

Automatisiertes Schwachstellenmanagement

*Sicherheitslücken erkennen,
priorisieren und beheben.*

Inhalt

1 Mut zur Lücke – nein, danke!	03
2 Von der Schwachstelle zur Cyber-Attacke	04
2.1 Begriffsklärung: Schwachstelle, Exploit und Co.	04
2.2 Der Lebenslauf einer Schwachstelle	05
2.3 Angriffsvektoren: So umgehen Attacken Ihre Firewall	05
3 Schwachstellen identifizieren und schließen	07
3.1 Nicht praktikabel: Manuelles Schwachstellenmanagement	07
3.2 Sicherheitslücken automatisiert aufspüren	07
3.3 Sicherheitslücken zentral und automatisiert schließen	09
4 Ausnahmen sicher managen	10

© 2026 baramundi software GmbH | Aussagen über Ausstattung und technische Funktionalitäten sind unverbindlich und dienen nur der Information. | Änderungen vorbehalten.



1 Mut zur Lücke – nein, danke!

Spektakuläre Cyberangriffe mit gestohlenen oder gelöschten Daten sorgen regelmäßig für Schlagzeilen. Dabei stammen viele Angriffe längst nicht mehr von hochqualifizierten Hackern, sondern von Kriminellen, die frei verfügbare Exploits und KI-gestützte Tools einsetzen. Künstliche Intelligenz macht es Angreifern einfacher als je zuvor, Schwachstellen auszunutzen und ihre Angriffe zu automatisieren – entsprechend nimmt die Zahl erfolgreicher Attacken kontinuierlich zu.

Klassische Schutzmechanismen stoßen an ihre Grenzen

Firewalls und Virens Scanner bieten gegen diese modernen Methoden oft keinen wirksamen Schutz, insbesondere wenn Systeme unzureichend konfiguriert oder Passwörter mehrfach wiederverwendet werden. IT-Administratoren müssen daher mehr denn je Verantwortung übernehmen, um Daten und Infrastruktur zu schützen. Finanzielle Schäden, Reputationsverlust und sogar rechtliche Folgen sind reale Risiken, wenn Systeme kompromittiert werden.

Automatisierung ist der Schlüssel zur Sicherheit

Angesichts der wachsenden Zahl an Schwachstellen ist es ohne Automatisierung praktisch unmöglich, den Überblick zu behalten und auf allen Endgeräten für Sicherheit zu sorgen. Dieses Whitepaper zeigt, welche Gefahren aktuell bestehen und wie IT-Abteilungen mit einer modernen Endpoint-Management-Lösung ein automatisiertes Schwachstellenmanagement etablieren, um Sicherheitslücken effizient zu identifizieren und schnell zu schließen.



2 Von der Schwachstelle zur Cyber-Attacke

In diesem Kapitel erfahren Sie, wie Schwachstellen zu Einfallstoren für Cyberangriffe werden und warum nur schnelles Patchen, moderne Sicherheitsmaßnahmen und geschulte Mitarbeitende wirksamen Schutz bieten.

2.1 Begriffsklärung: Schwachstelle, Exploit und Co.

Eine Schwachstelle ähnelt einem offen gelassenen Fenster: Sie ist ein sicherheitsrelevanter Fehler in einem IT-System. Ein Angriff ist zwar nicht zwangsläufig gegeben, doch das Risiko steigt, je länger die Schwachstelle bestehen bleibt. Kritisch wird es, wenn ein Exploit verfügbar ist, also ein Werkzeug, das gezielt diese Lücke ausnutzt. Dann hat der Angreifer sprichwörtlich die Leiter in der Hand, um das offene Fenster zu erreichen.

Solche Exploits können heute einfach und anonym über das Internet bezogen werden als Teil einer florierenden Schattenindustrie. Über Exploits wird Schadsoftware, sogenannte Payload, eingeschleust, die Daten stiehlt, Systeme verschlüsselt oder Geräte in Botnets einbindet. Tools wie Metasploit, einst für Sicherheitsanalysen entwickelt, ermöglichen auch technisch weniger versierten Nutzern das Ausführen solcher Angriffe. In der IT-Sicherheit gilt daher: Eine Kette ist nur so stark wie ihr schwächstes Glied, eine einzelne ungepatchte Schwachstelle kann die gesamte Infrastruktur gefährden.



