KASPERSKY lab

THE POWER OF PROTECTION

GUT GERÜSTET FÜR DIE ZUKUNFT

Sonderbericht zu Risikominderungsstrategien für hoch entwickelte Bedrohungen

kaspersky.com/de/enterprise
#EnterpriseSec

INHALT

HOCH ENTWICKELTE, HARTNÄCKIGE BEDROHUNGEN UND DIE BEDROHUNGSLAGE

Cybersicherheit ist alles andere als ein bloßes Zahlenspiel. Wenn eine einzige Sicherheitsverletzung ausreicht, um Ihrem Unternehmen ernsthaften Schaden zuzufügen, genügt es einfach nicht, nur den Großteil der Angriffe abwehren zu können.

Aus diesem Grund ist es besser, sich auf die gefährlichsten anstatt auf die am häufigsten auftretenden Bedrohungen zu konzentrieren.

Die Malware-Bedrohungslage teilt sich auf in **bekannte** (70 %), **unbekannte** (29 %) und **hoch entwickelte** Bedrohungen (1 %).

Der Schutz vor bekannten Bedrohungen, die ca. 70 % der Malware ausmachen, ist relativ einfach. Solange wir den Schadcode erkennen, können wir ihn auch blockieren. Herkömmliche, signaturbasierte Methoden reichen hierfür in der Regel aus.

Weitere 29 % der Malware gelten als „unbekannte Bedrohungen". Für ihre Bekämpfung sind schon ausgefeiltere Methoden vonnöten. Aber durch die Nutzung von Verfahren, die über herkömmliche Antiviren-Software hinausgehen, z. B. durch heuristische Methoden und dynamisches Whitelisting, können wir auch dieser Bedrohung wirkungsvoll begegnen.

Es bleibt also noch ein weiteres Prozent. Dies sind hoch entwickelte Bedrohungen, die facettenreich, hartnäckig und zielgerichtet sind. Diese Art von Bedrohung, die darauf ausgerichtet ist, ein Netzwerk zu infiltrieren und dort vertrauliche Daten zu sammeln, kann über Jahre hinweg unerkannt bleiben.

Ein APT (Advanced Persistent Threat), die als „Darkhotel" von sich Reden gemacht hat, nutzte über einen Zeitraum von sieben Jahren die WiFi-Netzwerke von Luxushotels, um dort die Daten von Gästen abzuschöpfen. Dieser APT war in vielerlei Hinsicht interessant, da er äußerst zielgerichtet vorging (das Augenmerk war auf leitende Angestellte und CEOs gerichtet) und uns sehr klar die IT-Sicherheitsprobleme vor Augen geführt hat, die entstehen, wenn Endpoints (Unternehmens-Laptops und -Tablets) die Sicherheit von Unternehmensnetzwerken verlassen.

Ein APT, der als „Darkhotel" von sich Reden gemacht hat, nutzte über einen Zeitraum von sieben Jahren die WiFi-Netzwerke von Luxushotels, um dort die Daten von Gästen abzuschöpfen.

Obwohl einige hochkarätige Unternehmen bereits Opfer dieser Art von raffinierten Attacken geworden sind, heißt dies nicht, dass Sie im Licht der Öffentlichkeit stehen müssen, um in das Visier von Cyberkriminellen zu geraten. Unternehmen müssen über eine Strategie verfügen, um die Risiken und Konsequenzen von APTs zu minimieren – egal, ob es sich dabei um Datenverluste, längere Ausfallzeiten oder ernsthafte Rufschädigung handelt. Und da APTs in der Regel unerkannt im Verborgenen operieren, ist Prävention weitaus weniger kostspielig als die Beseitigung der Schäden nach einem erfolgten Angriff (da der Angriff bereits vor einiger Zeit passiert sein und bereits monate- oder sogar jahrelang beträchtlichen Schaden angerichtet haben kann).

Für diese Art von Problem gibt es keine Lösung. Obwohl sie hilfreich sind, reichen die Methoden, die wir zur Bekämpfung von bekannten oder unbekannten Bedrohungen einsetzen, alleine für APTs nicht aus. Eine immer raffinierter und komplexer werdende Bedrohungslage erfordert einen mehrstufigen Sicherheitsansatz, bei dem eine Kombination aus integrierten Technologien eine umfassende Erkennung und Schutz vor bekannter, unbekannter und hoch entwickelter Malware sowie anderen Bedrohungen bietet.

Dieser Bericht soll Sie dabei unterstützen, sich effektiver auf die Abwehr von APTs vorzubereiten.

Die durchschnittlichen Kosten eines Malware-Vorfalls betragen 56.000 US-Dollar für kleine und mittlere Unternehmen und 649.000 US-Dollar für Großunternehmen.[1]

APTs können immense Schäden anrichten. 2014 trug Kaspersky Lab dazu bei, Carbanak das Handwerk zu legen. Bei dieser komplexen Attacke gelang es einer internationalen Verbrecherorganisation, eine Reihe von Finanzinstituten um 1 Milliarde US-Dollar zu erleichtern. Nachdem sie das Netzwerk einer der Banken infiltriert hatte, konnte die Gruppe alles aufzeichnen, was auf den Bildschirmen der Mitarbeiter vor sich ging, und lernte so schnell, wie man unerkannt Geld überweisen konnte.

