DATENBLATT

MANDIANT®
A FireEye® Company

# Incident-Response-Services

## Sorgen Sie für eine schnelle, umfassende und effiziente Untersuchung, Eindämmung und Behebung von kritischen Sicherheitsvorfällen

### FALLSTUDIE: MANDIANT N AKTION

Ein international agierender Anbieter von Professional Services mit Zehntausenden Computern weltweit beauftragte Mandiant mit der Untersuchung einer möglichen Sicherheitsverletzung, die wichtige Kundendaten betraf.

**Tag 1** – Mandiant beginnt vier Stunden nach Eingang der Anfrage mit der Implementierung einer cloudbasierten Lösung für den Endpunktschutz auf 18.000 Systemen.

- Die Untersuchung wird noch am selben Tag eingeleitet.
- Innerhalb von vier Stunden nach Untersuchungsbeginn werden Beweise für einen Hackereinbruch gefunden.

**Tag 6** – Der Großteil der Untersuchung ist abgeschlossen. Insgesamt wurden über 18.000 Endpunkte überprüft und umfassende Echtzeitanalysen auf 80 Systemen durchgeführt.

**Tag 7** – Der Angriff wird ohne Beeinträchtigung des Geschäftsbetriebs eingedämmt. Mandiant überwacht das Netzwerk weiterhin, um sicherzustellen, dass der Angreifer nicht erneut eindringt.

**Tag 11** – Der Geschäftsbetrieb des Kundenunternehmens läuft wieder normal.
Die gesamte Untersuchung wurde per Fernzugriff durchgeführt.

Das FireEye-Unternehmen Mandiant zählt seit 2004 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.

Im Rahmen von Tausenden Incident-Response-Einsätzen haben wir eine umfassende Erfahrung mit der Analyse und Abwehr von Cyberbedrohungen mithilfe der branchenführenden Bedrohungsdaten und Lösungen für Netzwerk- und Endpunktschutz von FireEye gesammelt.

Die Erkenntnisse, die unsere Experten bei der Bekämpfung der größten und spektakulärsten Sicherheitsvorfälle gewinnen, versetzen uns in die Lage, die Reaktion auf Sicherheitsvorfälle umfassend zu unterstützen – von technischen Eindämmungsmaßnahmen bis hin zum Krisenmanagement.

Wir helfen unseren Kunden bei der raschen und effizienten Untersuchung sowie der Einleitung von Gegenmaßnahmen, sodass sie sich schnellstmöglich wieder auf das Wesentliche konzentrieren können: ihr Kerngeschäft.

### Überblick

Durch den Einsatz von cloudbasierten und unternehmensintern installierten Lösungen kann die Untersuchung schnellstmöglich eingeleitet werden, während die Vertraulichkeit der Daten des Kundenunternehmens jederzeit sichergestellt ist. Auf diese Weise kann Mandiant innerhalb weniger Stunden mit der Analyse des Datenverkehrs und der Prüfung der Statusinformationen Tausender Endpunkte beginnen. Dabei ziehen unsere Experten detaillierte Bedrohungsdaten und Angaben zu den neuesten Taktiken, Techniken und Prozessen (TTPs) der Angreifer heran, die aus eigenen Untersuchungen aktueller Vorfälle und anderen Informationsquellen stammen.

Wir bei Mandiant wissen, dass eine umfassende Reaktion auf Sicherheitsverletzungen über die rein technischen Aspekte der Untersuchung, Eindämmung und Wiederherstellung hinausgeht. Daher unterstützen wir unsere Kunden auch bei der Kommunikation mit der Unternehmensleitung, der Öffentlichkeitsarbeit und der Einhaltung der in einem solchen Fall geltenden Richtlinien und Gesetze. Ein ganzheitliches Krisenmanagement ist für die Minimierung von Imageschäden und den Umgang mit Haftungsansprüchen unerlässlich.

**Tabelle 1:** Vorfälle, bei denen Madiant Unterstützung leistet

| | |
|---|---|
| **Diebstahl geistigen Eigentums** | Ausschleusung von Betriebsgeheimnissen oder sonstigen sensiblen Daten |
| **Finanzkriminalität** | Diebstahl von Kreditkartendaten, Manipulation des elektronischen Zahlungsverkehrs, Erpressung und Ransomware |
| **Diebstahl personenbezogener Daten** | Ausschleusung von Informationen, anhand derer Personen identifiziert werden können |
| **Diebstahl medizinischer Daten** | Ausschleusung von Patientenakten und anderen vertraulichen Daten |
| **Insider-Bedrohungen** | Unangemessene oder illegale Aktivitäten von Mitarbeitern, Zulieferern oder anderen Insidern |
| **Sabotageangriffe** | Angriffe, die Daten oder Systeme irreparabel schädigen, um das betroffene Unternehmen in eine Notlage zu bringen |

