FORTINET

SOLUTION GUIDE

Bei der Bekämpfung moderner, komplexer Angriffe als Unternehmen handlungsfähig bleiben

Den Boden bereiten

Das Konzept moderner, hoch entwickelter Angriffe, auch Advanced Persistent Threats (APT oder komplexe persistente Bedrohungen) genannt, hat sich in den Sprachgebrauch und das kollektive Denken der IT eingebrannt. Beflügelt durch Nachrichten von ständig neuen Datendiebstählen bekommen komplexe, persistente Bedrohungen den Nimbus des Mythischen, werden aber dennoch größtenteils verkannt. Lange ging man davon aus, dass komplexe, persistente Bedrohungen für alle Datendiebstähle verantwortlich seien, auch dann, wenn nachfolgende Untersuchungen ergaben, dass eigentlich menschliches Versagen oder eine mangelhafte Netzwerkarchitektur das Eindringen ins Netzwerk ermöglicht haben.

Durch die Fachpresse und Anbieter-Marketing wurde Anwendern der Eindruck vermittelt, dass eine einzige Technologie die Probleme lösen und ihnen umfassenden Schutz vor komplexen, persistenten Bedrohungen bieten kann. Unabhängig davon, ob ein Angriff tatsächlich auf eine komplexe, persistente Bedrohung zurückzuführen ist oder einfach durch einen entschlossenen Hacker mit einer neuen Malware initiiert wurde – wichtig ist zu verstehen, dass ein Netzwerk keine eindimensionale, homogene Einheit ist. Netzwerke bestehen heute aus vielen Technologien, die über mehrere, räumlich getrennte Standorte verteilt sind. Sowohl Technologien und Standorte als auch der Faktor Mensch stellen bei der Verteidigung der Netzwerke potenzielle Schwachstellen dar. Nur wenn man die Anforderungen und Herausforderungen von beiden Faktoren versteht, kann eine umfassende Abwehrstrategie implementiert werden.

Um zu verstehen, wie das Netzwerk geschützt werden kann und letztlich auch auf welche Daten es Cyberkriminelle abgesehen haben, muss man sich in den Hacker hinein versetzen. Zugriff auf ein bestimmtes Netzwerk zu erlangen, kann das Ergebnis eines

Vorbeugen, Erkennen, Abwehren

ausgeklügelten Angriffs oder aber reiner Zufall sein. Wenn genügend Netzwerke massiv mit Malware bombardiert werden, tut sich irgendwann ein Türchen auf. Um zu verhindern, dass diese Angriffe auf Ihr Netzwerk Erfolg haben, muss die Verteidigung genauso ausgeklügelt sein wie der Angriff selbst. Gartner propagierte zum ersten Mal bereits im August 2013 einen mehrstufigen Ansatz zur Abwehr von komplexen Bedrohungen, der sowohl die Analyse als auch nachgelagerte Untersuchungen einschließt. Das Konzept wurde seither weiterentwickelt, ist aber immer noch die Grundlage umfassender Verteidigungsstrategien.

Ziel aller Angriffe ist es, zunächst das Netzwerk zu infiltrieren. Daher muss der Fokus anfangs darauf gelegt werden, das Eindringen jeglicher Malware in das Netzwerk zu verhindern. Das ist die Aufgabe der Vorbeugung: Versuche vereiteln, die Abwehrmaßnahmen des Netzwerks zu durchbrechen. Die Bandbreite der Technologien und Produkte, die Angriffe abwehren sollen, ist groß und ausgereift. Wobei es für jeden potenziellen Angriffsvektor speziell entwickelte Technologien gibt. Netzwerk- und Web-Firewalls, Sicherheits-Gateways für Nachrichten und Plattformen für den Endgeräteschutz sind nützliche Komponenten einer Abwehrstrategie.