[1] Die höchsten Kosten für eine Sicherheitsverletzung, Kaspersky Lab.

GROSSUNTERNEHMEN SIND ZUR ZIELSCHEIBE GEWORDEN – FÜNF SCHLÜSSELPUNKTE

Als Großunternehmen sind Sie sich der bestehenden IT-Sicherheitsrisiken natürlich bewusst. Diese Bedrohungen werden jedoch immer zielgerichteter und raffinierter.

1 Der erste Schritt für eine Strategie zu einem angemessenen Umgang mit APTs besteht darin zu begreifen, dass auch Sie zu den potentiellen Zielen gehören. Egal ob es sich um geistiges Eigentum, Kontaktdaten oder Finanzinformationen handelt – auch Ihr Unternehmen besitzt Daten, die für Kriminelle von Interesse sein könnten. Und selbst, wenn es nicht Ihre Daten sind, an denen sie interessiert sind – Cyberkriminelle könnten Ihr Netzwerk missbrauchen, um an Ihre Partner oder Kunden zu gelangen (so wie im Fall von Darkhotel).

2 Zweitens müssen wir ein größeres Bewusstsein für unsere Schwachstellen schaffen. In Unternehmen, in denen eine große Zahl von Mitarbeitern mit unterschiedlichen Geräten, Programmen und Plattformen arbeitet, kann es sich als schwierig erweisen, sämtliche Risiken und potentielle „Angriffsvektoren" im Auge zu behalten, die möglicherweise von Kriminellen genutzt werden könnten. Bei APTs werden Schwachstellen – seien diese menschlicher oder technischer Natur – gezielt ausgenutzt. Je größer und komplexer ein Unternehmen also ist, umso größer auch die Zahl der möglichen Einfallstore.

3 Das Aufkommen von BYOD-Geräten (Bring Your Own Device) und flexible Arbeitsmethoden machen diese Herausforderung nur größer. Neben ihren systemeigenen Anfälligkeiten werden Smartphones und Tablets außerdem häufig für den Zugriff auf ungesicherte Netzwerke genutzt. Hinzu kommt, dass insbesondere bei Betriebssystemen wie dem Apple iOS oft nur schwer festzustellen ist, ob ein Gerät infiziert wurde oder nicht. Mobile Mitarbeiter sind wie bewegliche Ziele: Geräte, die außerhalb des Sicherheitsperimeters Ihres Unternehmens betrieben werden, sind schwieriger zu überwachen und machen eine wirkungsvolle Endpoint-Sicherheit zu einem nicht zu unterschätzenden Bestandteil Ihrer Sicherheitsstrategie.

4 Die große Bandbreite unterschiedlicher Endpoints zusammen mit der großen Vielzahl von Methoden, die Cyberkriminelle für die Infizierung von Netzwerken einsetzen, bedeutet, dass punktuelle Sicherheitsmaßnahmen insgesamt einfach nicht ausreichen. Zuverlässige Strategien zur Minimierung eines möglichen Schadens hingegen bestehen aus einer Kombination aus Sicherheitsinformationen, Sicherheitsrichtlinien und speziellen Sicherheitstechnologien, die nicht einfach nur bekannte Bedrohungen blockieren, sondern aktiv nach neuen Risiken Ausschau halten und gleichzeitig Methoden wie z. B. das Whitelisting nutzen, um die Ausführung noch unbekannter Bedrohungen zu verhindern.

5 Die Risikominderung muss neu auf den Endpoint ausgerichtet werden. Cyberkriminelle nutzen Schwachstellen aus – und der Schwachpunkt von Unternehmen ist oft der Endpoint, weil dort die Sicherheit nicht nur durch das Gerät selbst, sondern auch durch den nachlässigen Umgang von Mitarbeitern oder die ungesicherten Umgebungen, in denen es eingesetzt wird, gefährdet ist. Wenn Ihre Endpoints nicht durch mehrstufige Schutzmechanismen gesichert werden, ist Ihr gesamtes Unternehmen gefährdet.

DARUM IST RISIKOMINDERUNG SO WICHTIG

Großunternehmen müssen deshalb bei der Risikominderung ansetzen, da die Prävention weitaus effektiver und kostengünstiger ist als die Behebungs des entstandenen Schaden nach einem erfolgten Angriff.

Die Cyberkriminellen, die APTs entwickeln, sind hochqualifiziert, entschlossen und verfügen über die entsprechenden Mittel. Wie alle Cyberkriminelle wählen sie – von einigen Ausnahmen abgesehen –, jedoch bevorzugt den Weg des geringsten Widerstands. Und obwohl bei APTs keine hundertprozentige Sicherheitsgarantie möglich ist, können Sie durch bestimmte Maßnahmen den Erfolg dieser Attacken erschweren.

