12 Funktionen, die ein effektives Intrusion-Prevention-System bieten sollte

So wählen Sie das geeignete Intrusion-Prevention-System aus

SonicWALL

Inhaltsverzeichnis

Einleitung

Neueste Generationen von Computerattacken zeichnen sich durch extrem ausgeklügelte Umgehungstechniken aus, die eine Erkennung des Angriffs verhindern sollen. Im schlimmsten Fall kann es dem Angreifer gelingen, aus der Ferne Befehle auf Systemebene auszuführen.

Moderne Intrusion-Prevention-Systeme (IPS) sind mit intelligenten Sicherheitsfunktionen ausgestattet. Sie können Malware noch vor dem Eindringen in das Netzwerk erkennen bzw. blockieren und bieten so effektiven Schutz vor raffinierten Umgehungsversuchen. Um Ihr Netzwerk effektiv zu schützen, sollte Ihr IPS alle Funktionen bieten, die im Folgenden beschrieben sind.

Werden Exploits nicht rechtzeitig erkannt und blockiert, kann dies die Sicherheit von Unternehmens-netzwerken ernsthaft gefährden.

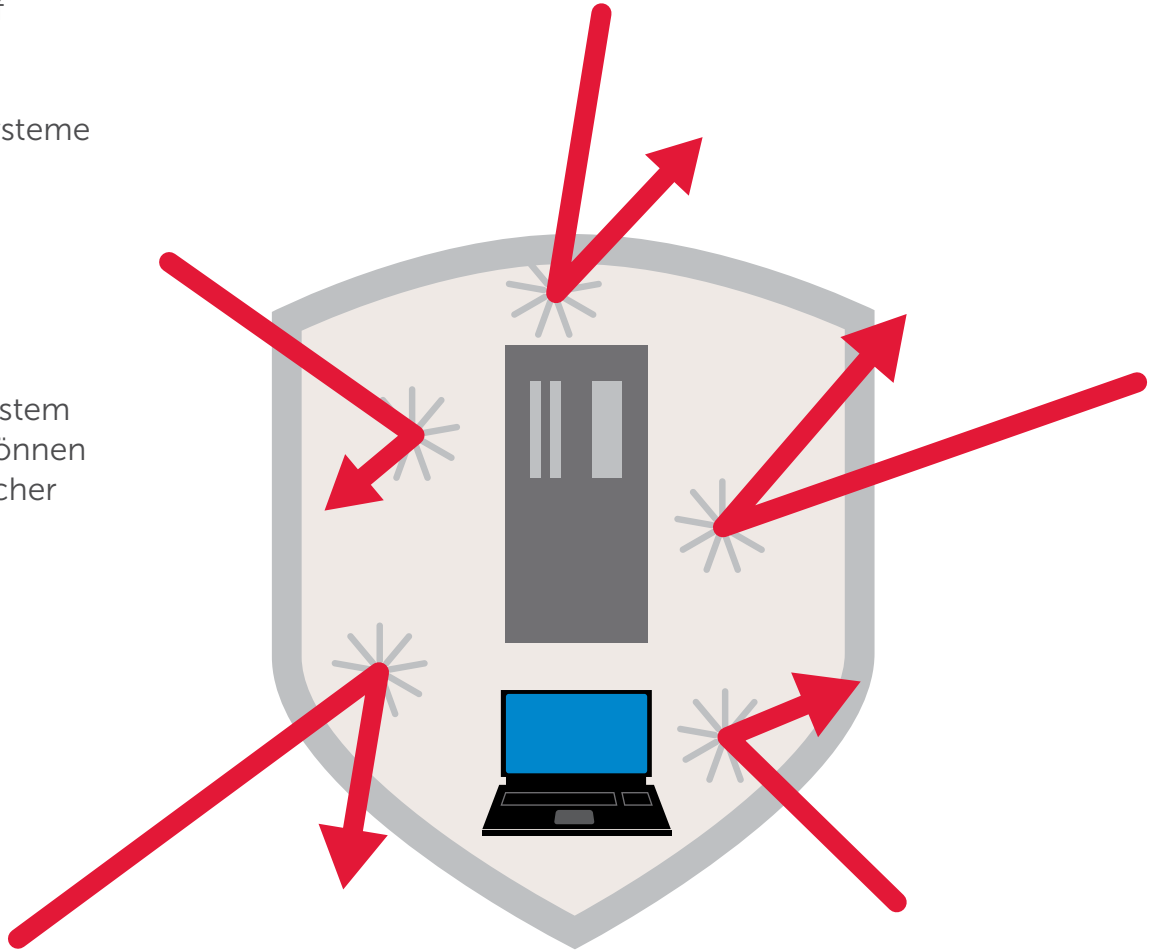
1. Funktion, die ein effektives IPS bieten sollte:

Vielfältige Schutzmechanismen gegen Angriffe auf Server und Clients

Grundsätzlich sollte Ihr IPS über eine umfangreiche Signaturendatenbank verfügen, um Angriffe auf Server und Clients erkennen zu können.

Darüber hinaus sollten Intrusion-Prevention-Systeme auch Schutz vor Anwendungsschwachstellen und Pufferüberläufen sowie die Erkennung von Protokollanomalien für eine Vielzahl bekannter Angriffsvektoren bieten.

