# Advanced Threat Protection – Einkaufsführer

**LEITFADEN ZUR STÄRKUNG DES SICHERHEITSPROFILS IHRES UNTERNEHMENS**

# Inhalt



# Einleitung

Der Umfang und die Auswirkungen von Datendiebstählen, die aus immer raffinierteren Angriffen erwachsen, nehmen kontinuierlich zu. Häufig werden solche Angriffe speziell entwickelt und getestet, um herkömmliche Sicherheitsmaßnahmen zu umgehen und gezielt bestimmte Unternehmen anzugreifen.

Um diesen komplexen Bedrohungen zu begegnen, empfehlen die meisten Sicherheitsanalysten, Experten und Anbieter eine Kombination aus verbesserter Prävention, modernen Methoden zur Erkennung komplexer Bedrohungen und Gegenmaßnahmen. Zwar scheinen sich die Lösungen auf den ersten Blick zu ähneln, doch bei näherer Betrachtung treten Unterschiede zu Tage.

Unter Zuhilfenahme dieses Leitfadens können Sie Ihr aktuelles und geplantes Sicherheitsprofil mit Baseline-Anforderungen vergleichen, um schließlich die richtigen Lösungen für Ihr Unternehmen zu finden.

# Advanced Threat Protection

Auch wenn neue Technologien wie Netzwerk-Sandboxing viel Beifall ernten, so kann doch kein einzelnes Produkt allein die Herausforderungen meistern, die aus den heutigen komplexen Bedrohungen erwachsen. Im Bericht *Best Practices for Detecting and Mitigating Advanced Persistent Threats*[1] kommt Gartner zu folgendem Schluss: „Wer in der Informationssicherheit tätig ist, muss strategische und taktische Best Practices umsetzen, um komplexe persistente Bedrohungen und gezielte Malware durch den Einsatz etablierter und neuer Sicherheitsmaßnahmen zu erkennen und abzuwehren."

Fortinet pflichtet dieser Feststellung bei und empfiehlt:

1. **Breite Abdeckung** im gesamten Unternehmen mit
2. der richtigen Mischung aus **Prävention, Erkennung und Abwehr**, die
3. **als Teil eines zusammenhängenden Sicherheitssystems** statt als Ansammlung einzelner Komponenten operiert.

Indem Sie sicherstellen, dass die Sicherheitsinfrastruktur Ihres Unternehmens alle drei Aspekte abdeckt, gewährleisten Sie die stärkste Verteidigung.

## BREITE ABDECKUNG

Die Unternehmensumgebung von heute ist dynamisch und entwickelt sich ständig weiter. Dabei wird sie vor allem durch Mobility, Cloud-Services, verschlüsselte Kommunikation und andere Faktoren vorangetrieben. Die Umsetzung von Sicherheitsmaßnahmen zum Schutz von Benutzern, Systemen und Daten wird damit erheblich komplexer. Bei der Bewertung und Verbesserung Ihrer Verteidigungsstrategien gegenüber den raffinierten Cyberbedrohungen von heute müssen Sie unbedingt den physischen Standort, die digitale Kommunikation und die schiere Menge der zu untersuchenden und zu schützenden Daten berücksichtigen.

## Physische Standorte

Unternehmen fangen per Definition an den Schnittstellen vom und zum Internet an. Diese können entweder in Rechenzentren konsolidiert oder auf lokale Niederlassungen verteilt sein und sind wichtige Kontrollstellen für Sicherheitsprüfungen. Auch die Bewertung des Datenverkehrs im Zusammenhang mit sensiblen Netzwerksegmenten im Core sind enorm wichtig. Eine Ausweitung der Prüfung auf Endgeräte, die Bedrohungen von außerhalb des Netzwerks ausgesetzt sein können, und auf Anwendungen und Daten in Public Cloud-Infrastrukturen sollte ebenfalls erfolgen. Zwar kann die Umsetzung der gleichen Kombination von Sicherheitstechnologien an allen Punkten eine Herausforderung darstellen, doch ein eingeschränkter Schutz erhöht das Risiko, das Schwachstellen entstehen, die ausgenutzt und überwunden werden können.

## Digitale Kommunikation

Die Analyse von Aktivitäten aus einer physischen Position gewährleistet nicht automatisch die Prüfung sämtlichen Datenverkehrs. Unternehmen müssen festlegen, für welche Kommunikationskanäle Sicherheitsanalysen stattfinden. In der Regel geschieht dies mithilfe von Protokollen. Web (HTTP) und E-Mail (SMTP) sind die gängigsten Ausgangspunkte und auch die beliebtesten Angriffsvektoren. Im *2015 Data Breach Investigations Report*[2] stufte Verizon das Web-Protokoll als den am häufigsten ausgenutzten Angriffsvektor ein, gefolgt von E-Mail. Auch eine Prüfung von Dateiübertragung und Speichermedien (per FTP oder SMB) muss erwägt werden. Vergessen Sie auf keinen Fall verschlüsselte Protokolle zu berücksichtigen, da Sie Cyberkriminellen damit Tür und Tor öffnen.