Genau wie APTs, die selbst oft mehrstufige Bedrohungen sind, muss auch eine wirkungsvolle APT-Abwehr mehrstufig sein. Einfache Sicherheitstools reichen hier nicht aus.

Aber wie sieht ein solcher Ansatz nun aus? Das Australian Signals Directorate (ASD) hat eine unserer Ansicht nach umfassende und gründlich recherchierte Liste von Strategien für den Umgang mit hoch entwickelten Bedrohungen zusammengestellt. Wir glauben, dass sich diese Strategien ebenso gut auf Unternehmen anwenden lassen und einen guten Ausgangspunkt darstellen.

Die Strategien lassen sich in vier Kategorien unterteilen:

1 SICHERHEITSRICHTLINIEN UND SCHULUNGEN

Bei der IT-Sicherheit geht es nicht nur um Technologien. Menschliches Fehlverhalten ist für Cyberkriminelle eine große Hilfe. Durch umfassende und regelmäßige Schulungen zum Thema Sicherheit, die angemessene Verhaltensweisen fördern und zur Umsetzung von relevanten und realistischen Richtlinien beitragen, verringern Sie das Risiko, dass Mitarbeiter Cyberbedrohungen in Ihr Unternehmen einschleppen.

2 NETZWERKSICHERHEIT

Die Struktur Ihres Netzwerks kann erheblich dazu beitragen, die potentiellen Auswirkungen einer Infizierung zu verringern. Es gibt eine Reihe unterschiedlicher Netzwerksicherheit, die das Risiko und die Auswirkungen von Bedrohungen reduzieren können. Indem Sie beispielsweise bestimmte Abschnitte des Netzwerks abschotten, reduzieren Sie die Anzahl von Endpoints, die Zugriff auf vertrauliche Daten haben, was zu einer erheblichen Verringerung des Risikos beiträgt.

3 SYSTEMVERWALTUNG

Die Kontrolle und Einschränkung der Benutzerverwaltungsrechte durch Sicherheitsrichtlinien kann zu einer erheblichen Verringerung der Schwachstellen in Ihrem Unternehmen führen. Hinzu kommt, dass die effektive Nutzung der in Ihre Programme integrierten Sicherheitsfunktionen einen erheblichen Unterschied ausmacht. Durch die Deaktivierung nicht benötigter Funktionen können Sie Ihre Software weiterhin optimal nutzen und gleichzeitig potentielle Einfallstore schließen.

Den Java-Code in Browsern zu deaktivieren, ist ein gutes Beispiel dafür, wie Sie Schwachstellen in den von Ihren Mitarbeitern genutzten Ressourcen eliminieren.

4 SPEZIALISIERTE SICHERHEITSLÖSUNGEN

Zusätzlich zu diesen Maßnahmen können bestimmte Funktionen von Spezialsoftware für wertvollen zusätzlichen Schutz sorgen. Die Integration solcher Lösungen muss nicht zwangsläufig mit beträchtlichen Investitionen oder einem hohen Aufwand verbunden sein. Tatsächlich reichen die drei weiter unten genannten spezialisierten Sicherheitslösungen zusammen mit einer Einschränkung der Administratorrechte (siehe die Systemverwaltungsstrategie oben) aus, um 85 % der Sicherheitsbedrohungen abzudecken. Die drei wichtigsten spezialisierten Sicherheitslösungen sind:

- Verwendung von Programmkontrolle, Whitelisting und „Default-Deny"-Modus
- Patchen der am häufigsten angegriffenen Programme
- Patchen der Schwachstellen in Ihren Betriebssystemen

WICHTIGE STRATEGIEN ZUR RISIKOMINIMIERUNG

Es gibt eine Reihe von Strategien, die das Risiko eines Sicherheitsvorfalls mindern. Großunternehmen sollten diese Strategien heute schon umsetzen oder zumindest in Erwägung ziehen.

PROGRAMMKONTROLLE UND WHITELISTING

Whitelisting ist ein leistungsstarkes Tool, das sich als sehr effizient gegen APTs und andere Attacken erwiesen hat. Anstatt die Frage zu stellen, ob ein Programm schädlich sein könnte, fragt das Whitelisting uns, ob wir sicher sind, dass es legitim ist. Hierdurch erhält der Administrator die Kontrolle, unabhängig vom Verhalten des Benutzers. Eine Whitelist besteht aus bekannten und vertrauenswürdigen Programmen – und nur diese Anwendungen können ausgeführt werden. Malware besteht in der Regel aus einer ausführbaren Datei und wird durch diesen Ansatz an der Ausführung gehindert. Dies ist das Gegenmodell zu den herkömmlichen Antiviren-„Blacklists", bei der die Ausführung eines Programms nur dann verhindert wird, wenn dieses in einer Liste von „bekannten Übeltätern" auftaucht.