Vor allem aber kommt es auf ihre Fähigkeit an, Angriffe zu blockieren. Wählen Sie daher ein System aus, dass regelmäßig aktualisiert wird. Nur so können Sie davon ausgehen, dass jederzeit größtmöglicher Schutz gewährleistet ist.



2. Funktion, die ein effektives IPS bieten sollte:

Prüfung des gesamten Verkehrs, unabhängig von Port oder Protokoll

Herkömmliche Intrusion-Prevention-Systeme bieten nur Schutz für eine begrenzte Anzahl an Ports und Protokollen. Angriffe können sich heute jedoch gegen jede Anwendung in Ihrem Netzwerk richten.

Um Schutz vor neuen und bereits bekannten Bedrohungen zu bieten, muss Ihr IPS den GESAMTEN Verkehr prüfen – nicht nur einige ausgewählte Ports und Protokolle.

Intrusion-Prevention-Systeme müssen jedes einzelne Paket in Ihrem Netzwerk mittels Deep Packet Inspection prüfen. Nur so können neue, ausgeklügelte Angriffe effektiv erkannt und blockiert werden.

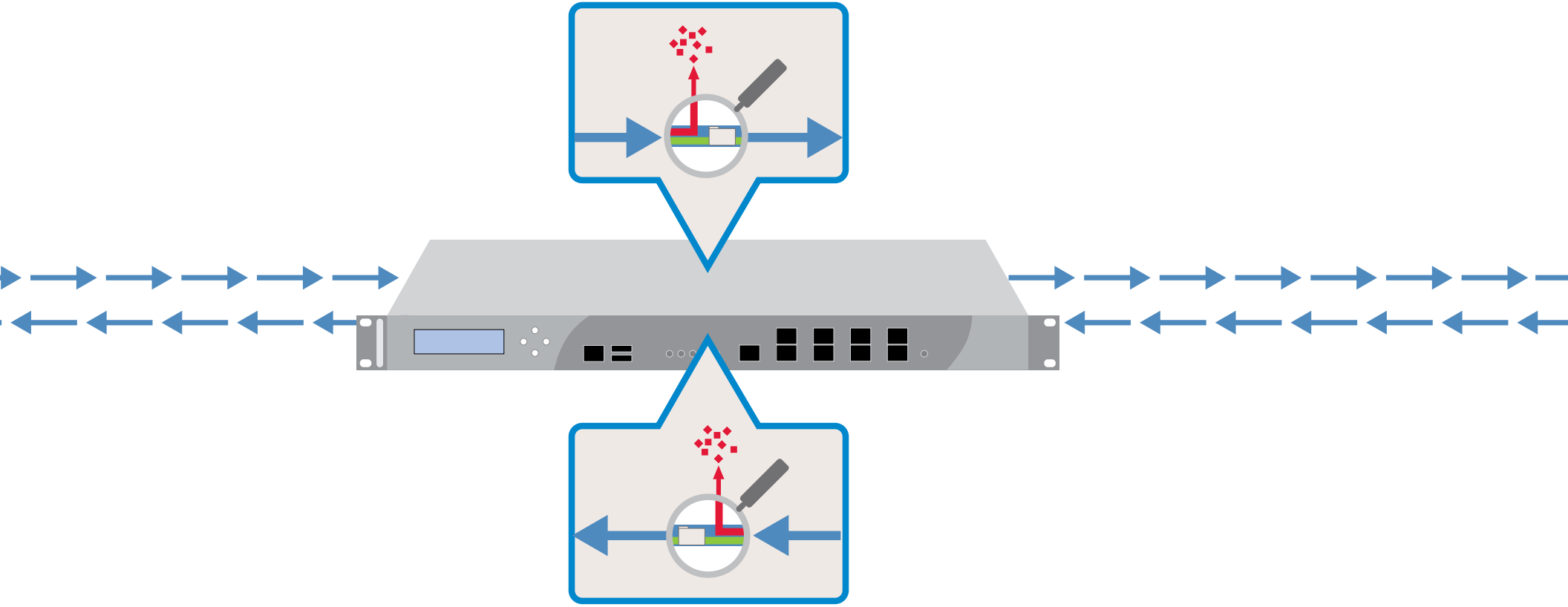
3. Funktion, die ein effektives IPS bieten sollte:

Prüfung des gesamten Verkehrs, sowohl in ein- als auch ausgehender Richtung

Angreifer können vertrauliche Informationen aus kompromittierten Systemen innerhalb Ihres Netzwerks übertragen oder – was noch schlimmer ist – sich Zugang zu Ihrem Firmengebäude verschaffen und von dort aus Angriffe starten. Um gegen diese Bedrohungen und andere interne Angriffe gewappnet zu sein, muss Ihr IPS sowohl den ein- als auch ausgehenden Verkehr prüfen.

Die meisten herkömmlichen IPS-Lösungen konzentrieren sich nur auf den eingehenden Verkehr. Somit ist das Unternehmen nicht vor Angriffen geschützt, die aus anderen Teilen des Netzwerks stammen.

