CROWDSTRIKE

BEWERTUNG VON CYBER-RISIKEN BEI FUSIONEN UND ÜBERNAHMEN

Fusionen und Übernahmen können Sicherheitsrisiken mit sich bringen. CrowdStrike Services übernimmt die notwendige kritische Analyse, damit Ihrer Organisation keine unnötigen Risiken und Kosten entstehen.

ÜBERBLICK

Sie würden nie eine Immobilie ohne sorgfältige Prüfung kaufen. Für die Investition von Millionenbeträgen in den Kauf eines Unternehmens gilt das erst recht. Ebenso sollte jedes Fusions- oder Übernahmeszenario einer eingehenden Untersuchung unterzogen werden. Zumal wenn die damit die Integration von Netzwerken oder Dienstleistungen des Übernahmekandidaten verbunden sind. Eine Bewertung der Cyber-Risiken bei Fusionen und Übernahmen durch die Spezialisten von CrowdStrike® Services schafft die notwendige Transparenz, ohne neue Risiken einzugehen.

CROWDSTRIKE LIEFERT DIE RICHTIGEN ANTWORTEN AUF DIE ENTSCHEIDENDEN FRAGEN

Der Ausbau der operativen Fähigkeiten Ihrer Organisation darf nicht zu einem höheren Risiko für Ihre Geschäftsabläufe führen. Mit einem potenziellen Fusions- oder Übernahmepartner können verschiedene und möglicherweise problematische Szenarien verbunden sein:

- Der Partner könnte Schwachstellen aufweisen, die Cyber-Kriminelle dazu nutzen könnten, Zugang zu Ihrem Netzwerk und zu sensiblen Daten zu erhalten.
- Das Netzwerk des Partners könnte durch Angreifer kompromittiert worden sein, die aus dem Unternehmen wertvolles geistiges Eigentum abziehen, was dessen ursprüngliche Bewertung erheblich beeinträchtigt.
- Dem Partner könnte es an ausreichenden Kontrollen nach dem Vorbild Ihrer aktuellen Informationssicherheitsstrategie fehlen, wodurch unbeabsichtigte Schwachstellen eröffnet werden.

Das Team von CrowdStrike Services führt auf Wunsch die Analysen, Tests und Gesamtdiagnosen dieser Szenarien durch. Unter Einsatz der Falcon-Plattform erhalten Sie auf Anhieb Einblick in die Endgeräteaktivitäten sowohl in der Umgebung des Kunden wie auch in der Umgebung des Übernahmepartners.

Das Ziel: Empfehlungen und Informationen, die Ihr Management-Team vor einer potenziellen Transaktion für fundierte Entscheidungen benötigt.

ERNÜCHTERNDE FAKTEN

$600 MILLIARDEN

beträgt der geschätzte Wert des allein in den USA gestohlenen geistigen Eigentums[1]

191 TAGE

beträgt die mittlere Verweilzeit von Angreifern in einer Umgebung, bevor diese erkannt und hinausgeworfen werden[2]

$4,8 MILLIONEN

betrugen weltweit die mittleren Gesamtkosten je Datendiebstahl im Jahr 2018[2]

1. The IP Commission Report zum Diebstahl geistigen Eigentums in den USA, Mai 2017
2. Ponemon Institute 2018 – Studie zu den Kosten von Datendiebstahl: Auswirkungen von Business Continuity Management – Oktober 2018

Bewertung von Cyber-Risiken bei Fusionen und Übernahmen

WARUM CROWDSTRIKE?

INVESTIGATIVE FÄHIGKEITEN

Das Team von CrowdStrike Services bringt technische Kenntnisse und investigative Fähigkeiten mit, die über Jahre im Rahmen von Einsätzen zur Abwehr von Sicherheitsvorfällen entwickelt wurden. Die Mitarbeiter im Expertenteam von CrowdStrike verfügen im Mittel über 10 Jahre Erfahrung. Sie stammen u. a. aus militärischen und staatlichen Geheimdiensten und führenden Sicherheitsberatungsfirmen. Was man nicht vergessen sollte: Cyber-Kriminelle sind Menschen. Das verlangt nach der Intuition hochkarätiger Fachleute mit der richtigen Erfahrung. Nur so lassen sich Schäden an geschäftskritischen Abläufen entdecken und eindämmen.