Um bestmögliche Sicherheit zu erreichen, können Administrator eine „Default-Deny"-Richtlinie umsetzen, die nur die Ausführung von vorher genehmigten Programmen zulässt und dadurch die Gefährdung erheblich reduziert. Obwohl dies ein effektives Mittel darstellt, Malware aus Ihrem Netzwerk fernzuhalten, müssen Sie gleichzeitig sicherstellen, dass hierdurch keine Tools blockiert werden, die Ihre Mitarbeiter für ein effektive Bewältigung ihres Arbeitsalltags benötigen. Durch eine fein abgestufte Programmkontrolle und dynamisches Whitelisting erhalten Sie zusätzliche Steuerungsmöglichkeiten. Sie können die Verwendung von Programmen gesondert nach Softwarekategorie, Geschäftsbereich, Benutzer oder anderen Faktoren blockieren oder kontrollieren.

Bevor Sie das Whitelisting wirkungsvoll einsetzen können, müssen Sie natürlich wissen, welche Programme bereits auf Ihren Endpoints laufen. Eine Bestandsaufnahme ist daher unerlässlich. Schließlich ist es schlecht möglich, etwas zu überwachen, von dem Sie gar nicht wissen, dass es existiert.

KASPERSKY-FUNKTION: PROGRAMMKONTROLLE MIT DYNAMISCHEM WHITELISTING

Die dynamische Whitelisting-Datenbank von Kaspersky Lab mit legitimen Programmen enthält weit über eine Milliarde Einträge und deckt damit 97,5 % aller Software ab, die im Unternehmenssektor zum Einsatz kommt. Dank unserer fortlaufenden Bedrohungsanalyse wird die Datenbank kontinuierlich über unser Cloud-basiertes Kaspersky Security Network aktualisiert.

Unsere Programmkontrolle geht über eine reine „Stopp/Start"-Funktion hinaus. Muss ein Programm blockiert werden, dürfen alle nicht modifizierten Teile des Betriebssystem normal weiter ausgeführt werden. Dies bedeutet, dass Attacken unterbunden werden können, ohne die Benutzeraktivität zu unterbrechen. Kaspersky Lab macht die Umsetzung eines „Default-Deny"-Modus zudem einfacher, da wir eine Testumgebung bereitstellen, in der Sie im Voraus ausprobieren können, ob es bei der Implementierung zu Schwierigkeiten kommen könnte.

KASPERSKY-FUNKTIONEN: VULNERABILITY ASSESSMENT UND PATCH MANAGEMENT

Die von unseren Produkten für Schwachstellen-Scans verwendete Datenbank ist riesig: Kaspersky Endpoint Protection for Business sucht und installiert automatisch Updates von Microsoft und anderen Herstellern. Dies bedeutet, dass alle Ihre Programme und Betriebssysteme automatisch aktualisiert werden, ohne dass hierfür Mitarbeiter abgestellt werden müssen.

„Im 'Default-Deny'-Modus können nur vertrauenswürdige Programme auf Ihrem Computer ausgeführt werden, und nach meiner Erfahrung wird der Großteil der bei APT-Attacken verwendeten Malware durch nicht vertrauenswürdige oder nicht gepatchte Programme eingeschleppt."

Costin Raiu, Leiter des Global Research and Analysis Team bei Kaspersky Lab.

PATCHEN VON SCHWACHSTELLEN IN PROGRAMMEN UND BETRIEBSSYSTEMEN

Programme wie auch Betriebssysteme enthalten Schwachstellen, die von Cyberkriminellen ausgenutzt werden können. Es ist unerlässlich, diese Sicherheitslücken im Auge zu behalten und zu schließen, bevor sie zur Einschleusung von Schadcodes genutzt werden können. Dabei sind es die gängigsten Programme, die häufig Schwachstellen aufweisen, wenn sie nicht gepatcht werden.

Patch-Management-Tools sind ein unerlässlicher Bestandteil einer mehrstufigen IT-Sicherheitsstrategie, da sie die Aktualisierung von Anwendungen auf einer Vielzahl von Endpoints automatisch erledigen. Nur auf diese Weise können Sie sicherstellen, dass potentielle Einfallstore für Angriffe so schnell wie möglich geschlossen werden.

Auch hier sei nochmals erwähnt, dass es keine zu 100% sichere Methode für die Abwehr von APTs gibt.

Aber bei fehlerfreier Umsetzung schützt Sie eine Kombination dieser vier Strategien (Administratorrechte, Programmkontrolle, Patch Management und Betriebssystem-Management) vor 85 % der zielgerichteten Angriffe. Zusammen erschweren sie den Start bzw. die unbemerkte Ausführung von Schadcodes. Der Grund hierfür ist ein gestaffelter Schutz mit mehreren Verteidigungslinien.

