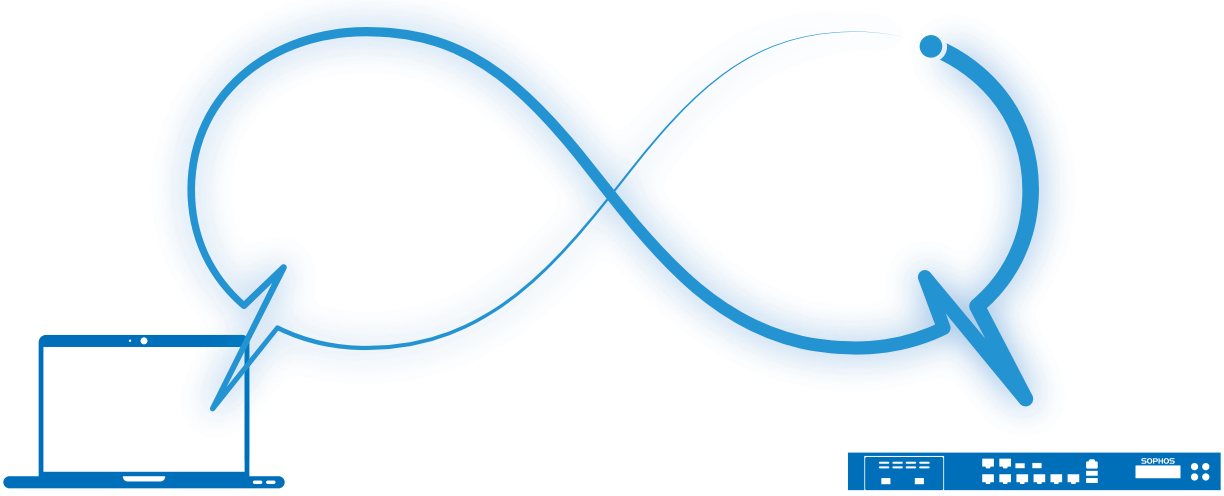
SOPHOS

Security made simple.



Synchronized Security – Eine revolutionäre Technologie

1) Leben in der Gefahrenzone – heutige Cyber-Risiken

Größere Angriffsfläche, immer komplexere und raffiniertere Angriffe

Unternehmen, egal ob kleine oder große, 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.

Erstens hat sich die sogenannte „Angriffsfläche" aufgrund der großen Anzahl an Mobilgeräten und Cloud-Services, die von den Mitarbeitern genutzt werden, sowie der virtuellen und Cloud-Infrastruktur, die von Unternehmen aller Größen eingesetzt werden, dramatisch vergrößert. Bedenken Sie folgende Fakten:

- Der durchschnittliche Benutzer in Deutschland verfügt über 3,1 internetfähige Geräte (Quelle: Naked-Security-Studie „How do you compare to Steve Wozniak?" durchgeführt mit 2226 Teilnehmern im Januar 2013).
- Unternehmen mit 250 bis 999 Mitarbeitern verwenden durchschnittlich 16 zugelassene Cloud-Apps, Unternehmen mit 1000 bis 4000 Mitarbeitern 14 und die größten Unternehmen nur 11 dieser Apps. (Quelle: Okta Business@work, 2015)
- Schätzungen für die Branche besagen, dass Cloud-Dienstleistungen im Jahr 2015 Umsätze von mehr als 16 Mrd. US-Dollar in 2015 generieren werden (Quelle: Gartner, http://www.gartner.com/newsroom/id/3055225)
- Bis Ende 2015 werden 4,9 Milliarden „Dinge" mit dem Internet verbunden sein. Bis 2020 wird diese Zahl auf 25 Milliarden wachsen. (Quelle: http://www.gartner.com/newsroom/id/2905717, 2014)

Aufgrund dieser wachsenden Angriffsfläche sieht sich die Welt auch mit einer steigenden Anzahl an Angriffen und Sicherheitslücken konfrontiert, die vermehrt zu Datenverlusten führen.

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 oftmals vielfach erprobt und werden sogar kommerziell unterstützt. Sie sind 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 (Quelle:Threatgeek.com).