## Leistung und Kapazität

Wenn Sie nicht richtig dimensioniert sind, können Sicherheitslösungen angesichts des zu analysierenden Paket- und Aktivitätsvolumens überlastet werden. Besonders wenn sie direkt im Produktionsablauf implementiert sind, muss sichergestellt werden, dass die gewählten Produkte ausreichend Portkapazität haben, um Pakete anzunehmen, genügend Software-Leistung, um sie zu bearbeiten, und reichlich Rechenkapazität, um das gesammelte Datenvolumen zu analysieren. Ausgelassene Datenpakete oder überlange Warteschlangen schränken die Abdeckung ein, auch wenn physische Position und digitale Kommunikation etabliert sind und unterstützt werden.

### Expertentipp Nr. 1

Wenn sich das Sicherheitsmodell eines Unternehmens entwickelt, werden wie selbstverständlich neue Sicherheitskomponenten eingeführt, oft von neuen Anbietern. So haben viele Unternehmen als Reaktion auf Mobility und Nutzer mit mehreren Geräten ihre Schutzmaßnahmen beispielsweise um Mobile Device Management-Lösungen (MDM) von speziellen Nischenanbietern ergänzt. Und da immer mehr Rechenleistung in die Cloud-Infrastruktur ausgelagert wird, haben viele Sicherheitslösungen von Start-Ups hinzugefügt, die sich auf diese elastischen Umgebungen konzentrieren. Leider führt dieser Ansatz mit Insellösungen zu einer ungleichmäßigen Sicherheitsabdeckung in der sich verändernden Unternehmensumgebung. Zwar können einige Sicherheitselemente (Prävention, Erkennung oder Abwehr) an anderer Stelle implementiert sein, es sind jedoch nicht immer die besten oder umfassendsten Lösungen für das stärkste Sicherheitsprofil.

## DER RICHTIGE FUNKTIONSMIX

Bisher haben sich die Sicherheitsinvestitionen von Unternehmen größtenteils auf die Prävention konzentriert, während die Komponenten Erkennung und Abwehr nur relativ begrenzt zum Zuge kamen. Eine im November 2015 von Forrester durchgeführten Studie ergab, dass 87 % der befragten Unternehmen in den letzten 12 Monaten[3] mindestens eine Sicherheitsverletzung erlebten, was die Bedeutung von Erkennung und Abwehr unterstreicht.

### Prävention

Eine erfolgreiche Prävention beruht auf der Zusammenarbeit mehrerer Technologien, um die Angriffsfläche zu reduzieren und Bedrohungen am Eindringen in das Netzwerk zu hindern. Diese Technologien umfassen u. a. Signaturen und Heuristik zum Blockieren von Schadcode (Anti-Malware), Datenverkehr (Intrusion Prevention) oder Anwendungen (Application Control), die reputationsbasierte Einstufung von Internetseiten (Web Filtering), E-Mail-Absendern (E-Mail-Reputation) oder IPs (Botnet-Erkennung) und mehr. Es ist wichtig, so viele Angriffe wie möglich zu vereiteln, um teure und zeitraubende Analysen und Anstrengungen zur Erkennung und Abwehr komplexer Bedrohungen zu reduzieren. Wenn Sie Ihre „traditionellen“ Produkte zur Bedrohungsprävention auf eine effektivere und proaktivere Lösung aufrüsten, können Sie sich weitaus besser gegen die raffinierten Bedrohungen von heute verteidigen. Bewerten Sie Ihre vorhandene Netzwerk-, Web-, E-Mail- und Endgerätesicherheit akribisch, um zu sehen, wie gut oder schlecht sie funktioniert. Denken Sie auch darüber nach, neuere Komponenten für die Bedrohungsprävention, wie Web Application Firewalls, hinzuzufügen, sofern das noch nicht geschehen ist.

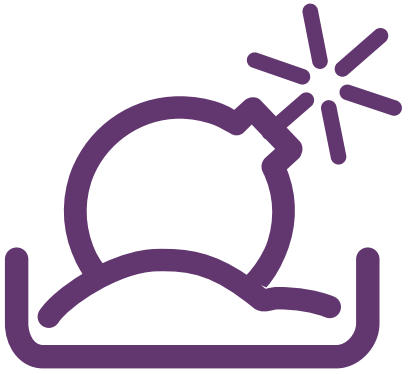

der Unternehmen verzeichneten in den **letzten 12 Monaten mindestens eine Sicherheitsverletzung**

## Erkennung

Neue Technologien zielen darauf ab, bisher unbekannte Bedrohungen, die bewährte Schutzmechanismen umgehen, zu identifizieren. Einer der beliebtesten und wichtigsten Ansätze ist dabei das Netzwerk-Sandboxing. In der Forrester-Studie *Sandbox Technology: Building an Effective Breach Detection and Response Strategy* [4] gaben 87 % der erfahrenen Sicherheitsexperten an, dass Sandboxes wichtige Daten zur Erkennung komplexer Bedrohungen liefern. Auch viele weitere Technologien sind eine Überlegung wert – von dynamischen Client-Reputationsanalysen über Netzwerkverhaltensanalysen bis hin zu Big Data-Analytik und mehr. Auch wenn Ihr Unternehmen für einige dieser Technologien möglicherweise noch nicht bereit zu sein scheint, denken Sie daran, dass die wichtige Technologie von heute auf eine kritische Technologie von gestern folgte und morgen wieder durch eine andere ersetzt wird. Diese Entwicklung spiegelt die sich stets verändernde Bedrohungslandschaft wider.