2014 machten Schwachstellen in Oracle Java, beliebten Browsern und in Adobe Reader 92 % der Malware-Exploits aus.[2]

[2] Kaspersky Security Bulletin 2014, Kaspersky Lab

WEITERE HOCHEFFEKTIVE STRATEGIEN

Wie eingangs erwähnt, ist Cybersicherheit kein Zahlenspiel. Obwohl Sie sich vor dem Großteil von Angriffen mit den mit den Strategien zur Risikominderung, die wir uns bereits angeschaut haben, schützen können, müssen Sie noch einen Schritt weitergehen.

Weitere Vorgehensweisen, die Sie nutzen können, um für zusätzlichen Schutz zu sorgen:

ABWEHR VON EXPLOITS IN BETRIEBSSYSTEMEN

Obwohl systemeigene Technologien erheblich zur Abwehr von allgemeinen Exploits in Betriebssystemen beitragen können, können Sie mithilfe von Speziallösungen noch mehr erreichen. Und dafür gibt es auch sehr gute Gründe. Denn auch wenn Sie die Patches für Ihre Programme und Betriebssysteme regelmäßig installieren, besteht immer noch die Gefahr, die von Zero-Day-Schwachstellen ausgeht.

KASPERSKY-FUNKTION: AUTOMATISCHER EXPLOIT-SCHUTZ (AEP)

Unser automatischer Exploit-Schutz führt eine Reihe von Sicherheitsprüfungen durch und konzentriert sich dabei besonders auf häufig angegriffene Programme wie Internet Explorer, Microsoft Office und Adobe Reader. Dank einer fortlaufenden Überwachung aller im Arbeitsspeicher befindlichen Prozesse ist AEP in der Lage, die für Exploits charakteristischen Verhaltensmuster zu erkennen, deren Anzahl weitaus geringer ist als die von Exploits selbst. Diese Herangehensweise ermöglicht es dem AEP von Kaspersky Lab, selbst Zero-Day-Exploits zu stoppen.[3]

[3] Gemäß einem von MRG Effitas durchgeführten unabhängigen Test bot AEP in 95 % der Fälle Schutz vor Exploit-basierten Angriffen auf Endpoints, und das selbst als alle anderen Verteidigungsmechanismen deaktiviert waren.

Aus diesem Grund ist es so wichtig, eine Lösung einzusetzen, die bekannte Bedrohungen entdeckt und neutralisiert, aber auch Anomalien und verdächtige Verhaltensmuster erkennt und so Schutz vor unbekannten Gefahren bietet. Auf diese Weise sind Sie sogar vor Angriffen geschützt, die so noch nicht beobachtet wurden.

HOST-BASIERTE ANGRIFFSÜBERWACHUNG

Bei APTs wird im Verborgenen operierende Malware eingesetzt, die bewiesenermaßen monate-, wenn nicht jahrelang unentdeckt bleiben kann. Einen Sicherheitsperimeter einzurichten, reicht also nicht aus – denn was, wenn der Schadcode sich bereits in Ihrem Unternehmen eingenistet hat? Benötigt wird hier ein Verfahren, das Programmaktivitäten erkennt und blockiert, die als „zu risikoreich" eingestuft werden, selbst wenn sie nicht offensichtlich schädlich sind. Hostbasierte Systeme zur Angriffsüberwachung (HIPS) schränken die Aktivitäten von Programmen gemäß deren Vertrauensstufe ein. Ein HIPS macht „Anomalien bei der Ausführung" ausfindig, d. h. wenn Programme unerwartete und potentiell risikobehaftete Funktionen oder Aktivitäten ausführen. Dies geschieht idealerweise unmittelbar nach der Installation eines Programms, also bevor es durch eine heimliche Malware-Attacke infiziert werden kann.

KASPERSKY-FUNKTION: AKTIVITÄTSMONITOR UND APPLICATION PRIVILEGE CONTROL

Zusammen überwachen diese beiden Funktionen die Ereignisse auf Ihren Computersystemen und sorgen so dafür, dass Programme keine böswilligen bzw. schädlichen Aktionen ausführen können. Der Aktivitätsmonitor ist mit seinem zugehörigen Rollback-Subsystem in der Lage, unerwünschte Änderungen zurückzusetzen. Privilege Control verhindert solche Änderungen, wenn sie durch Programme mit einer geringen Vertrauensstufe eingeleitet wurden.

DYNAMISCHE ANALYSE VON E-MAILS- UND WEBINHALTEN

Genau wie ein signaturbasiertes Verfahren nichts gegen Zero-Day-Angriffe ausrichten kann, ist die herkömmliche „statische Analyse", bei der die Inhalte von E-Mails und Webseiten mit einer Datenbank bekannter Malware abgeglichen werden, bei neuartigen Bedrohungen machtlos.

Aus diesem Grund ist eine dynamische Analyse unerlässlich. Sie benötigen eine Lösung, die im Quellcode von Webseiten und E-Mails enthaltene, verdächtige Charakteristiken erkennt – z. B. das Suchen und Modifizieren von Programmdateien – und diese blockiert, bevor sie geöffnet werden.

Bei einer „Zero-Day"-Attacke wird eine unbekannte Schwachstelle in einem Betriebssystem oder in einem Programm ausgenutzt, bevor ein Patch zur Verfügung steht.

