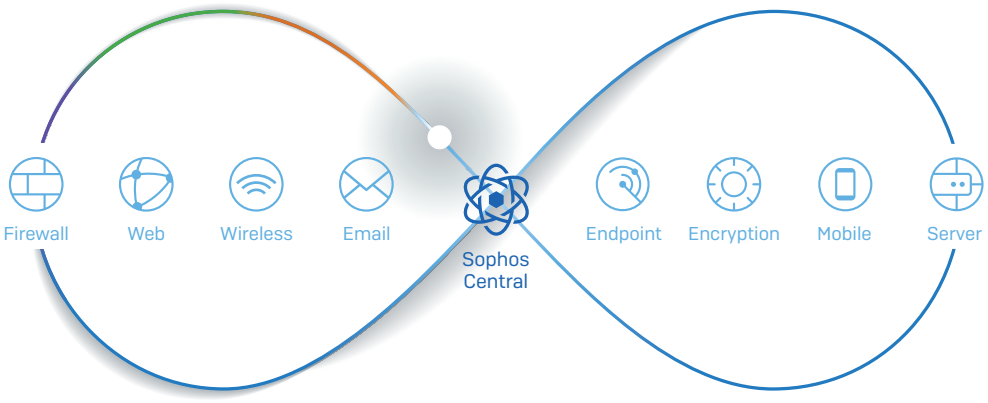
SOPHOS
Security made simple.



Synchronized Security: Eine revolutionäre Technologie

Sophos-Whitepaper Juni 2017

1) 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 setzen zunehmend virtuelle und Cloud-Infrastrukturen ein. Die sogenannte „Angriffsfläche" hat sich dadurch dramatisch vergrößert.

Bedenken Sie folgende Fakten:

- **Geräte:** Der durchschnittliche digitale Konsument besitzt mittlerweile drei verbundene Geräte.[1]
- **Anwendungen:** Mitarbeiter nutzen beruflich im Durchschnitt 16 Cloud-Anwendungen – Box, SalesForce und Microsoft Office 365 stehen auf der Beliebtheitsskala ganz oben.
- **Internet der Dinge:** Prognosen von Gartner zufolge werden bis 2020 fast 21 Mrd. „Dinge" mit dem Internet verbunden sein.[3]

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

Außerdem sind dank kommerziell unterstützten Malware-Toolkits, die auf den Grau- und Schwarzmärkten angeboten werden, immer weniger Fachkenntnissen notwendig, um im großen Stil immer raffiniertere Angriffe durchzuführen.

Zudem kopieren Cyberkriminelle die cloudbasierten Geschäftsmodelle seriöser Unternehmen und bieten „Malware-as-a-Service" an (z. B. Ransomware als Serviceleistung) – komplett mit Geld-zurück-Garantie. Damit sind für Cyber-Angriffe noch weniger Fachkenntnisse erforderlich und die Hacker können sich darauf verlassen, dass die Tools laufend aktualisiert werden.

All diese Entwicklungen haben dazu geführt, dass Cyberkriminelle nun in der Lage sind, schneller zu agieren als die meisten Unternehmen Schritt halten können. Dies zeigen die Ergebnisse des Verizon 2016 Data Breach Investigation Report:

- Hacking und Malware sind die beiden Hauptgründe für Datenpannen.
- Angreifern gelingt es immer schneller, ihre Opfer zu kompromittieren – die Zeitspanne bis zur Kompromittierung beträgt in fast allen Fällen höchstens ein paar Tage, oft sogar nur Minuten oder noch weniger.
- Das Erkennungsdefizit (die Zeitspanne zwischen Kompromittierung und Erkennung) erhöht sich und es dauert länger, bis die Angriffe erkannt werden.

Außerdem kommt der Verizon-Report zu dem Schluss, dass finanzielle Bereicherung bei mehr als 80 % dieser Angriffe das Hauptmotiv darstellt. Für kleine und mittelständische Unternehmen können die finanziellen Folgen verheerend sein.

Immer mehr Angriffe, immer komplexere Angriffsszenarien und zunehmende Datenverluste. Die Frage ist: Was müssen wir anders machen, um uns zu schützen?