Code-Spektrum

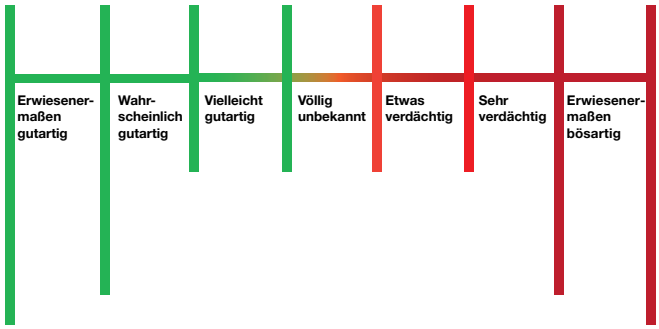

ABBILDUNG 1: DAS BEKANNTE UND DAS UNBEKANNTE

Leider ist bei zu vielen Netzwerken hier bereits Schluss. Alle vorgenannten Technologien sind zur Abwehr bereits bekannter Bedrohungen (oder zumindest sehr verdächtiger Aktivitäten), für die es bereits Gegenmaßnahmen gibt, notwendig. Die Abwehr bekannter Bedrohungen deckt sicherlich einen Großteil der Bedrohungslandschaft wirksam ab. Die sprunghafte Zunahme von Malware sowohl in Bezug auf Menge als auch Varianten, erfordert jedoch, die Abwehrmechanismen durch zusätzliche, spezielle Technologien zu flankieren, die sich um die „unbekannten" Bedrohungen kümmern, die in Netzwerke eindringen. Das ist die Aufgabe der Erkennung.

Die Erkennung beruht auf der Prämisse, dass ungeachtet der Stabilität und des Umfangs seiner Abwehrmaßnahmen, jedes Netzwerk gehackt werden kann. Erkennungstechnologien sind darauf ausgerichtet, zu erkennen, dass jemand eingebrochen ist – idealerweise bevor das Netzwerk Schaden nimmt oder Daten ausgeschleust werden. Einige Erkennungstechnologien sind Erweiterungen der Methoden, die zur Vorbeugung eingesetzt werden, beispielsweise Analysen der Client-Reputation und des Netzwerkverhaltens. Diese vorausschauenden Technologien sollen Grundmuster für das Verhalten von Netzwerknutzern ermitteln und reagieren, sobald das Verhalten von diesem Grundmuster abweicht. Ungewöhnliches Verhalten kann ein erstes Anzeichen dafür sein, dass sich Malware im Netzwerk befindet, zum Beispiel Bot-Malware, die auf Befehle von ihrem Befehls- und Steuerungsserver reagiert. Auch durch die Überwachung der Aktivitäten bekannter Kommunikationskanäle können aktive Bots erkannt werden.

Eine weitere Technologie, das Sandboxing, hat bei der Erkennung bisher unbekannter Bedrohungen stark an Popularität gewonnen. Zwar ist das Sandboxing als Technologie nicht neu (Virusforschungslabors verwenden es bereits seit Jahren zur automatischen Analyse von Samples), seine Anwendung im Rahmen der Sicherung von Kundennetzwerken aber schon. Die Anwendung dieses Konzepts, bei dem verdächtige Software in einer sicheren, kontrollierten Umgebung ausgeführt wird, um festzustellen, ob sie bösartig ist, erweiterte das Erkennungsinstrumentarium von Unternehmen um ein leistungsstarkes neues Tool. Sandboxing ist sogar die in der Advanced Threat Defense Architecture von Gartner postulierte Schlüsseltechnologie zur Analyse von Schadensroutinen.

Im Netzwerk gefundene, potenzielle Malware (unbekannte Malware, da sie die vorbeugenden Technologien umgehen konnte) kann in die Sandbox verschoben werden, um sich dort selbst auszuführen. Stellt sich das Sample in der Sandbox als bösartig heraus, kommt die dritte Stufe ins Spiel, die Abwehr.

Die Abwehr hat zum Ziel, auf die Bedrohung zu reagieren, ihr Ausmaß zu erfassen, sie einzudämmen und zu bereinigen. Umfassende Verwaltung und Analyse der Netzwerksicherheit, Systeme zur Verwaltung von Sicherheitsdaten und -ereignissen (Security Information and Event Management, SIEM), Personal für professionelle Dienstleistungen sowie kontinuierliche Updates der Bedrohungs- und Vorbeugungsdaten gehören alle zu einer umfassenden Abwehrstrategie.

Die Fortinet-Lösung

Die Advanced Threat Protection-Lösung (ATP) von Fortinet enthält als einzige alle drei oben genannten Schlüsselkomponenten – Vorbeugen, Erkennen und Abwehren.

