Spurensicherung

Angreifer dingfest machen

Immer mehr Mittelständler nehmen die Risiken von Cyberattacken ernst und rüsten mit Firewall und Intrusion-Prevention-Systemen auf. Das ist erfreulich, aber nur die halbe Lösung im Kampf gegen Hacker und Spione. IT-Forensik ist ein wichtiger Teil des Security Incident Managements. Das müssen viele IT-Verantwortliche allerdings erst noch verinnerlichen.

Von Tim Cappelmann und Sven Steinert, AirITSystems

Für den deutschen Mittelstand spielt IT-Security eine zunehmend wichtige Rolle. So beginnen sich technische Lösungen wie Security Information and Event Management (SIEM), Firewalls und Intrusion-Prevention-Systeme (IPS) bei den Unternehmen durchzusetzen. Damit begegnen IT-Verantwortliche vor allem zwei Herausforderungen: Sie sorgen für die notwendige Prävention und für die Erkennung von IT-Sicherheitsvorfällen (IT Security Incidents). Die Analyse und das nachträgliche Aufarbeiten dieser Incidents ist aber noch lange keine Normalität in den IT-Abteilungen. Das ist ein entscheidender Fehler. Denn oft bringt erst die digitale Ermittlung Gewissheit, ob Firmeninformationen nach außen gedrungen sind oder ob sich durch fahrlässiges Handeln beispielsweise unentdeckt Malware verbreitet hat. Darüber hinaus liefern einzig IT-forensische Methoden gerichtsverwertbare Beweise zur Strafverfolgung.

Abwehr allein ist zu wenig

Die klassische Absicherung nach außen reicht heute in den wenigsten Fällen aus: Was ist, wenn doch einmal Malware das eigene Netz erreicht? Und wie erkenne ich Bedrohungen aus dem eigenen Netzwerk? Das übernehmen Monitoring-Geräte und Services wie das Security Information and Event Management. SIEM-Systeme nutzen die Abermillionen Meldungen, die jede Unternehmens-IT tagtäglich produziert, und setzen sie miteinander in Beziehung. Auf diese Weise lassen sich anormale Muster zum Beispiel in Netzwerken erkennen.

An diesem Punkt setzt normalerweise das Security Incident Management ein; hier endet auch der Leistungsbereich des SIEM. Es erkennt Anomalien und identifiziert deren Ausbreitung. Den Vorfall aufklären muss eine Disziplin, die in deutschen Unternehmen bisher oft vernachlässigt wurde: das Incident Management – die IT-Forensik.

Forensik-Toolkits für Firmen

Intelligente Suiten wie EnCase oder Foundstone befähigen Unternehmen heute, interne Ermittlungen gemeinsam mit externen Forensikexperten selbst durchzuführen. Solche Anwendungen sichten und sichern Daten über das gesamte Netzwerk, auf Mitarbeitersystemen in externen Büros und auf mobilen Endgeräten. Dies geschieht, ohne dabei wichtige Beweismittel zu verändern oder zu zerstören. Das ist besonders bei zielgerichteten Malware-Attacken wichtig, wie sie oft im Kontext der Industriespionage intern wie extern vorkommen.

Charakteristisch für solche Angriffe ist, dass sie auf einzelne Unternehmen oder Behörden zielen. Sie werden mit hohem Aufwand durchgeführt und sollen über einen längeren Zeitraum auf vertrauliche Daten zugreifen oder kritische Infrastrukturen kontrollieren. Dabei muss die Malware gar nicht von außen kommen. Der verseuchte USB-Stick eines nicht so wohlmeinenden oder allzu arglosen Kollegen kann ebenso der Anfang allen Übels sein.

Ohne forensische Maßnahmen ist einem solch zielgerichteten Security Incident kaum zu begegnen. Meldet ein SIEM beispielsweise anormale Logdaten-Muster vom Arbeitsplatz des Betroffenen, wäre schnell zu verifizieren, ob es sich tatsächlich um Malware handelt. Ist die Verifikation positiv, gilt es, so schnell wie möglich Gegenmaßnahmen einzuleiten – etwa das betroffene System zu isolieren und vom Netz zu nehmen. Damit der gesamte Vorgang auch später noch zu analysieren ist, muss der Ist-Zustand gesichert werden, über ein Speicherabbild, gesicherte Festplatten usw. Auf dieser Grundlage lässt sich dann Ursachenforschung betreiben: Ist die Malware bereits bekannt? Welche Teile des Systems sind betroffen? Gibt es versteckte Ablagen? Tauchen in den Dateien bestimmte Schlüsselwörter auf? Wie kam die Malware auf das System und wer ist dafür verantwortlich? In der Analyse lässt sich auch herausfinden, welche Dateien im System möglicherweise verändert wurden. Zudem lassen die Schadprogramme oft selbst Rückschlüsse auf die Angreifer zu.