Sicherheitskette der Endpoint Security

2.2 Der Lebenslauf einer Schwachstelle

Software ist ein hochkomplexes Produkt und selbst bei den besten Qualitätskontrollen bleiben Sicherheitslücken oft unvermeidlich. Entscheidend ist, wie schnell und konsequent mit ihnen umgegangen wird. Solange sie unentdeckt bleiben, ist das Risiko gering. Werden sie jedoch bekannt, entsteht folgende Dynamik:

- ➔ Entwickler, Sicherheitsexperten oder Hobby-Programmierer entdecken Schwachstellen und melden sie über Foren, Datenbanken und direkt an den Hersteller.
- ➔ In der Regel steht zeitnah ein Patch bereit, der die Lücke schließt.
- ➔ Gleichzeitig jedoch nutzen Exploit-Entwickler veröffentlichte Informationen und Patches, um nachvollziehen zu können, wie sich Schwachstellen ausnutzen lassen.
- ➔ Solange der Patch nicht auf allen betroffenen Systemen installiert ist, sind erfolgreiche Angriffe über die bekannte Schwachstelle möglich.



Gefährdung bis zum Schließen der Lücke auf allen Geräten

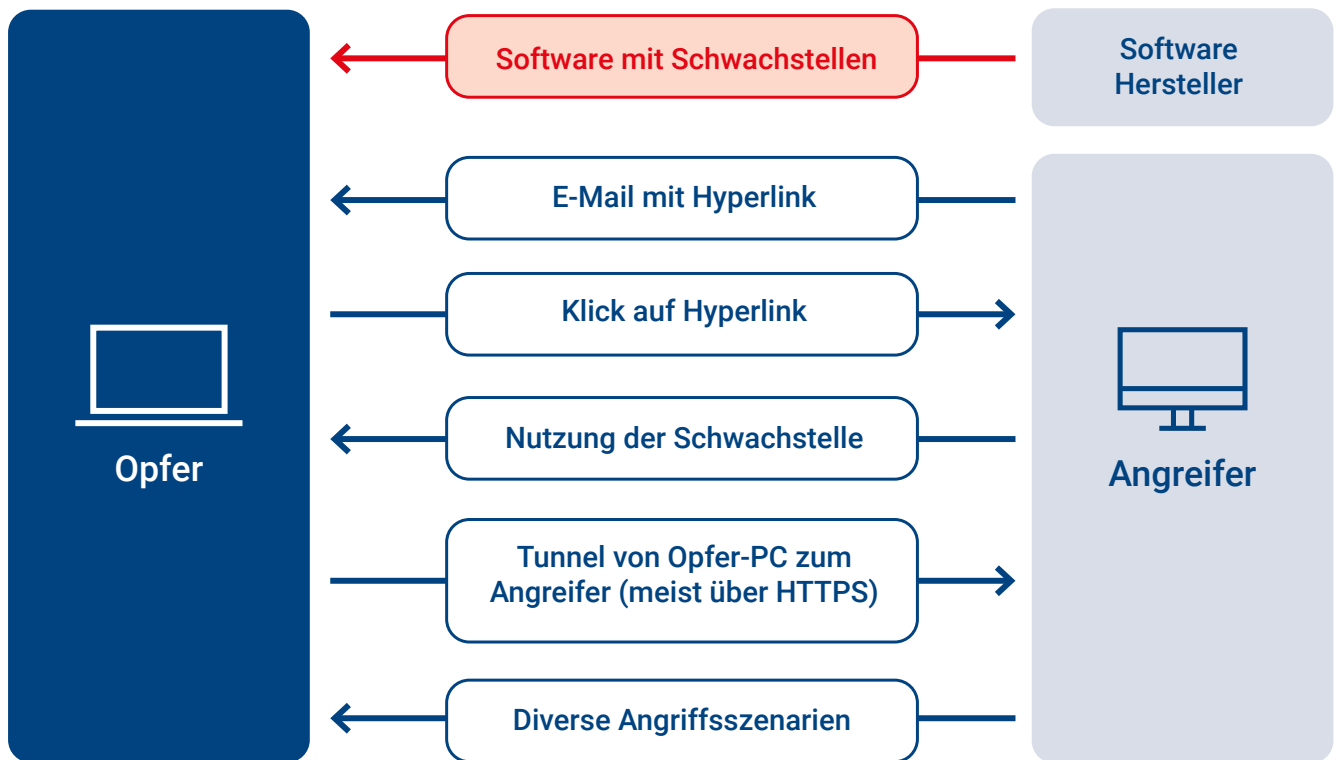
2.3 Angriffsvektoren: So umgehen Attacken Ihre Firewall

Cyberkriminelle greifen Firewalls heute nicht mehr direkt an, sondern nutzen subtilere Umgehungsstrategien wie kompromittierte VPN-Gateways, gestohlene Credentials und ungepatchte Software. KI beschleunigt diese Angriffe massiv: Sie analysiert Schwachstellen in Echtzeit, automatisiert Exploit-Entwicklung und generiert hochpersonalisierte Phishing-Mails, wodurch der Abstand zwischen Bekanntwerden einer Lücke und massenhaften Attacken auf Tage oder Stunden schrumpft.