ABBILDUNG 2: DAS FORTINET ADVANCED THREAT PROTECTION-FRAMEWORK

Vergegenwärtigt man sich, dass es mehrere parallele Angriffsvektoren gibt, die Hacker oder Cyberkriminelle nutzen können, um sich Zugang zu einem Netzwerk zu verschaffen, muss der Schwerpunkt einer ATP-Lösung auf dem maximal möglichen Schutz liegen, bei dem alle Lösungselemente zusammenarbeiten. Mit einer Reihe punktuell greifender Einzelprodukte ist das nicht möglich. Nur wenn die verschiedenen Elemente der Lösung zusammenarbeiten, entfalten die drei Aktionsbereiche, Vorbeugen, Erkennen und Abwehren, ihre volle Wirkung. Sie bilden den Kern der Fortinet-Lösung zum Schutz vor komplexen Bedrohungen.

Vorbeugen: Mehr als nur den Netzwerkzugang sichern

Eine erfolgreiche Vorbeugung nutzt mehrere Technologien, die zusammen die Angriffsfläche verkleinern und verhindern, dass Bedrohungen ins Netzwerk eindringen. FortiGate, die Appliance für die Netzwerksicherheit von Fortinet, ist weit mehr als nur die schnellste Firewall der Branche.

FortiGate, mit seinen vielschichtigen Services, angetrieben durch die in allen Geräten integrierte, leistungsstarke ASIC-Technologie, war und bleibt das wichtigste Alleinstellungsmerkmal auf dem Markt. Aufbauend auf der vollumfänglichen Firewall-Funktionalität können zusätzliche, weitergehende Funktionen durch eine einfache und kostengünstige Lizenzierung aktiviert werden. Je nach den Anforderungen des Kunden können Dienste wie Intrusion Prevention (IPS), Applikationskontrolle, URL-Filter, Antivirus (AV) und Endgerätekontrolle aktiviert und für einen effektiven Standortschutz gleichzeitig ausgeführt werden.

Der Netzwerkzugriff über WAN oder Internet ist aber nur ein möglicher Angriffsvektor. Zwei weitere beliebte Angriffspunkte sind öffentlich zugängliche Websites und Mailserver. Diese Systeme benötigen speziellen Schutz. Fortinet begegnet dieser Herausforderung mit FortiWeb, der Firewall für Webanwendungen (WAF oder Web Application Firewall) und dem sicheren E-Mail-Gateway, FortiMail.

FortiWeb ist eine voll ausgestattete WAF. Sie folgt im Hinblick auf die 10 gefährlichsten Sicherheitsrisiken für Webanwendungen den Empfehlungen des Open Web Application Security Project (OWASP).

ABBILDUNG 3: DIE 10 GEFÄHRLICHSTEN SICHERHEITSRISIKEN FÜR WEBANWENDUNGEN LAUT OPEN WEB APPLICATION SECURITY PROJECT

FortiGate verfügt zwar über einen URL-Filter, dennoch arbeiten Firewalls primär auf Netzwerkebene. Daher schützen sie Websites und deren Anwendungen möglicherweise nicht vor Bedrohungen wie SQL-Injection, websiteübergreifendes Scripting (XSS) und Fernausführung von Code. FortiWeb bietet Schutz auf Anwendungsebene und wurde für die speziellen Anforderungen heutiger webbasierter Anwendungen entwickelt.

Die dritte vorbeugende Komponente der ATP-Lösung von Fortinet ist FortiMail. FortiMail ist zwischen dem Netzwerk und dem Mailserver Ihres Unternehmens angesiedelt und scannt E-Mails, bevor sie den Server erreichen und an die Endbenutzer zugestellt werden. Wie auch FortiWeb ergänzt FortiMail FortiGate durch einen hoch entwickelten Spamschutz, seinen eigenen Virenscanner und einen URL-Filter, der bekannte bösartige Dateien und URLs in Phishing-Mails erkennen soll. E-Mails werden mit minimalem Ressourceneinsatz in Echtzeit überprüft und enthaltene Bedrohungen blockiert – und das meist schon auf der Verbindungsebene. Wenn der Zielserver verfügbar ist, müssen E-Mails nicht in eine Warteschlange gestellt werden. So können bis zu 28 Millionen Nachrichten pro Stunde mit nur einer Appliance geschützt werden.

