Digitale Forensik

Die Analyse nach dem Vorfall.

Sie wurden Opfer eines Cyberangriffs und benötigen Hilfe zur Aufklärung? Unser Team aus erfahrenen IT-Forensikern identifiziert die Ursache, den Umfang und den Verursacher des Angriffs für Sie. Außerdem begleiten wir Sie beratend zum Thema Kommunikation und erstellen behördenpezifische bzw. compliance-spezifische Reports für Sie.

Kernfragen zur Vorfalluntersuchung

Bei unserer technischen Vorfalluntersuchung konzentrieren wir uns auf die Beantwortung folgender Fragen:

- Wie hat der Angriff stattgefunden? Welche Schwachstellen wurden ausgenutzt?
- Welche Systeme sind von dem Angriff betroffen?
- Welche Schäden wurden verursacht bzw. welche Daten wurden abgegriffen?
- Wer war der Verursacher?
- Wie können zukünftige Angriffe vermieden werden?

Unser IT-Forensik Labor

Unser Team verfügt über ein umfangreiches IT-Forensik Labor, um eine effiziente Bearbeitung aller Vorfälle zu ermöglichen. Mithilfe professioneller Werkzeuge und Methoden werten wir Log-Dateien und Datenträger nach dem Angriff aus und identifizieren unerwünschte Netzwerkaktivitäten. Sie erhalten nach Abschluss der Vorfallanalyse einen umfangreichen forensischen Bericht, der zusätzlich Maßnahmenempfehlungen zur Vermeidung weiterer Angriffe enthält. Darüber hinaus stellen wir behördenspezifische Meldungen für Sie aus.

Unser Vorgehensmodell

Wir führen forensische Untersuchungen in sechs Phasen durch. Die Vorgehensweise beruht auf internationalen Standards und Best Practices wie SANS, NIST und dem BSI. Alle Schritte und deren Ergebnisse werden jeweils dokumentiert.

Vorgehensmodell-Phasen

Vorbereitung

Im Rahmen der Vorbereitung besprechen wir gemeinsam mit Ihnen die Ausgangssituation und erläutern unser Vorgehen. Vorfallsabhängig werden dazu geeignete forensische Werkzeuge durch uns identifiziert und bereitgestellt.

Datensammlung

In dieser Phase erfolgt die Sammlung wichtiger Daten von potentiell betroffenen Komponenten. Dabei erfassen wir unter anderem die aktuelle Systemzeit und das Systemdatum, alle zu dem Zeitpunkt auf dem System laufenden Prozesse (Systemzustand), die am System geöffneten Netzwerkverbindungen (Sockets) und die am System angemeldeten Nutzer.

Untersuchung

Nach Abschluss der Datensammlung erfolgt deren Untersuchung. Hierbei werden den Vorfall betreffende Daten extrahiert. Eine Reduktion der Daten ergibt sich dadurch, dass bestimmte Daten aus der weiteren Untersuchung ausgeschlossen werden können (z. B. durch die Überprüfung gegen bekannte Checksummen). Jedoch kann sich ebenso die Notwendigkeit ergeben, die Untersuchung auf weitere Komponenten der IT-Anlage auszuweiten.

Datenanalyse

Da häufig mehrere Teilkomponenten von einem Vorfall betroffen sind, ergeben sich auch mehrere einzelne Untersuchungen auf diesen Komponenten. Diese Ergebnisse zu einem einheitlichen Zeitverlauf zusammenzuführen und in einen logischen Zusammenhang zu bringen, geschieht in der Phase der Datenanalyse.

Dokumentation

Nach Abschluss der Datenanalyse erfolgt die formale Dokumentation der Untersuchungsergebnisse. Hierbei führen unsere IT-Forensiker die einzelnen, im Untersuchungsverlauf protokollierten Schritte zu einem oder mehreren Berichten zusammen. Wir erstellen zielgruppenspezifische Berichte, so enthält der Bericht für das Management andere technische Details als beispielsweise der Bericht für den Administrator einer Anlage. Auch behördenspezifische Meldungen werden in dieser Phase mit unserer Unterstützung für Sie erstellt.

Nachbearbeitung

Optional werden im Rahmen der Nachbearbeitung verbesserungswürdige Abläufe durch uns identifiziert. Wir treffen technische Maßnahmenempfehlungen, die die Verhinderung zukünftiger Angriffe zum Ziel haben und erarbeiten mit Ihnen konkrete Vorschläge zur Verbesserung der im Unternehmen vorhandenen Response-Strategie, d.h. des Prozesses der Vorfallsbehandlung innerhalb des Unternehmens.

Dieses Produktblatt hat Gültigkeit, sofern keine aktuellere Version veröffentlicht wurde. *Erstellungsdatum Produktblatt 28.11.2018*

Was ist im Notfall zu tun?

Lassen Sie alles unverändert.

Selbstverständlich geht es in einzelnen Fällen primär darum, nach einem Sicherheitsvorfall schnellstmöglich das Schadensausmaß zu reduzieren und den Regelbetrieb wiederherzustellen. Aber nicht nach jedem Vorfall ist es aus Sicherheitssicht richtig, das betroffene System direkt neu aufzusetzen. Denn das bedeutet häufig, dass die Ursache unbekannt bleibt und das System weiterhin anfällig für erneute Angriffe ist. Änderungen am System sollten also vermieden werden, um die Ursachenforschung nicht zu erschweren.

Halten Sie fest, was passiert ist.

Dokumentieren Sie, was sich wann ereignet hat und was Sie getan haben. Diese Informationen sind für die Arbeit unseres Forensik-Teams überaus wertvoll.

Wenden Sie sich bei Fragen gerne direkt an uns.
Telefon: +49 6102 8631-190 | E-Mail: vertrieb@usd.de