Wenn Sie nur den eingehenden Verkehr prüfen, können Sie lediglich Eindringlinge aus Ihrem Netzwerk fernhalten – aber was ist mit Angreifern, die sich vielleicht schon im Netzwerk befinden?



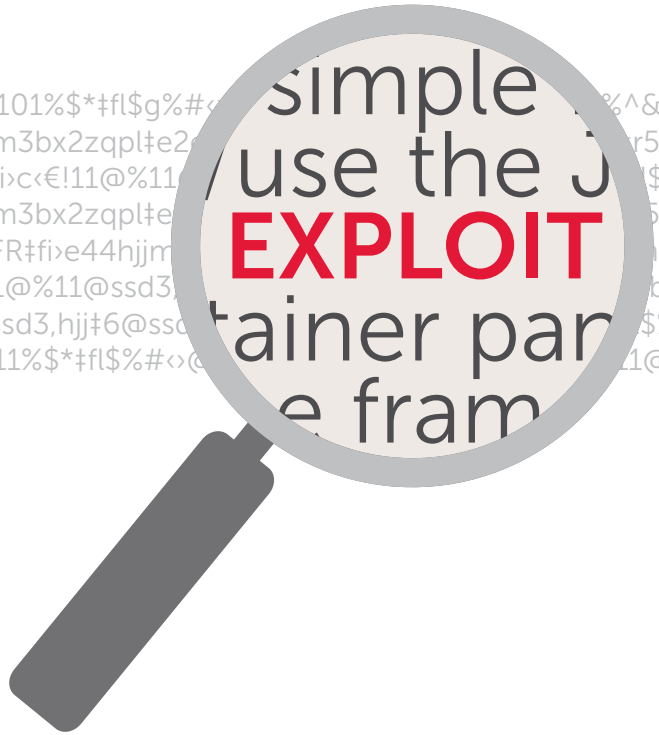
4. Funktion, die ein effektives IPS bieten sollte:

Standardisierung des Verkehrs zur Vermeidung von Umgehungs- und Verschleierungsversuchen

Heutzutage verwenden Hacker raffinierte Verschlüsselungstechniken, um unerkannt zu bleiben. Diese können über alle Ports und Netzwerkebenen hinweg eingesetzt werden, sowohl im ein- als auch ausgehenden Verkehr.

Effektive Intrusion-Prevention-Systeme müssen den Verkehr auf ein übliches Format standardisieren können, um ausgefeilte Umgehungs- und Verschleierungsversuche zu erkennen und abzuwehren.

Technisch versierte Cyberkriminelle kennen die neuesten IPS-Technologien und versuchen mit allen Mitteln, ihre Angriffe zu verschleiern. Ihr IPS muss in der Lage sein, raffinierte Umgehungsversuche zu enttarnen, um den eigentlichen Angriff erkennen und verhindern zu können.



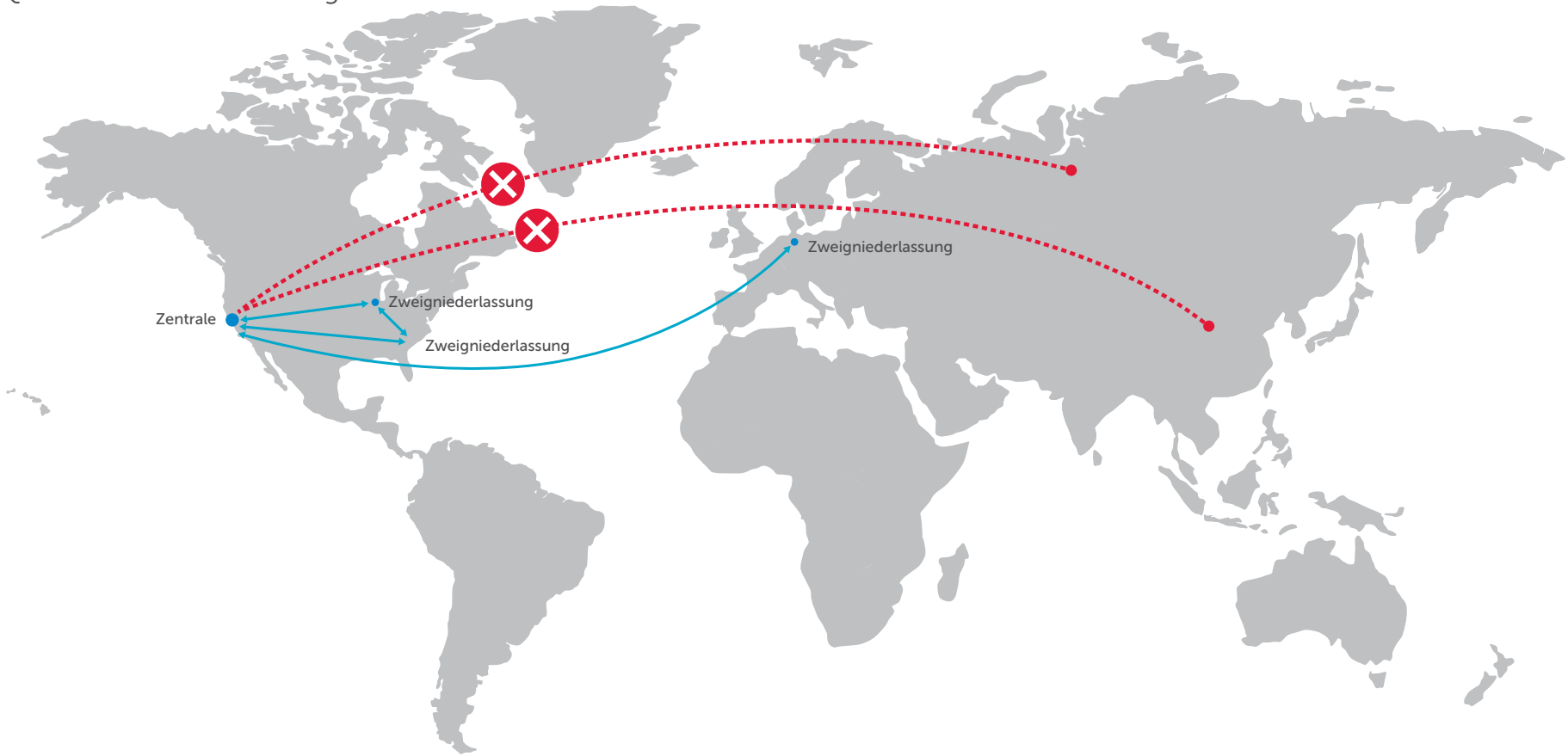
5. Funktion, die ein effektives IPS bieten sollte:

