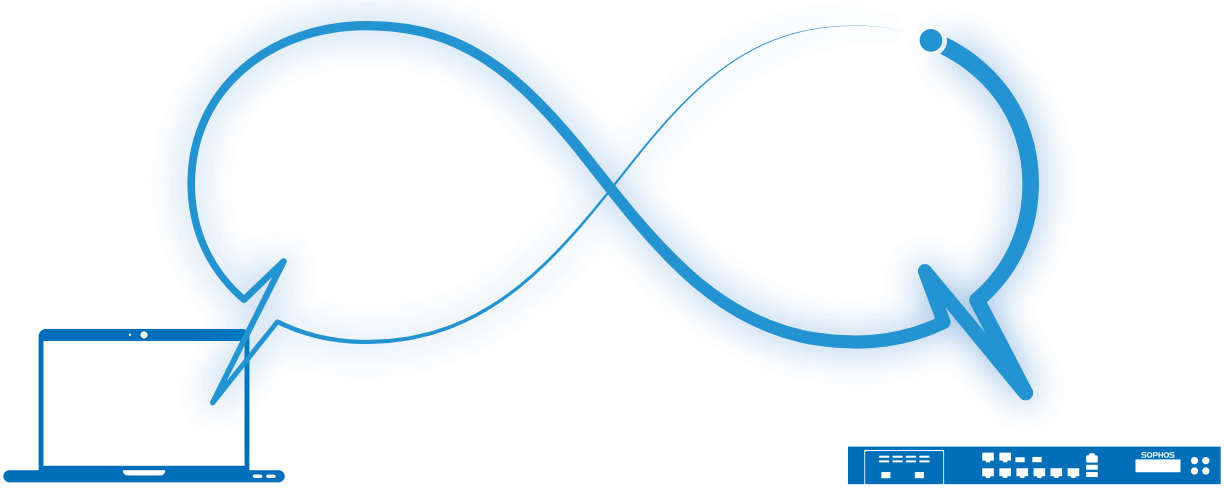
SOPHOS

Security made simple.



Synchronized Security: Eine revolutionäre Technologie

1) Leben in der Gefahrenzone – heutige Cyber-Risiken

Größere Angriffsfläche, immer komplexere und raffiniertere Angriffe

Unternehmen jeder Größe müssen heute lernen, wie sie in einer Welt mit immer weiter wachsendem Cyber-Risiko überleben und wachsen können. Dieses Risiko steigt aus mehreren Gründen immer weiter, unter anderem aufgrund der größer werdenden Angriffsfläche und der wachsenden Komplexität und Raffinesse der Angriffe.

Mitarbeiter nutzen immer mehr mobile Geräte und Cloud-Services und Unternehmen jeder Größe setzen virtuelle und Cloud-Infrastrukturen ein. Die sogenannte „Angriffsfläche" hat sich dadurch dramatisch vergrößert.

Bedenken Sie folgende Fakten:

- **Geräte:** Der durchschnittliche Benutzer in Deutschland verfügt über 3,1 internetfähige Geräte.[1]
- **Anwendungen:** Unternehmen mit 250 bis 999 Mitarbeitern verwenden durchschnittlich 16 zugelassene Cloud-Apps, Unternehmen mit 1000 bis 4000 Mitarbeitern 14 und die größten Unternehmen 11 dieser Apps.[2]
- **Internet der Dinge:** Bis Ende 2015 waren geschätzte 4,9 Milliarden „Dinge" mit dem Internet verbunden. Bis 2020 wird diese Zahl auf 25 Milliarden ansteigen.[4]

Aufgrund dieser wachsenden Angriffsvektoren werden wir mit einer steigenden Anzahl von Angriffen, Sicherheitsverletzungen und Datenverlusten konfrontiert.

Zweitens nimmt die Komplexität und Raffinesse der Angriffe stetig zu. Selbst weniger begabte Angreifer haben auf dem Grau- und Schwarzmarkt die Möglichkeit, kommerziell unterstützte, raffinierte Toolkits zu erwerben.