Leider werden offenbar gerade kleine und mittlere Unternehmen unverhältnismäßig häufig Opfer der zunehmenden bestätigten Datenverluste. Dies zeigen die Ergebnisse des Verizon 2015 Data Breach Investigation Report:

Bedrohungslandschaft

- Im Jahr 2014 gab es 79.790 Sicherheitsvorfälle, davon waren 2.122 bestätigte Datenverluste
- Dies entspricht einem Anstieg der Sicherheitsvorfälle von 26 % und einem astronomisch hohen Zuwachs an Datenverletzungen von 55 % im Vergleich zum Jahr 2013.
- Mittlere Unternehmen waren von über 53 % der bestätigten und klassifizierten Datenverluste betroffen, obwohl diese nur 1,4 % der Sicherheitsvorfälle ausmachten.
- Sicherheitsvorfälle und Datenverluste in kleineren Unternehmen sind in vielen verschiedenen Branchen zu finden, wobei die Bereiche Finanzdienstleistungen, Immobilien, Einzelhandel und Gesundheit am häufigsten betroffen sind.

Die Kombination aus größerer Angriffsfläche und wachsender Komplexität der Angriffe führt zu immer mehr Datenverlusten. Diese Entwicklung ist alarmierend und zeigt, dass dringend neue Denkansätze für effektive Sicherheitslösungen benötigt werden.

Kleine Teams, knappe Ressourcen, wenig Spezialisten

Wenn die Anzahl der Angriffe und Datenverletzungen steigt, wird man in der Regel versuchen, zusätzliche Mitarbeiter auf das Problem anzusetzen. Kleine und mittlere Unternehmen verfügen jedoch meist nur über kleine IT-Sicherheitsteams. Die Erweiterung oder Neuzuweisung von Ressourcen, auch wenn dies eine effektive Strategie wäre, ist keine realistische Option für kleinere Unternehmen. Wie Sie in der Abbildung sehen können, sind die IT-Sicherheitsteams in kleinen und mittleren Unternehmen in Bezug auf Größe und Bandbreite sehr begrenzt:

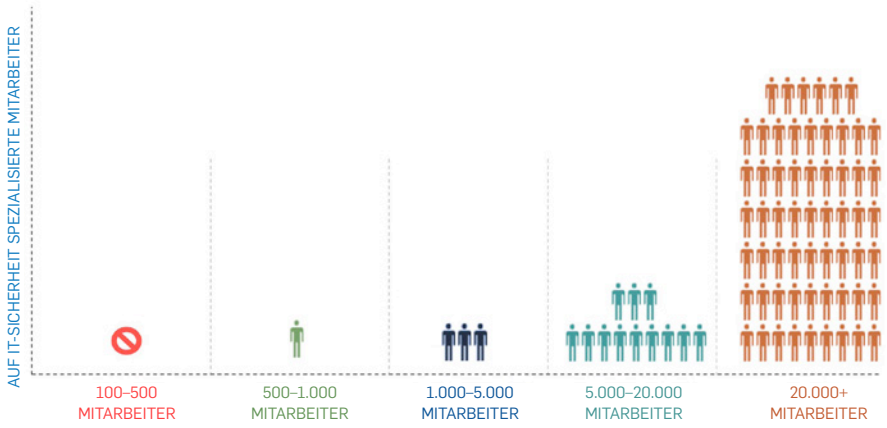


Abbildung 1: IT-Sicherheitsabteilungen von mittleren Unternehmen sind klein und haben nur begrenzte Ressourcen (Quelle: US Dept of Homeland Security, 2014)

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.

Zusammengefasst lässt sich Folgendes sagen: Die Angriffsfläche hat sich ernorm vergrößert, Angriffe nehmen zu und werden immer raffinierter, dazu stehen für die IT-Sicherheit oft nur kleine Teams mit begrenzten Ressourcen zur Verfügung. 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!

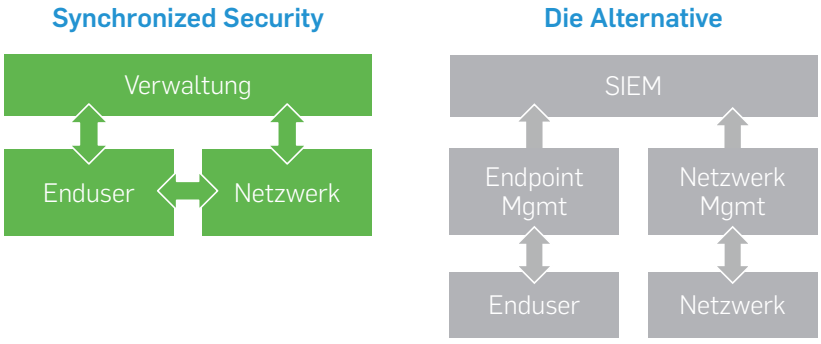
Architektur mit mehreren Schichten und schlechter Integration. Komplex und kurzsichtig. Kontextunabhängig. Isolierte Entscheidungen. Diese Beschreibungen treffen auf die meisten aktuellen Sicherheitslösungen zu. Vom Virenschutz, IPS, Web-, E-Mail- und Netzwerk-Gateway mit der Technologie von gestern bis hin zu den heutigen Produkt-Suites, UTMs, Sandboxes und Endpoint-Erkennungs- und Reaktionslösungen – heutzutage kommen in der Regel IT-Sicherheitslösungen zum Einsatz, die sehr komplex sind und unabhängig voneinander arbeiten. Angesichts der koordinierten Angriffe auf gesamte IT-Ökosysteme ist es kein Wunder, dass diese Lösungen nicht Schritt halten können. Ein Angriff beginnt zwar oft an einem Endpoint, breitet sich dann jedoch schnell über das gesamte Netzwerk aus und zieht Daten über die ausgehende Internetverbindung ab.