Überwachen und Blockieren von Verkehr basierend auf dem geografischen Ursprung

Genauso wie der Inhalt kann auch manchmal der Ursprung des Verkehrs – oder der Ort, an den er geleitet wird – ein Hinweis dafür sein, dass etwas nicht in Ordnung ist. Manche Orte sind bekannte Brutstätten für kriminelle Aktivitäten.

Intrusion-Prevention-Systeme sollten in der Lage sein, eine IP-Adresse geografisch zurückzuverfolgen, um zu prüfen, ob Quelle oder Ziel verdächtig sind.

Mit Ihrem IPS sollten Sie ungewöhnliches Verhalten (z. B. Netzwerkverkehr aus oder in fremde Länder) ohne Weiteres erkennen und stoppen können.

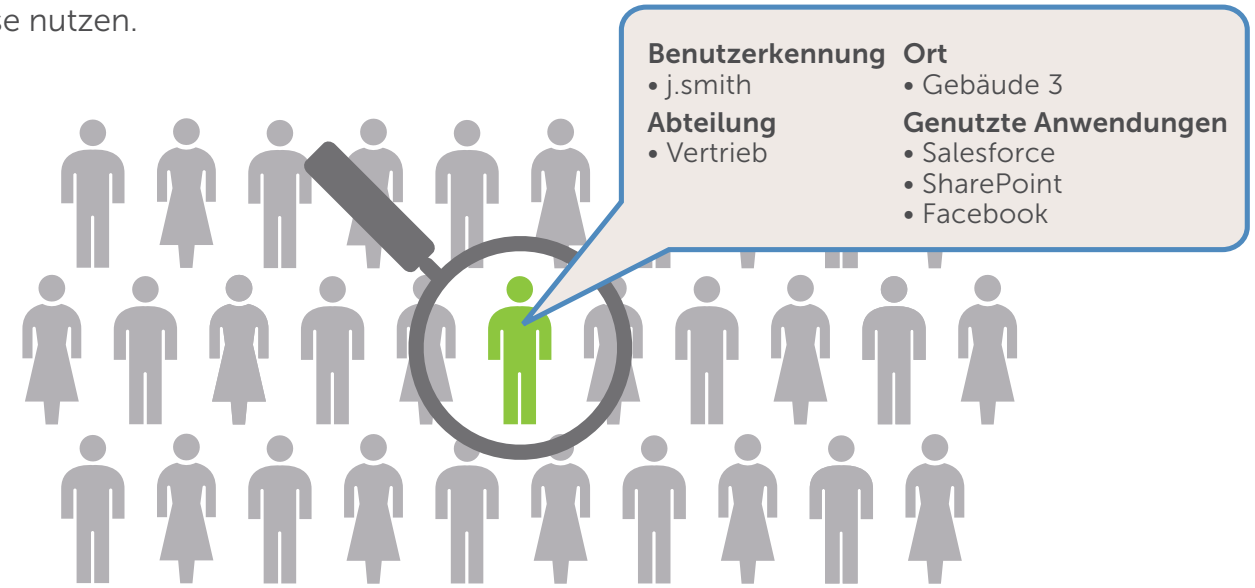


6. Funktion, die ein effektives IPS bieten sollte:

Kontextuelle, benutzerbasierte Prüfung

Manche Benutzer sind vertrauenswürdiger als andere. Dies sollte bei ihren Zugriffsrechten berücksichtigt werden. Effektive Intrusion-Prevention-Systeme sollten nicht nur kontextuelle Informationen zu den Anwendungen im Netzwerk bieten, sondern auch zu den Usern, die diese nutzen.

