CROWDSTRIKE

FALCON COMPLETE

Vollständig verwalteter Endgeräteschutz –
ein Service der Experten von CrowdStrike

BEDROHUNGEN SCHNELL ERKENNEN, EINDÄMMEN UND BEHEBEN

Ein wirksames Programm zur Endgerätesicherheit praktisch umzusetzen, kann schwierig sein. Die notwendigen Werkzeuge setzen oft detaillierte Kenntnisse voraus. Zudem verlangen richtige Implementierung, Unterstützung und Wartung oft umfangreiche Ressourcen. Daher gelingt es vielen Unternehmen und Institutionen nicht, das Beste aus den erworbenen Technologien für die Endgerätesicherheit herauszuholen.

Noch schwieriger sieht es für Organisationen aus, die die geltenden Empfehlungen für die Endgeräte-Sicherheitslage umsetzen möchten. Denn ein höheres Sicherheitsniveau erfordert noch mehr Ressourcen, da Wartung und Administration ggf. noch komplexer sind.

Das Ergebnis? Vielen Unternehmen gelingt es nicht, ein grundlegendes Endgerätesicherheitsprogramm erfolgreich zu implementieren – ganz zu schweigen von einem wirklich umfassenden Schutz. Kritisch wird es, wenn schwere Sicherheitsvorfälle auftreten und die Organisation nicht die Zeit oder das Fachwissen zur Behebung der Probleme hat, was für die Organisation existenzgefährdend werden kann.

CYBERANGRIFFE ALS STRESSTEST FÜR DIE IT

- **63 Stunden:** Das ist die durchschnittliche Zeit, die ein Unternehmen benötigt, um eine Bedrohung zu erkennen und zu beseitigen. (VansonBourne - Juli 2018)
- **3,5 Millionen:** Das ist die Zahl der Stellen im Bereich der Cybersicherheit, die voraussichtlich bis 2021 unbesetzt bleiben werden, da Unternehmen und Institutionen mit dem dramatischen Anstieg der Cyberkriminalität nicht Schritt halten können. (Cybersecurity Jobs Report 2018-2021 - CyberSecurity Ventures)

Bei der Implementierung eines Endgerätesicherheitsprogramms treten oft insbesondere folgende Probleme auf:

