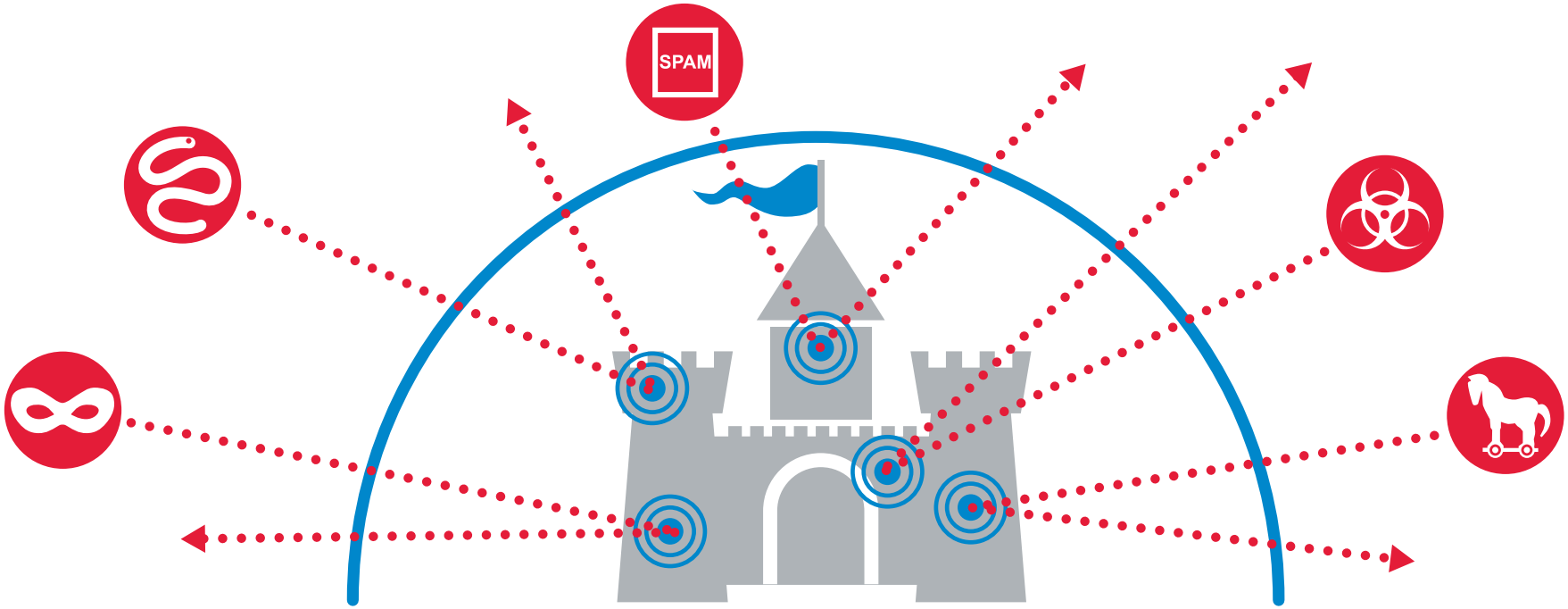
Die verschiedenen Arten von Cyberangriffen

und wie Sie diese abwehren können

Einführung

Die Cyberkriminellen von heute wenden verschiedene komplexe Techniken an, um beim Eindringen in Unternehmensnetzwerke unerkannt zu bleiben und geistiges Eigentum stehlen zu können. Um einer Erkennung durch Systeme zur Angriffsvermeidung (Intrusion Prevention System, IPS) zu entgehen, greifen sie oftmals auf codierte Bedrohungen zurück, die auf komplizierten Algorithmen basieren. Sobald eine Sicherheitslücke auf einem Ziel erfolgreich ausgenutzt werden konnte, versuchen die Angreifer Malware auf das kompromittierte System zu laden und sie zu installieren. Dabei ist es oftmals so, dass es sich bei der Malware um eine neu entwickelte Variante handelt, die herkömmliche Virenschutzlösungen noch nicht kennen.

In diesem E-Book informieren wir Sie über die Strategien und Tools, mithilfe derer Cyberkriminelle versuchen Ihr Netzwerk zu infiltrieren, und erläutern, wie Sie sich effektiv schützen können.



