SOPHOS
Security made simple.

Next-Generation Web Security – die Waffe gegen moderne Bedrohungen

Von **Peter Craig**, Senior Product Marketing Manager

In diesem Whitepaper erklären wir Ihnen, warum Unternehmen Next-Gen Web Security als erste Verteidigungslinie zum Schutz ihrer Systeme und Benutzer benötigen. Außerdem erfahren Sie, welche Funktionen in keiner Web-Security-Lösung fehlen dürfen, damit Ihr Unternehmen Next-Gen Security erhält, die ihrem Namen auf wirklich gerecht wird.

Sophos-Whitepaper November 2016

Moderne Malware – intelligenter und gefährlicher als je zuvor

Dass Malware-Angriffe immer raffinierter und gezielter werden, ist eine unerfreuliche Tatsache, mit der sich Unternehmen heutzutage zwingend auseinandersetzen müssen. In der modernen Welt ist Hacking ein lukratives Geschäft und professionelle Hacker haben es vor allem auf Profit abgesehen.

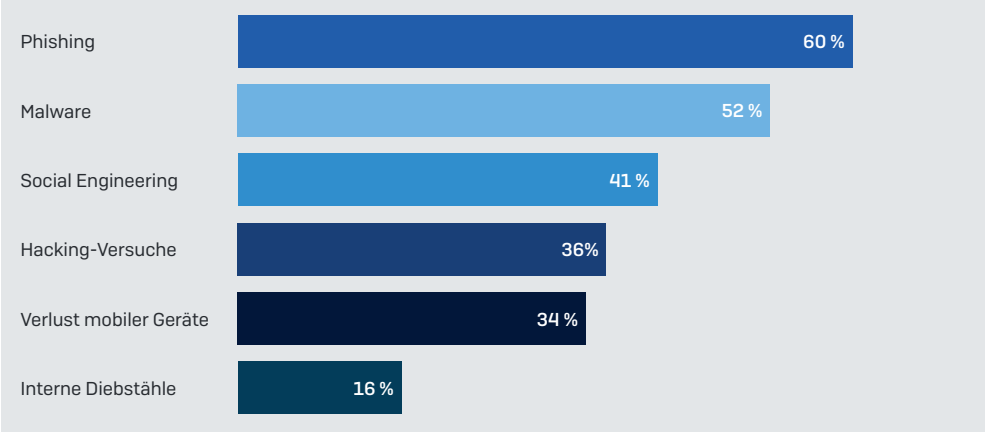
Kaum ein Tag vergeht, ohne dass ein Unternehmen mit einer Datenpanne Schlagzeilen macht. Und dies sind nur die wirklich brisanten Fälle, bei denen es große, namhafte Unternehmen getroffen hat – tatsächlich sind jedoch Unternehmen jeder Größe gleichermaßen gefährdet.

Ausgangspunkt ist in fast allen Fällen das Internet.

Die SophosLabs verzeichnen täglich rund 30.000 neue Schad-URLs. 59 % sind eigentlich seriöse Websites, die jedoch manipuliert wurden. 85 % aller Malware-Schädlinge – u. a. Viren, Würmer, Spyware, APTs und Trojaner – stammen aus dem Internet.

Einer Studie der ISACA zufolge wurden 52 % aller Unternehmen bereits Opfer eines Malware-Angriffs, dem es gelang, bis ins Unternehmensnetzwerk vorzudringen.

Von welchen Angriffen war Ihr Unternehmen 2015 betroffen?



(Quelle: ISACA 2016, State of Cybersecurity - Implications for 2016)

Diese Angriffe bereits abzufangen, bevor sie in Ihr Netzwerk gelangen können, ist die effektivste Abwehrmethode. Hierzu benötigen Sie eine leistungsstarke Web-Security-Lösung, die Bedrohungen mit einer ganzen Reihe von Verfahren zuverlässig abfängt. Darüber hinaus wird es immer wichtiger, Ihre Web Security so zu ergänzen, dass ein koordiniertes Sicherheitssystem entsteht. In diesem System gibt es dann mehrere Lösungen, die Kontextinformationen austauschen und so eine schnellere Erkennung und Reaktion ermöglichen.

Worauf Unternehmen bei Next-Gen-Web-Lösungen achten sollten

Verschiedene Lösungen von mehreren Anbietern zu vergleichen, kann sehr mühselig sein. Die Beschreibungen sind oft schwammig, ähnliche Funktionen basieren unter Umständen auf verschiedenen Verfahren und einige Anbieter behaupten, Next-Gen-Lösungen anzubieten, ohne die entsprechenden Funktionen vorweisen zu können.

