SICHERHEITSLÖSUNG DER ENTERPRISE-KLASSE FÜR DIE BUDGETS KLEINER UND MITTLERER UNTERNEHMEN

ÜBERBLICK

Die meisten Unternehmen nutzen E-Mail und Webprotokolle für kommerzielle Zwecke. Daher setzen die meisten Cyberangriffe dort an. Eine effektive Sicherheitslösung erkennt und verhindert bekannte Bedrohungen ebenso wie neue, noch unbekannte Angriffe. Mit den preisgekrönten Technologien von FireEye können Sie mehrstufige und Multi-Vektor-Angriffe aufdecken und abwehren. Wir stellen Ihren Sicherheitsteams effektive Tools zur Verfügung, die den Betrieb vereinfachen und die Produktivität steigern, da sie deutlich weniger Fehlalarme generieren. Diese Lösungen sind erschwinglich und anwenderfreundlich, sodass kleine und mittlere Unternehmen sich einfach schützen und dadurch wieder vermehrt auf ihr Kerngeschäft und das Geschäftswachstum konzentrieren können.

FireEye war Vorreiter in Bezug auf Technologien zur Erkennung unbekannter Angriffe, aber die Lösungen wurden zuerst nur von großen Unternehmen implementiert. Cyberkriminelle machen da jedoch keinen Unterschied: Sie greifen Organisationen aller Größen an. Kleine und mittlere Unternehmen (KMU) mussten feststellen, dass sie nicht immun sind und dass auch sie sich vor komplexen Bedrohungen schützen müssen.

SICHERHEITSRISIKEN

KMU sind zahlreichen Sicherheitsrisiken ausgesetzt. Das liegt zum einen daran, dass ständig neue Bedrohungen aufkommen und zum anderen an der Art und Weise, in der KMU das Sicherheitsmanagement angehen.

Die äußerst dynamische Bedrohungslage führt zu Problemen, weil viele Unternehmen keinen umfassenden Überblick über ihre Sicherheitsmaßnahmen haben. Ältere Technologien zur Erkennung und Abwehr von Bedrohungen am Perimeter basieren in der Regel auf Angriffssignaturen und sind vielen aktuellen Bedrohungen daher prinzipiell nicht gewachsen. Angreifer haben inzwischen Methoden, um die Signatur ihrer Malware zu ändern, sodass jede Signatur in jedem Unternehmen nur einmal auftaucht. Darüber hinaus wird bei vielen Angriffen gar keine Malware eingesetzt.

Die SOC (Security Operations Center) stellen oft eine Herausforderung dar, da KMU meist zu viele Sicherheitswarnungen erhalten und zu wenig Mitarbeiter haben, die sich damit befassen könnten. Viele dieser Warnungen erweisen sich letztendlich als Fehlalarme – allerdings erst, nachdem Analysten viel Zeit mit der Untersuchung verschwendet haben. Aufgrund der großen Anzahl dieser Fehlalarme besteht die Gefahr, dass wichtige Warnmeldungen, die eine unmittelbare Reaktion erfordern, erst zu spät oder gar nicht bearbeitet werden.

Dazu kommen weitere Probleme: KMU müssen Mitarbeiter mit dem erforderlichen Fachwissen einstellen, die die Warnmeldungen analysieren können. In den meisten Unternehmen arbeiten diese Experten in der IT-Abteilung, was zu einem Interessenkonflikt führen kann. KMU, die eine mehrstufige Sicherheitsstrategie verfolgen, müssen unter Umständen diverse Sicherheitstools verwenden. Viele dieser Tools werden nur unzureichend, von externen Sicherheitsanbietern oder gar nicht gepflegt. Im günstigsten Fall entstehen dadurch nur unnötig hohe Kosten, im schlimmsten Fall ist das Unternehmen erheblichen Risiken ausgesetzt. Zwischen all diesen Problemen besteht ein Zusammenhang: KMU müssen die Kosten unter Kontrolle behalten und mit wenig Personal diverse Sicherheitstools verwalten, die zu viele Warnmeldungen ausgeben.

FireEye

DIE LÖSUNG

FireEye kombiniert Network Security Essentials (NXE) und Email Threat Prevention Cloud (ETP), um Unternehmen vor web- und E-Mail-basierten Bedrohungen zu schützen.[1] Diese beiden Vektoren werden bei 90 % aller Cyberangriffe genutzt. Unsere Lösung schont Ihr Sicherheitsbudget: Da Fehlalarme vermieden werden, können Ihre Mitarbeiter schneller und effizienter auf tatsächliche Sicherheitsvorfälle reagieren.

Das Herzstück der Technologien von FireEye bildet die leistungsstarke FireEye MVX-Engine (Multi-Vector Virtual Execution™). Mit ihr lassen sich komplexe, mehrstufige Angriffe und kombinierte Bedrohungen identifizieren, die auf mehrere Angriffsvektoren (z. B. Web und E-Mail) verteilt sind und isoliert betrachtet ungefährlich erscheinen.