Netzwerke rund um die Uhr mit Malware bombardieren

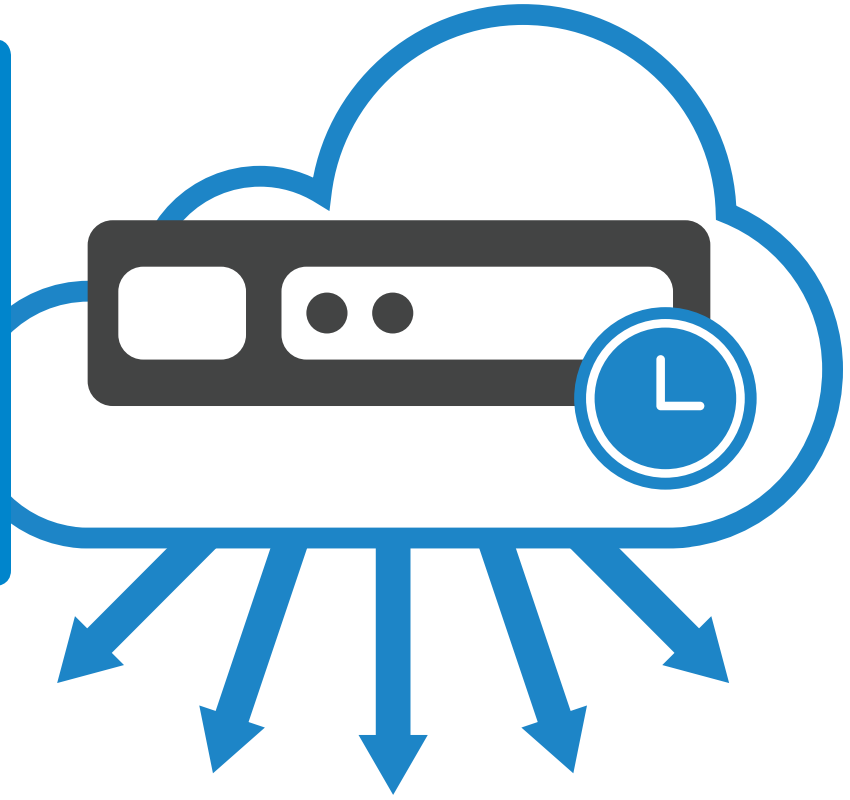
Viele Anbieter von Firewalls der nächsten Generation (NGFW) stellen als Bestandteil eines mehrschichtigen Sicherheitsansatzes eine Technologie für netzwerkbasierten Malwareschutz bereit. Bei den meisten dieser Systeme ist es jedoch so, dass sie auf maximal 5.000 bis 30.000 Malwaresignaturen im Onboard-Systemspeicher der NGFW beschränkt sind. Das Problematische bei diesem Ansatz ist, dass der Malwareschutz bei vielen dieser Systeme nicht oft genug aktualisiert wird, teilweise z. B. nur einmal pro Tag. Dadurch sind die Netzwerke anfällig für kontinuierliche, sich stets weiterentwickelnde Angriffe.

Gegenmaßnahme 1

Netzwerke effektiv schützen – jede Minute, an jedem Tag

Da stündlich Hunderte von Malwarevarianten entwickelt werden, benötigen Organisationen minutenaktuelle Abwehrmechanismen, um sich in Echtzeit vor den neuesten Bedrohungen schützen zu können. Eine effektive Firewall muss kontinuierlich aktualisiert werden – 24 Stunden am Tag, sieben Tage die Woche. Aufgrund der immensen Anzahl von Malwaretypen und -varianten ist der verfügbare Speicher von Firewalls zudem nicht ausreichend. Deshalb sollten Firewalls mit Cloud-Speichern arbeiten, um ein umfassendes Volumen an Malware und Malwarevarianten berücksichtigen und diese bestmöglich identifizieren zu können.

Setzen Sie auf eine Firewall, die dank optimaler Nutzung der Cloud Abwehrmechanismen zum Schutz vor Malware in Echtzeit bereitstellen kann.



Netzwerke mit verschiedenen Arten von Malware infizieren

Cyberkriminelle nutzen für ihre Angriffe auf Netzwerke verschiedene Malwaretypen. Die fünf häufigsten Typen sind Viren, Würmer, Trojaner, Spyware und Adware.