Bei der Beurteilung und Wahl einer Next-Gen-Web-Lösung sollten Sie auf drei wichtige Punkte achten:

1. Schutz
2. Performance
3. Einfache Bedienung

In den folgenden Abschnitten beschreiben wir die wichtigsten Funktionen der drei oben genannten Punkte. Wir gehen dabei nicht auf jedes technische Detail ein, sondern möchten Ihnen vielmehr vermitteln, was eine Next-Gen-Web-Lösung können sollte.

Schutz

Der gebotene Schutz ist das A und O jeder Sicherheitslösung, gleichzeitig jedoch auch der Bereich, in dem es am meisten Interpretationsspielraum gibt – insbesondere, was Next-Gen Security betrifft:

Erweiterter Schutz vor Internet-Bedrohungen	Automatische Bedrohungsupdates	Erkennung anonymisierender Proxyserver
Alle heruntergeladenen Webseiten-Inhalte werden mit Verfahren wie JavaScipt-Emulation gescannt	Regelmäßige Bedrohungsupdates werden automatisch installiert	Verhindert, dass Benutzer Ihre Richtlinien für sicheres Internet-Surfen umgehen

Sandboxing	URL- und Live-Protection-Filterung	Richtlinien für sicheres Surfen im Netz
Verdächtige Dateien werden unter kontrollierten Bedingungen ausgeführt und beobachtet, evasive Malware und gezielte Bedrohungen werden blockiert	Neu und bereits früher infizierte Websites werden automatisch blockiert	Websites werden auf Basis von Stichwörtern, Kategorien, IP und Domains blockiert

Datenverkehr-Scans	Application Control	Mobile Management
HTTP-, HTTPS-, IMAP-, SMTP-, UDP- und DNS-Datenverkehr wird auf verdächtige Aktivitäten gescannt	Anwendungen werden identifiziert, klassifiziert und kontrolliert und von ihnen genutzte Daten werden geprüft	Mobile Geräte werden innerhalb und außerhalb des Netzwerks geschützt

Performance

Selbst der beste Schutz ist wenig wert, wenn die Surfgeschwindigkeit der Endbenutzer leidet. Achten Sie bei einer Web-Lösung deshalb auf Folgendes:

Intelligent Traffic Routing (FastLane)	Globale Infrastruktur
Datenverkehr wird an das optimale Gateway geleitet, um die Download-Geschwindigkeit zu erhöhen	In der Nähe Ihres Standorts bereitgestellte Infrastruktur gewährleistet beste Performance ohne Ausfallzeiten

Einfache Bedienung

Leistungsstarker Schutz bedeutet nicht, dass eine Lösung kompliziert in der Bedienung sein muss. Sparen Sie mit folgenden Funktionen wertvolle Zeit ein:

Detailliertes Reporting	Zentrale Verwaltung
Vorkonfigurierte Reports, damit Sie wichtige Informationen sofort griffbereit haben – Netzwerkprotokolle, Benutzeraktivitäten	Eine Management-Konsole, über die Sie alle Sicherheitslösungen verwalten können. Ein Benutzername, ein Passwort

Gezielte Bedrohungen effektiv bekämpfen – warum Unternehmen Sandboxing benötigen

Wie bereits erwähnt, werden Malware-Angriffe immer ausgefeilter und nehmen zunehmend ganz gezielt bestimmte Unternehmen ins Visier. Im Klartext bedeutet das, dass immer mehr neue und noch unbekannte Malware im Umlauf ist, gegen die herkömmliche Sicherheitslösungen machtlos sind.

Genau deshalb gewinnt Sandboxing auf dem Gebiet der Web Security immer mehr an Bedeutung.

Eine ordnungsgemäß konfigurierte Sandbox arbeitet mit Ihrer Web-Security-Lösung zusammen und fängt neue, komplexe Bedrohungen ab, bevor sie Schaden anrichten können. Wenn eine Web-Security-Lösung auf eine verdächtige, noch unbekannte Datei stößt, leitet sie diese an die Sandbox weiter. Hier wird die Datei in der sicheren Sandbox-Umgebung ausgeführt und beobachtet, um zu ermitteln, ob sie schädlich ist oder nicht.

Detaillierte Bedrohungs- und Vorfallinformationen werden anschließend weitergemeldet und ermöglichen eine gründliche forensische Analyse. Sollten Sie sich außerdem für eine Cloud-Sandbox-Lösung entscheiden, profitieren Sie von einer kollektiven Sicherheitsintelligenz, da Daten zu Bedrohungen und Ereignissen von Unternehmen weltweit zusammengetragen und allen Kunden zeitnah zur Verfügung gestellt werden.