Diese „Kits" sind vielfach erprobt und alles andere als leicht zu erkennen und zu bekämpfen. Das UnRecom Remote Access Tool Kit, oder kurz RAT, das erstmals im Mai 2014 auf Threatgeek.com erwähnt wurde, kam beispielsweise mehrmals zum Einsatz, unter anderem für AlienSpy und erst kürzlich für JSOCKET. Es wird von Datenverletzungen bis hin zu einem politischen Attentat praktisch mit allem in Verbindung gebracht.[5]

Leider werden Forschungsergebnissen zufolge gerade kleine und mittlere Unternehmen unverhältnismäßig häufig Opfer der zunehmenden bestätigten Datenverluste. Dies zeigen die Ergebnisse des Verizon 2016 Data Breach Investigation Report:

- Im Jahr 2015 gab es 100.000 Sicherheitsvorfälle, davon waren 3.141 bestätigte Datenverluste.

Bedrohungslandschaft

- Dies entspricht einem Anstieg der Sicherheitsvorfälle von 23 % und einem astronomisch hohen Zuwachs an Datenverletzungen von 48 % im Vergleich zum Jahr 2014.
- Unternehmen mit weniger als 1000 Mitarbeitern waren von 20 % der bestätigten und klassifizierten Datenverluste betroffen, obwohl diese weniger als 1 % der Sicherheitsvorfälle ausmachten.
- Sicherheitsvorfälle und Datenverlust in kleineren Unternehmen sind in vielen verschiedenen Branchen zu finden, wobei die Bereiche Finanzdienstleistungen, Immobilien, Einzelhandel und Gesundheit am häufigsten von Angriffen betroffen sind.

Schätzungen des Privacy Rights Clearinghouse gehen zudem davon aus, dass im Jahr 2014 51 % aller Datenpannen auf Hacking oder Malware zurückzuführen waren. Gleichzeitig kommt der Verizon-Report zu dem Schluss, dass die überwiegende Anzahl dieser Angriffe finanziell motiviert waren. Für die am meisten gefährdeten kleinen und mittleren Unternehmen können die Kosten infolge von Angriffen den finanziellen Ruin bedeuten.

Vermehrte Angriffe, immer komplexere Angriffsszenarien und zunehmende Datenverluste: Wir müssen uns fragen: Was müssen wir anders machen?

Kleine Teams, knappe Ressourcen, wenig Spezialisten

Wenn die Anzahl der Angriffe steigt, wird man in der Regel versuchen, zusätzliche Mitarbeiter auf das Problem anzusetzen. Viele Unternehmen verfügen jedoch nur über kleine IT-Sicherheitsteams. Die Erweiterung oder Neuzuweisung von Ressourcen ist keine realistische Option für kleine und mittlere Unternehmen.

Wie Sie in Abbildung 1 sehen können, sind IT-Sicherheitsteams mit Ausnahme von Großunternehmen in Bezug auf Größe und Ressourcen sehr begrenzt:

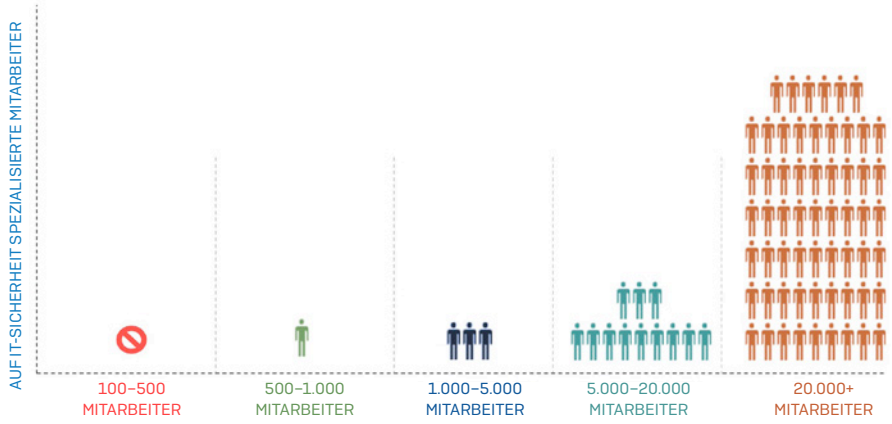


Abbildung 1: IT-Sicherheitsabteilungen von mittleren Unternehmen sind klein und haben nur begrenzte Ressourcen (Quelle: US Dept of Homeland Security, 2014)

