DATENBLATT

FireEye

FireEye Managed Defense

Schnellere Erkennung und Abwehr von Bedrohungen dank Daten und Erkenntnissen aus erster Hand

HIGHLIGHTS

- **Optimale Nutzung bereits getätigter Investitionen:** MDR-Funktionen (Managed Detection and Response) können in jedes SOC (Security Operation Center) integriert werden.
- **Großes Expertenteam:** Wir bieten Ihnen die Unterstützung Tausender Bedrohungsanalysten, Malware-Experten, Incident-Response-Teams, Datenkuratoren und Forensikexperten.
- **Systematische Spurensuche:** Analysten nutzen proaktiv proprietäre Techniken für die Spurensuche und können dabei auf die Produkte und Erfahrung von FireEye zurückgreifen.
- **Überblick in Echtzeit:** Das anpassbare Portal ist Ihr Anlaufpunkt für die Kommunikation, Berichterstellung und Zusammenarbeit. Außerdem bietet es über „Community Protection"-Dashboards Einblicke in laufende Untersuchungen und Abwehrmaßnahmen für neue Bedrohungen.
- **Marktführende Bedrohungsdaten:** Sicherheitsanalysten haben aktuelle Daten aus Sensoren, Incident-Response-Einsätzen und der Beobachtung von Cyberkriminellen zur Hand und können Bedrohungen in Ihrem System daher schneller identifizieren.
- **Threat Assessment Manager:** Die Sicherheitsexperten sind Ihr Ansprechpartner, wenn Sie zusätzliche Unterstützung benötigen, beispielsweise Analysen von Malware-Varianten, umfassende forensische Analysen oder Incident-Response-Einsätze vor Ort.
- **Schutz rund um die Uhr:** Die SOC in Deutschland, Irland, Japan, Singapur, Australien und den USA (Virginia und Kalifornien) stehen Ihnen rund um die Uhr zur Verfügung.

Angriffsmethoden werden beständig weiterentwickelt, doch die meisten Unternehmen nutzen immer noch reaktive, technologiebasierte Sicherheitslösungen zum Schutz ihrer wertvollsten Ressourcen. Mit Technologie allein können Sie hartnäckige Hacker nicht aufhalten, aber es ist sehr schwer und meist auch zu teuer, qualifizierte Sicherheitsexperten zu finden, einzustellen, zu schulen und zu binden – insbesondere solche, die sich auf das Aufspüren gut getarnter Angriffe spezialisieren.

Eine bessere Option ist die Zusammenarbeit mit einem vertrauenswürdigen Partner, der Ihr Netzwerk rund um die Uhr überwacht, proaktive Analysen durchführt und dabei die neuesten Bedrohungsdaten aus der Praxis berücksichtigt. Genau das bietet FireEye Managed Defense.

Datengestützte Erkennung und Abwehr von Bedrohungen

FireEye Managed Defense ist ein Managed Service zur Bedrohungserkennung und -abwehr (Managed Detection and Response, MDR), der das branchenweit anerkannte Cybersicherheits-Know-how, FireEye-Technologien und einzigartige Kenntnisse zu den Angreifern einsetzt, um die Auswirkungen von Sicherheitsverletzungen zu minimieren.

Managed Defense erhält kontinuierlich die branchenweit umfangreichsten Cyberbedrohungsdaten aus aller Welt. Unsere Experten werten Daten aus unseren Sensoren, der Beobachtung von Cyberkriminellen und ihrer Kampagnen sowie Incident-Response-Einsätzen aus, darunter Untersuchungen der schwerwiegendsten Cyberangriffe weltweit. Diese aktuellen Bedrohungsdaten und Erkenntnisse aus der Praxis informieren die Spurensuche und die Untersuchung der Hackeraktivitäten, sodass unsere Analysten auch die technisch versiertesten Angreifer aufspüren können. Unsere erfahrenen Sicherheitsexperten stellen eine umfassende Einschätzung der Hackeraktivitäten zusammen und geben spezifische Empfehlungen zur Schadensbehebung. Sie stellen die nötigen Kontextinformationen bereit, damit Sie die Bedrohung nachvollziehen, die Risiken einschätzen und angemessene Maßnahmen ergreifen können.

Funktionsweise

FireEye Managed Defense greift auf unseren hauseigenen Technologiestack zurück, um einen unternehmensweiten Überblick in Echtzeit zu gewinnen – auch über industrielle Steuersysteme und Cloud-Infrastrukturen.