Computerviren wurden für gewöhnlich durch das Weitergeben infizierter Disketten übertragen. Mit der Weiterentwicklung der Technologie haben sich dann auch die Mittel zur Verbreitung vervielfältigt. Heute werden Viren meist über Dateifreigaben, Web-Downloads und E-Mail-Anhänge in Umlauf gebracht.

Computerwürmer existieren bereits seit den 1980er-Jahren. Sie verbreiteten sich aber erst, als Netzwerkinfrastrukturen in Organisationen gebräuchlich wurden. Anders als Computerviren können Würmer ohne jegliche menschliche Interaktion durch Netzwerke schleichen.

Trojaner sind speziell dafür konzipiert, sensible Daten in Netzwerken zu finden und abzugreifen. Bei vielen Typen von Trojanern ist es so, dass sie die Kontrolle über das infizierte System übernehmen und dem Angreifer eine Hintertür öffnen, damit er später darauf zugreifen kann. Trojaner werden auch oft für die Erstellung von Botnets verwendet.

Spyware ist normalerweise an sich kein bösartiger Code, aber dennoch sehr lästig, da Webbrowser damit infiziert werden und danach praktisch nicht mehr funktionsfähig sind. Zuweilen wurde Spyware auch als seriöse Anwendung getarnt, die dem Benutzer auf irgendeine Art von Vorteil ist. Tatsächlich wurden aber heimlich Verhaltens- und Nutzungsmuster erfasst.

Adware wird, wie es der Name vermuten lässt, zur Verbreitung von Werbung verwendet, die für den Angreifer mit finanziellen Vorteilen verbunden ist. Wenn ein System erst mit Adware infiziert wurde, wird der Betroffene beim Versuch, auf das Internet zuzugreifen, mit Pop-ups, Toolbars und anderen Arten von Werbung bombardiert.

Cyberkriminelle nutzen für ihre Angriffe verschiedene Malwaretypen, um Sie unvorbereitet zu treffen.

Gegenmaßnahme 2

Netzwerke vor jeglicher Art von Malware schützen

Jede Firewall sollte Organisationen effektiv vor Viren, Würmern, Trojanern, Spyware und Adware schützen. Dies gelingt am ehesten, wenn alle Schutzmechanismen in einen Single-Pass-Ansatz mit niedriger Latenz integriert werden. Folgende Funktionen und Merkmale sind besonders wichtig:

- **Netzwerkbasierter Malwareschutz**, um Angreifer daran zu hindern, Malware auf ein kompromittiertes System zu laden oder zu übertragen
- **Kontinuierliche und zeitnahe Aktualisierung**, um Netzwerke rund um die Uhr vor Millionen von neuen Malwarevarianten zu schützen – und zwar sobald sie erkannt werden
- **Service zur Angriffsvermeidung (Intrusion Prevention Service, IPS)**, um Angreifer daran zu hindern, Sicherheitslücken im Netzwerk auszunutzen

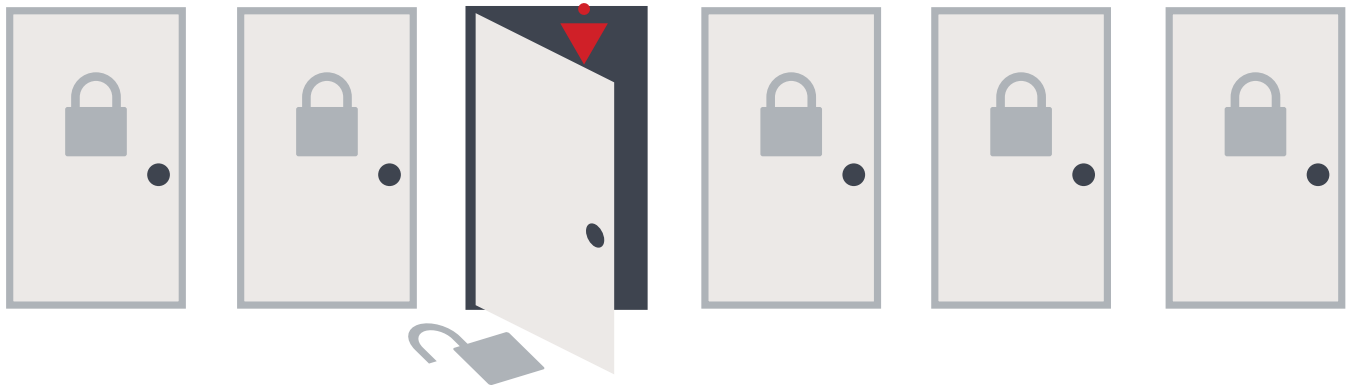
Sie können Ihr Netzwerk noch besser vor Malware schützen, indem Sie sicherstellen, dass jeder, der Zugriff auf das Netzwerk hat, über eine aktuelle Virenschutzsoftware verfügt. Wenn Organisationen die Verwendung einer Virenschutzsoftware auf PCs erzwingen und gleichzeitig eine Netzwerk-Firewall einsetzen, können sie die Möglichkeiten, die sich Cyberkriminellen bieten, um das Netzwerk zu kompromittieren, bedeutend einschränken.

