Was die IT-Forensik leisten kann

Von Benjamin Liebe

cirosec GmbH
Edisonstraße 21
74076 Heilbronn
Tel: 07131 / 59455-0
Fax: 07131 / 59455-99
info@cirosec.de
www.cirosec.de

Wer schon vor einem Datenabfluss seine technischen Möglichkeiten für die "Zeit danach" kennt, meistert Sicherheitsvorfälle leichter.

Verschafft sich ein Angreifer unberechtigt Zugriff auf Daten, handelt es sich um einen IT-Sicherheitsvorfall. Die richtige Reaktion auf ein solches Ereignis besteht aus einer Kette von Handlungen, innerhalb der die IT-Forensik zur Analysephase gehört.
Die klassische IT-Forensik erlaubt es, anhand vorhandener Spuren offene Fragen zu beantworten, die nach einem möglichen Vorfall bestehen. Dazu gehört beispielsweise die Frage nach Art und Menge der preisgegebenen Daten oder danach, welche Schritte der Angreifer genau unternommen hat. Schnelle Antworten direkt zu Beginn eines Vorfall kann sie hingegen nicht geben. Deshalb ist es in akuten Fällen nicht sinnvoll, zunächst auf das Ergebnis einer forensischen Untersuchung zu warten und erst danach über weitere Schritte zu entscheiden.
Stattdessen gilt es, zusätzlich andere Methoden zur Erstbewertung einzusetzen und später das Bild mit den nach und nach eintreffenden Erkenntnissen der forensischen Untersuchung zu vervollständigen.

Ansatzpunkte für Untersuchungen

Erkenntnisse über einen Vorfall lassen sich aus verschiedenen Quellen gewinnen. Die klassische IT-Forensik, wie sie auch zur Aufklärung von Straftaten verwendet wird, verlässt sich hauptsächlich auf die Analyse von Datenträgern, Dateisystemen und darin abgelegten Dateien. Insbesondere bei Vorfällen in Server-Umgebungen können die Datenmengen jedoch beträchtlich sein. Eine Kopie und Auswertung der Informationen dauert lange, eine kurzfristige Lieferung von Antworten ist unmöglich.
Daneben hat sich in den letzten Jahren die Auswertung des Hauptspeichers als anerkanntes Verfahren etabliert. Bei schnell entdeckten oder sogar noch laufenden Angriffen bietet es gute Chancen auf aussagekräftige Hinweise. Die anfallenden Datenmengen sind in diesen Fällen meist überschaubarer als bei einer Datenträgeranalyse. Das Erstellen eines Speicherabbilds "auf Verdacht" ist somit leichter. Für eine aussagekräftige Auswertung sind jedoch Know-how und Werkzeuge nötig, die in den wenigsten Fällen kurzfristig vorhanden sind.
Besser geeignet für eine schnelle Erstbewertung sind andere Methoden. Statt der langwierigen Sicherung der Festplatte kann es sinnvoll sein, zuvor bei den noch laufenden Systemen über das Netzwerk Informationen über den Systemzustand abzufragen. Dieses Verfahren liefert in manchen Fällen bereits erste Hinweise - zum Beispiel eine Auflistung der bestehenden Netzverbindungen oder aller innerhalb einer Gruppe von Servern laufenden Prozesse. Auch die Auswertung der Netzkommunikation - zum Beispiel durch Daten von Firewalls, Proxys

oder aus Netflow - und zentral gespeicherter Protokolle hat eine große Bedeutung. Sicherheitsvorfälle, die sich über mehrere Systeme erstrecken, indem sich der Angreifer von einem System zum nächsten hangelt, lassen sich damit oft deutlich schneller nachvollziehen. Neben dem klassischen Hacking ist bei einer steigenden Zahl von Vorfällen auch Malware im Spiel. Die Analyse der an einer Stelle entdeckten Malware kann wichtige Hinweise liefern, um auch die Präsenz auf weiteren Systemen zu erkennen.

Anspruchsvolle Organisation

Die Abwicklung eines IT-Sicherheitsvorfalls ist eine anspruchsvolle Aufgabe: Das Management verlangt regelmäßige Status-Updates, digitale Spuren sollen möglichst schnell gesammelt und ausgewertet sowie der Angriff wirksam abgewehrt werden. Die Koordination der Aktivitäten sollte stets in der Hand eines internen Teams liegen - das kennt im Gegensatz zu Externen die internen Ansprechpartner und Prozesse. Je nach dem Erfahrungsstand der beteiligten Personen kann zusätzlich die Unterstützung durch einen Dienstleister hilfreich sein. Er hilft unter anderem bei der Einschätzung der Situation und beim Entwurf einer Abwehrstrategie. Die forensische Datensammlung sollten - eine entsprechende Vorbereitung vorausgesetzt - dafür ausgebildete Systembetreuer jedoch selbst vornehmen. Denn: Bei neuen Auffälligkeiten können sie deutlich schneller reagieren als externe Dienstleister. Die anschließende Auswertung der Daten geben viele Unternehmen nach außen, da sie das Wissen und die Werkzeuge für eine Analyse nicht selbst vorhalten können. Bei größeren Vorfällen mit mehreren betroffenen Systemen kann es sinnvoll sein, parallel mehrere Dienstleister für unterschiedliche Untersuchungen einzusetzen. In diesem Fall ist der regelmäßige Austausch von Erkenntnissen sinnvoll. Ob intern oder extern - für ein gezieltes Vorgehen ist es wichtig, klare Fragen an die forensische Analyse zu formulieren und rechtzeitig Prioritäten zu setzen.