- **Schwierigkeiten bei der vollständigen Implementierung und korrekten Konfiguration der erworbenen Technologie:** Je nach Größe und Arbeitsbelastung der IT-Teams fehlt es Unternehmen möglicherweise an Werkzeugen und Bandbreite, um die Lösung schnell und erfolgreich auf den Endgeräten zu implementieren. Darüber hinaus fehlt Zeit und Fachwissen zur ordnungsgemäßen Konfiguration von Richtlinien, die den Sicherheitsanforderungen entsprechen und den Schutz der Endgeräte gewährleisten. Diese Situation kann dazu führen, dass die Endgerätelösung nur unvollständig bereitgestellt und lückenhaft konfiguriert wird. Das macht die Organisation anfällig für Sicherheitsverletzungen.
- **Schwierigkeiten beim täglichen Umgang mit Alarmen und Vorfällen:** Der Umgang mit der oft großen Zahl von Alarmen, die von einer Endgerätesicherheitslösung erzeugt werden, kann selbst Unternehmen überfordern, die über ein eigenes Sicherheitsteam oder ein SOC (Security Operation Center) verfügen. Die richtige Interpretation der Alarme erfordert nicht nur ausreichendes Personal, sondern auch Mitarbeiter mit ausreichenden Kenntnissen im Bereich der Internetsicherheit, die die Meldungen verstehen und die richtigen Entscheidungen treffen. Dem steht meist die knappe Personaldecke entgegen, sodass Alarme unbeachtet bleiben, was versierten Angreifern Tür und Tor öffnet.
- **Schwierigkeiten bei der ordnungsgemäßen Behebung von Sicherheitsvorfällen:** Knappe Ressourcen und fehlendes Spezialwissen können dazu führen, dass sich Organisationen schwer damit tun, Art und Umfang eines Vorfalls rechtzeitig richtig einzuordnen. Vorfälle können dann nicht effizient behoben, nicht vollständig angegangen oder nicht rechtzeitig behandelt werden – mit entsprechenden Folgen für die Sicherheitslage. Die richtige Behebung von Vorfällen verlangt Fertigkeiten und Erfahrung. Vielen Unternehmen und Institutionen fehlt es an den nötigen Ressourcen. Sie sind daher gezwungen, ihre Endgeräte neu aufzusetzen, da sie über keine Alternativen in Form geeigneter Gegenmaßnahmen verfügen, wie beispielsweise Netzwerkeindämmung, Hash-Prävention, Löschen/Ändern von Registrierungsschlüsselwerten oder Stoppen/Deaktivieren/Neustarten von Diensten. Doch selbst ein Re-Imaging ist keine Gewähr dafür, dass der Vorfall anschließend vollständig behoben ist.
- **Fehlende Mittel für den Aufbau eines umfassenden Endgerätesicherheitsprogramms:** Die Kosten für den Aufbau eines umfassenden Sicherheitsprogramms, das rund um die Uhr mit Sicherheitsexperten besetzt ist, können viele Organisationen nicht stemmen. Das macht eine hohe Sicherheitsreife unerreichbar.
- **Fehlende Zeit zur Umsetzung des Programms:** Selbst wenn die finanziellen Mittel für den Aufbau eines internen Endgerätesicherheitsprogramms vorhanden sind, kann sich die Umsetzung einer ausgereiften Sicherheitsstrategie hinziehen. Von der Suche und Einstellung des geeigneten Personals und dem Erwerb der entsprechenden Technologie bis hin zur Festlegung von Richtlinien und der Definition von Prozessen zur Reaktion auf Vorfälle (IR) können Monate, wenn nicht Jahre vergehen. Zudem wird derartigen Programmen oft eine geringere Priorität eingeräumt als anderen dringenden IT-Projekten. Das führt zu langen Implementierungsprozessen und macht die Unternehmen verwundbar.
- **Schwierigkeit, Fachleute zu finden und zu halten:** Es ist nicht einfach, das für die effiziente Sicherung der Endgeräte erforderliche Fachpersonal zu akquirieren. Eine weitere Problematik ist die Bindung der Mitarbeiter und die fortlaufende Schulung entsprechend der immer anspruchsvolleren Bedrohungslandschaft. Der Fachkräftemangel ist ein branchenweites Problem.
- **Notwendige Komponenten sind nicht vorhanden:** Selbst wenn Unternehmen sich dazu entschließen, ihre Endgerätesicherheit auszulagern, werden sie feststellen, dass es nicht so einfach ist, alle notwendigen Komponenten zu finden. Ein besonders schwieriger und sensibler Schritt ist die Wiederherstellung bzw. Schadensbehebung. Die meisten Sicherheitsanbieter schrecken davor zurück, eine solche Komponente anzubieten, weil dies ihre Fähigkeiten und Erfahrungen übersteigt.

FALCON COMPLETE

ANWENDUNGSFALL: SCHWIERIGKEITEN BEI DER IMPLEMENTIERUNG DER TECHNOLOGIE

Herausforderung	Je nach Größe und Arbeitsbelastung Ihrer IT-Teams verfügen Sie möglicherweise nicht über die Tools und die Bandbreite, die für eine schnelle und vollständige Implementierung der Endgerätesicherheit erforderlich sind, sodass Ihr Unternehmen anfällig für Sicherheitsverletzungen ist.
Lösung	Falcon Complete™ hilft, die Endgerätesicherheit erfolgreich zu operationalisieren und zu optimieren: ■ **Fachwissen zur Konfiguration:** CrowdStrike® hilft Ihnen bei der Einrichtung der Richtlinienverwaltung und der Anwendung der gewünschten Präventionsrichtlinien auf der Grundlage Ihrer Kenntnisse und Ihrer Erfahrung. ■ **Tuning und Abstimmung:** Wir überprüfen kontinuierlich mit Ihnen die Richtlinien zur Prävention und Erkennung, um den optimalen Betrieb aller Funktionen der Falcon-Plattform sicherzustellen. ■ **Fortlaufendes Management:** Die Endgeräte in einem Netzwerk unterliegen im Laufe der Zeit Veränderungen: Neue Geräte, neue oder ausscheidende Mitarbeiter und innerbetriebliche Veränderungen sorgen für viel Bewegung. Das zieht administrative Anpassungen nach sich, damit die Präventionsrichtlinien weiterhin wirksam sind und die Endgeräte-Agents ihre Aufgaben wahrnehmen können.