Setzen Sie auf einen mehrschichtigen Malware-schutz, um Bedrohungen effektiv zu begegnen.

Die am wenigsten geschützten Netzwerke finden und kompromittieren

Viele Firewall-Anbieter werben zwar damit, dass ihre Lösungen erstklassigen Schutz vor Bedrohungen gewährleisten, jedoch konnten sich im Praxiseinsatz nur wenige bewähren. Organisationen, die eine minderwertige Firewall einsetzen, glauben vielleicht, dass ihre Netzwerke geschützt sind, doch erfahrene Cyberkriminelle können mithilfe komplizierter Algorithmen das System zur Angriffsvermeidung umgehen. So werden sie nicht erkannt und können das System kompromittieren.

Einige Firewalls bieten zwar zuverlässigen Schutz, beeinträchtigen aber die Leistung. In einem solchen Fall sind Organisationen versucht, die Sicherheitsmaßnahmen zu deaktivieren oder einzuschränken, um eine hohe Netzwerkleistung gewährleisten zu können. Diese Vorgehensweise ist extrem riskant und sollte deshalb vermieden werden.

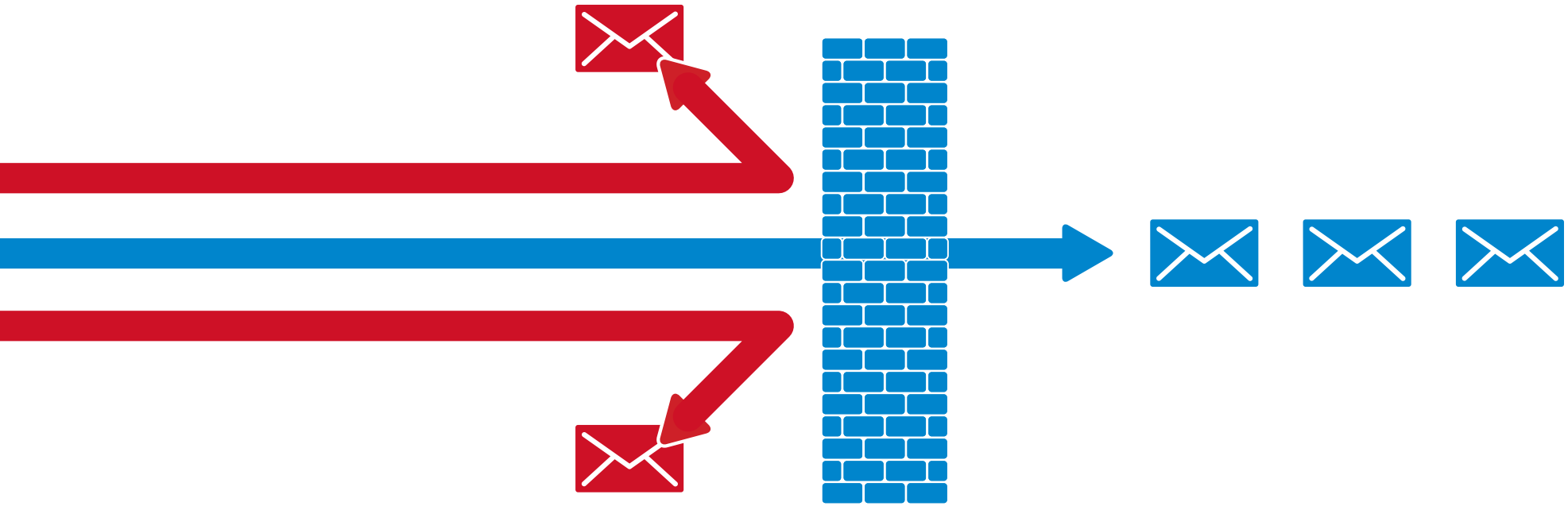


Cyberkriminelle greifen oft die Netzwerke an, bei denen sie die meisten Schwachstellen ausfindig machen konnten.