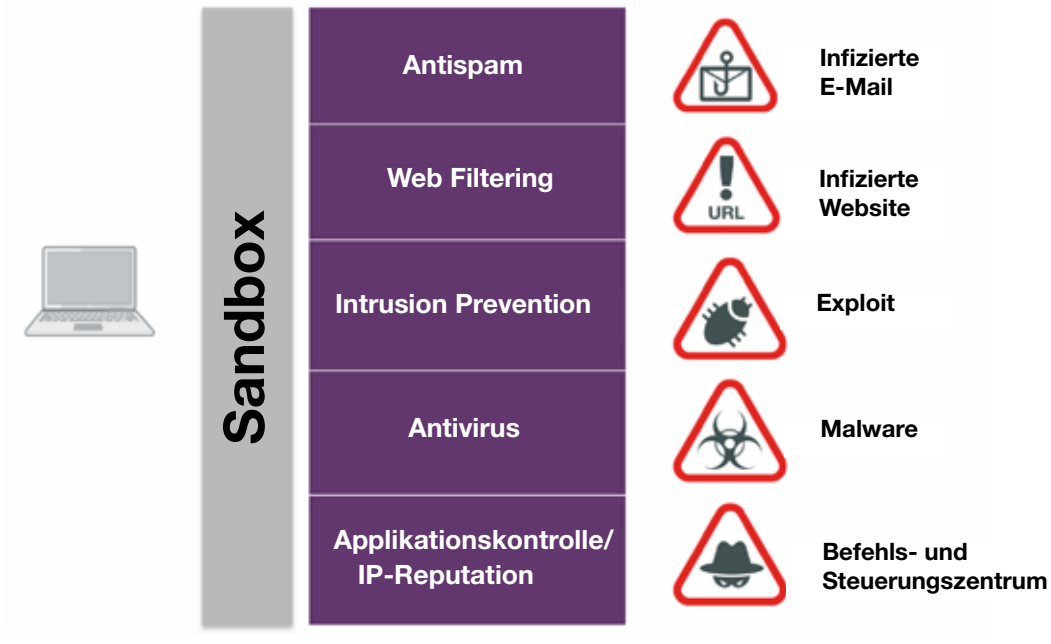
## Abwehr

Natürlich ist die Erkennung laufender Angriffe ohne eine entsprechende Reaktion zur Schadensbegrenzung und Verhinderung von umfangreichen Datendiebstählen nur von begrenztem Wert. Unternehmen müssen sicherstellen, dass ihre Erkennungssysteme geeignete Daten liefern, um eine effektive Reaktion zu gewährleisten. Analog dazu benötigen Sicherheitsexperten die richtigen Prozesse und Werkzeuge, um eine schnelle Abwehr sicherzustellen. Forensiktools, unterstützende Services und selbst die Integration in Ihre vorhandenen Bedrohungspräventionsprodukte spielen dabei eine wichtige Rolle. Je besser gestützt oder automatisiert Ihr Reaktionsprozess ist, desto wirkungsvoller die Abwehrbemühungen.



**87 % der Experten**

gaben an, dass Sandboxes wichtige Daten zur Erkennung komplexer Bedrohungen liefern

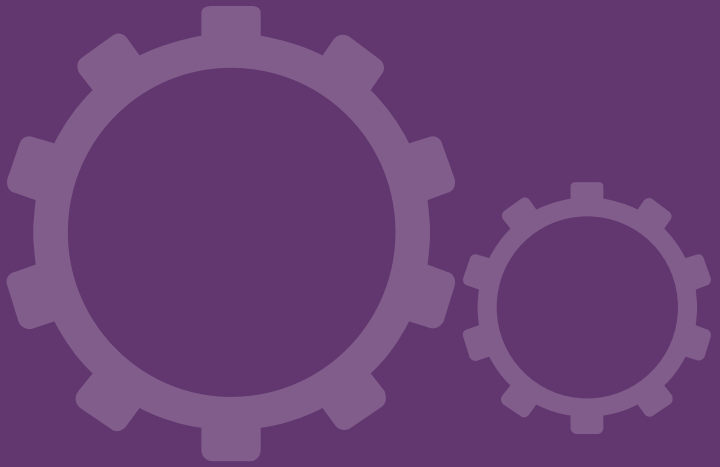



## Expertentipp Nr. 2

Eine der besten Möglichkeiten, die Effektivität zu bewerten, sind unabhängige Vergleichstests in der Praxis. Auch wenn diese Umgebungen von Ihrer abweichen, haben sie den Vorteil, dass sie durch die Nutzung großer Bestände komplexer Malware Produkte unter gleichen Bedingungen testen können. NSS Labs, Virus Bulletin und AV Comparatives sind renommierte Testeinrichtungen, die transparente Testmethoden nutzen und regelmäßige Produktvergleiche durchführen. Je nachdem, wie umfassend Sie in Ihrer eigenen Umgebung testen können und würden, können diese Tests ein hilfreiches Vergleichstool darstellen. Zumindest für kritische Sicherheitskomponenten ist ein rigoroser Vergleichstests mehrerer Lösungen vor Ort ideal. Dabei muss mindestens die Effektivität der einzelnen Komponenten nachvollziehbar erhoben werden.