ANWENDUNGSFALL: SCHWIERIGKEITEN BEIM TÄGLICHEN UMGANG MIT ALARMEN UND VORFÄLLEN

Herausforderung	Die große Zahl von Alarmen, die von einer Endgerätesicherheitslösung erzeugt wird, ist kaum zu bewältigen. Die damit verbundenen Ermüdungserscheinungen können dazu führen, dass Meldungen nicht oder nicht richtig beachtet werden, was Sicherheitsverletzungen Tür und Tor öffnet.
Lösung	Falcon Complete verwaltet sämtliche Alarme und ergreift die erforderlichen Maßnahmen: ■ **Handling von Vorfällen:** Das Team von Falcon Complete erarbeitet mit Ihnen eine Reihe von Musterleitfäden zur Ergreifung von Gegenmaßnahmen in einem bestimmten Erkennungsszenario. ■ **Sichtung von Vorfällen aus der Ferne:** Sobald die Falcon-Plattform eine Warnung ausgibt, prüft das Team von Falcon Complete, ob es sich um einen falsch-positiven oder um einen echten Vorfall handelt und klassifiziert ihn entsprechend im Vorfallmanagementsystem. ■ **Behebung von Vorfällen aus der Ferne:** In Übereinstimmung mit den für Sie erstellten Musterleitfäden kann das Team von Falcon Complete Gegenmaßnahmen als Reaktion auf Vorfälle einleiten, um Angriffe vollständig zu stoppen und Vorfälle zu beheben.

ANWENDUNGSFALL: SCHWIERIGKEITEN BEI DER ORDNUNGSGEMÄSSEN BEHEBUNG VON SICHERHEITSVORFÄLLEN

Herausforderung	Fehlende Kenntnisse und Erfahrung können dazu führen, dass Mitarbeiter wochenlang versuchen, einen Vorfall zu bereinigen, dabei wertvolle Ressourcen verschwenden und schließlich davon ausgehen, dass die Umgebung bereinigt wurde, obwohl das nicht der Fall ist.
Lösung	Falcon Complete greift ein und führt alle zur Behebung des Vorfalls erforderlichen Maßnahmen durch: ■ **Behebung von Vorfällen aus der Ferne:** Gemäß den definierten Musterleitfäden versucht Falcon Complete, den Alarm zu interpretieren und dann durch Kombination spezifischer Gegenmaßnahmen eine Strategie zur Behebung zu entwickeln. ■ **Fernzugriff auf das Endgerät:** Das Team von Falcon Complete unterbricht und beseitigt laufende Angriffe, bereinigt kompromittierte Endgeräte oder entfernt Malware-Artefakte zur weiteren Analyse.

VORTEILE

Falcon Complete deckt alle Aspekte der Endgerätesicherheit ab, von der Bereitstellung, Konfiguration, Wartung und Überwachung bis hin zur Handhabung von Alarmen, der Reaktion auf Vorfälle und deren Behebung. Das gewährleistet eine effektive Endgerätesicherheit und senkt das Risiko von Sicherheitsverletzungen.

Sie profitieren von einer Überwachung rund um die Uhr an allen Tagen des Jahres und einer Unterstützung bei der Behandlung von Vorfällen. So ist sichergestellt, dass keine Warnungen unter den Tisch fallen und dass sich das Risiko eines schwerwiegenden Verstoßes verringert.

Das Team von Falcon Complete widmet sich der vollständigen Lösung des Vorfalls, sodass Sie sich nicht damit befassen müssen.