Gegenmaßnahme 3

Eine Firewall einsetzen, die erstklassigen Schutz vor Bedrohungen und hohe Leistung bietet

Sie sollten sich für eine Firewall entscheiden, die unabhängig getestet und von ICSA Labs für netzwerkbasierten Malwareschutz zertifiziert wurde. Zusätzlich sollten Sie ein Multi-Core-Design in Betracht ziehen, sodass Dateien jeder Größe und jeden Typs gescannt werden können und auf Änderungen in puncto Datenverkehr reagiert werden kann. Alle Firewalls benötigen eine Engine, die Netzwerke vor internen und externen Angriffen schützt – ohne dass die Leistung beeinträchtigt wird.



Malware oft ändern und global angreifen

Viele Cyberkriminelle sind mit ihren Angriffen erfolgreich, weil sie kontinuierlich neue Malware erfinden und diese mit anderen Angreifern auf der ganzen Welt teilen. Das bedeutet, dass auf allen Kontinenten stündlich neue Bedrohungen auftauchen. Viele Cyberkriminelle führen Blitzangriffe durch: Sie dringen ein, nehmen, was sie bekommen können, und sind wieder weg, bevor jemand Alarm schlagen kann. Dann wiederholen sie den Angriff woanders.

Es tauchen stündlich neue Bedrohungen auf allen Kontinenten auf.