KASPERSKY-FUNKTIONEN: WEB-KONTROLLE UND WEB-ANTI-VIRUS

Mit unserer Web-Kontrolltechnologie können Sie festlegen, ob Benutzer auf Webseiten zugreifen dürfen oder nicht, entweder auf individueller Basis oder gemäß einer Klassifizierung des Webseitentyps (z. B. Glücksspiel usw.). Durch die Überwachung des HTTP(S)-Verkehrs wird sichergestellt, dass die auf den Endpoints aufgerufenen Ressourcen mit den Einträgen auf Ihrer Whitelist übereinstimmen.

Gleichzeitig führt die Web-Antiviren-Funktion eine dynamische Analyse der HTTP(S)- und FTP-Protokolle aus, um dort Schadcode zu entdecken und so vor APTs zu schützen, bei denen Downloads oder Drive-by-Infektionen für die Infiltrierung von Systemen eingesetzt werden.

KASPERSKY-FUNKTIONEN: MAIL-ANTI-VIRUS UND SECURITY FOR MAIL SERVER

Durch Verwendung von statischen und dynamischen Analysen und heuristischen Methoden trägt Kaspersky Endpoint for Business dazu bei, per E-Mail übertragene Bedrohungen zu blocken. Indem unsere Technologie emuliert, wie Anhänge möglicherweise agieren könnten, sind wir in der Lage, dateibasierte Exploits in E-Mail-Anhängen zu erkennen.

Kaspersky Security for Mail Server verhindert zudem durch seine DLP-Technologie (Data Loss Prevention), dass wertvolle Informationen Ihr Unternehmen verlassen. Indem Dateien als „nicht für die Weitergabe geeignet" deklariert werden, stellen Sie sicher, dass diese nicht als E-Mail-Anhang versendet werden können.

DER KASPERSKY-ANSATZ: MEHRSTUFIGER SCHUTZ

Die Bedrohungslage ist äußerst komplex und entwickelt sich schnell weiter. Hier bei Kaspersky Lab arbeiten wir zusammen mit großen Unternehmen an einer mehrstufigen Strategie, die Risikominderung und Threat Intelligence Services umfasst.

Als technologieorientiertes Unternehmen Firma haben wir in die Entwicklung von Tools investiert, die Ihnen die Möglichkeit geben, eine ausgewogene Risikominderungsstrategie zu entwickeln. Und da sie alle auf ein und derselben Codebasis beruhen, sind die Tools nahtlos miteinander integriert und ermöglichen so eine umfassende Sicherheitsstrategie, die keine unnötigen Lücken in Ihrer Abwehr zulässt.

Im Zentrum unseres Ansatzes stehen unsere vielfach ausgezeichnete Anti-Malware-Technologie und die Endpoint-Firewall. Zusammen wehren sie die **bekannten** Bedrohungen ab, also 70 %. Mithilfe von **höher entwickelten** Verfahren, z. B. der Verhaltensanalyse, Heuristik, Programmkontrolle, dem dynamischen Whitelisting und der Web-Kontrolle, schützen wir Sie vor **unbekannten** Bedrohungen. Für hoch entwickelte Bedrohungen halten wir eine zusätzliche Schutzschicht in Form von hoch entwickelten Tools bereit, z. B. Kaspersky Automatic Exploit Prevention und den Aktivitätsmonitor.

INFORMATIONEN UND DETEKTION ZUR RASCHEN IDENTIFIZIERUNG VON GERADE STATTFINDENDEN ANGRIFFEN

Obwohl ein sorgfältiger Risikominderungsansatz unerlässlich ist, sollten zu Ihrer APT-Abwehrstrategie auch Maßnahmen gehören, mit denen Sie eine gerade stattfindende Attacke zuverlässig, d. h. ohne zeitaufwändige Fehlalarme, erkennen können. Ihre Strategie sollte darüber hinaus Technologien vorsehen, die eine Attacke rasch abblocken können, um den Schaden für Ihr Unternehmen möglichst gering halten.

Wir empfehlen hierfür Erkennungsfunktionen auf Ebene von Endpoint und Netzwerk, „intelligentes Sandboxing" sowie den Einsatz einer umfassenden Ereignisdatenbank.

Seit einiger Zeit steht die Erkennung auf Netzwerkebene bei einigen IT-Anbietern hoch im Kurs, und viele von ihnen haben entsprechende Appliances entwickelt und vorgestellt. Wir sind jedoch der Auffassung, dass eine Alternativlösung, die auf einer verteilten Sensorarchitektur beruht, hier deutliche Vorteile bringt. Durch die Platzierung von Sensoren an Schlüsselpunkten im Netzwerk – die allesamt einen zentralen Punkt mit Daten versorgen – lässt sich die Detektionsrate erheblich steigern. Außerdem ermöglicht unsere Lösung eine bessere Skalierbarkeit und ist darüber hinaus kostengünstiger, wenn es um die Sicherheit in komplexen Großnetzwerken geht

JENSEITS DER TECHNOLOGIE: THREAT INTELLIGENCE SERVICES

Obwohl sich durch die oben genannten Strategien das Risiko für Unternehmen erheblich reduzieren lässt, kann keine Sicherheitslösung hundertprozentigen Schutz garantieren.

