\Program Files\WindowsApps\king.com.CandyCrushS...
- ☒ C:\Program Files (x86)\VMware\VMware Player\ssleay32.dll

Alles auswählen Auswahl zurücksetzen

Speichern Abbrechen

Ausnahmen für Schwachstellen definieren

5 Vom Schwachstellenmanagement zur Endpoint Security

Ein automatisiertes Schwachstellenmanagement 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 erkannt werden, um schnell Gegenmaßnahmen einzuleiten. 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 des Endpoint Managements ermöglichen das Verschlüsseln mobiler Datenträger (z. B. USB-Sticks), verhindern unzulässige Kopien auf mobile Speichermedien oder blockieren – mit Hilfe von App Block- und Allowlisting – den Start unbekannter, nicht autorisierter Anwendungen im Unternehmensnetzwerk und unterstützen den Administrator wirkungsvoll dabei, für bestmögliche Sicherheit zu sorgen.

Über die baramundi software GmbH

Die baramundi software GmbH ermöglicht Unternehmen und Organisationen das effiziente, sichere und plattformübergreifende Management von Arbeitsplatzumgebungen. 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 oder Mobilgeräten.

Der Firmensitz der baramundi software GmbH 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.com

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-Endpoints, Server und Mobilgeräte automatisiert verwalten und absichern.

<https://www.baramundi.com/de-de/it-training/webinare/>

Wir freuen uns Sie kennenzulernen!

Kontaktieren Sie uns!



baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Germany

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

 +44 2071 93 28 77
request@baramundi.com
www.baramundi.com

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

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

 +43 19 28 01 36 00 10
request@baramundi.com
www.baramundi.com

 +39 340 8861886
request@baramundi.com
www.baramundi.com

 +41 77 280 49 79
request@baramundi.com
www.baramundi.com

baramundi software USA, Inc.
30 Speen St, Suite 501
Framingham, MA 01701, USA

 +1 508-861-7561
requestUSA@baramundi.com
www.baramundi.com