# BETRIEB ALS INTEGRIERTES SYSTEM

Im Kampf gegen komplexe Bedrohungen müssen diese Komponenten nicht nur an den richtigen Stellen eingesetzt werden, sondern auch als zusammenhängendes System agieren. Ist dies nicht der Fall, hat Ihr Sicherheitsprofil zu viele Lücken, die von Cyberkriminellen ausgenutzt werden können, um sich Zugang zu Ihrem Netzwerk zu verschaffen. Ohne ein integriertes System müssen diese Lücken durch menschliches Eingreifen überbrückt werden und weiten sich im Laufe der Zeit aus. Wenn Sie also Ihre Sicherheitsinfrastruktur als Gesamtsystem bewerten, müssen Sie besonders die Integrationspunkte, automatisierte oder zumindest gestützte Maßnahmen und gemeinsam genutzte Informationszentralen unter die Lupe nehmen.



## Integrationspunkte

Der Datenaustausch kann auf verschiedenen Wegen erfolgen. Eine Möglichkeit ist die Konsolidierung über physische Standorte hinweg. Dabei können beispielsweise Firewalls für die Unternehmenszentrale, für Zweigniederlassungen und sogar für Cloud-Infrastrukturen einmalig konfigurieren. Auch Protokolle können über sichere E-Mail-Gateways und Firewalls hinweg konsolidiert werden. Die zweite Möglichkeit besteht im Austausch zwischen Sicherheitselementen. So können zum Beispiel Präventionskomponenten Objekte zur Analyse an Komponenten zur Erkennung von komplexen Bedrohungen weitergeben und diese wiederum zur schnellen Abwehr Daten an die Reaktionssysteme übermitteln. Drittens können Daten mittels neuer Standard-APIs und -Formate einem größeren Empfängerkreis zur Verfügung gestellt werden. So beschleunigen JSON-APIs oder STIXX/TAXII-Standarddatenstrukturen die Integration auf breiter Basis. Solange diese Standards für den Datenaustausch noch nicht genormt sind, achten Sie zumindest auf die Integration Ihrer eigenen Sicherheitselemente.

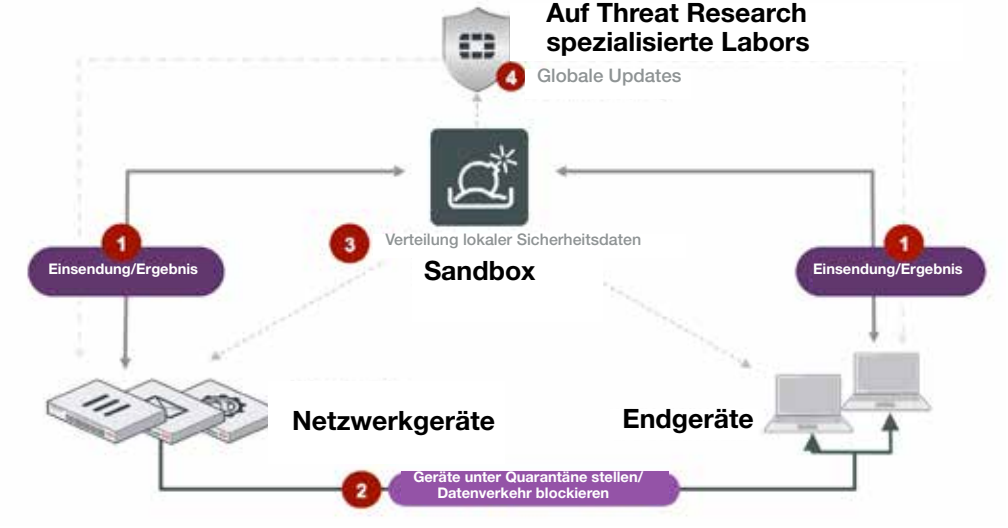
## Automatisierung

Der Austausch von Daten allein reicht aber nicht. Sie müssen auf diesen Daten beruhende Maßnahmen auch automatisieren können (oder zumindest unterstützen, sofern eine Überwachung durch Mitarbeiter gewünscht wird). Hilfreich ist es beispielsweise, wenn Ihre Advanced Threat-Erkennung automatisch Updates mit Bedrohungsdaten erstellt und an Ihre Bedrohungsprävention weitergibt, damit diese neuen Bedrohungen umgehend blockiert werden können. Ebenso können Anzeichen für Manipulationen weitergegeben werden, um administrative Maßnahmen zu beschleunigen. Gefähr-

dete Systeme können unter Quarantäne gestellt und/oder stark gefährdete IP-Adressen blockiert werden.

