UNVERZICHTBARE CYBERSICHERHEIT FÜR KLEINE UND MITTLERE UNTERNEHMEN

ÜBERBLICK

Zahlreiche Studien belegen, dass kleine und mittlere Unternehmen (KMU) in besonders hohem Maße durch komplexe Cyberangriffe gefährdet sind. Statistiken zufolge sind sie das Ziel von 77 Prozent aller Angriffe. Aufgrund knapper Budgets fällt es vielen KMU schwer, sich umfassend vor komplexen Bedrohungen zu schützen.

Um das unbedingt erforderliche Mindestmaß an Sicherheit zu gewährleisten, benötigen sie eine Strategie zur Erkennung und Abwehr komplexer Bedrohungen sowie einen Notfallplan für unvorhergesehene Sicherheitsvorfälle. Mit den preisgekrönten Technologien von FireEye können sie mehrstufige und auf mehrere Vektoren verteilte Angriffe aufdecken und abwehren. Gleichzeitig erhalten Sicherheitsteams relevante Bedrohungsdaten, damit sie IT-Notfallpläne selbst oder mithilfe eines Partners umsetzen können. Zusätzlich zu diesen proaktiven Technologien bieten FireEye und seine Partner Incident-Response-Services an.

Diese effektiven Lösungen sind erschwinglich und anwenderfreundlich, sodass kleine und mittlere Unternehmen sich einfach schützen und weiter auf ihr Kerngeschäft und das Geschäftswachstum konzentrieren können.

DIE HERAUSFORDERUNG

Regierungen und Großkonzerne sind sich der Gefahr durch komplexe Cyberbedrohungen seit längerer Zeit bewusst. Meist sind dort bereits Sicherheitskonzepte und Technologien im Einsatz, die die Risiken von Datenlecks minimieren. Diese Unternehmen und Institutionen sind häufig mit großzügigen Sicherheitsbudgets ausgestattet und aufgrund gesetzlicher oder regulatorischer Auflagen zur Einhaltung hoher Sicherheitsstandards verpflichtet. Kleinen und mittleren Unternehmen mangelt es an den Mitteln dieser Top-Player – dennoch sind sie ähnlichen Risiken ausgesetzt.

Die Medien berichten zwar hauptsächlich über Hackerangriffe auf Großkonzerne, doch das spiegelt nur einen Teil der Realität wider - auch KMU geraten zunehmend ins Visier von Cyberkriminellen.[1] Warum? Sie speichern mehr Daten (Kreditkartennummern, personenbezogene Daten, Patientendaten, geistiges Eigentum usw.) als Privatpersonen und schützen diese weniger effektiv als Großunternehmen – die perfekte Kombination für Angreifer.

KMU, die Business Process Outsourcing (BPO) oder Information Technology Enabled Services (ITES) für größere Unternehmen bereitstellen, sind für Datendiebe besonders interessant. Diese Kriminellen nutzen das Vertrauensverhältnis zwischen Serviceanbieter und Servicenehmer aus, indem sie in die weniger gut gesicherte Infrastruktur des kleineren Unternehmens eindringen und sich von dort aus Zugang zur lukrativeren Umgebung des größeren Unternehmens verschaffen. Die meisten Cyberangreifer folgen dem Weg des geringsten Widerstands, um ihre Ziele zu erreichen.

Große Unternehmen setzen in ihrer Lieferkette deshalb vermehrt auf Anbieter, die ein hohes Maß an Cybersicherheit vorweisen können. Folglich müssen kleine und mittlere Unternehmen ihre Fähigkeiten zur Vermeidung und Erkennung von Cyberangriffen ausbauen, um diesen Anforderungen gerecht zu werden und im Wettbewerb zu bestehen.

