CROWDSTRIKE

ENDPOINT RECOVERY SERVICES

Schnelle Wiederherstellung ohne Betriebsunterbrechung nach Advanced Persistent Threats und sonstigen Angriffen

EIN WETTLAUF GEGEN DIE ZEIT

Nach einem Datendiebstahl oder sonstigen Sicherheitsverletzungen kommt es auf eine schnelle Behebung und Wiederherstellung an, damit die Auswirkungen auf Ihr Geschäft so gering wie möglich bleiben. Advanced Persistent Threats, also komplexe, zielgerichtete und hochwirksame Angriffe auf Ihre IT-Netzwerke, können in kürzester Zeit Ihre Endgeräte infizieren, lateral auf sämtliche Systeme übergreifen und die Geschäftsprozesse lahmlegen.

Diese sehr professionell geführten und anhaltenden Cyberangriffe manifestieren sich oft unentdeckt an mehreren Stellen in Ihrem Netzwerk. Von dort infizieren sie über einen längeren Zeitraum Ihre Systeme mit Malware oder greifen sensible Daten ab. Diese minutiös geplanten Angriffe sind darauf ausgelegt, Ihre Organisation zu infiltrieren und bestehende Sicherheitsmaßnahmen unentdeckt zu umgehen. Ein Aspekt ist hierbei besonders wichtig: Wenn keine koordinierten und wirksamen Gegenmaßnahmen zur Entfernung aller Infektionspunkte ergriffen werden, kann der Angreifer die Systeme im Anschluss an die vermeintliche Behebung neu infizieren. Das führt zu weiteren Verzögerungen und Unterbrechungen der Geschäftstätigkeit.

SCHNELLIGKEIT IST TRUMPF

Nach einem Datendiebstahl kommt es darauf an, dass Ihre Sicherheitsverantwortlichen alle Entscheidungen schnell und präzise treffen. Davon hängt ab, ob Sie nach einem Angriff Ihre normale Geschäftstätigkeit mit den geringstmöglichen Auswirkungen wieder aufnehmen können oder nicht. Heute werden Angriffe so versiert geführt, dass sie oft unbemerkt bleiben – nicht zuletzt aufgrund ungeeigneter Abwehrtechnologien. Die Folge: Nach der Entdeckung treten die IT-Mitarbeiter mit ungeeigneten Mitteln oder ohne ausreichende Kenntnisse einen Wettlauf gegen die Zeit an und versuchen, die extrem destruktive Malware zu stoppen.

Hier kommen die CrowdStrike® Endpoint Recovery Services ins Spiel: Mit der richtigen Kombination aus Technologie, Aufklärungsdaten und Fachwissen unterstützen unsere Fachleute Sie bei der Erkennung, Analyse und Behebung von bekannten Sicherheitsvorfällen und ermöglichen die schnelle Wiederherstellung ohne Betriebsunterbrechung. Die Lösung von CrowdStrike ist innerhalb von wenigen Stunden nach einem Datendiebstahl einsatzbereit. So können Sie schneller wieder zur Tagesordnung übergehen und vor allem sicher sein, dass Ihre Angreifer nicht wiederkehren.

DIE VORTEILE IM ÜBERBLICK

Bofortiger Stopp von Angriffen: Sie setzen die CrowdStrike Falcon®-Plattform umgehend ein und schalten Angreifer unverzüglich aus. Zudem unterbinden Sie weitere Kompromittierungsversuche in Ihrer Umgebung.

Schnelle Wiederherstellung von Umgebungen: Sie identifizieren bösartige Artefakte und Persistenzvektoren schnell und umfassend, während Sie gleichzeitig eine erneute Gefährdung verhindern. Die durchschnittliche Zeit bis zur Bereinigung beträgt 72 bis 96 Stunden.

Minimierung von Betriebsunterbrechungen: Sie stellen den Geschäftsbetrieb effizient und effektiv wieder her, ohne neue Images installieren oder neue Geräte verteilen zu müssen.

Senkung der Wiederherstellungskosten: Sie verkürzen die durchschnittliche Wiederherstellungszeit von einigen Wochen oder Monaten auf Tage – und zwar ohne Unterbrechungen – sodass Sie den regulären Betrieb unverzüglich wieder aufnehmen können.

Kontinuierliche Unterstützung: Nach der Wiederherstellungsphase (in der Regel die ersten 72 bis 96 Stunden) überwacht und behebt CrowdStrike Services weiterhin mögliche Sicherheitsbedrohungen.

ENDPOINT RECOVERY SERVICES

WICHTIGE PHASEN DER WIEDERHERSTELLUNGSARBEITEN

Die CrowdStrike Endpoint Recovery Services werden in 30-Tage-Schritten angeboten und ermöglichen so die schnelle Wiederherstellung von Endgeräten in Ihrem Netzwerk. Während des Einsatzes überwacht CrowdStrike Ihre Umgebung und greift dabei auf die globale Sicherheitsexpertise des Teams von Falcon OverWatch™ zurück, um neue oder wiederkehrende Angriffe zu verhindern.

