DATENBLATT

MANDIANT®
A FireEye® Company

Vorfallseinschätzung

Decken Sie aktuelle oder frühere Angriffsaktivitäten in Ihrer Infrastruktur auf.

VORTEILE VON MANDIANT

Das FireEye-Unternehmen Mandiant zählt seit mehr als 14 Jahren zu den Vorreitern in den Bereichen Cybersicherheit und Cyberbedrohungsdaten. Unsere IT-Notfallteams sind bei den gravierendsten Sicherheitsvorfällen weltweit im Einsatz. Nicht zuletzt deshalb sind wir stets umfassend über altbekannte und neue Hackergruppen und deren sich ständig wandelnde Tools, Taktiken und Prozesse informiert.

Vorteile

- Umfassende Durchsuchung der Unternehmensinfrastruktur nach Indizien für aktuelle oder frühere Hackeraktivitäten
- Erstellung eines detaillierten Überblicks über Risiken und Schwachstellen der IT-Systeme
- Identifizierung der Defizite bestehender Sicherheitsmaßnahmen
- Empfehlungen zur Verbesserung der Notfallpläne und Abwehrbereitschaft des Unternehmens
- Flexible Nutzung unternehmensintern bereitgestellter oder Cloud-basierter Technologien

In der gegenwärtigen Lage sind Verletzungen der Cybersicherheit unvermeidlich.

Kevin Mandia
Chief Executive Officer von FireEye

Der Mandiant-Service zur Vorfallseinschätzung basiert auf unserer reichhaltigen Erfahrung mit der Bekämpfung raffinierter Hacker sowie auf branchenführenden Bedrohungsdaten und FireEye-Technologien. Mithilfe der Analysen unserer Experten können Sie:

- aktuelle und frühere Hackereinbrüche in Ihre Unternehmensinfrastruktur aufdecken,
- das Risiko Ihres Unternehmens einschätzen – anhand einer detaillierten Aufstellung der Schwachstellen sowie der nicht ordnungsgemäß eingesetzten, nicht richtlinienkonformen oder falsch konfigurierten Komponenten Ihrer Sicherheitsinfrastruktur,
- Sicherheitsprozesse optimieren, um künftige Angriffe und Bedrohungen effektiver abwehren zu können.

Die proaktive Suche nach Eindringlingen ist alternativlos
In den Medien wird immer wieder über schwerwiegende Datendiebstähle berichtet. Allerdings machen diese Fälle nur einen kleinen Teil der weltweit stattfindenden Hackereinbrüche aus. Deshalb sollten Sie stets darüber im Bild sein, ob Ihre Infrastruktur infiltriert wurde und wie sich das Risiko eines Hackereinbruchs minimieren lässt. So können Sie verhindern, dass Ihr Unternehmen auf unliebsame Weise Schlagzeilen macht.

Unser Ansatz
Wir bauen auf unsere reiche Erfahrung mit der Abwehr von Hackereinbrüchen und setzen auf eine Kombination aus branchenführenden Bedrohungsdaten und flexibel miteinander kombinierbaren FireEye-Technologien, um maßgeschneiderte Analysen zu erstellen, mit denen sich geschäftliche Zielsetzungen schnell und effizient realisieren lassen. Diese Berichte geben nicht nur über aktuelle und frühere Hackeraktivitäten Auskunft, sondern bieten unseren Kunden außerdem:

Mit Kontextinformationen angereicherte Bedrohungsdaten
Betroffene Unternehmen erhalten detaillierte Angaben zu Angreifern und ihren Motiven.

Präzise Risikoanalysen
Es werden unzureichend geschützte und fehlerhaft konfigurierte Komponenten sowie fehlende Patches und veraltete Sicherheitssoftware identifiziert.

Optimierungsempfehlungen:
Unsere Experten schlagen Maßnahmen vor, mit denen Ihre Incident-Response-Prozesse verbessert werden können.

FireEye

Die Berater von Mandiant nutzen FireEye-Produkte, um Endpunkte zu überprüfen, den Datenverkehr im Netzwerk zu überwachen, E-Mails zu analysieren und Logdateien nach Hinweisen auf Hackeraktivitäten zu durchsuchen. Außerdem setzen sie signaturunabhängige Lösungen ein, um bisher unerkannte Angreifer aufzuspüren. Dabei können sich die Kunden ganz nach Bedarf für die Technologien entscheiden, die für ihre Umgebung und ihre Anforderungen am besten geeignet sind.

- Überwachung der Endpunkte: Die Agenten von FireEye Endpoint Security erkennen Malware und Hackeraktivitäten auf Windows-, macOS- und Linux-Endpunkten in Echtzeit und stellen Informationen zu den Taktiken, Techniken und Prozessen (TTPs) der Angreifer bereit. Mandiant unterstützt sowohl die unternehmensinterne als auch die Cloud-basierte Bereitstellung.
- Überwachung des Netzwerks: Die Sensoren von FireEye Network Security werden an strategischen Punkten Ihrer Unternehmensinfrastruktur installiert. Sie identifizieren schädliche Aktivitäten wie beispielsweise die Kommunikation der Malware mit einem Command and Control-Server sowie unbefugten Datenzugriff und Prozesse zur Ausschleusung von Daten.
- Überprüfung von E-Mails: Die unternehmensintern bereitgestellten oder Cloud-basierten FireEye-Lösungen können so konfiguriert werden, dass der eingehende und ausgehende E-Mail-Verkehr passiv überwacht wird. Zusätzlich können die Experten von Mandiant Analysefunktionen zur dynamischen Prüfung von Anhängen nutzen und so versuchte Hackereinbrüche schneller erkennen als mit anderen signaturbasierten Produkten.
- Überprüfung von Logdateien: Die Berater von Mandiant setzen verschiedene Technologien ein, um die Logdateien von Anwendungen und Infrastrukturkomponenten auf Spuren schädlicher Aktivitäten zu untersuchen.

Überwachung der Endpunkte

- Echtzeit-Warnmeldungen bei verdächtigen oder schädlichen Aktivitäten
- Identifizierung von bekannter Malware mithilfe der Antivirus-Engine des FireEye-Agenten
- Unterstützung aller gängigen Betriebssysteme:
  - Windows
  - macOS
  - Linux
- Erkennung von Anomalien, die auf eine Infektion mit raffinierter Malware hindeuten

Überwachung des Netzwerks

- Analyse aller übertragenen Datenpakete – basierend auf einer frei wählbaren Signaturdatenbank
- Automatisierte Erkennung und Entschlüsselung des Datenaustauschs mit Command-and-Control-Servern

Überwachung von E-Mails

- Aufdeckung gezielter Phishing-Angriffe, mit denen sich Hacker nach der erfolgreichen Eindämmung ihrer Aktivitäten erneut Zugang verschaffen möchten
- Signaturunabhängige MVX-Engine (Multi-Vector Virtual Execution™) zum Abgleich von E-Mail-Anhängen und URLs mit einer umfassenden Kreuzmatrix der Betriebssysteme, Anwendungen und Browser
- Unterstützung von Analysen zum Abgleich mit Images der Betriebssysteme Microsoft Windows und macOS
- Erfassung versteckter Bedrohungen in Dateien, einschließlich passwortgeschützter und verschlüsselter Anhänge

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