Mit unvollständigen Informationen ist es nicht einfach, die richtige Entscheidung zu treffen. Ein gutes IPS sollte mehrdimensionale Daten liefern, damit Administratoren fundierte Entscheidungen treffen können.



Active Directory kann in das IPS integriert werden, um eine Beziehung zwischen den genutzten Anwendungen und der Vertrauens-würdigkeit einzelner Benutzer herzustellen.

7. Funktion, die ein effektives IPS bieten sollte:

Erstellen und Installieren von benutzerdefinierten Signaturen

Um Schutz vor neuen Bedrohungen zu bieten, müssen IPS-Signaturen häufig aktualisiert werden. Ihr IPS sollte benutzerdefinierte Signaturen unterstützen, um das Netzwerk mit einer zusätzlichen Sicherheitsschicht gegen proprietäre Anwendungen zu schützen.

Die Signaturen in Ihrem IPS sind zwar extrem wichtig, doch in manchen Fällen reichen sie alleine nicht aus – z. B. bei alten CRM-Systemen, die speziell für Ihr Unternehmen entwickelt wurden. Ein effektives IPS sollte die Möglichkeit bieten, benutzerdefinierte Signaturen zu erstellen, um diese Lücken zu schließen.

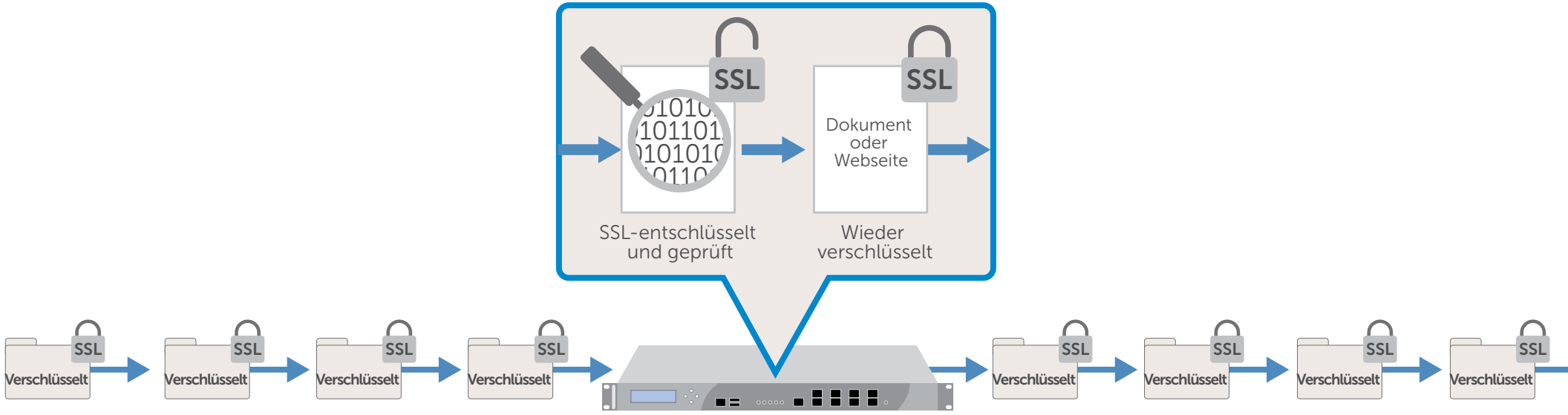
Benutzerdefinierte Signaturen, die speziell auf Ihre Umgebung zugeschnitten sind, schützen Sie vor ausgeklügelten Angriffen.

8. Funktion, die ein effektives IPS bieten sollte:

Prüfung von SSL-verschlüsseltem Datenverkehr

Der webbasierte Verkehr wird heute häufig mittels SSL (Secure Sockets Layer) verschlüsselt, um sensible Daten wie z. B. bei Kreditkartentransaktionen zu schützen. Allerdings verwenden auch Cyberkriminelle SSL-verschlüsselte Daten, um ihre Angriffe zu verschleiern.

Das Internet ist mit Drive-by-Download-Seiten übersät, die mittels SSL unbemerkt Malware verbreiten. Ein effektives IPS sollte in der Lage sein, SSL zu entschlüsseln, um solche Angriffe abzuwehren.