FALCON COMPLETE – KNOW-HOW UND TECHNOLOGIE VON CROWDSTRIKE FÜR IHRE SICHERHEIT

CrowdStrike Falcon Complete stellt Ihnen auf einzigartige Weise die Technologie, die Plattform, die aussagekräftigen Aufklärungsdaten und das Know-how zur Verfügung – für eine umfassende und durchgängige Endgerätesicherheit. Mit Falcon Complete können Kunden die Endgerätesicherheit den bewährten Sicherheitsexperten von CrowdStrike anvertrauen; das gilt für die Implementierung ebenso wie für das Handling und die Reaktion auf Sicherheitsvorfälle. Das Ergebnis ist eine sofort optimierte Sicherheitslage, ohne den Aufwand, den Overhead und die Kosten für die interne Administration eines umfassenden Endgerätesicherheitsprogramms.

Falcon Complete baut auf der CrowdStrike Falcon®-Plattform auf und ist die umfassendste Lösung von CrowdStrike für den Endgeräteschutz. Die Lösung bietet unübertroffene Sicherheit durch Kombination von Falcon Prevent™ Antivirus der neuesten Generation (NGAV), Falcon Insight™ Endgeräteerkennung und Reaktion (EDR) und Falcon OverWatch™ als verwaltete Bedrohungssuche mit dem Fachwissen und dem 24/7-Einsatz des CrowdStrike-Teams. Das Team verwaltet und überwacht aktiv die Falcon-Plattform für Kunden und behebt bei Bedarf Vorfälle per Fernzugriff. Falcon Complete verbindet die Effektivität der Falcon-Plattform mit der Effizienz eines engagierten Teams von Sicherheitsexperten, das in Ihrem Namen zielgerichtete Maßnahmen auf der Basis definierter Musterleitfäden ergreift.

VERLÄSSLICHE ENDGERÄTESICHERHEIT

Falcon Complete ist die umfassende Lösung für den gesamten Lebenszyklus der Endgerätesicherheit, die alle Bereiche der Endgerätesicherheit abdeckt, einschließlich der zuverlässigen Behebung von Vorfällen per Fernzugriff – damit Sie sich nicht darum kümmern müssen. Sie erzielen damit ein Höchstmaß an Endgerätesicherheit und vereinfachen gleichzeitig die Implementierung und den täglichen Betrieb Ihres Endgeräteschutzprogramms. Falcon Complete stellt Ihnen auf einzigartige Weise die Technologie, die Plattform, die aussagekräftigen Aufklärungsdaten und das Know-how zur Verfügung – für ein umfassendes Handling und eine durchgängige Endgerätesicherheit.

WAS IST DAS BESONDERE AN FALCON COMPLETE?

- Auslagerung der Endgerätesicherheit an erfahrene Mitarbeiter aus dem Falcon-Team von CrowdStrike
- Unterstützung bei der Bereitstellung und Konfiguration
- Handling von Alarmen und Vorfällen rund um die Uhr
- Proaktive Sichtung und Eindämmung von Vorfällen
- Wirksames Handling von Vorfällen und deren Behebung
- Transparente Berichterstattung und Metriken

WARUM CROWDSTRIKE?

CrowdStrike Falcon ist eine cloud-basierte Lösung, die Ihr Unternehmen schützt und gleichzeitig die individuellen Anforderungen Ihrer Geschäftstätigkeit erfüllt. Die Bedrohungen, mit denen Sie konfrontiert sind, entwickeln sich ständig weiter. Sie benötigen daher eine Lösung, die Ereignisse proaktiv erkennt und verhindert. CrowdStrike baut seine Lösungen auf der Fähigkeit auf, Sicherheitsverletzungen zu erkennen und zu verhindern – auch die der besonders versierten Angreifer. Auf einer Plattform, die sich nahtlos in Ihrem Unternehmen einsetzen und skalieren lässt, und mit einem engagierten Team von Sicherheitsexperten schützt CrowdStrike Ihr Unternehmen mit einer Lösung, die einerseits darauf ausgelegt ist, Sicherheitsverletzungen zu stoppen, und die sich andererseits mit Ihren Anforderungen weiterentwickelt.

ERFAHREN SIE MEHR UNTER
WWW.CROWDSTRIKE.DE

Email: germany@crowdstrike.com
Web: www.crowdstrike.de

Testen Sie jetzt kostenlos den Virenschutz der nächsten Generation