Nach einem Angriff muss Ihr Unternehmen die folgenden Fragestellungen klären:

- Welche Daten wurden genau entwendet? Nur dann können Sie entsprechende Maßnahmen einleiten, um den durch den Datenverlust einstehenden Schaden möglichst gering zu halten.
- Auf welche Weise wurde der Angriff ausgeführt? Nur auf diese Weise können sie spezielle Schwachstellen oder Sicherheitslücken schließen.

Deshalb ist es so wichtig, die bestmögliche forensische Analyse zur Verfügung zu haben. Sie bietet Ihnen raschen Zugang zu der nötigen Sicherheitsexpertise.

Kaspersky Lab bietet eine Reihe unterschiedlicher Intelligence Services an, bei denen Sie zusätzlich zwischen verschiedenen Servicestufen wählen können:

- Malware-Analyse – für Kunden, die über ein eigenes internes Forensik-Team verfügen
- Digitale Forensik-Dienste, einschließlich Malware-Analyse
- Umfassende Vorfallsreaktionsdienste, einschließlich Forensik

WARUM KASPERSKY LAB?

Kaspersky Lab ist eines der Unternehmen, die an vorderster Front gegen APTs kämpfen. Unser GReAT-Team (Global Research and Analysis Team) war an der Entdeckung vieler der weltweit gefährlichsten und aufwändigsten Bedrohungen beteiligt, von Red October bis hin zu der vor kurzem entdeckten „Equation Group", die Cyberspionage-Tools entwickelt.

Wurden Cyberwaffen erst einmal entwickelt, können sie ohne große Probleme durch Modifikationen umgestaltet und auf kommerzielle Angriffsziele ausgerichtet werden. So können selbst Waffen, die unter großem Aufwand von staatlicher Seite entwickelt werden, in die Hände von Verbrecherorganisationen geraten.

Wir nutzen die aus der Analyse von APTs gewonnen Erkenntnisse, um staatliche Stellen zu beraten, wie sie sich gegen Cyberattacken verteidigen können. Aber wir gehen noch einen Schritt weiter. Wir nutzen sämtliche Erkenntnisse aus diesem Tätigkeitsfeld für die Entwicklungen von Lösungen, die auch für Großunternehmen wirkungsvoll und gleichzeitig alltagstauglich sind.

Zu diesem Zweck kombinieren wir unsere Sicherheitsexpertise mit technologischen Innovationen. Unser Anteil an Mitarbeitern, die im Bereich Forschung und Entwicklung arbeiten, ist deutlich höher als bei den meisten anderen Unternehmen.

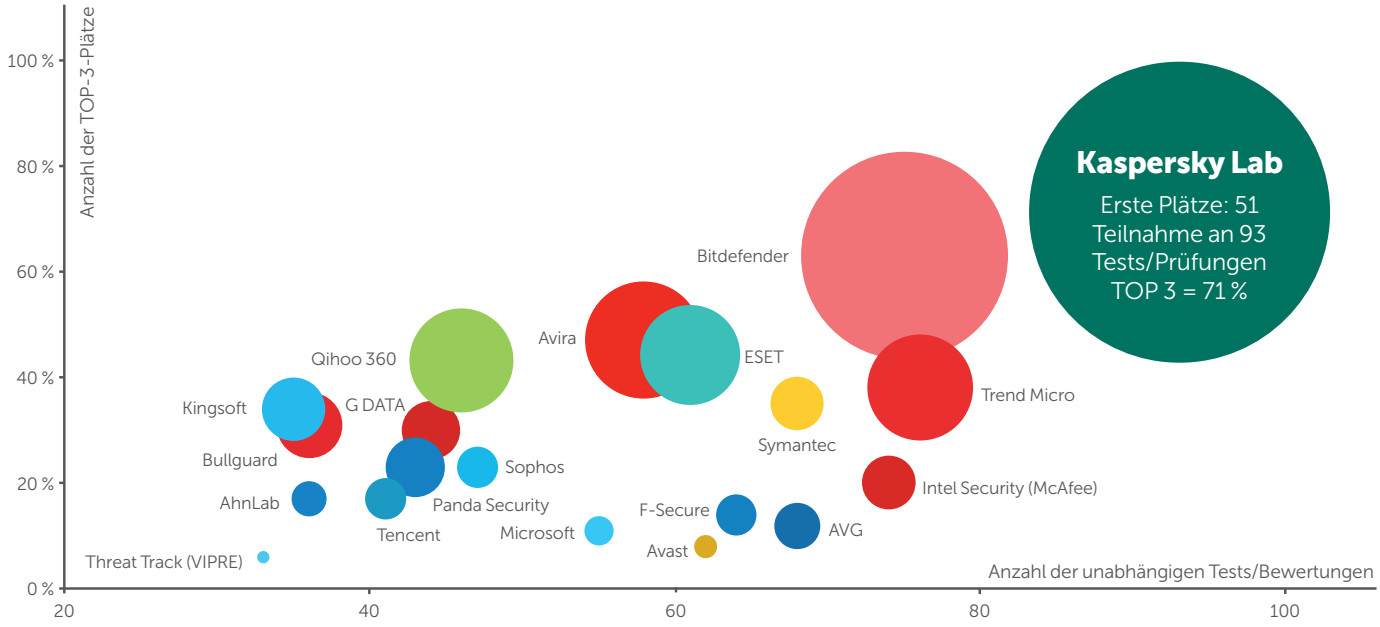
Das Ergebnis ist ein mehrstufiger Sicherheitsansatz, der zum Ausgangspunkt für alle Großunternehmen werden kann, die vorhaben, eine Sicherheitsstrategie zur Abwehr von APTs zu entwickeln.