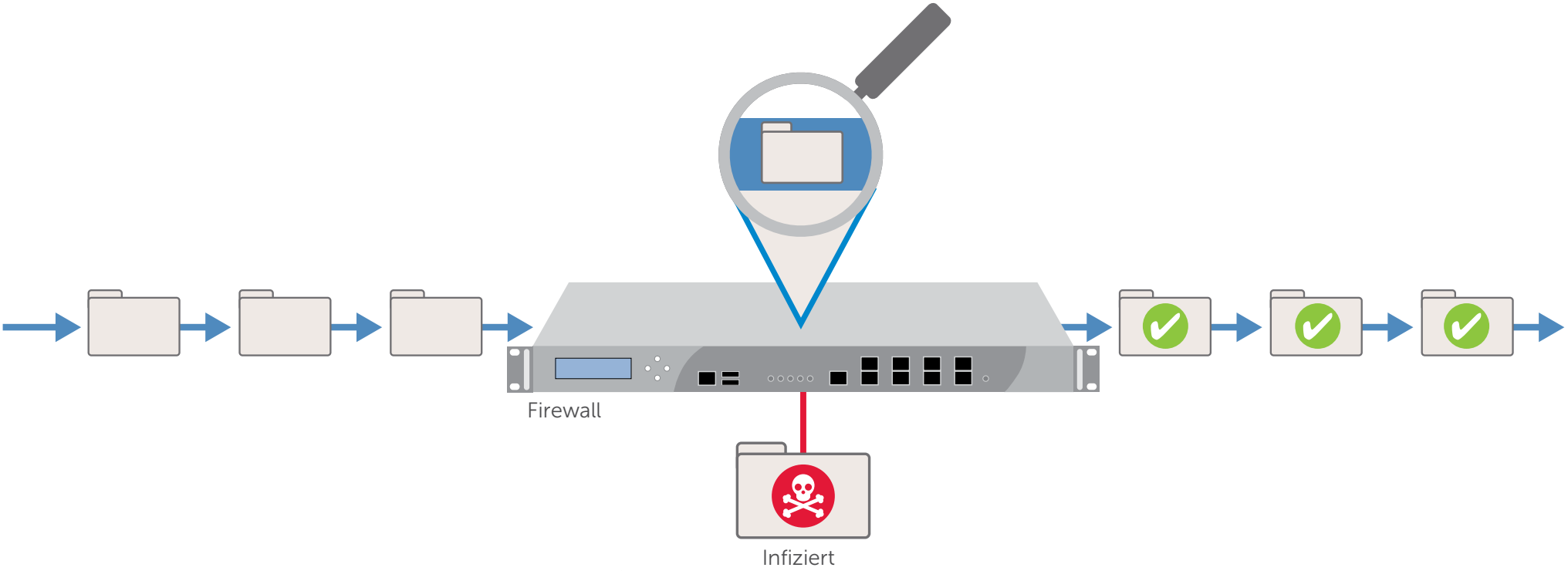
Herkömmliche IPS sind nicht in der Lage, SSL-verschlüsselte Angriffe zu erkennen oder abzuwehren.

9. Funktion, die ein effektives IPS bieten sollte:

Erkennen und Blockieren von Malware bei Eintritt in das Netzwerk

Mit der rasanten Verbreitung von Schadsoftware im Internet sind zusätzliche Sicherheitsschichten am Gateway wichtiger denn je, um die IT-Infrastruktur zu schützen.

Effektive Intrusion-Prevention-Systeme müssen alle Arten von Angriffen abwehren können, einschließlich Trojaner, Viren und Würmer, die sich in scheinbar unbedenklichem Verkehr verbergen können.



Herkömmliche IPS können Malware, die in das Netzwerk eingeschleust wird, weder erkennen noch blockieren.

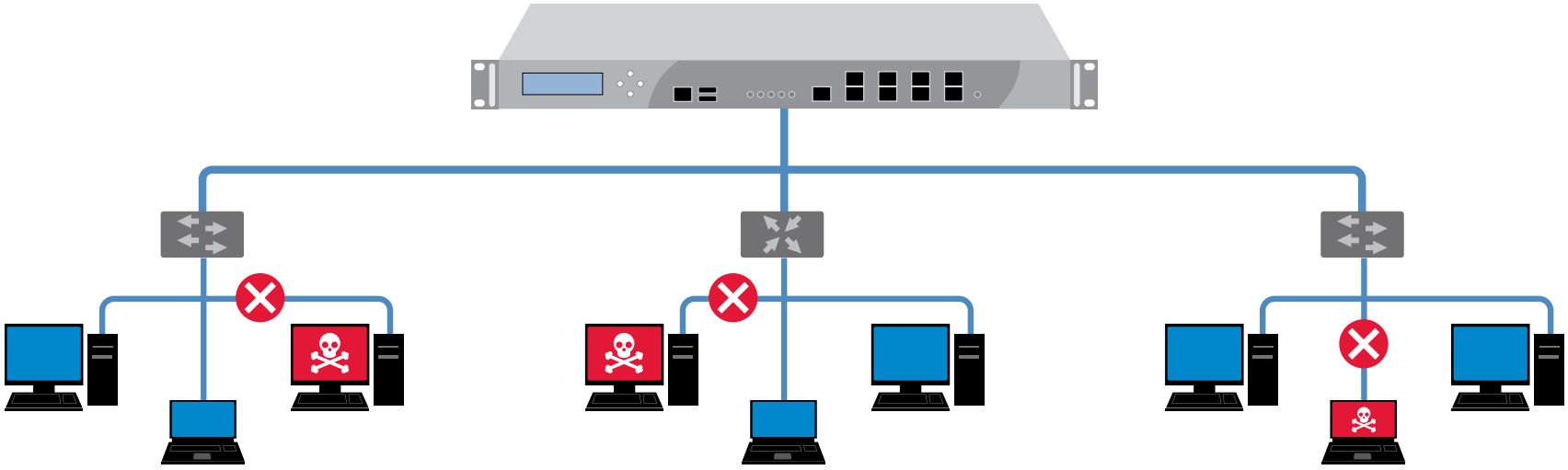
10. Funktion, die ein effektives IPS bieten sollte:

Erkennen und Blockieren der Kommunikation bei bereits kompromittierten Systemen

Botnets und organisierte Angriffe nutzen häufig gängige Ports und Protokolle, um Command-and-Control-Verkehr zu verbergen, der von bereits kompromittierten Systemen übermittelt wird.