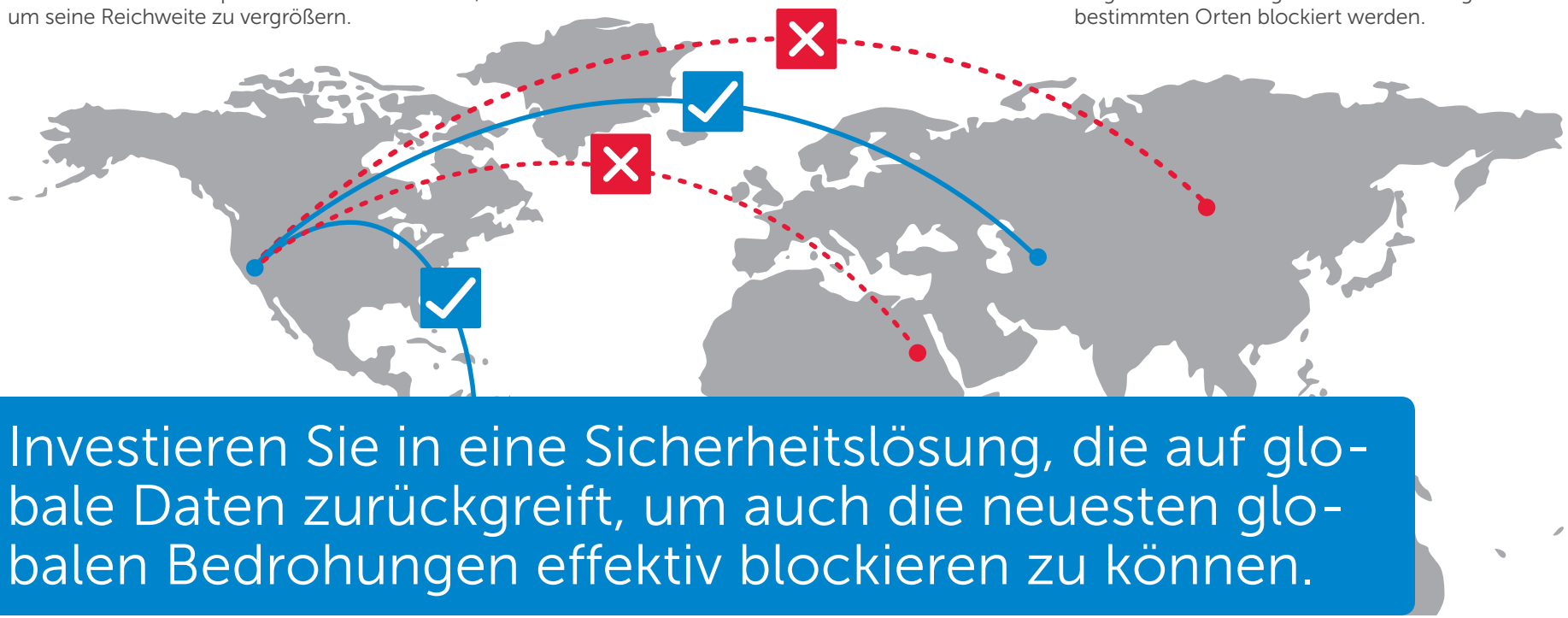
Gegenmaßnahme 4

Eine Firewall einsetzen, die effektiven Schutz vor globalen Bedrohungen gewährleistet

Um einen effektiven Schutz zu gewährleisten, muss schnell auf Bedrohungen reagiert werden können. Dies gelingt am ehesten, wenn Sie auf einen Firewall-Anbieter setzen, der über ein eigenes, sofort einsatzbereites internes Team mit Experten zur Entwicklung von Gegenmaßnahmen verfügt – denn so ist sichergestellt, dass Ihre Firewall so schnell wie möglich mit Abwehrmechanismen zum Schutz Ihres Netzwerks vor neuen Bedrohungen aktualisiert werden kann. Außerdem sollte dieses Team mit zahlreichen anderen Sicherheitsexperten zusammenarbeiten, um seine Reichweite zu vergrößern.

Es gibt keine Firewall-Appliance, die die Millionen von existierenden Malwaretypen abwehren kann. Es kann sein, dass ältere, weniger genutzte Bedrohungssignaturen aus der lokalen Firewall gestrichen werden, wodurch Sie dann wiederum angreifbar sind. Mit einer auf ein breites Spektrum ausgelegten Lösung, die die Analysen der lokalen Firewall mittels eines globalen, umfassenden cloudbasierten Malwarekatalogs erweitert, kann dies vermieden werden.

Zuletzt können verdächtige Aktivitäten auch anhand von Datenverkehr erkannt werden, der von Orten ausgeht, wo Sie geschäftlich nicht tätig sind. Eine einfache Firewall bietet Funktionen zur Identifizierung und zum Blockieren anhand geographischer Regionen. Doch bei einer ausgeklügelteren Firewall profitieren Sie zudem noch von Funktionen zur Botnet-Filterung, mit denen das Risiko durch bekannte globale Bedrohungen reduziert werden kann, da der Datenverkehr aus gefährlichen Domänen sowie eingehende und ausgehende Verbindungen zu bestimmten Orten blockiert werden.



Investieren Sie in eine Sicherheitslösung, die auf globale Daten zurückgreift, um auch die neuesten globalen Bedrohungen effektiv blockieren zu können.

Fazit

Die Anzahl an Cyberangriffen nimmt aktuell zu, doch es gibt effektive Abwehrmöglichkeiten. Wenn Sie soweit sind und Lösungen zur Angriffsabwehr evaluieren möchten, können Sie unser Whitepaper "Achieving Deeper Network Security" (Höhere Netzwerksicherheit erreichen) herunterladen, um sich eingehender zu informieren.

Über Dell Software

Dell Software unterstützt Kunden dabei, ihr Potenzial durch den Einsatz von Technologie voll auszuschöpfen – mit skalierbaren, erschwinglichen und benutzerfreundlichen Lösungen, die die IT vereinfachen und Risiken minimieren. Das Portfolio von Dell Software deckt Kundenanforderungen in fünf Schlüsselbereichen ab: Rechenzentrums- und Cloud-Verwaltung, Informationsverwaltung, Verwaltung mobiler Mitarbeiter sowie Sicherheit und Datensicherung. In Kombination mit Hardware und Services von Dell versetzen unsere Softwareprodukte Kunden in die Lage, effizienter und produktiver zu arbeiten und schnellere Geschäftsergebnisse zu erzielen. www.dellsoftware.com

Bei Fragen zur möglichen Nutzung dieses Dokuments
wenden Sie sich bitte an:

Dell Software
5 Polaris Way
Aliso Viejo, CA 92656
www.Dell.com
Informationen zu unseren regionalen und internationalen Büros finden Sie auf unserer Webseite.

Ebook-TypesOfCyberAttacks-GM-US-25949