DATENBLATT

Beurteilung der Fähigkeit zur Angriffsabwehr

Evaluieren Sie Ihre Fähigkeit zur Erkennung, Abwehr und Eindämmung komplexer Angriffe

Was spricht für FireEye Mandiant?

FireEye Mandiant zählt seit 2004 zu den Vorreitern in den Bereichen Cybersicherheit und Cyberbedrohungsdaten. Unsere IT-Notfallteams sind bei komplexen Sicherheitsvorfällen weltweit im Einsatz und sind daher bestens mit etablierten und neuen Hackern und deren fortwährend aktualisierten Tools, Taktiken und Prozessen (TTP) vertraut.

Überblick

Ganz gleich, ob Sie ein IR-Team aufbauen, bestehende Prozesse optimieren oder in unterstützende Technologien investieren: Mandiant kann Sie bei der Verbesserung Ihrer Sicherheitsstrategie gegen komplexe Bedrohungen und raffinierte Angreifer unterstützen. Bei der Beurteilung der Fähigkeit zur Angriffsabwehr evaluiert FireEye Mandiant die Fähigkeiten eines Unternehmens zur Abwehr von Cyberbedrohungen, typischerweise einschließlich des Security Operations Centers (SOC) und der IR-Lösungen. Die Beurteilung wird unter der Leitung von Mandiant-Beratern durchgeführt, die branchenübliche Best Practices und persönliche Erfahrungen bei der Reaktion auf Angriffe in verschiedenen Regionen und Branchen einbringen. Anschließend erstellen diese Berater einen Bericht mit einem detaillierten Plan und nach Priorität geordneten Empfehlungen für Verbesserungen.

Auch nach erheblichen Investitionen in die Cybersicherheit können viele Sicherheitsteams nicht mit Gewissheit sagen, wie zuverlässig und wirksam sie einen gezielten Angriff erkennen, analysieren und abwehren könnten. Die Berater von Mandiant beurteilen anhand ihrer Erfahrung aus der Reaktion auf verschiedenste Bedrohungen (von Standardmalware über Ransomware und Cyberkriminalität bis hin zu APT-Angriffen im Auftrag feindlicher Regierungen), wie gut Ihr Unternehmen auf die Bedrohungen vorbereitet ist, die mit der größten Wahrscheinlichkeit auf Sie zukommen, und geben Empfehlungen für nützliche, praktikable Verbesserungen.

Unser Ansatz

Die Berater von Mandiant nutzen eine Kombination aus verschiedenen Methoden (Dokumentationsprüfung, Analyse der Protokollierungskonfiguration, Workshops zu bestimmten Themen, Planübungen und Tests mithilfe simulierter Bedrohungen), um die Cyberabwehr-Fähigkeiten Ihres Unternehmens in den folgenden sechs Kernbereichen gründlich zu testen:

- **Governance:** Grundlagen für eine effektive Cyberabwehr, Ausrichtung an den Unternehmenszielen
- **Kommunikation:** Prozesse für die Kommunikation mit internen und externen Stakeholdern vor, bei und nach einem Sicherheitsvorfall
- **Transparenz:** Mitarbeiter, Prozesse und Technologien, die Bedrohungen in der gesamten Infrastruktur des Unternehmens erkennen
- **Bedrohungsdaten:** Informationen über Hacker und ihre Tools, Taktiken und Prozesse (TTPs), die zur Erkennung und Abwehr von Bedrohungen genutzt werden können
- **Reaktion:** Überprüfung, Kategorisierung und Einstufung von Vorfällen; Auswahl und Umsetzung geeigneter Gegenmaßnahmen
- **Kennzahlen:** Messungen und Strategien zur kontinuierlichen Analyse und Verbesserung der Abwehrfähigkeiten

Nach der Beurteilung erstellen die Berater von Mandiant einen Bericht mit einem detaillierten Plan und nach Priorität geordneten Empfehlungen für Verbesserungen.

Mehrstufiges Modell: Unternehmen unterscheiden sich in ihrer Größe, dem Reifegrad ihrer Sicherheitsstrategie und ihrer Zielsetzung. Deshalb wird jede Beurteilung der Fähigkeit zur Angriffsabwehr auf die Anforderungen des jeweiligen Unternehmens zugeschnitten. Die Beurteilung der Kernkompetenzen wird durch verschiedene unterstützende Aktivitäten ergänzt.