Angreifer versuchen oft, die Kommunikation infizierter Systeme zu verbergen. Dazu manipulieren sie Protokolle, um den Verkehr aus dem Netzwerk zu leiten. In vielen Fällen nutzen Botnets ähnliche Methoden, um mit bekanntermaßen kompromittierten Servern zu kommunizieren.

Intrusion-Prevention-Systeme sollten in der Lage sein, Anomalien zu erkennen und die IP-Reputation zu prüfen. Nur so können sie die Kommunikation blockieren, die von kompromittierten Systemen sowie Botnets ausgeht.



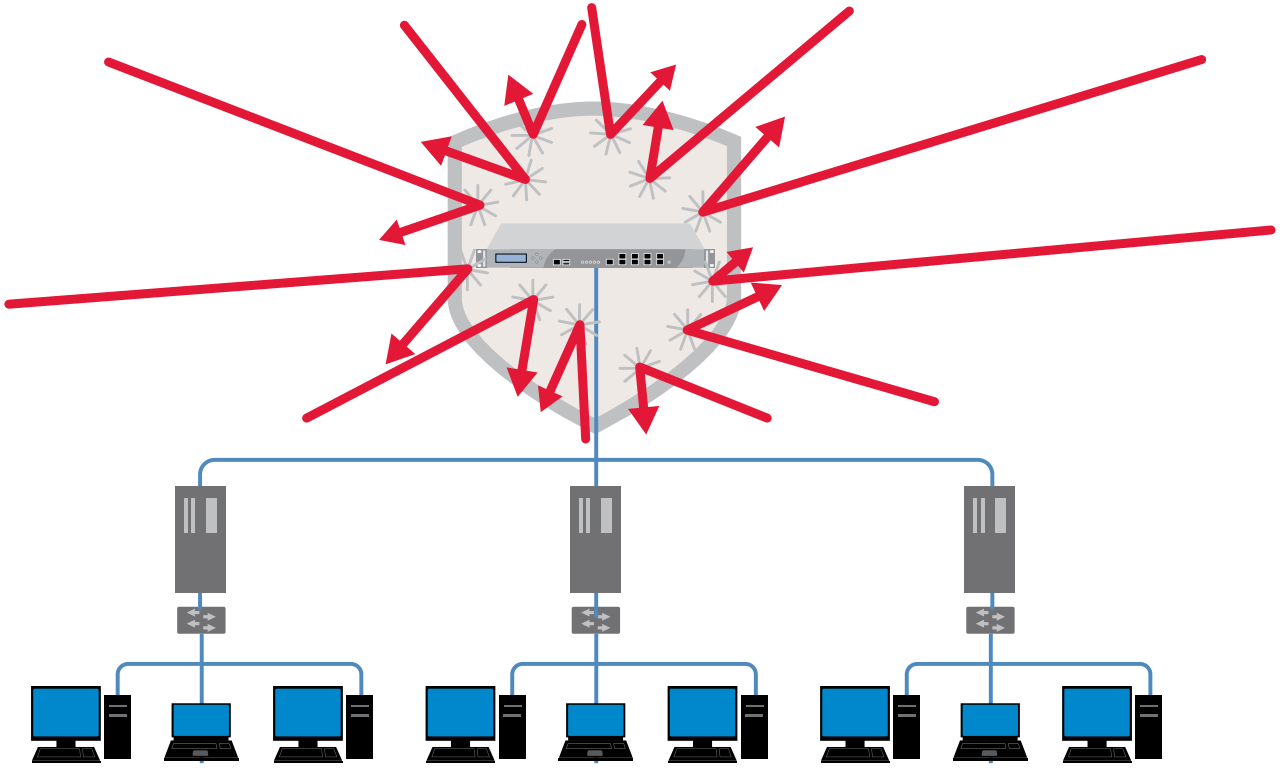
11. Funktion, die ein effektives IPS bieten sollte:

Schutz vor Denial-of-Service- und Flood-Angriffen

Viele Angreifer versuchen, mittels Denial-of-Service- und Flood-Angriffen die gesamte Internetkommunikation eines Unternehmens in ein- und ausgehender Richtung zu blockieren.

Ein ausgereiftes Intrusion-Prevention-System muss Unternehmen vor Angriffen schützen, die das Geschäft zum Erliegen bringen können.

Das Internet ist heute für die Geschäftstätigkeit vieler Unternehmen extrem wichtig. Angriffe, die den Zugriff auf das Web behindern, können daher großen Schaden anrichten. Ihr IPS sollte alle Arten von Angriffen abwehren können – unabhängig davon, wie sie ausgelöst werden.



12. Funktion, die ein effektives IPS bieten sollte:

Bereitstellung von Analysedaten zum Verkehr und Integration mit anderen Analysetools

Trends wie Social Media und die Consumerization der IT haben zu Anwendungschaos in Unternehmensnetzwerken geführt. Damit Sie den Überblick behalten, sollte Ihr IPS externes Reporting an datenstrombasierte Protokolle wie NetFlow und IPFIX unterstützen.