Und selbst wenn beschlossen wird, das interne IT-Sicherheitsteam zu vergrößern, ist es gar nicht so einfach, geeignete Mitarbeiter für diesen Bereich zu finden. Der BurningGlass 2015 Cybersecurity Job Report gibt an, dass die Vakanzen im Bereich Cyber-Sicherheit zwischen 2010 und 2014 um 91 % angestiegen sind. Dieses Wachstum ist um 325 % schneller als bei Arbeitsplätzen im Bereich IT insgesamt.

Wir werden mit einer weit größeren Anzahl von Angriffen konfrontiert, die raffinierter (und erfolgreicher) sind als je zuvor, und es gibt einfach nicht genügend qualifizierte Mitarbeiter, um die Gefahren hinreichend einzudämmen. Unternehmen sind damit einem größeren Risiko als je zuvor ausgesetzt, Opfer von Cyber-Angriffen zu werden.

2) Aber wir haben doch so viel in unsere Sicherheitslösungen investiert!

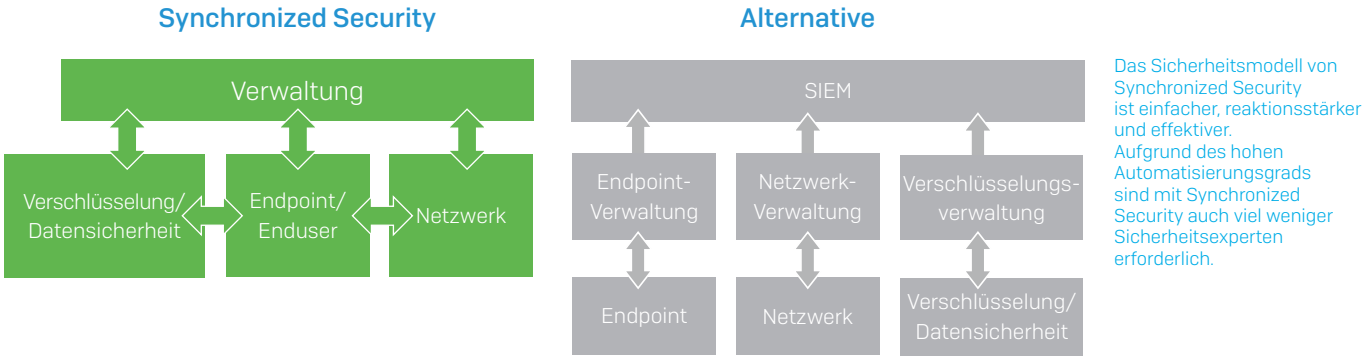
Architektur mit mehreren Schichten und schlechter Integration. Komplex und kurzsichtig. Kontextunabhängig. Isolierte Entscheidungen. Diese Beschreibungen treffen auf die meisten aktuellen Sicherheitslösungen zu.

Heutzutage kommen in der Regel immer noch IT-Sicherheitslösungen zum Einsatz, die sehr komplex sind und unabhängig voneinander arbeiten. Von Virenschutz, Datenverschlüsselung, Web-, E-Mail- und Netzwerk-Gateways bis hin zu moderneren Produkt-Suites, UTMs, Sandboxes sowie Endpoint-Schutz- und Reaktionslösungen. Angesichts der koordinierten Angriffe auf gesamte IT-Ökosysteme ist es kein Wunder, dass diese Lösungen kaum Schritt halten können. Ein Angriff kann an einem Endpoint beginnen, breitet sich jedoch schnell über das gesamte Netzwerk aus und zieht unverschlüsselte Daten über die ausgehende Internetverbindung ab.