1 Symantec: „2015 Internet Security Threat Report“. April 2015.
2 https://staysafeonline.org/

FireEye

Spear-Phishing-E-Mails und Ransomware stellen ein zunehmendes Risiko für KMU dar. Oft unterschätzen KMU diese Gefahr, obwohl sie wegen teils unzureichender Sicherheitsstrategien und -technologien ein ideales Ziel für eine Erpressung mittels Ransomware abgeben.

Herkömmliche signaturabhängige Sicherheitstechnologien können diese Bedrohungen nicht erkennen, weil ihre Entwickler bewusst polymorphe Strukturen nutzen, um jeder Instanz eine neue, noch unbekannte Signatur zu geben. Letztlich kommen KMU nicht umhin, sich gegen die Risiken von komplexen Bedrohungen und Ransomware zu wappnen. Das belegt nicht zuletzt folgende Zahl: Schätzungen zufolge stellt die Hälfte der Kleinunternehmen, die einem Cyberangriff zum Opfer fallen, binnen sechs Monaten den Geschäftsbetrieb ein.[2]

DIE LÖSUNG

Um Ihr Unternehmen erfolgreich vor den raffinierten Cyberkriminellen von heute zu schützen, muss eine Sicherheitslösung folgende Kriterien erfüllen:

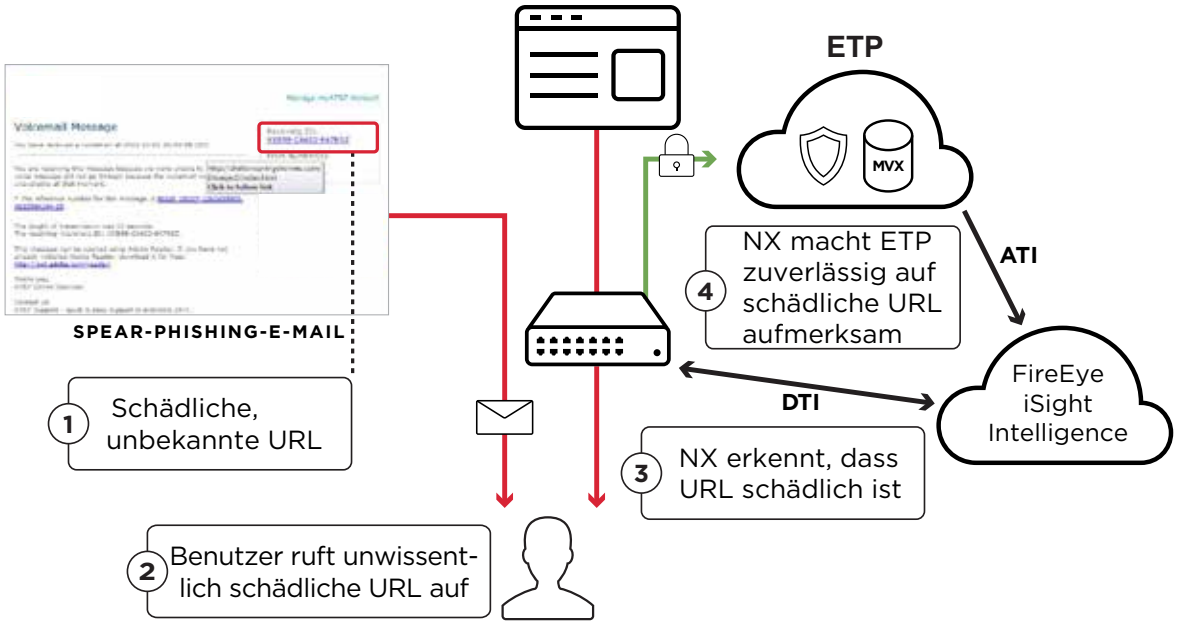
- Überwachung der am häufigsten genutzten Bedrohungsvektoren auf verdächtige Aktivitäten
- Identifizierung neuer Bedrohungen (inklusive Zero-Day-Angriffen) sowie Erkennung bekannter, gängiger Bedrohungen
- Aufdeckung mehrstufiger, auf mehrere Angriffsvektoren verteilter Angriffe
- Nutzung aktueller Bedrohungsdaten ("Threat Intelligence") zur frühzeitigen Erkennung von schwerwiegenden Bedrohungen und beteiligten Hackergruppen