Innerhalb oder außerhalb des Netzwerks? Mit mobilen Geräten und Drittanbieter-Anwendungen Schritt halten

Da Bring Your Own Device (BYOD) in Unternehmen immer beliebter wird, sind Security- und Verwaltungsfunktionen für mobile Geräte momentan das Thema. Außerdem kommen auch Drittanbieter-Anwendungen (z. B. Dropbox, TOR, Salesforce.com) häufig außerhalb Ihres Unternehmensnetzwerks zum Einsatz. Diese müssen ebenfalls vor Datenverlusten und unangemessener Nutzung geschützt werden.

Für mobile Geräte bedeutet das, dass Richtlinien remote bereitgestellt werden müssen, damit die Geräte innerhalb und außerhalb des Unternehmensnetzwerks sicher und richtlinienkonform bleiben. Für Anwendungen (auf mobilen Geräten und Computern) bedeutet es, dass Ihre Web-Security-Lösung in der Lage ist, diese Anwendungen zu identifizieren, klassifizieren und zu kontrollieren.

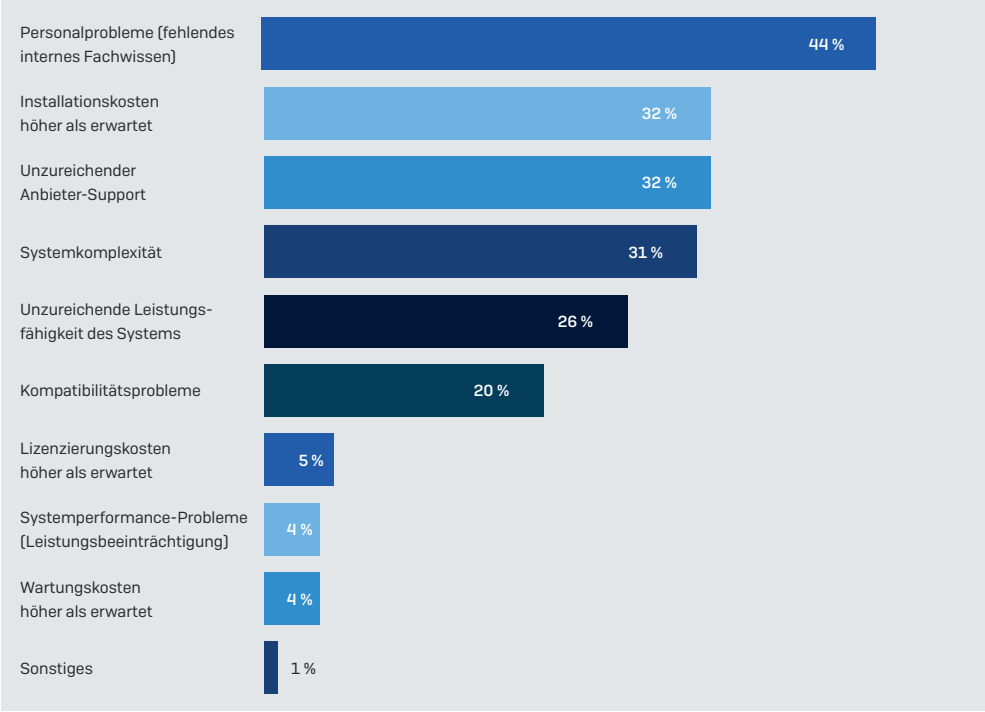
So gestalten Sie Ihre Sicherheit synchronisiert, leistungsstärker und einfacher

Zur Implementierung von Next-Gen Web Security bieten sich für Unternehmen im Wesentlichen zwei Methoden an. Entweder eine bereits integrierte Lösung, die noch umfassenderen Schutz vor Malware und DLP (Data Leakage Protection) bietet, oder ein kompliziertes Geflecht von Technologien, die manuell integriert werden müssen, damit sich Benachrichtigungen korrelieren und priorisieren lassen.

Bei einer manuellen Integration muss der IT-Manager aktiv eingreifen und Daten von jeder Lösung manuell analysieren, um über eine Reaktion zu entscheiden und diese zu koordinieren. Vor allem mittelständische Unternehmen tun sich mit dieser manuellen Integration schwer, da sie nicht genügend fachkundiges Personal haben.