Der Export von Analysedaten aus dem IPS gewährleistet wertvolle Einblicke in den Netzwerkverkehr sowie größere Transparenz.

In manchen Fällen lassen sich anhand historischer Daten (aus den letzten Wochen oder Monaten) aktuelle Entwicklungen besser einordnen und verstehen. Unternehmen können Analysedaten an einen externen Partner weiterleiten und so historische Informationen wie verborgene Kommunikationsdaten, Angriffe auf Clients/Server, VPN-Nutzung, VoIP-Datenverkehr oder die Nutzung von Internetanwendungen beliebig lange speichern.

Sie haben die Wahl: punktuelle Lösungen vs. konsolidierte Lösungen

In der Vergangenheit mussten Unternehmen separate Best-in-Class-Firewalls und -Intrusion-Prevention-Systeme einsetzen, um ihre Netzwerke zu schützen. Heute können Unternehmen auf erstklassige Firewalls und Intrusion-Prevention-Systeme zurückgreifen, ohne separate Geräte, GUIs und Implementierungen verwalten zu müssen.

Next-Generation Firewalls mit konsolidierten IPS-Funktionen – wie etwa die Dell™ SonicWALL™ SuperMassive™ E10800 – kombinieren erweiterte kontext-und contentbasierte Sicherheitsfunktionen, optimalen Schutz vor Sicherheitsbedrohungen und Umgehungsversuchen sowie umfassende Anwendungskontrolle in einem einzigen Gerät.

Konsolidierte Lösungen bieten ein höheres Maß an Sicherheit, eine einfachere Verwaltung (weniger Konsolen sowie gebündelte Daten zur Sicherheit), niedrigere TCO (Total Cost of Ownership) und flexiblere Implementierungsoptionen.

Intrusion-Prevention-System von Dell SonicWALL

Mit ihrer patentierten[1] Reassembly-Free Deep Packet Inspection® (RFDPI)-Engine können Dell SonicWALL Next-Generation Firewalls jedes einzelne Byte des ein- und ausgehenden Verkehrs auf allen Netzwerkebenen umfassend prüfen – unabhängig von Protokoll oder SSL-Verschlüsselung.

Die konsolidierten IPS-Lösungen von Dell SonicWALL bieten umfassende Intrusion Prevention sowie eine zusätzliche Sicherheitsschicht mit Malware-Schutz, Application Intelligence und Anwendungskontrolle. Dazu gewährleisten sie eine hohe Performance, geringe Latenzzeiten sowie flexible Implementierungsoptionen (TAP, Inline und Gateway).

Dell SonicWALLs IPS bietet folgende erweiterte, kontextspezifische Sicherheitsfunktionen:

- Ermittlung des geographischen Standorts
- Identifizierung von Benutzern und Anwendungen
- Prüfung und Erkennung von Dokumenten und Inhalten
- Suche nach benutzerdefinierten und vom Administrator festgelegten Inhalten, wie z. B. Text-Strings oder Kreditkartennummern

*U.S.- Patente 7,310,815; 7,600,257; 7,738,380; 7,835,361

NSS Labs Security Value Map 2012 für IPS

Die Dell SonicWALL SuperMassive E10800 Next-Generation Firewall mit integriertem Intrusion-Prevention-System hat in der NSS Labs Security Value Map™ (SVM) 2012 für IPS nicht nur die heiß begehrte „Recommend"-Bewertung erhalten, sondern auch noch viele führende IPS-Anbieter hinter sich gelassen.

„Die Dell SonicWALL SuperMassive unter SonicOS 6.0 bietet größtmöglichen Schutz gegen bekannte Umgehungstechniken. Sie hat bei allen entsprechenden Tests in allen Bereichen Höchstnoten erhalten." – NSS Labs

„Unternehmen, die ein High-End-Multi-Gigabit-Netzwerk betreiben und ihr aktuelles IPS upgraden möchten, bietet Dell SonicWALL SuperMassive unter SonicOS 6.0 mit seiner erweiterten Architektur ein extrem hohes Maß an Sicherheit und Performance." – NSS Labs

Weitere Informationen

• Laden Sie sich die NSS Labs Security Value Map 2012 für IPS herunter

Wenn Sie uns Feedback zu diesem E-Book, anderen E-Books oder Whitepapers von Dell SonicWALL zukommen lassen möchten, senden Sie eine E-Mail an folgende Adresse: feedback@sonicwall.com.

Über Dell SonicWALL

Dell™ SonicWALL™ bietet intelligente Netzwerksicherheits- und Datenschutzlösungen, die es Kunden und Partnern erlauben, ihre globalen Netzwerke dynamisch zu sichern, zu überwachen und zu skalieren. Das weltweite Dell SonicWALL-Frühwarnsystem garantiert dabei ultraschnellen Schutz vor unterschiedlichsten Bedrohungen. Von Gartner und NSS Labs wird Dell SonicWALL als einer der Marktführer anerkannt. Weitere Informationen erhalten Sie auf unserer Website unter **http://www.sonicwall.com/de**.

SonicWALL