FireEye Essential Security kombiniert FireEye Network Security (NX) Essentials und FireEye Email Threat Prevention Cloud (ETP), um Unternehmen vor Web- und E-Mail-basierten Bedrohungen zu schützen. Dies ist wichtig, da bei 90 Prozent aller Cyberangriffe mindestens einer dieser beiden Angriffsvektoren benutzt wird. Essential Security entlastet Ihr Sicherheitsbudget, da Fehlalarme vermieden werden. So können Ihre Sicherheitsverantwortlichen 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 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 (siehe Abbildung 1). Wenn ein solcher Zusammenhang erkannt wurde, können die darauffolgenden Angriffsphasen – zum Beispiel das Ausschleusen entwendeter Daten über das Internet – automatisch unterbunden werden. Außerdem erleichtert dies die Identifizierung und Abwehr von Folgeangriffen, die auf ähnliche Tools, Taktiken und Prozesse (TTPs) setzen.

ABBILDUNG 1: VEKTORÜBERGREIFENDER SCHUTZ MIT NETWORK SECURITY ESSENTIALS UND EMAIL THREAT PREVENTION



Zudem stellt Essential Security Unternehmen kontextspezifische, sofort verwertbare Bedrohungsdaten zur Verfügung, sodass sie im Angriffsfall schneller reagieren können. Für Firmen mit begrenzten Mitteln bietet die Lösung zahlreiche Vorteile: Sie reduziert Betriebskosten, indem sie Sicherheitstechnologien konsolidiert, besonders gefährliche Angriffe automatisch abblockt und statt einer Warnungsflut zuverlässige Alarmmeldungen generiert.

Der hohe Automatisierungs-, Effizienz- und Wirkungsgrad dieser Lösung erleichtert Unternehmen die Implementierung und die routinemäßige Administration der Netzwerk- und E-Mail-Sicherheit und verbessert so ihre Sicherheitslage.

ANGRIFFSERKENNUNG UND -ABWEHR

Network Security Essentials

Bei Network Security Essentials handelt es sich um eine erschwingliche Plug-&-Play-Lösung für die Netzwerksicherheit, die in weniger als 60 Minuten einsatzbereit ist. Sie erkennt und stoppt bekannte sowie unbekannte Cyberangriffe auf das Netzwerk und senkt somit das Risiko kostspieliger Sicherheitsverletzungen. Mithilfe der MVX-Engine analysiert Network Security Essentials den Webdatenverkehr und erfasst Exploits, ausführbare Malware-Dateien und protokollübergreifende Callbacks. 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 unbekannte Zero-Day-Angriffe mit hoher Präzision und sehr wenigen Fehlalarmen – ein Ergebnis, das konventionelle oder Next-Generation-Firewalls, Standalone-IPS oder Antivirus-Lösungen nicht erreichen.

E-Mail-Sicherheit: Email Threat Protection Cloud (ETP)

Betrügerische E-Mails sind oft die erste Stufe eines groß angelegten Angriffs. FireEye ETP wird als Software as a Service (SaaS) bereitgestellt und überprüft E-Mails auf Anzeichen von Spear Phishing und gängigen Virus- oder Spambedrohungen.

Als Cloud-Angebot ist ETP schnell und einfach einsatzbereit. Die patentierte MVX-Technologie wehrt proaktiv komplexe E-Mail-Angriffe ab. Die Lösung bietet zudem Inline-Schutz vor Spam und Viren. Sie können sowohl E-Mail-Postfächer in Ihrem Unternehmen als auch in der Cloud mit ETP schützen.