Wie aus der Abbildung unten hervorgeht, ist dieser Personalmangel der Hauptgrund für die Enttäuschungen nach dem Kauf von Sicherheitstechnologien.

Warum Unternehmen einige ihrer Technologie-Investitionen bereuen (zwei Antworten zulässig)



(Quelle: Ponemon Institute 2015, 2015 Global Study on IT Security Spending & Investments)

Der Enterprise Strategy Group zufolge wird dieses Problem auf unabsehbare Zeit bestehen bleiben:

„...46 % der Unternehmen räumen mittlerweile ein, dass sie bei weitem nicht genügend Cybersecurity-Fachkräfte haben ... ein erheblicher Anstieg gegenüber dem Vorjahr (28 %) ..."[1]

Viele Anbieter adressieren diese weit verbreitete Problematik mit ihren Lösungen nur unzureichend. Ihre Lösungen mögen an sich zwar sehr wirksam sein. Doch häufig sind die Lösungen kompliziert zu bedienen und bieten Unternehmen nicht die notwendige Automatisierung und Koordinierung, damit diese wirklich optimalen Schutz erhalten.

Viele Unternehmen können sich den Luxus einer gesonderten Cybersecurity-Abteilung schlichtweg nicht leisten. Einige haben nicht einmal auf IT-Sicherheit spezialisierte Mitarbeiter. Wenn dann noch Sicherheitslösungen genutzt werden, die Informationen nicht koordinieren, werden wichtige Benachrichtigungen schnell übersehen und kompromittierte Systeme sind nicht selten die Folge.

Selbst IT-Abteilungen von Großunternehmen verschwenden wertvolle Zeit mit nicht koordinierten Systemen. Verschiedene Logins und Konsolen, doppelte Informationen und Benachrichtigungen – all dies kann mehr Zeit kosten, als Sie denken.

Innovative Sophos Next-Gen Web Protection

Sophos Next-Gen Web Protection bietet leistungsstarken Schutz vor Web-Bedrohungen, optimiert die Surfgeschwindigkeit der Benutzer und lässt sich über eine zentrale Kontroll-Engine einfach installieren, konfigurieren und verwalten. Ihre Benutzer und Geräte bleiben sicher und geschützt – innerhalb und außerhalb des Netzwerks.

- Next-Generation Web Protection mit Advanced Threat Detection, URL- und Live-Protection-Filterung, Datenverkehr-Scans, Erkennung anonymisierender Proxyserver usw.
- 24-Stunden-Bedrohungs-Monitoring der SophosLabs mit automatischen Updates im Laufe des Tages
- Scannt HTTP-, HTTPS-, IMAP-, SMTP-, UDP- und DNS-Datenverkehr auf Schadaktivitäten
- Echtzeitdaten zur Reputation von Websites
- „Fast Lane"-Technologie leitet Datenverkehr intelligent zum optimalen Sophos-Gateway weiter, um die Download-Geschwindigkeiten zu erhöhen
- Richtlinien für sicheres Internet-Surfen – Websites werden auf Basis von Stichwörtern, Kategorien, IP und Domains blockiert
- Einfache Installation, Konfiguration und Verwaltung
- Weltweit über 10 Standorte verfügbar

Sophos Web Protection ist zudem Teil des integrierten Portfolios von Sophos, das sich aus Produkten zusammensetzt, die für besten Schutz perfekt aufeinander abgestimmt sind. Dank der einfachen Verwaltung über Sophos Central kontrollieren Sie Ihre Web, Endpoint, Server, Email, WiFi und Mobile Security über eine zentrale, intuitive Oberfläche. Sie erhalten also modernsten Schutz, mit dem Sie Zeit sparen und sich in Ruhe Ihrer Arbeit widmen können.

Fazit

Web-Bedrohungen sind schon jetzt allgegenwärtig und werden in Zukunft noch zahlreicher und komplexer werden. Die meisten Unternehmen sind darauf nicht vorbereitet, weil sie zu wenig Ressourcen und fachkundiges Personal haben. Sophos löst diese Problematik mit leistungsstarken, integrierten Lösungen, die sich einfach bedienen lassen und eine hohe Performance garantieren. Leistungsstarker Schutz, einfache Bedienung und Performance – auf diese drei Bereiche sollte jedes Unternehmen bei der Wahl einer Web-Security-Lösung achten.

[1] Enterprise Strategy Group 2016, Cybersecurity Skills Shortage: A State of Emergency

Jetzt kostenfrei testen

Kostenlose 30-Tage-Testversion
unter www.sophos.de/freetrials

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

16-06-24 WPDE (DD-2373)

SOPHOS