Unser Vertrauen in unsere eigenen Lösungen hat dazu geführt, dass wir an mehr unabhängigen Tests teilgenommen haben als die meisten anderen Anbieter. Dabei haben wir Malware-Erkennungsraten von über 99 % erzielt. Bei den 93 unabhängigen Tests, an denen wir 2014 teilgenommen haben, sind wir 66 Mal unter den ersten Drei gelandet und 51 Mal als Sieger hervorgegangen[4]. Diese Ergebnisse suchen ihresgleichen. Unsere Technologien werden außerdem von über 130 OEM-Partnern eingesetzt – wahrscheinlich nutzen Sie Kaspersky Lab also bereits.

[4] http://media.kaspersky.com/en/business-security/TOP3_2014.pdf

KASPERSKY LAB BIETET DEN BESTMÖGLICHEN SCHUTZ*

Im Jahr 2014 haben die Produkte von Kaspersky Lab an 93 unabhängigen Tests und Bewertungen teilgenommen. Unsere Produkte waren 51 Mal auf Platz 1 und 66 Mal in den Top 3.



* Anmerkungen:
Laut dem Gesamtergebnis eines im Jahr 2014 durchgeführten unabhängigen Tests von Unternehmens-, Verbraucher- und mobilen Produkten.

Das Gesamtergebnis umfasst Tests, die von den folgenden unabhängigen Testlaboren und Zeitschriften durchgeführt wurden:
AV-Comparatives, AV-Test, Dennis Technology Labs, MRG Effitas, NSS Labs, PC Security Labs, VirusBulletin.
Die Größe des Kreises entspricht der Anzahl erster Plätze.

HEUTE HANDELN, UM DIE ZUKUNFT ZU SICHERN

Eine immer raffinierter und komplexer werdende Bedrohungslage verlangt nach einer mehrstufigen Sicherheitsplattform, die Schutz vor bekannten, unbekannten und hoch entwickelten Bedrohungen bietet.

Besuchen Sie **kaspersky.com/de/enterprise**, wenn Sie mehr über unsere einzigartige Expertise und unsere Security Solutions for Enterprise erfahren möchten.

MEHR INFOS

SPRECHEN SIE MIT UNS

#EnterpriseSec

Auf YouTube ansehen

Werden Sie unser Fan auf Facebook

Folgen Sie uns auf Twitter

Treten Sie uns auf LinkedIn bei

Lesen Sie unseren Blog

Treten Sie uns auf Threatpost bei

Schauen Sie sich uns auf Securelist an

ÜBER KASPERSKY LAB

Kaspersky Lab ist der weltweit größte Privatanbieter von Lösungen für den Schutz von Endpoints. Das Unternehmen rangiert unter den vier Top-Anbietern von Sicherheitslösungen für Endpoint-Benutzer*. In seiner 17-jährigen Firmengeschichte hat Kaspersky Lab stets eine Vorreiterrolle bei der IT-Sicherheit gespielt und bietet großen Unternehmen, KMUs und Einzelverbrauchern wirksame digitale Lösungen für die Datensicherheit. Der Hauptsitz des Unternehmens ist in Großbritannien registriert. Kaspersky Lab ist zurzeit in nahezu 200 Ländern und Regionen weltweit tätig und sorgt für den Schutz von mehr als 400 Millionen Anwendern weltweit. Weitere Informationen erhalten Sie unter: www.kaspersky.de.

* Das Unternehmen belegte im Rahmen des IDC-Rating „Worldwide Endpoint Security Revenue by Vendor 2013" den vierten Rang. Die Aufstellung stammt aus dem IDC-Bericht „Worldwide Endpoint Security 2014-2018 Forecast and 2013 Vendor Shares" (ID #250210, August 2014). In dem Bericht wurden Softwarehersteller auf Grundlage ihrer Erlöse aus dem Verkauf von Sicherheitslösungen für Endpoints im Jahr 2013 eingestuft.