Als Reaktion auf diese Tatsache haben IT-Sicherheitsexperten und Dienstleister 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 und 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 dem 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 6 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.



3) Synchronized Security: Ein völlig neuartiger Ansatz

Eine revolutionäre Idee

Seit Jahrzehnten hat die IT-Sicherheitsbranche Netzwerk- und Endpoint-Sicherheit als zwei komplett unterschiedliche Bereiche betrachtet. Das ist so, als ob man einen Mitarbeiter für Gebäudesicherheit außerhalb des Gebäudes und einen anderen im Gebäude positioniert, ohne dass die beiden miteinander kommunizieren können – ein absurder Gedanke. Genau hier setzt unsere neue, synchronisierte Sicherheit an: Sie sorgt dafür, dass die beiden Mitarbeiter miteinander sprechen. Wir geben jedem der beiden ein Funkgerät in die Hand, sodass ein erkanntes Problem sofort an den anderen kommuniziert werden kann.

Wie wäre es, wenn wir ganz von vorn beginnen – mit einem neuartigen Ansatz, der auf einer anderen Denkweise basiert? Und so unseren IT-Sicherheitsteams ermöglichen, sich erfolgreich gegen die raffinierten Angriffe zu verteidigen? Mit einem Ansatz, der einen besseren Schutz bietet und eine automatisierte Kommunikation in Echtzeit zwischen den Netzwerk- und Endpoint-Sicherheitslösungen 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 und Geräten abdecken; nur so kann sie uns effektiv gegen Angreifer schützen, die nicht einzelne Punkte, sondern unser gesamtes System angreifen.

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.

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. Die Gegenüberstellung in Abbildung 2 zeigt die Herausforderungen noch einmal deutlich auf.

Heutige, mehrschichtige Lösungen	Gewünschte, neuartige Lösung
Einzig auf die Bedrohung konzentriert; agieren, ohne über alle Vorgänge im System informiert zu sein	Konzentriert sich auf das gesamte IT-Ökosystem, verfügt beim Agieren über Informationen zu allen Vorgängen im System
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
Komplex	Einfach

Abbildung 2: Die heutigen Lösungen müssen drastisch 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.

Der Sophos Security Heartbeat

Synchronisierte Sicherheit ermöglicht es den Endpoint- 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- 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, sobald ein Angriff auf diesen erkannt wird. So ist sichergestellt, dass keine vertraulichen Daten abgezogen oder Daten an einen Command-and-Control-Server gesendet werden. Diese Erkennung und Reaktion, die sonst oft Wochen oder Monate dauert, ist dank synchronisierter Sicherheit innerhalb von Sekunden möglich.

Zusammenfassung

Nie war das Risiko von Cyber-Angriffen so hoch wie heute: Der immer größer werdenden Angriffsfläche und den immer zahlreicheren, raffinierteren Angriffen stehen in kleinen und mittleren Unternehmen meist kleine IT-Sicherheitsteams mit begrenzten Ressourcen gegenüber. Die heute verfügbaren mehrschichtigen Ansätze sind nicht erfolgreich, ebenso-wenig wie die Bemühungen, die Unzulänglichkeiten dieser Lösungen mit Analysen und mehr Analysten 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. Die gute Nachricht: Sophos bietet Ihnen ab sofort diese innovative Technologie, die all dies ermöglicht – den Sophos Security Heartbeat.

Sie möchten mehr erfahren und unsere neuartige Technologie testen? Besuchen Sie unsere Seite www.sophos.de/heartbeat.

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

Oxford, GB | Boston, USA

2015-10-13 WP-DE (GH)

SOPHOS