Die Aufdeckung der Zusammenhänge zwischen schädlichen URLs und Spear-Phishing-E-Mails ist von entscheidender Bedeutung, um Multi-Vektor-Angriffe im Keim zu ersticken. Die Cloud-MVX-Engine bietet einen Überblick über diese Zusammenhänge, sodass die Unternehmen die darauffolgenden Angriffsphasen – zum Beispiel das Ausschleusen gestohlener Daten über das Internet – automatisch unterbinden können. Außerdem erleichtert dies die Identifizierung und Abwehr von Folgeangriffen, die auf ähnliche Tools, Taktiken und Prozesse (TTPs) setzen.

Der hohe Automatisierungs-, Effizienz- und Wirkungsgrad dieser Lösung erleichtert Unternehmen die Implementierung und die tägliche Administration der Netzwerk- und E-Mail-Sicherheit und verbessert so den Sicherheitsstatus.

Network Security Essentials

Bei Network Security Essentials handelt es sich um eine erschwingliche Plug-&-Play-Netzwerksicherheitslösung, die in weniger als 60 Minuten einsatzbereit ist und die Risiken von Sicherheitsverletzungen minimiert.

Neben der patentierten, signaturunabhängigen Cloud-MVX-Engine umfasst Network Security Essentials eine datengestützte Analysetechnologie zur Identifizierung und Blockierung bekannter und unbekannter Bedrohungen. Die datengestützte Analysetechnologie besteht aus einer Reihe von kontextbezogenen, regelbasierten Engines, die mithilfe von aktuellen Informationen zu Geräten, Angreifern und Opfern schädliche Aktivitäten erkennen und unterbinden. Zudem verfügt die Lösung über ein Intrusion Prevention System (IPS), das herkömmliche Angriffe mithilfe eines konventionellen Signaturabgleichs erkennt und Schutz vor Spyware und Adware bietet. Network Security Essentials identifiziert sowohl bekannte Bedrohungen als auch noch unbekannte Zero-Day-Angriffe mit hoher Präzision und sehr wenigen Fehlalarmen – ein Ergebnis, das konventionelle oder Next-Generation-Firewalls, Standalone-IPS oder Antivirensoftware nicht erreichen können. So haben Sicherheitsteams wieder Zeit, sich auf kritische Aufgaben zu konzentrieren.

Flexible Bereitstellungsoptionen

Für Network Security Essentials ist eine virtuelle oder physische Appliance vor Ort erforderlich, die im Inline- oder im Überwachungsmodus implementiert werden kann. Network Smart Node ist eine On-Premise-Appliance, die an verschiedenen Standorten eingesetzt werden kann – vom primären Netzwerkperimeter bis zu Zweigstellen und Remote-Niederlassungen – überall, wo direkter Internetzugang besteht. Das herunterladbare Image der virtuellen Maschine (Abbildung 1) wird in der Regel bevorzugt, da es kostengünstig ist und schnell implementiert werden kann. Network Smart Nodes nutzen die datengestützte Analysetechnologie und signaturabhängige IPS-Erkennung zur Identifizierung und Abwehr verdächtiger Aktivitäten. Sie senden verdächtige Objekte, die weiter untersucht werden sollten, über eine verschlüsselte Verbindung an den Cloud-MVX-Service in der Private Cloud von FireEye. Network Smart Node und der Cloud MVX-Dienst sind auch als integrierte Appliance erhältlich (Abbildung 2). FireEye empfiehlt die Version mit 50 Mbit/s für kleine und die Version mit 100 Mbit/s für mittelgroße Unternehmen.

E-Mail-Sicherheit: Email Threat Protection Cloud

E-Mails sind das Einfallstor für viele groß angelegte Angriffe. ETP ist ein cloudbasiertes Software-as-a-Service-Angebot (SaaS), das E-Mails auf Anzeichen von Spear Phishing und gängigen Viren oder Spam untersucht. Für die proaktive Abwehr komplexer E-Mail-Angriffe nutzt ETP die patentierte Technologie Cloud MVX. Die Lösung bietet zudem Inline-Schutz vor Spam und Viren. ETP kann E-Mail-Posteingänge sowohl vor Ort als auch in der Cloud im Inline- oder Überwachungsmodus schützen.

Bedrohungsdaten

Cloudbasierte FireEye-Bedrohungsdaten ergänzen die Warnmeldungen der FireEye-Produkte. Die Bedrohungsdaten werden alle 60 Minuten aktualisiert und enthalten Informationen zu neuen Malware-Profilen, Exploits, Angreifern und Opfern sowie anderen Erkenntnissen zu Bedrohungen. Sie ergänzen die Cloud-MVX-Engine um cloudgestützte Analysen und Technologien für maschinelles Lernen, mit denen sich komplexe Bedrohungen aufspüren lassen. Dadurch enthalten FireEye-Warnmeldungen oft wichtige Kontextinformationen, zum Beispiel die potenzielle Identität der Hacker, wahrscheinliche Motive sowie Details zur Malware. Diese Angaben erleichtern es Sicherheitsexperten, gezielte Zero-Day-Angriffe und bekannte Malware zu erkennen und abzuwehren.