Da diese drei Systeme (FortiGate, FortiWeb und FortiMail) auch als Einzellösungen angeboten werden, verfügt jedes einzelne über alle erforderlichen Funktionen, um Malware vom Eindringen ins Netzwerk abzuhalten. Werden sie zusammen implementiert, können ihre vereinten Funktionen einen verzahnten Schutz über alle potenziellen Angriffsvektoren hinweg erzeugen. Dabei kann eine gemeinsame Funktion als der Mörtel betrachtet werden, der alles zusammenhält: die leistungsstarke Antivirus-Engine, die in allen drei Produkten enthalten ist und bei Fortinet eine Schlüsselkomponente der Vorbeugung bildet.

Der leistungsstarke Virenschutz spielt in der Tat eine wichtige Rolle bei der Abwehr komplexer Bedrohungen. Das liegt daran, dass ein Großteil der verwendeten Malware bereits bekannt ist (oder eine Variante bekannter Malware darstellt). Die Schutzwirkung bleibt also erhalten. Seine Wirksamkeit beruht auch darauf, dass die Zielsysteme regelmäßig aktualisiert werden, um Sicherheitslücken zu schließen, die durch Hacker oder Cyberkriminelle ausgenutzt werden können. Einige dieser Systeme werden jedoch aufgrund der Gleichgültigkeit von Endbenutzern nicht aktualisiert oder können aus einem anderen Grund nicht aktualisiert werden und bieten so eine große und verlockende Angriffsfläche. Der Virenschutz von Fortinet wird kontinuierlich von externen unabhängigen Stellen getestet und stets als eine der effizientesten Antivirus-Lösungen auf dem Markt eingestuft.

Die netzwerkbasierten Antivirus-Funktionen werden durch FortiClient ergänzt, die Desktop-Client-Software von Fortinet, die mit derselben Antivirus-Engine ausgestattet ist. Weil der leistungsstarke Virenschutz von Fortinet das gesamte Netzwerk bis hin zum Desktop umspannt, ist das Netzwerk als Ganzes noch besser geschützt.

Ein weiterer Aspekt, der das Eindringen von Bedrohungen ins Netzwerk verhindert, ist die Benutzerauthentifizierung. Durch zunehmendes E-Mail-Phishing werden auf betrügerische Weise Anmeldedaten für den Zugang zu Netzwerken abgeschöpft. Hier sorgt eine zweistufige Authentifizierung für eine zusätzliche Sicherheitsebene zur Identifizierung von legitimen Benutzern. Zusammen mit FortiGate stellen FortiAuthenticator und FortiToken dem Netzwerk eine leistungsstarke, zweistufige Authentifizierungsfunktion zur Verfügung, entweder als Einzelsystem oder in Kombination mit Ihrer bereits implementierten Authentifizierungslösung. Durch die Kombination Ihrer Identität mit Ihrem Wissen können Lücken in der Identitätsstrategie für den Benutzerzugriff geschlossen werden. Sobald ein Benutzer ordnungsgemäß authentifiziert und identifiziert ist, können die Funktionen für Endgerätesteuerung und Zugangsrichtlinien von FortiGate sicherstellen und kontrollieren, dass jedem Nutzer und jedem Gerät der vorgesehenen Zugang gewährt wird.

Erkennen: Keine bösen Überraschungen mehr

Wenn ein Eindringling, unabhängig von menschlichem Versagen oder mangelhafter Netzwerkarchitektur, Erfolg hat, ist in den meisten Fällen unbekannte Malware im Spiel. Also Malware, die von den Schutzmechanismen nicht gestoppt werden konnte, weil sie nicht als bösartig erkannt wurde. Mögliche Gründe dafür sind: Polymorphie, Komprimierung, Verschlüsselung und Kennwortschutz. Deshalb ist eine zweite Verteidigungsstufe erforderlich, die sich um das Unbekannte oder Unerkannte kümmert. Wie bereits erwähnt müssen zur Erkennung eine Reihe von Technologien und Methoden eingesetzt werden, einschließlich der Sandbox.

Eine Sandbox soll Malware erkennen, die sämtliche, im Netzwerk vorhandenen Schutzmechanismen umgangen hat. Im Idealfall erkennt eine Sandbox Malware innerhalb von Sekunden nach ihrem Eindringen zu 100 %. Im echten Leben und obwohl eine 100%ige Aufdeckungsrate möglich ist, variiert die Zeit, die zur Erkennung des Eindringens benötigt wird, von Anbieter zu Anbieter erheblich.