PRÄVENTION

- In den ersten 24 Stunden nach Beauftragung beginnt die schnelle Bereitstellung und Konfiguration der Falcon-Plattform und der Sensoren anhand leistungsstarker Präventionsrichtlinien. Damit werden die Ausführung aktiver Angriffe und die laterale Bewegung der Angreifer gestoppt

WIEDERHERSTELLUNG

- In den nächsten 72 bis 96 Stunden nutzt das CrowdStrike Services-Team die Falcon-Plattform, um Angriffe zu analysieren und speicherresidente Malware, Persistenzmechanismen und andere aktive Angriffskomponenten vollständig zu bereinigen und zu beseitigen.
- Anhand der in der Falcon-Konsole identifizierten Sicherheitsereignisse spricht das Services-Team Empfehlungen aus. Die Verbindung aus Erkenntnissen, die aus den Angriffen gewonnen wurden, und analysierten Datenpunkten verleiht dem Team Einblick in mutmaßliche Ursachen, Angriffstechniken bzw. Schwachstellen, damit weitere Vorfälle verhindert werden und eine gezielte Wiederherstellung erfolgen kann
- Der Schwerpunkt des Engagements liegt auf der schnellen und effizienten Wiederherstellung von Endgeräten ohne Geschäftsunterbrechung. Eine vollständige forensische Untersuchung erfolgt hier nicht.

ÜBERWACHUNG

- INach der Wiederherstellung und für den Rest der Beauftragung überwacht CrowdStrike Ihre Umgebung weiter auf ein erneutes Auftreten des vorherigen Vorfalls und erkennt und behebt alle neuen Vorfälle oder Versuche, in Ihr Netzwerk einzudringen
- Das Team von Falcon OverWatch™ für die Bedrohungssuche überwacht auch solche Angriffstechniken, die darauf ausgelegt sind, selbst die besten Sicherheitstechnologien zu umgehen. Hierbei kommuniziert es direkt mit dem Recovery-Team, sobald es Hinweise auf Angriffe gibt und Gegenmaßnahmen erforderlich sind.

DOKUMENTATION

- Zum Abschluss des Einsatzes erstellt das Recovery-Team einen Abschlussbericht (Zusammenfassung und technische Beschreibung), bestehend aus Beobachtungen, Analysen und Wiederherstellungsmaßnahmen während des Einsatzes.

WARUM CROWDSTRIKE?

CrowdStrike ist branchenführend beim Schutz von Endgeräten und bei der Reaktion auf Vorfälle. Wir bieten die richtige Kombination aus Technologie, Bedrohungsaufklärung und Know-how, um Datendiebstähle schnell erkennen, Angriffe untersuchen, Angreifer vertreiben und Ihre Endgeräte säubern zu können. So sorgen wir dafür, dass Ihr Geschäftsbetrieb nach einem Angriff mit minimaler Unterbrechung weiterläuft.

Führende Technologieplattform: Die cloud-native Falcon-Plattform ist innerhalb weniger Stunden einsatzbereit. Angriffe werden schnell erkannt und untersucht, Angreifer werden aus Ihrer Umgebung vertrieben.

Abhilfe auf Basis von Bedrohungs-aufklärung: Für die globale Bedrohungsaufklärung nutzt CrowdStrike die neuesten Angriffsindikatoren (Indicators of Attack, IOAs) und Gefährdungsindikatoren (Indicators of Compromise, IOCs). So erkennen wir selbst die perfidesten Advanced Persistent Threats, die möglicherweise in Ihrer Umgebung unentdeckt operieren.

CCybersicherheits-Expertise: Die Sicherheitsfachleute von CrowdStrike besitzen jahrelange Erfahrung und Fachwissen. Sie arbeiten direkt mit den infizierten Endgeräten, entfernen alle verbleibenden Artefakte und Persistenzmechanismen und verhindern so eine erneute Infektion, ohne dass ein Re-Image der Rechner erforderlich ist.

Schnelle Wiederherstellung: Dank der marktführenden Endgerätetechnologie von CrowdStrike, der globalen Bedrohungsaufklärung und der unübertroffenen Sicherheitsexpertise ist Ihre Umgebung nach professionellen Angriffen und Advanced Persistent Threats schneller wiederhergestellt.

ÜBER CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), ein weltweit führendes Unternehmen im Bereich der Cybersicherheit, definiert mit seiner von Grund auf neu konzipierten Endgeräteschutzplattform die Sicherheit im Cloud-Zeitalter neu. Die schlanke Single- Agent-Architektur der CrowdStrike Falcon®-Plattform nutzt Cloud-skalierte Künstliche Intelligenz und sorgt unternehmensweit für Schutz und Transparenz. So werden Angriffe auf Endgeräte sowohl innerhalb als auch außerhalb des Netzwerks verhindert. Mit Hilfe des firmeneigenen CrowdStrike Threat Graph® korreliert CrowdStrike Falcon weltweit und in Echtzeit über 5 Billionen endpunktbezogene Ereignisse pro Woche. Damit ist die CrowdStrike Falcon Plattform eine der weltweit fortschrittlichsten Datenplattformen für Cyber-Sicherheit.