Kleine Teams, knappe Ressourcen, wenig Spezialisten

Wenn die Anzahl der Angriffe steigt, wird man in der Regel versuchen, zusätzliche Mitarbeiter auf das Problem anzusetzen. Da die meisten Unternehmen jedoch nur kleine IT-Security-Abteilungen haben, ist eine Erweiterung oder Neuzuweisung von Ressourcen gerade für viele kleine und mittlere Unternehmen keine realistische Option.

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

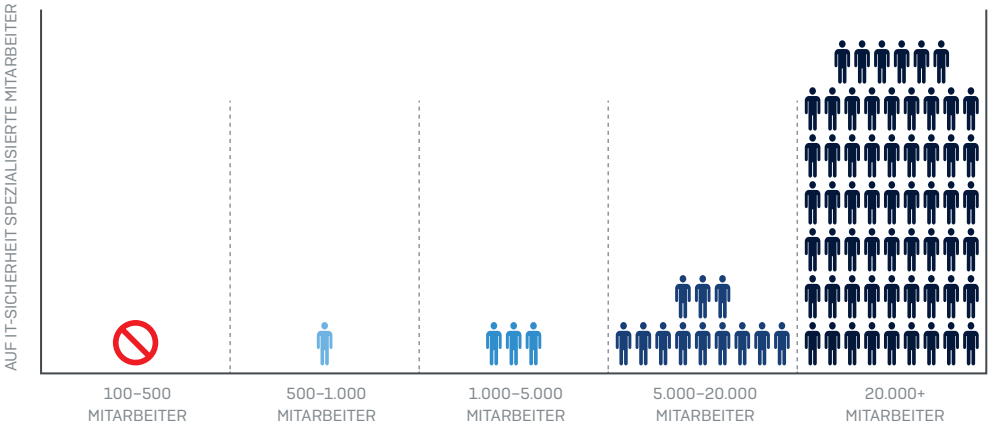


Abbildung 1: IT-Sicherheitsabteilungen in mittleren Unternehmen sind klein und haben nur begrenzte Ressourcen (Quelle: US Dept of Homeland Security, 2014)

Und selbst wenn beschlossen wird, das interne IT-Sicherheitsteam zu vergrößern, ist es gar nicht so einfach, geeignete Mitarbeiter für diesen Bereich zu finden. Forschungsergebnissen der Enterprise Strategy Group zufolge räumen ganze 46 % der Unternehmen ein, nicht genügend auf Cybersecurity spezialisierte Mitarbeiter zu haben.[4] Dies wiederum erhöht den Druck auf bestehende IT-Abteilungen, mit weniger Ressourcen mehr zu erreichen.

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, die sich einfach darauf verlassen, dass ihre Mitarbeiter mit dem Problem schon fertigwerden, gehen ein extrem hohes Risiko ein.

2) Herkömmliche Sicherheitskonzepte

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

Angreifer starten koordinierte Angriffe auf ein gesamtes IT-Ökosystem, nicht auf einzelne Produkte.

Wenn wir uns vor Augen führen, wie sich die IT-Security-Branche entwickelt hat, verwundert das kaum. Anstatt eine übergreifende Lösung für die wachsende Gefahr durch Cyber-Bedrohungen zu finden, haben sich IT-Security-Anbieter auf die Entwicklung von Einzelprodukten konzentriert, die jeweils nur auf ganz bestimmte Punkte in der Angriffskette eingehen. Daher mussten überlastete IT-Abteilungen bislang mühselig verschiedene Insellösungen zu einem System integrieren. Das ist so, als würden Autohersteller einzelne Autoteile liefern und es dem Kunden überlassen, die Teile zu einem Auto zu montieren.

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 vieler einzelner Produkte so zu erfassen und zu verstehen, dass sich Risiken schnell erkennen und beheben lassen und Datenverluste gestoppt werden 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. Datenverluste und Datenpannen sind weiter auf dem Vormarsch und IT-Abteilungen sind heillos überlastet. Laut einem neuen Bericht des Ponemon Institute bleiben 74 % der Sicherheitsverletzungen länger als sechs Monate unentdeckt. Mittlere Unternehmen haben in der Regel noch größere Schwierigkeiten mit dem Umgang dieses Risikos 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) Revolutionäre IT-Sicherheit

Jahrzehntelang hat die IT-Sicherheitsbranche Netzwerk-, Endpoint- und Datensicherheit als komplett unterschiedliche Bereiche betrachtet. Das ist so, als würde man einen Mitarbeiter für Gebäudesicherheit außerhalb des Gebäudes, einen anderen im Gebäude und einen dritten vor dem Safe positionieren, ohne dass die drei miteinander kommunizieren können – ein absurder Gedanke.