Ein wichtiges Unterscheidungsmerkmal der Produkte besteht in der Beziehung zwischen Erkennung und Schutz. Wenn die Sandbox nur der Erkennung dient, muss jede durchlaufende Datei getestet werden. Das Problem dieser Vorgehensweise ist, dass sie viel Zeit in Anspruch nimmt – Zeit, die die Malware nutzen kann.

Um die Zeit bis zur Erkennung zu verkürzen, ist es sinnvoll, eine Art Vorfilter in die Sandbox zu integrieren, um die Anzahl der Dateien, die die Sandbox durchlaufen müssen, zu reduzieren. Indem ein Teil des Schutzes in die Erkennung verlagert wird, kann das Netzwerk ein Eindringen schneller erkennen und darauf reagieren.

FortiSandbox ist eine umfassende, mehrstufige Sandbox mit zwei Vorfilter-Funktionen, einem leistungsstarken Virenschutz und direktem Zugriff über die Cloud auf die Bedrohungsdaten von FortiGuard, der Abteilung von Fortinet, die für die Analyse von Bedrohungen, die Bedrohungsdaten und die Forschung zuständig ist. Was durch diese beiden separaten Prozesse nicht eliminiert wurde, wird an eine umfangreiche virtuelle Sandbox weitergeleitet, die auch Code-Emulation einsetzt, um festzustellen, ob es sich um bösartigen Code handelt oder nicht. Stellt sich die Probe als bösartig heraus, leitet FortiSandbox Daten zur Malware an FortiGuard Labs weiter. Dort werden sie analysiert und schließlich in Form von Updates an alle Fortinet-Produkte weltweit verteilt.

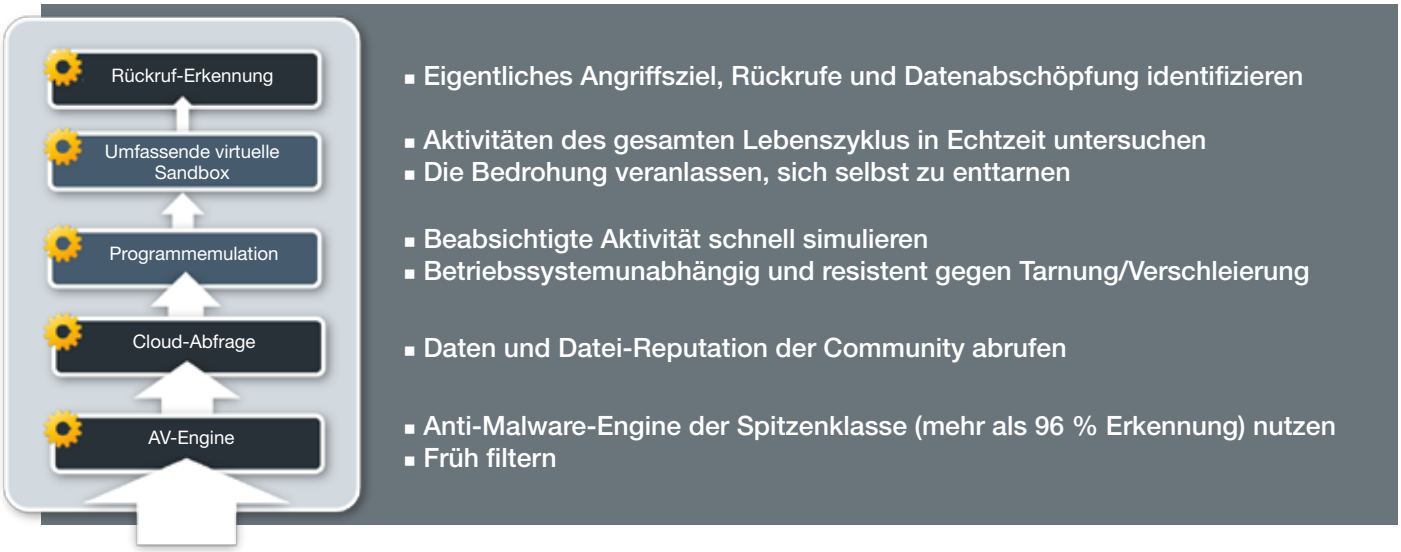

ABBILDUNG 4: METHODEN VON FORTISANDBOX ZUR ERKENNUNG VON BEDROHUNGEN

Da eine Sandbox eine typische Desktop-Umgebung emuliert, müssen sowohl Betriebssysteme, wie Windows XP oder Windows 7, als auch Anwendungen, wie Microsoft Office, Teil der Sandbox sein. Für jede FortiSandbox sind Windows und Office offiziell lizenziert, sodass der Einkauf und die Rechtsabteilung sich um die Lizenzierung keine Gedanken machen müssen.