IT-Sicherheitsexperten haben versucht, die „Punkte" zwischen den Datenquellen zu verbinden, indem sie Correlation Engines, große Datenbanken, Security Information and Event Management-Systeme (SIEMs), aufkommende Programmiersprachen zum Datenaustausch wie STIX und OpenIOC sowie zahlreiche Analysten einsetzten. Doch auch mit den fortschrittlichsten Tools ist es nahezu unmöglich, die Daten der einzelnen Produkte zu erfassen und zu verstehen, um so Risiken schnell erkennen und beheben sowie Datenverluste stoppen zu können.

Die Event- und Log-Korrelation hängt noch immer von komplexen Korrelationsregeln, endlosem Field-Mapping und Filterdefinitionen sowie von stundenlanger Arbeit durch hochqualifizierte, schwer zu findende Analysten ab. SIEMs erfordern zudem hohe Kapitalinvestitionen und sorgen für kontinuierliche Betriebsausgaben. Der Informationsaustausch, in welchem sicherlich der Schlüssel für die Zukunft der Sicherheit liegt, ist für eine breite und einfache Adaption noch nicht ausgereift genug.

Die Ergebnisse, oder vielmehr die fehlenden Ergebnisse, sprechen für sich. Wie wir gesehen haben, nehmen Datenverluste und das Risiko stetig zu, ein Rückgang ist nicht in Sicht. Zudem sind nur wenige Spezialisten verfügbar. Laut einem neuen Bericht des Ponemon Institute bleiben 74 % der Sicherheitsverletzungen länger als sechs Monate unentdeckt. Am schlimmsten ist jedoch, dass mittlere Unternehmen noch größere Schwierigkeiten mit dem Umgang dieses Risikos zu haben scheinen als ihre größeren Konkurrenten, die über bessere Ressourcen verfügen. Ganz klar kann die Antwort auf dieses Problem nicht die Bereitstellung eines weiteren nicht integrierten Einzelprodukts, weiterer Konsolen, weiterer Mitarbeiter oder schwerfälliger SIEMs sein. Diese Ansätze sind nicht erfolgreich. Gefunden werden muss ein neuer, effektiverer Ansatz.



Das Sicherheitsmodell von Synchronized Security ist einfacher, reaktionsstärker und effektiver. Aufgrund des hohen Automatisierungsgrads sind mit Synchronized Security auch viel weniger Sicherheitsexperten erforderlich.

3) Synchronized Security: Ein völlig neuartiger Ansatz

Eine revolutionäre Idee

Jahrzehntelang hat die IT-Sicherheitsbranche Netzwerk-, Endpoint- und Datensicherheit als komplett unterschiedliche Bereiche betrachtet. Das ist so, als ob man einen Mitarbeiter für Gebäudesicherheit außerhalb des Gebäudes, einen anderen im Gebäude und einen dritten vor Ihrem Safe positioniert, ohne dass diese miteinander kommunizieren können – ein absurder Gedanke. Genau hier setzt unsere neue, synchronisierte Sicherheit an: Sie sorgt dafür, dass die Mitarbeiter miteinander sprechen. Wir händigen jedem dieser drei ein Smartphone aus, sodass sie untereinander schnell und einfach kommunizieren und ihre Handlungen koordinieren können. Dieses Konzept ist einfach, aber gleichzeitig auch revolutionär.

Wie wäre es, wenn wir ganz von vorn beginnen – mit einem neuartigen IT-Security-Ansatz, der auf einer anderen Denkweise basiert? Mit einem effektiveren Ansatz, der für besseren Schutz sorgt und eine automatische Echtzeit-Kommunikation zwischen Netzwerk-, Endpoint-Security- und Verschlüsselungslösungen ermöglicht? Mit einem Schutz, der über die gesamte Bedrohungsfläche synchronisiert ist? Einem Schutz, der hochautomatisiert ist, sodass er all dies ohne zusätzliche Mitarbeiter und Arbeitsstunden schafft.

Hierfür benötigen wir ein System, das folgende Eigenschaften erfüllt:

Auf das gesamte Ökosystem konzentriert: Wir müssen Datenverluste im gesamten IT-Ökosystem verhindern, erkennen und stoppen können; dazu ist es notwendig, dass wir über alle Vorgänge im System Bescheid wissen.