Hoher Aufwand

Um die Kontrolle über die eigenen Systeme zurückzugewinnen und alle Dienste wiederherzustellen, benötigen betroffene Unternehmen oft mehrere Wochen oder länger - das zeigt die Mehrheit der untersuchten Vorfälle im Verizon Data Breach Investigations Report 2012. Allein die forensische Analyse eines einzelnen Systems nimmt schnell über eine Woche in Anspruch. Das verdeutlicht, wie wichtig Aktivitäten sind, die parallel zur IT-Forensik ihre Wirkung entfalten. Es zeigt auch, dass die vollständige Analyse eines Vorfalls mit mehreren involvierten Systemen sehr teuer sein kann. Hinzu kommen das Incident Handling und die Wiederherstellung.

Empfehlungen für den Ernstfall

Oft liefert IT-Forensik erst Tage nach einem Sicherheitsvorfall Ergebnisse. Zum Beispiel lagen nach Angaben von Sony erste verlässliche Erkenntnisse zum Einbruch in das Playstation Network im Frühjahr 2011 erst sechs Tage nach der Entdeckung vor. Eine Zeitspanne, die desto größer wird, je schlechter das Unternehmen auf den Ernstfall vorbereitet ist.

- Ein professioneller Umgang mit Datenlecks erfordert Vorbereitungen auf vielen Ebenen. Dazu gehört eine sorgfältig erstellte Sammlung von Sofortmaßnahmen mit Checklisten und Aussagen zu den damit verbundenen technischen und betrieblichen Konsequenzen. Sie hilft gerade in zunächst unklaren Situationen bei den ersten Schritten in Richtung Schadensbegrenzung. Zudem erleichtert sie die Sicherstellung von Daten. Neben den Sofortmaßnahmen sollte auch die Dokumentation der IT-Umgebung griff- bereit sein. Das ermöglicht im Ernstfall einen schnelleren Zugriff, da oft nicht jeder am Vorfall Beteiligte die Umgebung kennt.
- Ebenso wichtig ist die Fähigkeit, forensische Datensammlungen selbst vornehmen zu können. So ist es möglich, Datenträger und Arbeitsspeicher von auffälligen Systemen möglichst schnell sicherzustellen, statt durch das Warten auf einen Dienstleister wertvolle Zeit zu verlieren oder durch falsches Vorgehen die Verwertbarkeit vor Gericht zu gefährden. Auch die Frage, welche Werkzeuge und Methoden am besten zur effizienten Sammlung von Informationen geeignet sind, lässt sich schon vorab in Ruhe klären.
- Die Auswertung der Daten gleicht häufig der Suche nach der Nadel im Heuhaufen. Oft ist schwer zu unterscheiden, was auf einem System "normal" ist und was nicht. Die Bereitstellung einer Basisinstallation als Vergleich ist daher hilfreich.
- Auch Unternehmen, die auf einen Dienstleister setzen, sollten sich auf den Ernstfall vorbereiten. Dazu gehört eine Vorauswahl mehrerer geeigneter Anbieter für forensische Dienstleistungen. Nicht jeder Partner kann spontan eine ausreichende Anzahl an Mitarbeitern für einen längeren Zeitraum zur Verfügung stellen. Ebenso wichtig ist die interne Abstimmung mit dem Einkauf, um den Beschaffungsprozess und dadurch bei Bedarf die Beauftragung zu beschleunigen. Bei größeren Unternehmen kann die Vereinbarung eines Rahmenvertrags/Service-Level-Agreements sinnvoll sein.
- In manchen Fällen kann es auch unerwartete rechtliche Hürden geben. Daher ist es wichtig, bereits vorab zu prüfen, welche Sofortmaßnahmen und Untersuchungsmethoden für das Unternehmen rechtlich vertretbar sind. Problematisch wird es vor allem, sobald Client-Systeme von Mitarbeitern betroffen sind oder Datenverkehr überwacht werden soll. Auch eine

Abstimmung zu notwendigen Rahmenbedingungen für die Herausgabe von Kopien der gesammelten Daten an externe Dienstleister ist sinnvoll, weil hier fast immer geschäfts- oder personenbezogene Daten enthalten sind, die besonderen gesetzlichen Bestimmungen unterliegen.

computerwoche.de 08.10.12