FortiSandbox unterstützt eine Reihe von Protokollen und Dateitypen, einschließlich Microsoft Office-Dateien, PDFs, komprimierte Dateien (.zip) und sogar Dateien in freigegebenen Netzlaufwerken.

Es ist jedoch kein Einzelgerät innerhalb der ATP-Lösung von Fortinet. Die einzelnen Lösungskomponenten, FortiGate, FortiMail, FortiWeb und FortiSandbox, sind dazu ausgelegt, zusammen eine integrierte Lösung zu offerieren. Wenn beispielsweise die Antivirus-Engine in FortiMail eine verdächtige Datei in einer E-Mail erkennt, hält sie diese zurück und leitet sie zur Analyse an FortiSandbox weiter. Abhängig davon, was FortiSandbox zurückmeldet, löscht FortiMail die E-Mail oder leitet sie an den Mailserver weiter, damit sie zugestellt werden kann. Dieses Zusammenwirken zweier Funktionen ist angesichts bekannter und unbekannter Bedrohungen am effizientesten.

Abwehren: Den Kreis schließen

Unternehmensnetzwerke sind ununterbrochen Angriffen unterschiedlichen Ursprungs aus der ganzen Welt ausgesetzt. Einige Angriffsversuche werden von verschiedenen implementierten Sicherheitstechnologien am Eindringen in das Netzwerk gehindert. Diejenigen, die diese erste Verteidigungslinie durchdringen, geraten ins Visier der Erkennungstechnologien, einschließlich der Sandbox. Sobald FortiSandbox das Eindringen von Malware ins Netzwerk bestätigt, müssen eine Reihe verschiedener Maßnahmen ergriffen werden. Der für die IT-Sicherheit Verantwortliche muss die Bedrohung bewerten und dann den Schaden begrenzen, die infizierten Systeme isolieren und die Sicherheit der Netzwerkressourcen sowie der Unternehmensdaten sicherstellen. Gleichzeitig müssen die für den Angriff verwendete Malware vollständig analysiert und die Sicherheitssysteme des Netzwerks aktualisiert werden, sodass die zuvor unbekannte Bedrohung bekannt wird.

Sicherzustellen, dass die Feedback-Schleife zwischen Erkennen und Vorbeugen geschlossen wird, ist in der ATP-Lösung von Fortinet die Aufgabe der Abwehr. FortiSandbox sendet erkannte Malware zur eingehenden Analyse an die FortiGuard Labs von Fortinet, um sich deren Ressourcen und Fachwissen zunutze zu machen. Die aus dem Zwischenfall gewonnenen Erkenntnisse werden im Anschluss in Form eines Updates sowohl an das Netzwerk als auch an andere Fortinet-Netzwerke zurückgemeldet. FortiGuard Labs und Services sind ein wichtiger Bestandteil der Abwehr aber auch der Lösung insgesamt, denn sie stellen sicher, dass die Lösung über den gesamten Lebenszyklus sicher und effizient bleibt.