Umfassend: Die Lösung muss umfassend sein und unser gesamtes IT-System mit mehreren Plattformen, Geräten, Benutzern und Daten abdecken; nur so kann sie uns effektiv gegen Angreifer schützen.

Effizient: Die Lösung muss die Arbeitslast des Teams verringern und zugleich den Schutz verbessern. Sie darf keine weitere Schicht zur Technologie und zur Arbeitslast hinzufügen.

Effektiv: Die Lösung muss die heutigen Bedrohungen über die gesamte Bedrohungsfläche hinweg effektiv verhindern, erkennen, untersuchen und beheben können.

Auf Daten konzentriert: Die Lösung konzentriert sich nicht nur auf Geräte und Netzwerke, sondern schützt wertvolle Daten unabhängig vom Speicherort und Zeitpunkt des Zugriffs.

Einfach: Die Lösung muss einfach zu kaufen, einfach zu verstehen, einfach zu installieren und einfach anzuwenden sein.

Diese Liste liest sich wie eine kaum lösbare Aufgabe. Die heute verfügbaren IT-Sicherheitsprodukte sind das Gegenteil: auf die Bedrohung konzentriert, komplex, nicht umfassend, ressourcenintensiv und insgesamt nicht so koordiniert wie die Angriffe, gegen die sie helfen sollen. Ganz klar sind Innovationen erforderlich, um erfolgreich zu sein. Diese Herausforderung wird in Abbildung 2 zusammengefasst.

Heutige, mehrschichtige Lösungen	Synchronized Security
Auf Bedrohungen konzentriert, operiert unabhängig von umgebenden Objekten und Ereignissen	Auf das gesamte Ökosystem konzentriert, operiert in vollem Bewusstsein umgebender Objekte und Ereignisse

Getrennt voneinander arbeitende Produkte	Produkte, die koordiniert zusammenarbeiten
Erfolgreicher Einsatz ist abhängig von der Anzahl der verfügbaren Mitarbeiter	Arbeitet erfolgreich durch automatisierte, innovative Technologie; keine zusätzlichen Mitarbeiter erforderlich
Unabhängige Verschlüsselungsverwaltung	Integrierter Verschlüsselungsschutz, der automatisch auf Bedrohungen reagiert
Kompliziert	Einfach

Abbildung 2: Die heutigen Lösungen müssen erheblich verändert werden

Um zu einer solchen Lösung zu gelangen, die effizient arbeitet und gleichzeitig einfach in der Bedienung ist, benötigt man eine innovative Technologie. Wir haben eine solche Technologie entwickelt – unseren Sophos Security Heartbeat.

Sophos Security Heartbeat

Synchronisierte Sicherheit ermöglicht es den Endpoint-, Verschlüsselungs- und Netzwerksicherheitslösungen der nächsten Generation, wichtige Informationen untereinander auszutauschen, wenn sie verdächtige Verhaltensweisen im IT-Ökosystem eines Unternehmens bemerken. Durch eine direkte und sichere Verbindung – unseren Sophos Security Heartbeat – agieren Endpoint-, Verschlüsselungs- und Netzwerkschutz als ein integriertes System. Dieses System ermöglicht es Unternehmen, Bedrohungen praktisch in Echtzeit zu verhindern, zu erkennen, zu analysieren und zu beseitigen, ohne dass zusätzliche Mitarbeiter benötigt werden.

Wenn die Sophos Next-Gen Firewall zum Beispiel eine hochentwickelte Bedrohung oder ein Datenleck erkennt, kann sie automatisch den Sophos Security Heartbeat nutzen, um sowohl im Netzwerk als auch am Endpoint einzugreifen: So kann sie die Bedrohung abwehren bzw. den Datenverlust sofort stoppen. Die durch den Sophos Security Heartbeat ermöglichte synchronisierte Sicherheit kann ebenso automatisch und nahezu sofort einen geschützten Endpoint isolieren und Schlüssel vorübergehend entziehen, sobald ein Angriff auf diesen erkannt wird. So ist sichergestellt, dass keine vertraulichen Daten abgezogen oder sensible Daten an einen Command-and-Control-Server gesendet werden. Dieser Grad von Erkennung, Schutz und Reaktion, der sonst oft Wochen oder Monate dauert, ist dank synchronisierter Sicherheit innerhalb von Sekunden möglich.