## Datenzentrale

Alle bisher erwähnten Maßnahmen sind rein taktischer Natur. Dabei ist die Umsetzung strategischer Maßnahmen, die das Sicherheitsprofil weiter schärfen, mindestens ebenso wichtig. Das umfasst die Entwicklung und großflächige Verteilung proaktiver Präventionsdaten, die Entwicklung neuer Sicherheitstechnologien für den Core und vieles mehr. Idealerweise werden Sicherheitsdaten sowohl lokal, d. h. direkt zwischen Ihren implementierten Komponenten, als auch global über ein auf Threat Research spezialisiertes Labor weitergegeben.




### Expertentipp Nr. 3

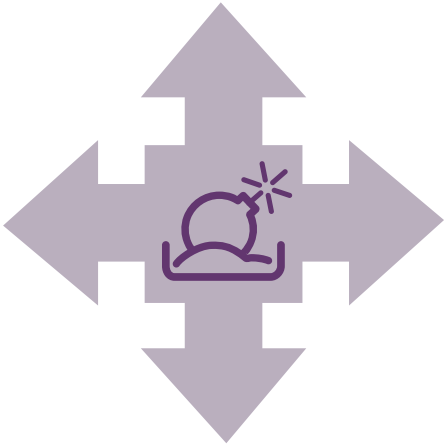
Integration und Datenaustausch sind zwar auch anbieterübergreifend möglich, Unternehmen sollten aber immer daran denken, dass sie bei Komplettlösungen eines Anbieters am ehesten mit der engsten Integration, der besten Automatisierung und dem schnellsten Datenaustausch rechnen können. Aber allein die Tatsache, dass mehrere Produkte von einem Anbieter stammen, ist noch keine Garantie, dass diese Komponenten integriert und automatisiert werden oder Daten untereinander austauschen können. Besonders häufig ist das bei Anbietern der Fall, die ihr Produktangebot regelmäßig durch Firmenübernahmen erweitern. Sehen Sie sich das Angebot also genau an, um sicherzugehen, dass eine enge Produktintegration unterstützt wird.

## FAZIT

Nicht alle komplexen Bedrohungen sind gleichermaßen raffiniert, aber viele umgehen herkömmliche Verteidigungsmaßnahmen. Das belegen die wiederkehrenden Schlagzeilen über Datendiebstähle, Branchenberichte und Analystenempfehlungen eindrucksvoll. Unternehmen, die sich besser gegen diese Bedrohungen schützen und verteidigen möchten, müssen mehr tun, als den neuesten, kurzlebigen Sicherheitstrends zu folgen, egal wie wichtig sie auch sind. Deshalb empfiehlt Fortinet besonders:

- ✓ Sorgen Sie in Ihrem dynamischen Unternehmen (vom physischen Standort bis zur Cloud) sowohl in der Breite als auch in der Tiefe für eine umfassende Abdeckung. Das beinhaltet auch den optimalen Mix aus Prävention, Erkennung und Reaktion für jeden Kontrollpunkt.
- ✓ Nutzen Sie rigorose unabhängige Testprozesse, um die Effektivität der einzelnen Sicherheitskomponenten zu bewerten. Ziel dabei ist, eine möglichst hohe Präventionsquote zu erreichen, bisher unbekannte Bedrohungen zu erkennen und auf diese zu reagieren.
- ✓ Arbeiten Sie auf eine kohärente Sicherheitslösung hin, die mithilfe von Integration, Automatisierung und einer gemeinsamen Datenzentrale (lokal sowie über globale Forschungsinstitute) Lücken schließt und die Kosten und Anstrengungen für das Durchschnittsunternehmen leistbar macht.