[1] Verizon 2015 Data Breach Investigations Report

BEISPIELKONFIGURATIONEN

Bei der Zusammenstellung einer Lösung sollten die folgenden Faktoren berücksichtigt werden: die Anzahl der zu überwachenden E-Mail-Posteingänge, das Volumen des Netzwerkverkehrs im System, die Art der Umgebung (virtualisiert oder physisch), die Einbindung der Cloud-Services und das Sicherheitsbewusstsein der Unternehmensleitung. FireEye und seine Partner helfen Ihnen gern, die passende Lösung für Ihre Anforderungen auszuwählen oder zusammenzustellen. Sehen Sie sich dazu auch die folgenden Beispielkonfigurationen an.

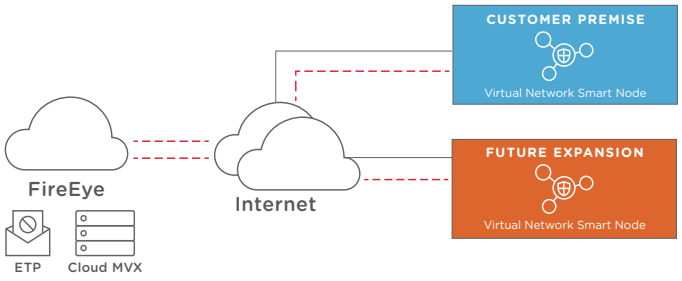

ABBILDUNG 1: ETP CLOUD UND CLOUD-MVX-ENGINE MIT VIRTUELLEN APPLIANCES

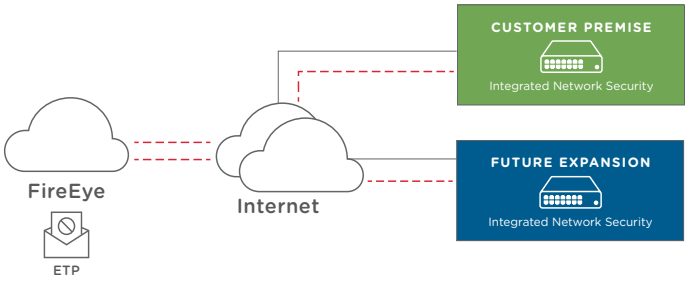

ABBILDUNG 2: ETP CLOUD UND PHYSISCHE INTEGRATED NETWORK SECURITY-APPLIANCES

	KLEIN 1	KLEIN 2	MITTELGROSS 1	MITTELGROSS 2
ART DER BEREITSTELLUNG	VIRTUELL/CLOUD	PHYSISCHE APPLIANCE	VIRTUELL/CLOUD	PHYSISCHE APPLIANCE
Anzahl der Mitarbeiter	200–250	200–250	450–550	450–550
Netzwerkverkehr	50 Mbit/s	50 Mbit/s	100 Mbit/s	100 Mbit/s
Empfohlene Beispiellösung	ETP mit 200 bis 250 Lizenzen Virtuelle NX1500 Cloud MVX	ETP mit 200 bis 250 Lizenzen Integrierte 2500NXE1	ETP mit 450 bis 550 Lizenzen Virtuelle NX2500 Cloud MVX	ETP mit 450 bis 550 Lizenzen Integrierte 2500NXE2

NÄCHSTE SCHRITTE

Kleine und mittlere Unternehmen sind ein bevorzugtes Ziel von Hackern, da ihre Sicherheitsmaßnahmen aufgrund begrenzter Budgets und unterschätzter Gefahren oft Lücken aufweisen. Grundlegende Sicherheitsmaßnahmen sind unbedingt erforderlich, um die daraus resultierenden Risiken zu mindern und das Unternehmenswachstum zu fördern. Außerdem müssen die Verantwortlichen in diesen Unternehmen den Sicherheitsstatus ihres Unternehmens richtig einschätzen können und Vertrauen in ihre Sicherheitsprogramme, -tools und -prozesse haben.

Mehr Informationen zu FireEye erhalten Sie unter:
www.FireEye.de

Über FireEye, Inc.

FireEye® ist ein führender Anbieter datengestützter Security-as-a-Service-Lösungen. FireEye fungiert als nahtlose und skalierbare Erweiterung der Sicherheitskapazitäten seiner Kunden und bietet über eine einheitliche Plattform die weltweit anerkannten Beratungsdienste von Mandiant®, innovative Sicherheitstechnologien und Bedrohungsdaten an, die denen staatlicher Sicherheitsbehörden in nichts nachstehen. FireEye hat über 5.000 Kunden in mehr als 67 Ländern, darunter mehr als 940 der Forbes-Global-2000-Unternehmen.

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035, USA
+1 408 321 6300/+1 877-FIREEYE (347 3393)/info@FireEye.com

www.FireEye.de