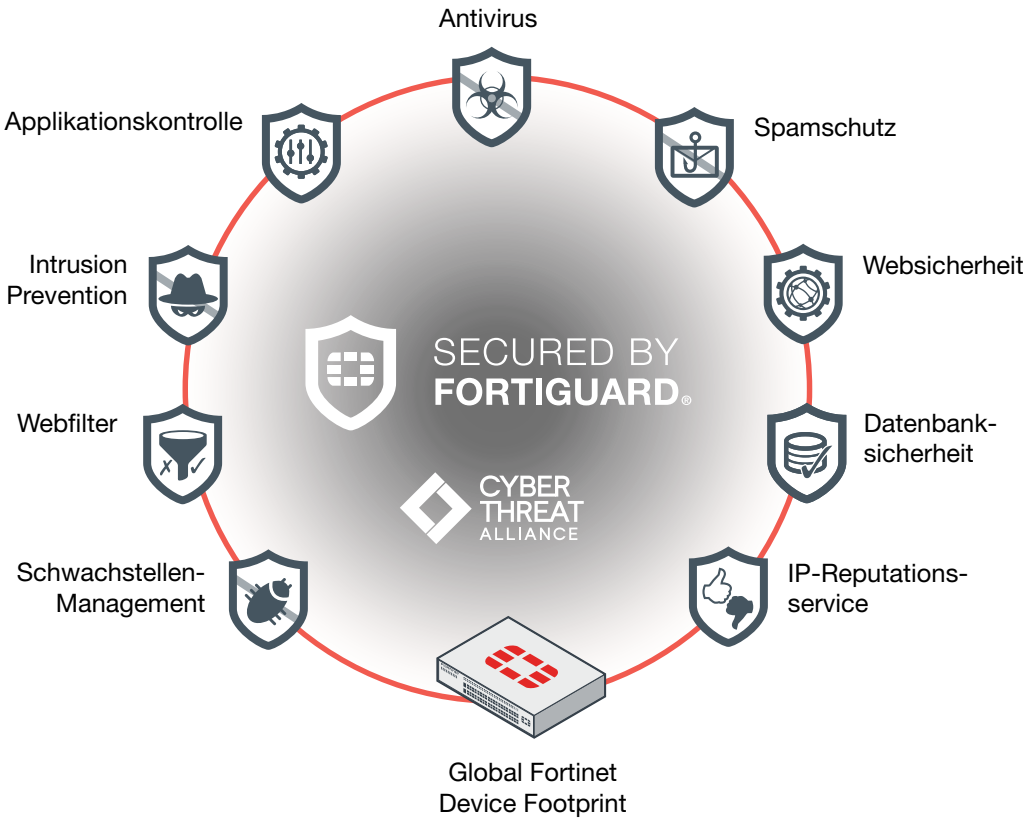

ABBILDUNG 5: DIE DIENSTE ZUR BEDROHUNGSABWEHR VON FORTIGUARD

FortiGuard Labs ist eine globale Organisation, führend bei der Erforschung von Bedrohungen, der Erkennung von Zero-Day-Bedrohungen und der Erfassung von Bedrohungsdaten. Als Mitglied der Cyber Threat Alliance und ähnlicher Initiativen macht Fortinet Daten zu Bedrohungen auch einer größeren Gruppe von Forschern zugänglich. Dadurch vergrößert Fortinet die Reichweite seiner Arbeit und intern im Rahmen dieses Framework gewonnener Bedrohungsdaten über die Grenzen des Unternehmens hinaus.

Schlussfolgerung

Aktuelle und laufende Ereignisse verdeutlichen das Ausmaß der Internetbedrohungen, denen Netzwerke heute tagtäglich ausgesetzt sind. Hacker und Cyberkriminelle sind talentiert, engagiert und entschlossen jede Schwachstelle im Netzwerk einer Organisation auszunutzen. Da sich diese Schwachstellen überall verstecken können, muss die Verteidigungsstrategie für das Netzwerk ebenso hoch entwickelt sein wie die Angriffe selbst.

Die Lösung von Fortinet zum Schutz vor komplexen Bedrohungen (ATP) wurde entwickelt, um den bestmöglichen Schutz gegen die raffinierten, modernen Angriffe zu bieten. Dadurch dass die Aktionen Vorbeugen, Erkennen und Abwehren koordiniert erfolgen, liefert die Fortinet-Lösung kontinuierlichen Schutz, sowohl vor derzeit bekannten als auch vor unbekannten, künftigen Bedrohungen.

Weitere Informationen zu Fortinet und unserem Produkt-Portfolio zum Schutz vor komplexen Bedrohungen erhalten Sie unter www.fortinet.com/solutions/advanced-threat-protection.html.

FORTINET®

www.fortinet.com

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

KONZERNSITZ
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
USA
Tel.: +1 (408) 235 7700
www.fortinet.com/sales

VERTRIEBSBÜRO EMEA
120 rue Albert Caquot
06560, Sophia Antipolis,
Frankreich
Tel.: +33 (0)4 8987 0510

VERTRIEBSBÜRO APAC
300 Beach Road 20-01
The Concourse
Singapur 199555
Tel.: +65 6513 3730

VERTRIEBSBÜRO LATEINAMERIKA
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel.: +52 (55) 5524 8480