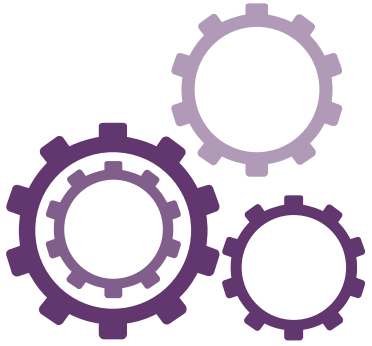
### Breite und Tiefe



### Rigorose Tests

1. Ⓐ Ⓑ Ⓒ Ⓓ
2. Ⓐ Ⓑ Ⓒ Ⓓ
3. Ⓐ Ⓑ Ⓒ Ⓓ
4. Ⓐ Ⓑ Ⓒ Ⓓ
5. Ⓐ Ⓑ Ⓒ Ⓓ

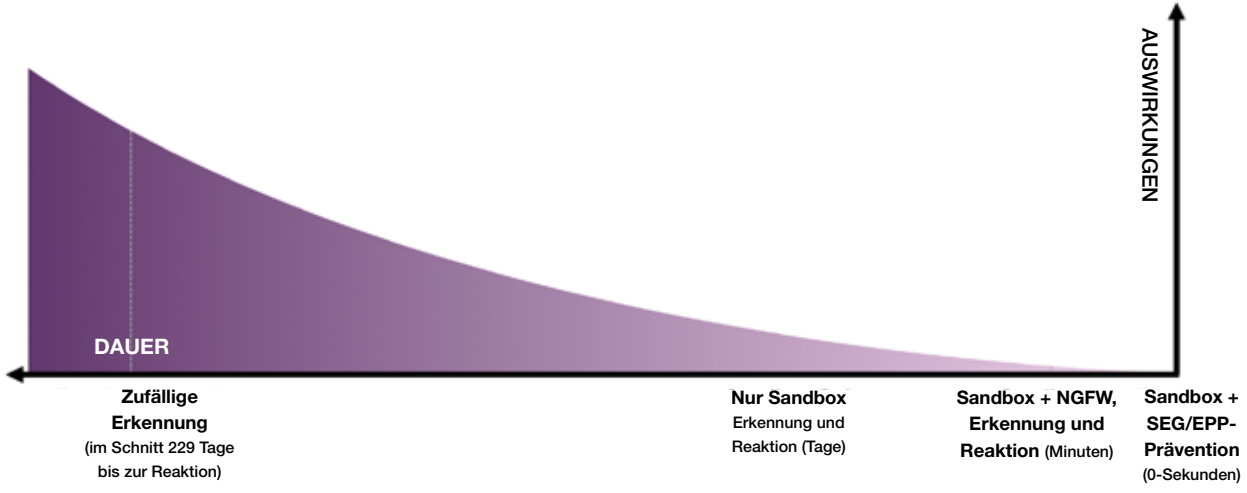
### Kohärente Verteidigung



Nicht in jedem Unternehmen ist die Sicherheitsinfrastruktur auf dem gleichen Stand. Messen Sie hier die höchste Priorität einer nachweislich effektiven Sandbox-Analyse bei, denn das ist für den Schutz der sensibelsten Unternehmensdaten kritisch. Sorgen Sie weiter dafür, dass diese in Ihrem Unternehmen so umfassend eingesetzt wird, wie es Ihr Budget und Ihre Ressourcen zulassen. Die von der Sandbox-Analyse aufgedeckten Risiken sollten Sie mit effektiven Abwehr- und Bereinigungsmaßnahmen flankieren. Ein sicheres E-Mail-Gateway mit einer integrierten Sandbox kann auch die neuesten gezielten E-Mail-Angriffe abwehren. Es ist ein hervorragender erster Schritt für Ihre Gefahrenabwehr und kann als Ergänzung aber auch als Ablösung Ihrer aktuellen E-Mail-Sicherheitslösung dienen.

Überdenken Sie bei Gelegenheit Ihre Netzwerk-, Webanwendungs- und Endgerätesicherheit. Priorisieren Sie die Beurteilung von Produkten, die auf Ihre Sandbox-Investition aufbauen. Damit weiten Sie die Abdeckung aus und kommen einer effektiveren Reaktion sowie einem kohärenteren System näher.

Die von Ihnen gewählte Lösung sollte, auch wenn Ihre Erstinvestition in die Sandbox möglicherweise noch keine Komponenten zur Bedrohungsprävention oder -abwehr enthält, unbedingt erweiterbar sein und besonders Möglichkeiten zur Integration hochwertiger Komponenten bieten. Ist dies nicht der Fall, bleibt Ihrem Unternehmen nur ein Flickenteppich aus Sicherheitsprodukten voller Lücken, der einen immensen Verwaltungs- und Reaktionsaufwand erfordert.



# Anhang: Checkliste für den Kauf von Advanced Threat Protection

Mithilfe der folgenden Checkliste können Sie Ihr aktuelles und geplantes Sicherheitsprofil bewerten, indem Sie einen genauen Blick auf die Abdeckung Ihrer Umgebung, den Mix Ihrer Sicherheitstechnologien sowie die Integrationsmöglichkeiten werfen. Das Endergebnis sind eine Reihe von grundlegenden Anforderungen, mit denen Sie schließlich den richtigen Lösungssatz für Ihr Unternehmen bestimmen können.

## I. UMGEBUNGSABDECKUNG BEURTEILEN

- ☐ Legen Sie fest, welche physischen Standorte Sie abdecken möchten, wie etwa Ein- und Austrittspunkte sowie interne Punkte des Netzwerks, zentrale E-Mail- und Datensysteme, mobile Endgeräte sowie Cloud-Rechenlasten.
- ☐ Entscheiden Sie, welche Protokolle Sie an jedem dieser Punkte untersuchen möchten (z. B. HTTP, SMTP, SMB und mehr, einschließlich verschlüsselter Versionen).
- ☐ Bestimmen Sie die erforderliche Kapazität (z. B. 1 G-, 10 G-, 40 G-Ports und/oder 1 GBit/s, 4 GBit/s, 10 GBit/s oder mehr, sowie die Anzahl von Objekten pro Zeitraum).
- ☐ Lesen und beurteilen Sie die neuesten unabhängigen Vergleichstests zu Sandbox- und verwandten Technologien, um die Ergebnisse einordnen zu können. Nutzen Sie Testeinrichtungen wie NSS Labs, Virus Bulletin, AV Comparatives und ICSA Labs.