Tabelle 1: Beurteilung der Fähigkeit zur Angriffsabwehr: die Stufen

Stufen und Beurteilungskomponenten	STUFE I Bewertung	STUFE II Bewertung Planübung	STUFE III Bewertung Planübung Technische Validierung
Typische Dauer (Wochen)	4	5	6
Review der Dokumentation	X	X	X
Workshops zu den sechs Kernbereichen der Cyberabwehr	X	X	X
Review der Protokollierungskonfiguration	X	X	X
Detaillierter Bericht über die Fähigkeiten zur Angriffsabwehr	X	X	X
Technische Besprechung des Berichts	X	X	X
Briefing der Unternehmensleitung (angepasste PowerPoint-Präsentation)		X	X
Übungen zu verschiedenen Fähigkeiten mit dem Incident-Response-Team		X	X
Bewertung der Fähigkeit zur Angriffsabwehr, Vergleich mit anderen Unternehmen derselben Branche		X	X
Plan zur Verbesserung der Fähigkeit zur Angriffsabwehr		X	X
Branchenspezifische Bedrohungstrends		X	X
Planübungen für Techniker		X	X
Planübungen für Manager			X
Test der Erkennungsvorrichtungen mit simulierten Bedrohungen (mit FireEye Verodin)			X

Zeitlicher Ablauf der Bewertung

In Abhängigkeit von der gewählten Stufe besteht die Bewertung aus vier bis sechs Phasen und dauert in der Regel vier bis sechs Wochen.

Review der Dokumentation (1 Woche)

Die Berater werten Ihre Incident-Response-Pläne und -Playbooks, Pläne für das Krisenmanagement und die Kommunikation im Krisenfall und andere relevante Dokumente aus.

Workshops und Übungen zu verschiedenen Fähigkeiten vor Ort (1 Woche)

In Workshops vor Ort besprechen die Berater alle sechs Kernkomponenten der Cyberabwehr mit Ihren Stakeholdern. Darüber hinaus führen sie mit den Mitgliedern des Incident-Response-Teams Übungen zu den erforderlichen Fähigkeiten durch. (Insgesamt finden bis zu sieben Workshops statt.)

Review der Protokollierungskonfiguration (½ Woche)

Die Berater werten Ausschnitte aus Ihren wichtigsten Logdateien aus, um zu bewerten, ob deren Konfiguration die effektive Erkennung und Analyse sicherheitsrelevanter Vorfälle unterstützt.

Planübungen (½ Woche)

In diskussionsbasierten Planübungen bewerten die Berater, wie gut Ihre Techniker und Manager auf die effektive Reaktion auf einen Vorfall vorbereitet sind. (Es finden bis zu zwei Planübungen statt.)

Test der Erkennungsvorrichtungen mit simulierten Bedrohungen (1 Woche)

Die Berater nutzen simulierte Angriffe auf Ihr Netzwerk, um die Wirksamkeit Ihrer Vorrichtungen zur Angriffserkennung zu testen. Die Simulationen werden selbstverständlich streng kontrolliert.

Berichterstellung und -besprechung (2 Wochen)

Sie erhalten einen Bericht mit nach Priorität geordneten strategischen und taktischen Empfehlungen und einer praxistauglichen Roadmap zur Verbesserung der Fähigkeit Ihres Unternehmens zur Angriffsabwehr.

ABSCHLUSSBERICHT

Nach der Bewertung erstellen und liefern die Berater von Mandiant einen Bericht mit:

- Einer Evaluierung Ihrer aktuellen Sicherheitsinfrastruktur
- Detaillierten Empfehlungen für deren Verbesserung
- Einer Zusammenfassung der Ergebnisse für Techniker
- Einer praxistauglichen Roadmap mit Empfehlungen für Initiativen zur Stärkung des Sicherheitsniveaus (Stufe II und Stufe III)
- Einer Zusammenfassung der Ergebnisse für Manager (Stufe II und Stufe III)

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-dach@FireEye.com

Über FireEye, Inc

FireEye spezialisiert sich auf datengestützte Sicherheit. FireEye erweitert die Sicherheitskapazitäten seiner Kunden nahtlos und skalierbar 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™