Häufige Einstiegsvektoren sind präparierte Webseiten, manipulierte Dateien (DOCX, PDF) oder personalisierte E-Mails, die aus öffentlich verfügbaren Social-Media-Daten erstellt werden. Nach der Erstinfektion nutzen Angreifer häufig **Living off the Land-Techniken** (z. B. PowerShell, WMI), um sich unauffällig im System zu bewegen und traditionelle Firewalls zu umgehen.

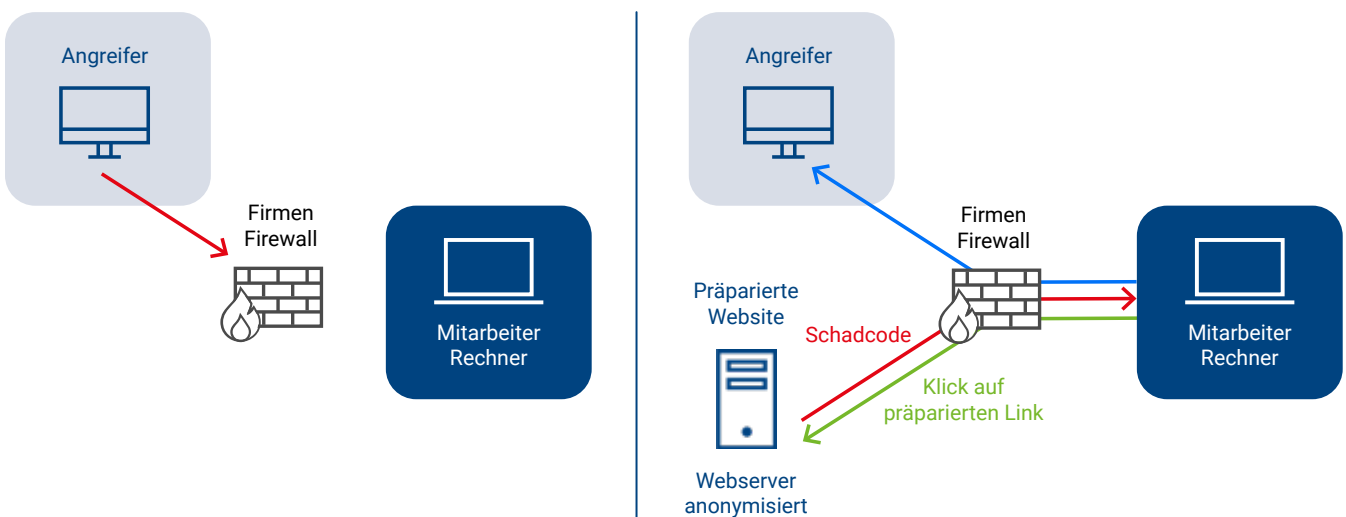


Ein klassisches Beispiel: Eine E-Mail mit der Betreffzeile „Wichtiges Dokument“ führt oft dazu, dass Mitarbeitende den Anhang oder Link öffnen. Der Exploit läuft geräuschlos im Hintergrund, der User sieht nur einen „fehlerhaften Anhang“.



Mögliches Angriffsszenario durch eine Software-Schwachstelle

Falls auf dem betroffenen PC eine Sicherheitslücke existiert, ist der Angriff gelungen: Die Schadsoftware kontaktiert den Angreifer über HTTPS oder DNS-Tunneling und bleibt so für klassische Firewalls unsichtbar.



Verbindungsaufbau zum Angreifer

Eine leistungsfähige Firewall, Endpoint-Security und Rechte-Management bleiben daher weiterhin essenziell, ergänzt durch konsequentes und schnelles Patch-Management und kontinuierliche User-Sensibilisierung.