Mithilfe dieser Schritte können Sie die benötigte Infrastruktur richtig dimensionieren und erkennen problemlos Loss Leader-Produkte mit beschränkter Funktionalität, die nicht nachhaltig und zu kostenintensiv sind. Darüber hinaus erliegen Sie keinen Marketing-Hypes von Anbietern, die eine mangelnde Effektivität unterschlagen.

## II. DEN MIX DER SICHERHEITSTECHNOLOGIEN FESTLEGEN

- ☐ Lernen Sie, welche Analysemethoden für die Prävention auf Standort- und Protokollbasis eingesetzt werden und stellen Sie sicher, dass Sie die fortschrittlicheren Methoden einsetzen, um möglichst viel zu blockieren (z. B. Signaturen, Heuristik, Reputation, Emulation und Entschlüsselung).
- ☐ Lernen Sie, welche Analysemethoden zur Erkennung komplexer Bedrohungen auf Standort- und Protokollbasis verwendet werden, wie Sandboxing, Verhaltensanalyse und Big Data-Analysen.
- ☐ Identifizieren Sie die Abwehrprozesse und -werkzeuge, die Ihnen als Reaktion auf Zwischenfälle zur Verfügung stehen. Dazu gehören u. a. Ihr Reaktionsteam, externe Services, Forensiktools und die Integration Ihrer Infrastruktur sowie der automatische Austausch zwischen mehreren Produkten.
- ☐ Identifizieren Sie die Methoden, mit denen die Effektivität Ihrer Bedrohungsprävention, -erkennung und -abwehr beurteilt werden (z. B. regelmäßige Penetrations- und Produktionseffektivität-Tests, Proof of Concept (PoC) zum Kaufzeitpunkt und unabhängige Testberichte).

Mithilfe dieser Schritte können Sie Ihre Investition im Hinblick auf alle drei Elemente fokussieren und ausbalancieren, um das bestmögliche Ergebnis zu erzielen. Konzentrieren Sie sich dabei vorrangig auf Möglichkeiten, komplexere Bedrohungen abzuwehren, und erst dann auf die aufwendigere Erkennung und Reaktion. Es wäre allerdings leichtsinnig, sich allein auf die Prävention zu verlassen und die Erkennung zu vernachlässigen – warum, konnten wir in den letzten Jahren sehen. Aber auch Investitionen in Prävention und Erkennung verringern Ihr Sicherheitsrisiko kaum, wenn die Möglichkeit zur Reaktion fehlt.

## III. AUSMASS DES BETRIEBS AUF SYSTEMEBENE

- ☐ Identifizieren Sie die Präventionskomponenten, deren Erkennungselemente sich integrieren lassen (z. B. übergreifende Firewall-Integration für Niederlassungen, Zentrale, Core und Cloud; E-Mail- und Websicherheit, Endgeräteschutz, Web Application Firewall, SIEM, Protokollverwaltung usw.).
- ☐ Definieren Sie, wie Komponenten zur Erkennung komplexer Bedrohungen Daten für die Reaktion bereitstellen (z. B. Dashboards und Berichte, Datenexport über APIs, etablierte Integrationen zur Weitergabe von Daten und automatischen Signaturen).
- ☐ Überprüfen Sie, welche unterstützten oder automatisierten Reaktionen von bereits implementierten Komponenten übernommen werden können (z. B. Geräte isolieren, Quellen blockieren oder Dateien entfernen).
- ☐ Ermitteln Sie, wie viele zentrale Datenknoten, lokale Tauschpunkte für Bedrohungsdaten und/oder globale Forschungslabors erforderlich sind.

Damit bestimmen Sie, wie effizient und effektiv all Ihre Präventions-, Erkennungs-, und Abwehrelemente als Sicherheitslösung zusammenarbeiten – unabhängig davon, wie gut sie für sich allein sind.

# Wirksamkeit der Advanced Threat Protection bewerten

Um zu beurteilen, wie wirkungsvoll die Verteidigungsmaßnahmen Ihres Unternehmens gegenüber den raffinierten Bedrohungen von heute sind, sollten Sie die Anzahl an implementierten Präventionstechnologien und Maßnahmen zur Erkennung und Abwehr komplexer Bedrohungen, die diese möglicherweise überwinden, sowie die Integrationspunkte zwischen all diesen Aspekten überprüfen.

Breit aufgestellte Präventionsmaßnahmen mit nur wenigen fortschrittlichen Erkennungs- oder Abwehrkomponenten machen Ihr Unternehmen äußerst anfällig. Auch bei vielen Einzelkomponenten bleiben Lücken. Prüfen Sie jetzt Ihr Sicherheitsprofil und treffen Sie die richtigen Entscheidungen, um einem integrierten System zur Prävention, Erkennung und Abwehr näher zu kommen.