Da Bedrohungen immer komplexer werden und IT-Abteilungen zunehmend an ihre Grenzen stoßen, ist dieses veraltete Konzept immer weniger praktikabel.

Synchronized Security ist ein branchenführendes Sicherheitssystem, bei dem integrierte Produkte dynamisch Bedrohungs-, Integritäts- und Sicherheitsinformationen austauschen. Das Ergebnis: schnellerer, besserer Schutz vor hochentwickelten Bedrohungen. Um bei unserem Beispiel zu bleiben: Man stattet alle drei Mitarbeiter für Gebäudesicherheit mit einem Funkgerät aus, damit sie miteinander kommunizieren und ihre Maßnahmen zur Gefahrenabwehr koordinieren können.

Dieses Konzept ist im Grunde ganz einfach, und dennoch revolutionär. Um Synchronized Security zu erreichen, sind drei Dinge erforderlich:

1. **Ein zentrales Sicherheitssystem**
   Den Kernpunkt unseres Synchronized-Security-Konzepts bildet eine zentrale Security-Plattform, die über Bedrohungs- und Sicherheitskontextdaten für alle Geräte und Datenbestände verfügt. Diese muss einfach bedienbar sein und Ihnen ermöglichen, Ihren gesamten Schutz an einem Ort zu verwalten. So müssen Sie nicht mehr von einer Konsole zur nächsten springen und sparen viel Zeit.
2. **Next-Gen-Technologie**
   Eine Synchronisierung darf nicht zu Lasten des Schutzes gehen. In jede Sicherheitskomponente muss die neueste Anti-Malware-Technologie integriert sein, damit Sie immer den bestmöglichen Schutz erhalten.
3. **Intelligenter Schutz**
   Das Sicherheitssystem muss den Sicherheitstechnologien ermöglichen, Informationen auszutauschen und Reaktionsmaßnahmen zu automatisieren. Hierzu zählt u. a. das Isolieren aller infizierten Geräte in Echtzeit, wodurch der Verlust von Daten und weitere Infektionen innerhalb Ihres Unternehmens verhindert werden. Das Ergebnis ist einzigartiger Schutz vor hochentwickelten, komplexen Bedrohungen.

Heutige, mehrschichtige Lösungen	Synchronized Security
Auf Bedrohungen konzentriert, operieren 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

4) Das etwas andere Konzept von Sophos

Der Synchronized-Security-Ansatz von Sophos ist einmalig. IDG zufolge kann kein anderes Unternehmen auch nur ansatzweise eine vergleichbare Kommunikation zwischen Endpoint- und Netzwerksicherheitsprodukten bieten. Aber wie gelingt uns das?

Mit unserer preisgekrönten Security-Plattform Sophos Central können Sie Ihre gesamte Sophos-Sicherheit an einem zentralen Ort verwalten: Endpoint, Mobile, Server, Web, Email, Wireless und Firewall Security sowie Verschlüsselung. Dabei handelt es sich nicht bloß um eine zentrale Management-Konsole. Synchronized Security bietet wesentlich mehr. Wie Gartner beschreibt, handelt es sich bei „Synchronized Security" um eine „Integration auf Richtlinienebene", während es bei einer zentralen Konsole lediglich eine „Integration der Benutzeroberfläche" gibt.