ÜBERLEGENE TECHNOLOGIE: DIE FALCON-PLATTFORM

Die proprietären Tools von CrowdStrike automatisieren Ermittlungsaufgaben und ermöglichen eine schnelle Auswertung von Netzwerkverkehr und hostbasierten Artefakten. Dies funktioniert auch in Netzwerken mit Hunderttausenden von Systemen. Verschaffen Sie sich bereits jetzt im Vorfeld möglicher Angriffe die nötigen Einblicke.

ERWEITERTE BEDROHUNGSAUFKLÄRUNG: CROWDSTRIKE INTELLIGENCE

Mit CrowdStrike haben Sie ein Team an Bord, das sich auf die Erforschung der neuesten Exploits und das Reverse Engineering bösartiger Software konzentriert. Das Team erstellt auch Profile der wichtigsten Angriffsgruppen – mit Instrumenten, Praktiken und Zielen sowie entsprechenden Gefährdungsindikatoren (IOCs) und Angriffsindikatoren (IOAs).

MANAGEMENTERFAHRUNG

Das Team von CrowdStrike Services besteht aus erfahrenen und vertrauenswürdigen Fachleuten. Diese Experten geben fundierte Ratschläge zu den geschäftlichen Auswirkungen von Sicherheitsproblemen, die während der Bewertung entdeckt werden.

Erfahren Sie mehr unter **https://www.crowdstrike.de/services/**
Kontakt: **Services@crowdstrike.com**
+49 (0)241 93688811

RISIKOERKENNUNG IN AKTION

Welche Risiken bei einem typischen Überprüfungsauftrag aufgedeckt werden können, veranschaulicht das folgende Beispiel. Im Zuge der Überprüfung eines Unternehmens, das ein Kunde von CrowdStrike übernehmen wollte, fandt das Team von CrowdStrike Services Folgendes:

- Zahlreiche Infektionen mit Commodity Malware, die sich unbemerkt in der Umgebung des Übernahmekandidaten verbreitet hatten
- Zahlreiche mangelhafte Sicherheitspraktiken, wodurch das Unternehmen weiteren Bedrohungen ausgesetzt war

Nach den von CrowdStrike aufgedeckten Risiken entschied der Kunde, von der Übernahme Abstand zu nehmen, um Datendiebstahl und Datenschutzverstöße zu vermeiden. Ein möglicher Datendiebstahl ist aber nicht das einzige Risiko, das vor einer Übernahme oder Investition zu beachten ist. Denkbar ist auch eine Kombination mehrerer Sicherheitsrisiken. Daher sollte eine Bewertung von Cyber-Risiken bei Fusionen und Übernahmen immer strategischer Bestandteil Ihres Unternehmens sein.

ÜBER CROWDSTRIKE SERVICES

CrowdStrike Services stattet Unternehmen und Institutionen mit dem nötigen Schutz und Know-how zur wirksamen Reaktion auf Sicherheitsvorfälle aus. Das Sicherheitsteam von CrowdStrike Services unterstützt Kunden dabei, Angreifer in Echtzeit zu identifizieren, zu verfolgen und zu blockieren. Dabei nutzt es die cloudbasierte Plattform CrowdStrike Falcon® mit integriertem Endgeräteschutz der neuesten Generation, Erfassung von Cyber-Bedrohungsdaten, Berichterstattung und proaktiver Bedrohungssuche rund um die Uhr. Dank diesem einzigartigen Konzept kann CrowdStrike unbefugte Zugriffe schneller unterbinden und weitere Datenschutzverstöße verhindern. Darüber hinaus bietet CrowdStrike proaktive Services an, mit denen Unternehmen ihre Fähigkeit verbessern können, Bedrohungen zu antizipieren, Netzwerke abzusichern und Datenschutzverstöße letztlich zu unterbinden.

FORRESTER WAVE: CROWDSTRIKE SERVICES ALS „LEADER“ POSITIONIERT

„Das ausgewiesene Expertenwissen verschafft CrowdStrike einen Vorteil bei Aufklärung von Bedrohungen und der nötigen Reaktion darauf.“

— Forrester Wave: Cybersecurity Incident Response (IR) Services Q1 2019