3 Schwachstellen identifizieren und schließen

In diesem Kapitel erfahren Sie, warum manuelles Schwachstellenmanagement in modernen IT-Umgebungen nicht praktikabel ist und wie automatisierte Lösungen Sicherheitslücken effizient erkennen und schließen.

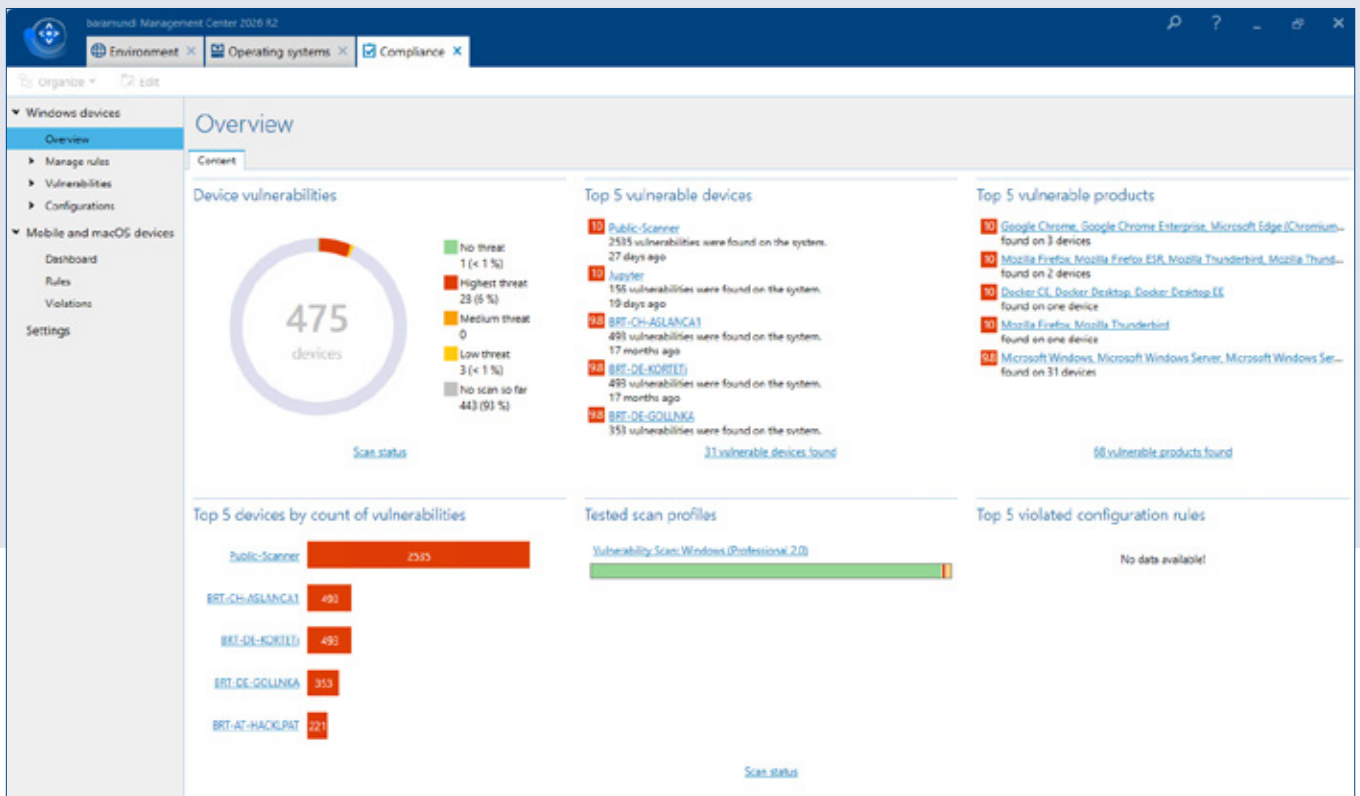
3.1 Nicht praktikabel: Manuelles Schwachstellenmanagement

Für IT-Admins ist eine manuelle Überprüfung aller PCs, Notebooks und Server auf Schwachstellen nahezu unmöglich. Sie müssten ständig Datenbanken und Blogs nach neuen Meldungen durchsuchen, Lücken bewerten, Updates paketieren, testen, verteilen und den Erfolg überprüfen. In großen, verteilten Netzwerken mit Mitarbeitenden im Außendienst oder Home-Office ist dieser Ansatz zum Scheitern verurteilt. Gleichzeitig muss der IT Verantwortliche jedoch die Compliance gewährleisten, den Patchstatus bei Bedarf reporten und im Ernstfall für Probleme einstehen.