Die erfahrenen Bedrohungsanalysten von FireEye erkennen und untersuchen Daten aus unseren Sensoren, Incident-Response-Einsätzen und der Beobachtung von Cyberkriminellen auf unbekannte oder bislang unentdeckte Bedrohungen und gehen ihnen aktiv nach.

Wenn sich Indikatoren für Sicherheitsverletzungen nachweisen lassen, informieren wir Sie unverzüglich. Zudem können Sie die neuesten Erkenntnisse in einem sicheren Portal abrufen, während unsere Analysten den Vorfall weiter untersuchen.

Wir stellen Ihnen einen detaillierten Bericht mit einer Zusammenfassung unserer Erkenntnisse, Kontextinformationen und Empfehlungen für die Schadensbehebung bereit, damit Sie effektive Gegenmaßnahmen ergreifen und die Aktivitäten der Hacker unterbinden können.

Methoden und Ziele der Hacker richtig einordnen
Um die immer komplexeren und gezielteren Cyberangriffe vorauszusehen und darauf zu reagieren, sollten Sie auch die Motivationen, Absichten, charakteristischen Merkmale und Methoden der Angreifer kennen. Dabei können Sie auf unsere Praxiserfahrung zurückgreifen.

Die Managed Defense-Analysten nutzen proprietäre Ermittlungsmethoden, um nach Hinweisen auf unbefugte Zugriffe auf Ihre Infrastruktur zu suchen, gegebenenfalls die Vorgehensweise der Angreifer nachzuvollziehen und den Umfang ihrer Fähigkeiten abzuschätzen.

Die erfahrenen Analysten nutzen ihre branchenführenden Einblicke in die Aktionen von über 16.000 Angreifern, darunter mehr als 30 staatlich gesponserte APT-Gruppen in China, Russland und anderen Ländern.

Diese Einblicke in das Verhalten der Angreifer ermöglichen es unseren Experten, die Gefährlichkeit einer Situation rasch einzuschätzen, die Fähigkeiten der Angreifer zu ermitteln, ihren nächsten Schritt vorauszusehen und einen Plan für angemessene Maßnahmen auszuarbeiten.

Abbildung 1: Auf Bedrohungsdaten gestützte Erkennung

Proaktive Suche nach Eindringlingen

Reaktion auf Angriffskampagnen

Identifizierung und Validierung von Warnmeldungen mit einer hohen Priorität

Proaktive Suche nach Eindringlingen
FireEye Managed Defense nutzt für die Spurensuche proaktive Analysen. Unsere Analysten greifen dabei auf ihre Erfahrungen und Kenntnisse zu den Hackern sowie ihren Taktiken, Techniken und Prozessen (TTP) zurück, um schädliche Aktivitäten aufzudecken. Sie suchen systematisch nach neuen TTP, da Hacker immer neue Methoden entwickeln und nutzen, um sich dauerhaft Zugang zu einmal infiltrierten Umgebungen zu sichern und unentdeckt zu bleiben.

Unsere Analysten haben Techniken zur Spurensuche entwickelt und aktualisieren diese fortlaufend mit den Bedrohungsdaten, die wir bei unseren Managed Defense-Kunden, Beratungseinsätzen von Mandiant, einem Unternehmen von FireEye, und über FireEye iSIGHT Intelligence-Funktionen erfassen.

Reaktion auf Angriffskampagnen
Als Managed Defense-Kunde profitieren Sie von dem Know-how und der Erfahrung, die FireEye beim Schutz von mehr als 6.300 Kunden vor Cyberangriffen gesammelt hat.

Wenn wir Angriffsversuche in Unternehmen erkennen, die Ihrem hinsichtlich Branche, Region oder Technologieprofil ähneln, oder wenn wir Änderungen in den Techniken der Hacker beobachten, beginnen wir umgehend mit der proaktiven Suche nach Hinweisen auf ähnliche Angriffe in Ihrem Netzwerk. Wenn Sie noch nicht angegriffen wurden, wir aber Anzeichen dafür finden, dass Sie zum Ziel einer bestimmten Taktik werden könnten, empfehlen wir Maßnahmen, mit denen Sie diese abwehren können.

Identifizierung und Validierung von Warnmeldungen mit einer hohen Priorität
FireEye Managed Defense-Analysten konzentrieren sich auf die schwerwiegendsten Bedrohungen und ignorieren die zahlreichen irrelevanten Warnmeldungen anderer Produkte. So spart Ihr Team Zeit und kann den Arbeitsaufwand verringern. Ihnen steht das gesamte Know-how unserer Analysten und Incident-Response-Teams zur Verfügung, um schwerwiegende Bedrohungen zu identifizieren. Dazu gehören auch Angriffe, die von herkömmlichen Sicherheitslösungen unter Umständen nicht erkannt wurden.