Sophos Synchronized Security bietet mit Security Heartbeat, den SophosLabs und Sophos Central einfache und hocheffektive Sicherheit für Endpoints und Netzwerke.

Erstmals kommt auch der Verschlüsselung eine bedeutende Rolle beim Bedrohungsschutz zu. Verschlüsselung, Schlüssel und die Möglichkeit, Dateien auszutauschen und zu verschlüsseln, sind nun direkt mit Ihrem Sicherheitszustand, dem Vertrauen und der Integrität des Benutzers, den Systemen und den Anwendungen verknüpft. Auf diese Weise können Risiken bewertet und Maßnahmen zur Durchsetzung von Verschlüsselungsrichtlinien getroffen werden, damit Unbefugte nicht an sensible Daten gelangen. Sollten Dateien dennoch gestohlen werden, kann der Angreifer sie nicht lesen. Darüber hinaus können Sie den Zugriff auf geschützte Anwendungen und Daten für mobile Geräte sperren, die Ihre Richtlinien nicht einhalten. Diese Kombination von integriertem und synchronisiertem Schutz für Benutzer, Netzwerke, Geräte und Daten ist einmalig, leistungsstark und einfach.

Zusammenfassung

Nie war das Risiko von Cyber-Angriffen so hoch wie heute. Angriffe werden immer zahlreicher und komplexer und insbesondere kleine und mittlere Unternehmen haben diesem Problem wenig entgegenzusetzen, weil sie nicht genügend IT-Sicherheits-Mitarbeiter haben.

Die bisherigen mehrschichtigen IT-Security-Ansätze sind nicht erfolgreich, ebenso wenig wie die Bemühungen, die Unzulänglichkeiten dieser Lösungen mit Analysen zu lösen.

Komplexe und kurzsichtige Lösungen, die sich einzig auf die Bedrohung konzentrieren und deren Erfolg stark von der Anzahl der verfügbaren IT-Sicherheits-Mitarbeiter abhängt, sind nicht effektiv für kleine und mittlere Unternehmen mit kleinen IT-Sicherheitsteams. Um den Trend der steigenden Anzahl an Sicherheitsvorfällen und Datenschutzverletzungen umzukehren, wird ein neuartiger Ansatz benötigt.

Gebraucht werden Lösungen, die über eine innovative Technologie miteinander kommunizieren und dadurch einfach und doch effektiv, automatisiert und koordiniert arbeiten. Durch die Synchronisierung von Daten, Endpoints und Netzwerken können Sicherheitsteams und Systeme schnell und effektiv auf moderne Bedrohungen reagieren. Sie möchten Sophos Security Heartbeat besser kennenlernen und erfahren, wie Synchronized Security von Sophos Ihr Unternehmen effektiver vor modernen Bedrohungen schützen kann? Besuchen Sie unsere Seite www.sophos.de/heartbeat.

[1] Naked-Security-Studie „How do you compare to Steve Wozniak?" durchgeführt mit 2226 Teilnehmern im Januar 2013).

[2] Okta Business@work, 2015

[3] Gartner, http://www.gartner.com/newsroom/id/3055225

[4] Gartner, http://www.gartner.com/newsroom/id/2905717, 2014

[5] Threatgeek.com

Synchronized Security

Weitere Infos unter
www.sophos.de/heartbeat

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

© Copyright 2016. Sophos Ltd. Alle Rechte vorbehalten.
Eingetragen in England und Wales, Nr. 2096520, The Pentagon, Abingdon Science Park, Abingdon, OX14 3YP, GB
Sophos ist die eingetragene Marke von Sophos Ltd. Alle anderen genannten Produkt- und Unternehmensnamen sind Marken oder eingetragene Marken ihres jeweiligen Inhabers.

05.09.2016 WP-DE (NP)

SOPHOS