3.2 Sicherheitslücken automatisiert aufspüren

Zur Automatisierung des Schwachstellenmanagements eignen sich Tools wie die baramundi Management Suite. Solche Systeme scannen Clients und Server in der gesamten IT-Umgebung kontinuierlich auf Sicherheitslücken, unabhängig vom Standort – ob am Firmensitz, in Niederlassungen oder mobil im Außendienst bzw. Home-Office. Gefundene Lücken lassen sich zentral und schnell schließen.

Dazu greift das System, z. B. der Schwachstellenscanner der baramundi Management Suite, auf stets aktuelle Datenbanken anerkannter Organisationen zu, um Sicherheitslücken in der gesamten IT-Umgebung zu identifizieren. Ein übersichtliches Dashboard zeigt den Sicherheitsstatus auf einen Blick, inklusive Priorisierungen und Lösungsvorschlägen, während detaillierte Listen einen gezielten Drill-down nach Gerät, Schwachstelle oder Gefährdungsgrad ermöglichen.



baramundi Management Suite: Übersicht über Gefährdung der Umgebung

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



Gefährdung bis zum Schließen der Lücke auf allen Geräten.



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

4 Ausnahmen sicher managen

In diesem Abschnitt erfahren Sie, wie Softwareausnahmen trotz Schwachstellen sicher verwaltet und dokumentiert werden können.

In komplexen IT-Umgebungen ist die Softwarevielfalt meist sehr hoch. Unterschiedlichste Standard-, Individual- und Betriebssystemkomponenten sind im Einsatz. Diese Software beinhaltet oft Komponenten wie SSL-Bibliotheken die Schwachstellen enthalten können. Ohne ein Update des Herstellers lassen sich diese Bibliotheken selten isoliert austauschen. Bei entbehrlicher Software hilft Deinstallation. Andernfalls kann eine Nutzen-Risiko-Abwägung zur Weiternutzung führen, wobei die OpenSSL-Bibliotheken im Programmverzeichnis als Ausnahmen deklariert werden. Gutes Schwachstellenmanagement einer Endpoint Management Lösung sorgt zum einen für Transparenz, etwa, ob eine potenzielle Sicherheitslücke besteht. Andererseits bietet es die Möglichkeit, Ausnahmen zu definieren, die als bewusste und im Unternehmen tolerierte Risiken dokumentiert werden können.



Beispiel aus der baramundi Management Suite

Im folgenden Beispiel wird die gefährdete Bibliothek im Kontext des VMware Players per definierter Ausnahmeregelung toleriert. Die gleiche Datei wird jedoch bei Anwendungen wie LibreOffice oder anderen Programmen nicht akzeptiert.

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

Über die baramundi software GmbH

Die baramundi software GmbH sorgt als Spezialist für Unified Endpoint Management (baramundi Management Suite) und Proactive Endpoint Operations (baramundi Proactive Hub) dafür, dass Unternehmen und Organisationen effizient, sicher und plattformübergreifend Arbeitsumgebungen und digitale Arbeitsplätze managen – On-Prem und in der Cloud. Der Hauptsitz der baramundi software GmbH befindet sich in Augsburg. Die Produkte und Services des im Jahr 2000 gegründeten Unternehmens sind komplett Made in EU. Beim Vertrieb, der Beratung und Betreuung von Kunden arbeitet baramundi weltweit erfolgreich mit Partnerunternehmen zusammen.

www.baramundi.com



Sie möchten mehr über die baramundi Management Suite erfahren?

Melden Sie sich zum Live-Webinar an! Erleben Sie im kostenfreien Webinar, wie Sie die baramundi Management Suite Ihre Endpoints, Server und Mobilgeräte automatisiert verwaltet und absichert.

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

Kontaktieren Sie uns.

Wir freuen uns auf Sie!



baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Germany
+49 821 56708-380
request@baramundi.com



+43 1 928 0136 0010
request@baramundi.com



+41 77 280 49 79
request@baramundi.com



+39 340 8861886
request-italia@baramundi.com



+48 735 91 44 54
request@baramundi.com



+44 2071 93 28 77
request@baramundi.com



baramundi software USA, Inc.
30 Speen St, Suite 501
Framingham, MA 01701, USA
+1 508 861 7561
requestUSA@baramundi.com



+49 821 56708-390
request@baramundi.com

Making IT Admins Smile