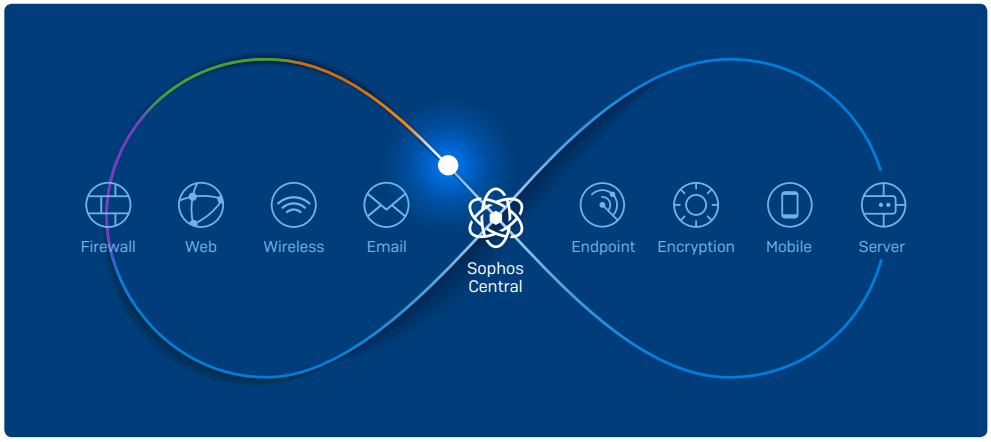


Abbildung 3: Synchronized Security mit Sophos

Next-Gen-Technologie ist in unsere Produkte integriert. Ihr Schutz vor Ransomware, Exploits, Malware und ATPs ist also immer und für alle Geräten und Datenbestände topaktuell. Die Leistungsstärke unserer Technologie wird regelmäßig durch Branchenexperten und -auszeichnungen bestätigt:

- Als einziger Anbieter sind wir Leader in den **Gartner** Magic Quadrants für Endpoint Protection Platforms und UTM
- **Computing's** Best Firewall 2016
- „Breakout Star" in **Forrester** Encryption Wave 2016
- **SC Magazine** Excellence Award for Encryption and Network Firewall
- **AV-Test** Best Android Security 2016

Synchronized Security basiert auf unserem patentierten Security Heartbeat™, einer sicheren Kommunikationsverbindung zwischen Sophos-Produkten, über die Bedrohungs-, Integritäts- und Sicherheitsinformationen ausgetauscht und im Falle von Kompromittierungen automatische Reaktionsmaßnahmen eingeleitet werden können. Dutzende Technologien arbeiten auf koordinierte Weise zusammen, um weltbesten Schutz vor koordinierten Angriffen zu bieten. Sophos Security Heartbeat reduziert den Zeitaufwand für Bedrohungserkennung, Schutz und Reaktion von Stunden, Tagen oder sogar Wochen auf Sekunden.

5) Synchronized Security: Stoppen moderner Bedrohungen

Um die Effektivität von Synchronized Security besser zu veranschaulichen, sollten wir uns ansehen, wie die Technologie bei zwei der aktuell besonders verbreiteten Bedrohungen funktioniert: Botnets und Ransomware.

Botnets

Botnets, d. h. Netzwerke „unschuldiger" Geräte, die von Hackern übernommen wurden, um koordinierte Cyber-Angriffe auszuführen, sind mittlerweile eine der fünf größten Sicherheitsbedrohungen weltweit. Sie werden für viele verschiedene Angriffe genutzt, u. a.:

- Cryptocoin Mining
- Datenhacks über Point-of-Sale-Systeme wie im Fall des US-Einzelhändlers Target
- DDoS- oder erweiterte DNS-Angriffe wie das Mirai-Botnet, das weltweit Websites lahmlegte
- Brute-Force-Passwort-Hacks und Spamming

Der Integritätsstatus und die Botnet-Bedrohungsinformationen werden per Security Heartbeat an die Sophos XG Firewall gesendet, die das kompromittierte Gerät isoliert, indem sie ihm den Netzwerkzugriff entzieht. Auf diese Weise wird verhindert, dass Botnet-Malware mit ihrem Command-and-Control-Server kommuniziert und weitere Anweisungen entgegennimmt. Zudem werden weitere Infektionen durch dieses Ausgangsgerät unterbunden.

Der Security Heartbeat tauscht diese Informationen auch mit der Sophos Encryption aus, die dem betroffenen System zur Verhinderung von Datendiebstahl die Schlüssel entzieht, bis das Problem behoben wurde.

Der gesamte Prozess, von der Erkennung über die Isolierung bis hin zum Schlüsselentzug, läuft praktisch in Echtzeit ab und verkürzt die Reaktion auf Vorfälle von Stunden auf Sekunden.

Sobald alle betroffenen Systeme isoliert wurden und nicht mehr vom Botnet genutzt werden können, entfernt unsere Endpoint Protection die Botnet-Malware automatisch.