Time to respond drastisch verkürzen

Zeit ist bei Security Incidents immer ein kritischer Faktor. Durch den hohen Automatisierungsgrad von SIEM-Systemen lassen sich die Antwortzeiten wesentlich minimieren. Zwar werden in jedem Fall Experten notwendig sein, um die entsprechenden Analysen durchzuführen und die darauffolgenden Maßnahmen einzuleiten. Mithilfe von Forensik-Tools sind sie jedoch wesentlich schneller handlungsfähig.

Klassischerweise ist IT-Forensik daher sehr teuer. Das liegt nicht nur am hohen Spezialisierungsgrad der Experten, sondern auch an der relativ langen Zeit, die verstreicht, bis der Incident in einem herkömmlichen Modell geklärt ist. Ohne den Einsatz von Security-Analytics-Systemen gehen in der Regel Wochen ins Land, bevor der Vorfall überhaupt analysiert wird. Zu diesem Zeitpunkt hat sich der User wahrscheinlich wegen Computerproblemen beim Helpdesk gemeldet. Sein Trouble Ticket gelangt zunächst in die Warteschlange, sodass ein bis zwei Tage verstreichen, bevor ein Analyst die Ereignisdaten manuell erfasst. Innerhalb der nächsten Tage prüft der Experte diese Daten und entdeckt, dass ein Forensiker einzuschalten ist. Dazu muss ein entsprechender Dienstleister gefunden werden. Dieser analysiert die Daten dann manuell. Und so weiter.

Das Problem dieser Response-Methode ist nicht nur der enorme Zeitverlust. Es können in der Zwischenzeit auch kritische Daten verloren gehen, ohne dass das gesamte Ausmaß der Sicherheitsverletzung bekannt wird.

Liegt die Verantwortung für Monitoring, Detection und Aufklärung in der Hand eines einzigen spezialisierten Dienstleisters, geht es wesentlich schneller. Dabei kommt es auch auf das Zusammenspiel von SIEM und Forensik-Tool an: Das SIEM, das als Managed Service zur Verfügung steht, meldet Zeitpunkt und Ausbreitung eines Vorfalls. Der Experte im System Operations Center (SOC) leitet Gegenmaßnahmen ein. Bereits jetzt erkennt er, dass die Expertise eines Forensikers notwendig ist, und informiert seinen Kollegen in der entsprechenden Fachabteilung. Der Prozess bis zum ausführlichen, gerichtsverwertbaren Bericht dauert dann wenige Tage statt Wochen. Zudem ist das gesamte Ausmaß des Vorfalls in kürzester Zeit bekannt, sodass die Experten Gegenmaßnahmen sehr viel effizienter und wirkungsvoller steuern können.

Zu mächtig für den Mittelstand?

Dem durchschnittlichen Mittelständler wird dieser Aufwand extrem hoch vorkommen. Viele Unternehmen gehen zudem immer noch davon aus, dass das Gros der Angriffe sowieso keine strafrechtlichen Konsequenzen habe. Zumal Polizei und Staatsanwaltschaft keine Geheimhaltung garantieren können. Dementsprechend groß ist auch die Sorge vor Image-Verlusten. Doch gerade aus diesem Umstand heraus ist es wichtig, dass Unternehmen selbst in der Lage sind, gemeinsam mit einem qualifizierten externen Dienstleister etwaige Sicherheitsvorfälle komplett zu ergründen. Nur so lassen sich wirksame und verhältnismäßige Vorkehrungen gegen den nächsten Vorfall treffen. In den vergangenen zwei Jahren ist immerhin mehr als die Hälfte aller deutschen Unternehmen digitaler Wirtschaftsspionage, Sabotage oder Datendiebstahl zum Opfer gefallen. Das hat eine BITKOM-Studie vom Sommer 2015 ergeben.

Digitale Forensik inhouse gemeinsam mit einem qualifizierten Experten zu betreiben, hat einen wesentlichen Vorteil: Laut IBM 2015 Cyber Security Intelligence Index lassen sich 31,5 % aller Cyber-Attacken auf eigene Mitarbeiter mit unlauteren Motiven zurückführen. Diese Angreifer sitzen nicht in fernen, unbekannten Landen, sondern direkt im eigenen Unternehmen, was die juristische Ahndung ermöglicht und nahelegt. Dann zeigt sich auch, wie groß der Know-how-Bedarf ist: IT-Forensik braucht Experten, die nicht nur über IT-Wissen verfügen, sondern wissen, wie Beweismittel zu sichern sind. Hier bietet sich die Zusammenarbeit mit Security-Spezialisten an, die Prävention, Incident Response und Forensik aus einer Hand bereitstellen – betreut von qualifizierten Experten.