## PRÄVENTIONSKOMPONENTEN

- ☐ Firewall (Niederlassungen)
- ☐ Firewall (Zentrale)
- ☐ Firewall (Core)
- ☐ Firewall (Cloud)
- ☐ Sicheres E-Mail-Gateway
- ☐ Secure Web Gateway
- ☐ Web Application Firewall
- ☐ Endgeräteschutz
- ☐ Sonstige

## ERKENNUNGSKOMPONENTEN

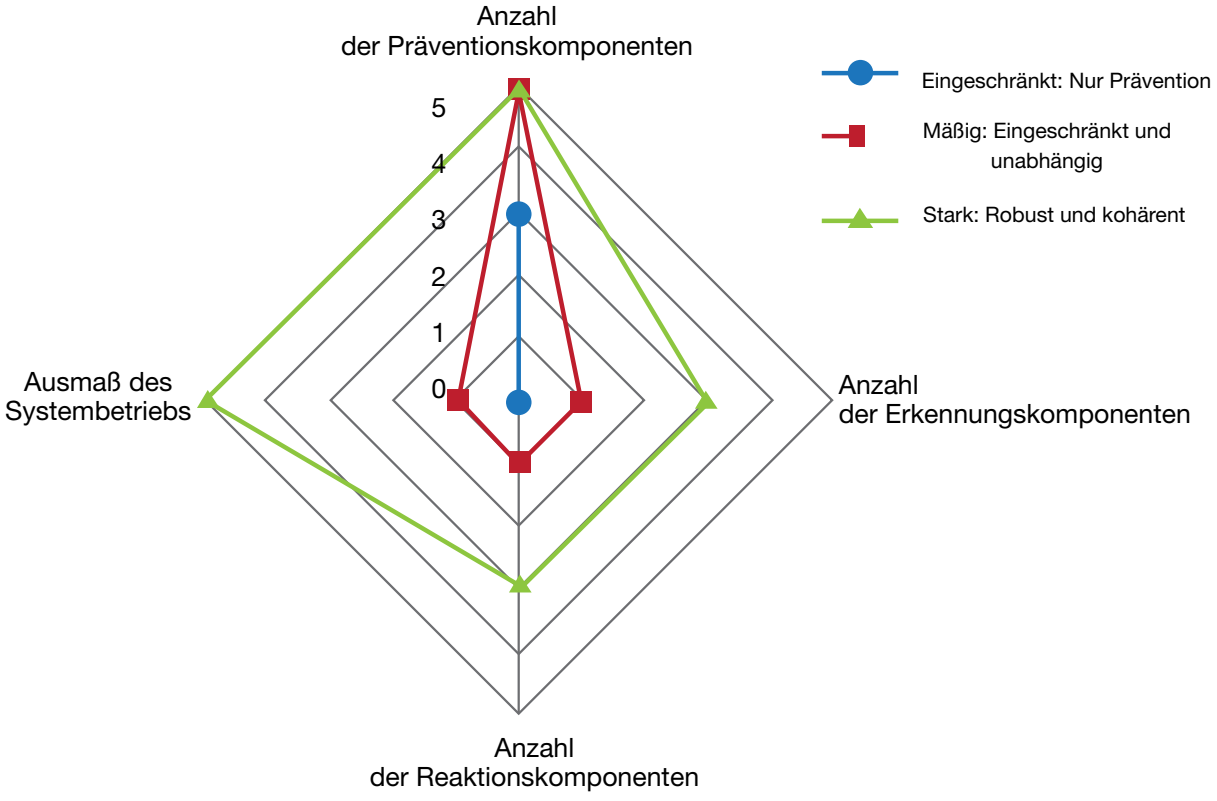
- ☐ Netzwerkverhalten
- ☐ Netzwerkforensik
- ☐ Endgeräteverhalten
- ☐ Sandbox
- ☐ Big Data
- ☐ Sonstige

## REAKTIONSKOMPONENTEN

- ☐ Reaktionsservices
- ☐ Endgeräteforensik
- ☐ Automatisierung

## INTEGRATIONSPUNKTE

- ☐ Firewall und Advanced Threat-Erkennung
- ☐ Sicheres E-Mail-Gateway und Advanced Threat-Erkennung
- ☐ Secure Web Gateway und Advanced Threat-Erkennung
- ☐ Web Application Firewall und Advanced Threat-Erkennung
- ☐ Endgeräteschutz und Advanced Threat-Erkennung




[1] https://www.gartner.com/doc/3043819/best-practices-detecting-mitigating-advanced

[2] http://www.verizonenterprise.com/DBIR/2015/

[3] http://www.fortinet.com/resource_center/analyst_reports/best-defense-next-generation-firewalls.html

[4] http://www.fortinet.com/resource_center/analyst_reports/sandbox-technology-breach-detection-response-strategy.html

Deutschland
Feldbergstraße 35
60323 Frankfurt
Deutschland
Verkaufsabteilung: +49 69 310 192 0

Schweiz
Riedmuehlestr. 8
CH-8305 Dietlikon/Zürich
Schweiz
Verkaufsabteilung: +41 44 833 68 48

Österreich
Wienerbergstrasse 7/D/12th floor
1100 Wien
Österreich
Verkaufsabteilung: +43 1 22787 120



v1.0 02.01.16