Nachdem die Systeme automatisch in ihren „sauberen" Ausgangszustand zurückgekehrt sind, kann der IT-Administrator den Integritätsstatus des Endpoints wieder auf GRÜN stellen. Diese Informationen werden per Security Heartbeat sofort mit dem Rest des Sicherheitssystems ausgetauscht. Die XG Firewall stellt den Netzwerkzugriff des Geräts wieder her, die Schlüssel werden zurückgegeben und Ihr Netzwerk ist Botnet-frei.

Ransomware

Ransomware ist ein äußerst lukratives Geschäft. Weltweit ist sie für bis zu 35 % aller IT-Bedrohungen verantwortlich und ein erfolgreicher Angreifer kann mit ihr bis zu 400.000 USD im Monat verdienen.

Ransomware wird in der Regel per E-Mail in Umlauf gebracht. Sobald ein nichtsahnender Benutzer eine infizierte E-Mail öffnet und die Ransomware aktiviert, stoppt die Anti-Ransomware-Technologie von Sophos Intercept X den Angriff auf Desktops, Laptops und Server; Sophos Mobile Security schützt mobile Geräte.

Synchronized Security stellt den Integritätsstatus gefährdeter Geräte in Sophos Central auf ROT. Diese Statusänderung und zugehörige Bedrohungsinformationen werden per Security Heartbeat an die Sophos XG Firewall gesendet, die das infizierte Gerät durch Entzug des Netzwerkzugriffs automatisch isoliert. So wird verhindert, dass Ransomware Informationen zurück an einen Command-and-Control-Server melden und weitere Infektionen verursachen kann.

Der Security Heartbeat kontaktiert gleichzeitig Sophos Encryption, damit dem betroffenen System bis zur Behebung des Problems die Schlüssel entzogen werden. Ähnlich wie beim Botnet-Prozess erfolgt unmittelbar nach der Erkennung die Isolierung des Systems und der Einzug der Schlüssel, wodurch die Reaktionszeit bei Vorfällen von Stunden auf Sekunden reduziert wird.

Nach erfolgter Bereinigung kann der IT-Administrator den Integritätsstatus des Endpoints wieder auf GRÜN stellen. Dieses Statusupdate wird per Security Heartbeat sofort an das übrige Sicherheitssystem übertragen. Die XG Firewall stellt den Netzwerkzugriff des Geräts wieder her, die Schlüssel werden zurückgegeben und der Benutzer kann wieder wie gewohnt arbeiten.

All dies geschieht automatisch und ohne jede Zeitverzögerung. Sie müssen nicht selbst aktiv werden.

Zusammenfassung

Immer mehr Unternehmen sind von der wachsenden Flut komplexer und koordinierter Angriffe überfordert. Überlastete IT-Abteilungen tun sich schwer, schnell genug auf Bedrohungen zu reagieren, die sich auf ihre stetig weiterwachsende IT-Infrastruktur Zugriff verschaffen.

Unternehmen, die weiterhin versuchen, diesem Problem mit verschiedenen Insellösungen Herr zu werden, gehen ein extrem hohes Risiko ein. Sollte sich die Herangehensweise an IT-Sicherheit nicht grundlegend verändern, wird sich diese Situation noch verschärfen.

Synchronized Security ist ein branchenführendes Sicherheitssystem, bei dem integrierte Produkte dynamisch Bedrohungs-, Integritäts- und Sicherheitsinformationen austauschen, um schneller und besser vor komplexen Bedrohungen schützen zu können. Das Ergebnis ist bester Schutz und maximale Benutzerfreundlichkeit, sodass IT-Sicherheitsexperten ihre Arbeit einfacher erledigen können.

Sie möchten mehr erfahren und Synchronized Security selbst testen?
Besuchen Sie www.sophos.de/synchronized-security.

[1] Global Web Index, 18. Februar 2016

[2] UK Business Insider, August 2015

[3] CNBC, Februar 2016

[4] ESG Brief, Cybersecurity Skills Shortage: A State of Emergency, Februar 2016

Synchronized Security

Weitere Infos unter
www.sophos.de/synchronized-security

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

17-02-15 WPDE (DD-2560)

SOPHOS