FireEye

## VORTEILE VON MANDIANT

- **Langjährige Erfahrung:** Die Analysten von Mandiant haben ihre Kenntnisse und Fähigkeiten im Rahmen der weltweit größten und komplexesten Vorfallsuntersuchungen perfektioniert.
- **Umfassende Bedrohungsdaten:** Wir nutzen branchenführende Bedrohungsdaten, die wir bei Incident-Response-Einsätzen gesammelt haben, sowie Dynamic Threat Intelligence (DTI), die von FireEye-Produkten und den Quellen von iSIGHT Intelligence stammt.
- **Führende Technologie:** Dank des Einsatzes modernster Cloud- und On-Premises-Technologien kann Mandiant Untersuchungen ohne Verzögerung einleiten. Diese Technologien ermöglichen eine schnelle und umfassende Reaktion auf Sicherheitsvorfälle und unterstützen die Überwachung des Datenverkehrs und das Monitoring von Endpunkten mit den Betriebssystemen Microsoft Windows, Linux und Mac OS X. Unter anderem lassen sich durch automatisierte, auf der MVX-Engine von FireEye Network Security basierende Sandbox-Analysen Malware-Infektionen aufdecken, die signaturabhängige Sicherheitslösungen nicht erkennen können.
- **Krisenmanagement:** Unsere Incident-Response-Teams verfügen über jahrelange Erfahrung mit der Beratung von Kunden bei der vorfallsbezogenen Kommunikation – zur Informierung der Führungskräfte, im Rahmen der Öffentlichkeitsarbeit und zur Einhaltung von Offenlegungsvorschriften.
- **Malware-Analyse:** Branchenführende Expertenteams analysieren die bei der Untersuchung gefundene Malware mit Reverse-Engineering-Verfahren, um sich mit ihrer Funktionsweise vertraut zu machen.

### Unser Ansatz

Mandiant führt bei einer Untersuchung immer eine gründliche Host- und Netzwerkanalyse durch, um sich ein vollständiges Bild von der betroffenen Umgebung zu machen. Unsere Incident-Response-Prozesse sind speziell darauf ausgelegt, Kunden bei der Reaktion auf einen Angriff zu unterstützen, die entstandenen Schäden zu beseitigen, die Einhaltung der geltenden Vorschriften sicherzustellen und Imageschäden zu vermeiden. Im Einzelnen geben die Ermittlungen der Experten von Mandiant üblicherweise Auskunft über:

- Betroffene Anwendungen, Netzwerke, Systeme und Benutzerkonten
- Schadsoftware und ausgenutzte Schwachstellen
- Datenbestände, die von Angreifern gesichtet oder gestohlen wurden

### Unterstützung bei einem Vorfall

1. **Implementierungsphase und Untersuchung erster Spuren:** Zunächst werden die für schnelle und umfassende Incident-Response-Prozesse nötigen Technologien implementiert. Zugleich untersuchen wir erste, vom Kunden gelieferte Indizien, um Gefahrenindikatoren zu definieren, mithilfe derer wir Aktivitäten von Angreifern identifizieren und die Umgebung auf Anzeichen schädlicher Aktivitäten untersuchen können.

2. **Planung des Krisenmanagements:** Unsere Fachleute erarbeiten gemeinsam mit Rechts- und Sicherheitsexperten sowie Führungskräften aus der IT und den Geschäftsbereichen einen Plan für das Krisenmanagement.

3. **Ermittlung des Umfangs des Angriffs:** Wir überwachen die Aktivitäten der Angreifer in Echtzeit und suchen nach forensischen Spuren ihrer vergangenen Aktivitäten, um das Ausmaß des Vorfalls zu ermitteln.

4. **Detaillierte Untersuchung:** Die Mandiant-Experten analysieren die Aktivitäten der Angreifer, um den ursprünglichen Angriffsvektor zu identifizieren, den Verlauf des Angriffs zu rekonstruieren und das Ausmaß der Infiltration zu ermitteln. Dies umfasst unter anderem:
   - Echtzeitanalysen
   - Forensische Analyse
   - Analyse des Netzwerkdatenverkehrs
   - Analyse von Logdateien
   - Malware-Analyse

5. **Schadensanalyse:** Wir ermitteln, welche Systeme, Einrichtungen, Anwendungen und Daten von dem Angriff betroffen sind.

6. **Schadensbehebung:** Unsere Experten entwickeln eine auf die Angreiferaktivitäten und die Anforderungen des Unternehmens zugeschnittene Strategie zur Eindämmung des Vorfalls und für die Schadensbehebung. Diese zielt darauf ab, den Angreifern den Zugang zu verwehren und die Sicherheitsinfrastruktur des Unternehmens zu stärken, um künftige Angriffe zu verhindern oder deren Auswirkungen zu minimieren.

### Abschlussberichte

Mandiant erstellt jeweils einen umfassenden Untersuchungsbericht, eine Kurzfassung für Führungskräfte und einen Bericht zur Schadensbehebung, der auch als Grundlage für Audit-Prozesse geeignet ist.

- **Kurzfassung für Führungskräfte:** Überblicksartige Zusammenfassung, in der der Angriffsverlauf, der Untersuchungsprozess, wichtige Erkenntnisse sowie Eindämmungs- und Schadensbehebungsmaßnahmen dargelegt werden
- **Untersuchungsbericht:** Details zum Verlauf des Angriffs und den Aktivitäten der Angreifer in der IT-Umgebung des Unternehmens. Dieser Bericht enthält eine Liste der betroffenen Computer, Standorte, Benutzerkonten und gestohlenen oder gefährdeten Daten.
- **Bericht über die Schadensbehebung:** Details zu den Eindämmungs- und Schadensbehebungsmaßnahmen sowie strategische Empfehlungen zur Stärkung der Sicherheitsinfrastruktur des Unternehmens.

Sie vermuten, dass Hacker Ihr Unternehmen im Visier haben? Dann senden Sie umgehend eine E-Mail an **investigations@mandiant.com** oder besuchen Sie unsere Website: **https://www.fireeye.com/company/incident-response.html**

**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