Threat Intelligence

Die cloudgestützte FireEye Threat Intelligence stützt sich auf proprietäre Bedrohungsdaten von weltweit aktiven Sensoren, sowie Erkenntnissen aus unseren globalen Incident Response Einsätzen und bereichert Warnmeldungen um wertvolle Informationen. Die Bedrohungsdaten werden alle 60 Minuten aktualisiert und enthalten Informationen zu neuen Malware-Profilen, Zero-Day-Exploits und anderen Bedrohungen.
Sie ergänzen die MVX-Engine um cloudgestützte Analysen und Maschinenlerntechnologien, mit denen sich komplexe Bedrohungen aufspüren lassen.

ABBILDUNG 2A: NETWORK SECURITY ESSENTIALS – INLINE-INSTALLATION

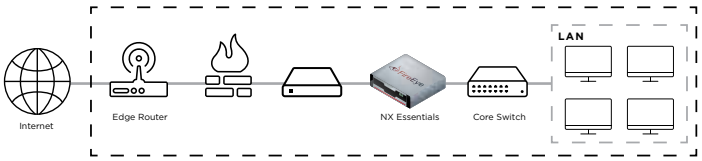
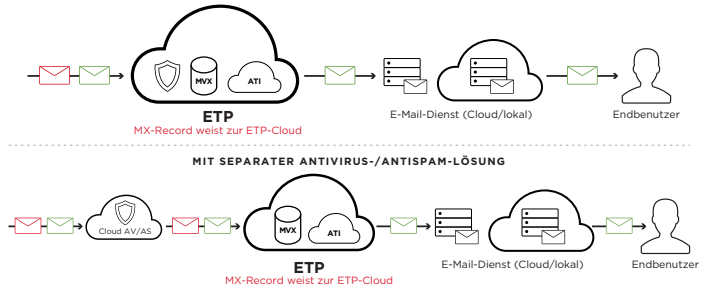


ABBILDUNG 2B: EMAIL THREAT PREVENTION – INLINE-INSTALLATION



Durch den anonymen Austausch von Daten zu Web-, E-Mail- und dateigestützten Bedrohungen bietet FireEye Dynamic Threat Intelligence (DTI) innerhalb seines globalen Cloud-Netzwerks stündliche Sicherheitsupdates. So können Angriffe, die FireEye gegenwärtig in seinem globalen Kundennetzwerk beobachtet, unmittelbar ausfindig gemacht und blockiert werden. DTI ist mit Network Security Essentials verfügbar.

ABBILDUNG 3A: NETWORK SECURITY ESSENTIALS – OUT-OF-BAND-INSTALLATION (SPAN/TAP)

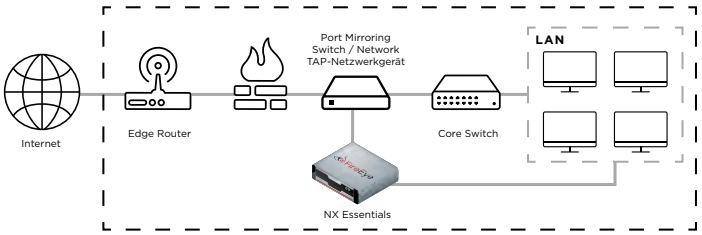
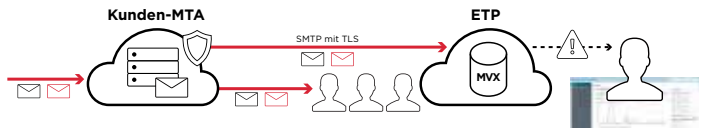


ABBILDUNG 3B: EMAIL THREAT PREVENTION – BCC-MODUS



FireEye Advanced Threat Intelligence (ATI) bietet detaillierte Informationen zu Tätern und Angriffszielen, die von erfahrenen Sicherheitsexperten und Incident-Response-Teams zusammengestellt wurden. Auf diese Weise liefern von FireEye generierte Warnmeldungen wertvolle Kontextinformationen zur mutmaßlichen Identität der Angreifer, ihren Motiven und der Beschaffenheit der benutzten Malware. Die Lösung erkennt effektiv gezielte Zero-Day-Angriffe und bekannte Malware und hilft Sicherheitsteams dabei, Hackern immer einen Schritt voraus zu sein. ATI ist in ETP enthalten.