Vorteile von Managed Defense

Erfahrung
Über 100.000 Stunden IR-Einsätze pro Jahr bei den schwerwiegendsten Sicherheitsvorfällen

Bedrohungsdaten
Zugriff auf zuverlässige Bedrohungsdaten, die denen staatlicher Sicherheitsbehörden in nichts nachstehen und von mehr als 150 Analysten zusammengetragen werden

Experten vor Ort
Sieben SOC auf der ganzen Welt, in denen lokale Technical Engagement Manager rund um die Uhr verfügbar sind

Adaptive Erkennung
Fundierte Kenntnisse der von den Angreifern genutzten TTP zur Aufdeckung der Methoden und Verhaltensweisen der Hacker

Leistungsstarke Abwehr
Proprietärer Technologie-Stack von FireEye-Technologien und -Bedrohungsdaten

- mehr als 50 Milliarden Analysen mithilfe virtueller Maschinen pro Tag
- Bearbeitung von 400.000 Malware-Varianten pro Tag
- 16 Millionen Sensoren weltweit zur Erhebung von Bedrohungsdaten
- umfassende Kontextinformationen zur Ergänzung der Sensordaten
- Aktualisierung der FireEye-Infrastruktur alle 60 Minuten

Abbildung 2: Schnelle Abwehrmaßnahmen dank umfassender Erfahrung

Ermittlung des Umfangs des Angriffs | **Schnelle Reaktion** | **Empfehlungen zur Schadensbehebung**

Ermittlung des Umfangs des Angriffs
Bei der Untersuchung prüfen die Managed Defense-Analysten alle Spuren und Warnmeldungen unter Verwendung sämtlicher FireEye-Bedrohungsdaten. Sie kontrollieren Ihren Netzwerkdatenverkehr oder die Endpunkte, um das Ausmaß der Infiltrierung zu ermitteln, und setzen alle infrage kommenden Vorfälle miteinander in Beziehung, um den zeitlichen Verlauf des Angriffs zu rekonstruieren. Dabei nutzen sie proprietäre Techniken und Bedrohungsdaten, die wir bei über 100.000 Stunden Incident-Response-Einsätzen entwickelt und zusammengetragen haben.

Schnelle Reaktion
Bei schwerwiegenderen Angriffen bitten die Managed Defense-Analysten unter Umständen Experten aus unseren Malware-, Bedrohungsdaten- und Incident-Response-Teams um Unterstützung, die detaillierte Analysen eingestufter Vorfälle liefern und Ihr gesamtes Netzwerk durchsuchen, um das volle Ausmaß der Infiltrierung zu ermitteln.

Empfehlungen zur Schadensbehebung
Nach der Untersuchung empfehlen die Managed Defense-Analysten Schritte zur Schadensbehebung, damit Sie möglichst schnell angemessene Maßnahmen ergreifen können.

Sollte ein groß angelegter Incident-Response-Einsatz notwendig sein, unterstützen die Forensikexperten von FireEye Sie bei der Behebung der Sicherheitsverletzung und der Einschätzung der Auswirkungen, um für eine rasche und präzise Aufklärung des Vorfalls zu sorgen.

Unterstützung und Bereitstellung von Informationen
Managed Defense-Kunden haben Zugriff auf ein sicheres Portal für die Kommunikation, die Zusammenarbeit und den Zugang zu Berichten und Bedrohungsdaten. Ihnen wird ein Threat Assessment Manager (TAM) als Ansprechpartner zugewiesen. TAM sind erfahrene Fachkräfte in den Bereichen Incident-Response-Einsätze und Forensik. Sie können Ihnen strategische Empfehlungen zur Verbesserung des Sicherheitsstatus Ihres Unternehmens geben.

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

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

Über FireEye, Inc.
FireEye spezialisiert sich auf datengestützte Sicherheit. FireEye fungiert als nahtlose und skalierbare Erweiterung der Sicherheitsumgebung 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. Mit diesem Ansatz übernimmt FireEye die Verantwortung für die Vorbereitung von Kundenunternehmen auf die Erkennung und Abwehr von Cyberangriffen. FireEye hat mehr als 6.600 Kunden in 67 Ländern, darunter über 45 Prozent der Forbes-Global-2000-Unternehmen.

FireEye