Installationsoptionen

Essential Security kann inline implementiert werden, um mehr Kontrollmöglichkeiten zu gewährleisten und laufende Angriffe in Echtzeit abzuwehren (siehe Abbildung 2). Einige Unternehmen wünschen sich zu Beginn einen konservativeren Ansatz, weshalb auch eine Installation im Out-of-Band- oder Überwachungsmodus (BCC-Modus für ETP) möglich ist, wie Abbildung 3 zeigt. Bei dieser Option wird der gesamte Datenverkehr auf verdächtige Aktivitäten überwacht. Sie erhalten regelmäßig Ergebnisberichte, die Lösung leitet jedoch keine automatischen Abwehrmaßnahmen ein. Auf Wunsch helfen FireEye und seine Partner Ihnen bei der Auswahl und Implementierung der Option, die Ihren Anforderungen am besten entspricht.

VORBEREITUNG AUF DEN ERNSTFALL

Vergessen Sie nicht, dass Erkennung und Prävention nur einen Teil des Problems beseitigen. Ebenso wichtig ist es, die technischen, rechtlichen, finanziellen und medialen Auswirkungen einer Sicherheitsverletzung im Auge zu behalten. Deshalb rät FireEye dringend zur Erstellung eines Notfallplans, idealerweise in enger Zusammenarbeit mit einem externen Sicherheitspartner. FireEye und seine Partner bieten ein breites Dienstleistungsspektrum zur Ausarbeitung und Validierung von IT-Notfallplänen sowie zur Untersuchung von Sicherheitsvorfällen an.

NÄCHSTE SCHRITTE

Kleine und mittlere Unternehmen sind ein bevorzugtes Ziel von Hackern, da ihre Sicherheitsinfrastrukturen aufgrund begrenzter Budgets und unterschätzter Gefahren oft Lücken aufweisen. KMU müssen sich auf ihr Kerngeschäft und das Unternehmenswachstum konzentrieren, um erfolgreich zu sein. Dennoch empfehlen wir dringend, dass auch diese Unternehmen für ein Mindestmaß an Sicherheit sorgen, um das Risiko eines schwerwiegenden Angriffs zu minimieren. Dazu müssen Sicherheitstechnologien und -prozesse implementiert werden, die vor technisch hochgerüsteten Cyberangreifern Schutz bieten. Auf längere Sicht stärkt dies auch das Vertrauen in die eigene Sicherheitsinfrastruktur.

Um mehr darüber zu erfahren, wie die Sicherheitslösungen von FireEye komplexe Angriffe erkennen und verhindern und wie Sie einen effektiven IT-Notfallplan entwickeln, besuchen Sie www.fireeye.com oder wenden Sie sich an Ihren Ansprechpartner vor Ort.

ÜBER FIREEYE

FireEye schützt weltweit wertvolle Ressourcen vor den raffinierten Cyberangreifern von heute. Unsere Kombination aus Technologie, Know-how und Bedrohungsdaten hilft Kunden dabei, die Auswirkungen von Sicherheitsverletzungen zu minimieren und Schäden schnell zu beseitigen. Die globale Sicherheits-Community von FireEye umfasst 4.400 Kunden in 67 Ländern, darunter mehr als 250 der Fortune-500-Unternehmen.

Weitere Informationen zu FireEye finden Sie unter:
www.FireEye.de

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

www.FireEye.de

© 2016 FireEye, Inc. Alle Rechte vorbehalten. FireEye ist eine eingetragene Marke von FireEye, Inc. Alle anderen Marken, Produkte oder Servicenamen sind Marken oder Dienstleistungsmarken der jeweiligen Eigentümer. SB.ESAA.DE-DE.082016