Professionelles Krisenmanagement bei Cyberangriffen

Christian Schaaf, Geschäftsführer der Corporate Trust Business Risk & Crisis Management GmbH

„100-prozentige Sicherheit gibt es nicht." Diese Aussage wird oft als Vorwand genutzt, um auf Präventionsmaßnahmen zu verzichten oder Probleme gar zu verharmlosen. Insbesondere für IT- Verantwortliche in Unternehmen wird es immer schwieriger, den richtigen Weg für das Unternehmen in der Prävention zu gehen – und das obwohl Vorkehrungen für ein professionelles Krisenmanagement bei IT-Vorfällen zunehmend wichtiger werden.

Durch das Internet haben sich vielfältige Chancen für die Wirtschaft ergeben, jedoch auch ganz reale Bedrohungen. Information ist heute die zentrale Währung im Netz – über individuelle Interessen, das Kaufverhalten sowie die geschäftlichen Kontakte. Wer Informationen hat, verfügt über Macht. Darüber hinaus werden Geschäfte immer häufiger digital abgewickelt und sind somit leicht auszuforschen. Ein Informationsvorsprung, und sei er auch noch so klein, kann bei relevanten Entscheidungen ausschlaggebend sein. Die Möglichkeiten für Nachrichtendienste, weltweite Datenströme zu überwachen, nehmen ständig zu. Spioniert wird aber nicht nur durch NSA & Co., sondern auch durch Konkurrenten oder die Organisierte Kriminalität. Immer häufiger werden Unternehmen über ihre IT-Geräte oder infizierte E-Mail-Anhänge angegriffen. Die Täter versuchen meist Zugangsdaten oder Passwörter auszuforschen, darüber auf die IT-Infrastruktur, Datenbanken oder E-Mail-Accounts zuzugreifen, um an vertrauliche Daten zu gelangen oder das Unternehmen mit diesem „Leck" zu erpressen. Selbstverständlich können Geräte auch so infiziert werden, dass sie im Rahmen eines „Bot-Netzes", d.h. innerhalb eines zusammengefügten Netzes von gekaperten Computern, für kriminelle Angriffe gegen andere Computer genutzt werden.

Essentiell: eine forensische Spurenauswertung

Wie schmerzhaft ein Cyberangriff sein kann, erlebte kürzlich auch ein mittelständisches Maschinenbauunternehmen. Ein neu installiertes WLAN ermöglichte endlich den kabellosen Internetzugang im gesamten Entwicklungsbereich. Nun konnte man sich überall mit dem Netzwerk verbinden, wichtige Geschäfte erledigen, bei Meetings Präsentationen leichter aus dem Netzwerk abrufen oder im neu geschaffenen Kreativ-Bereich auf dem Laptop an der aktuellen Entwicklung arbeiten. Da häufig externe Mitarbeiter oder Geschäftspartner im Unternehmen waren, wurde das Passwort im Meetingraum an das Whiteboard geschrieben. Während eines Interviews mit einem Fernsehsender war das Passwort im Hintergrund zu sehen.

Angreifer konnten sich so auf die Anlage aufschalten und den gesamten Netzwerkverkehr abhören. Die Täter erbeuteten nicht nur Zugangsdaten für die Kundendatenbank, sondern auch Passwörter für E-Mail-Accounts und vertrauliche Dokumente. Innerhalb von kurzer Zeit konnten die Angreifer die komplette Kontrolle über das Windows Netzwerk des Unternehmens erlangen.

Eine forensische Auswertung der Spuren durch Corporate Trust ergab, dass die Täter einen Domain Controller „kaperten" und so vielfache Zugriffsberechtigungen im Netzwerk hatten. Im Gegensatz zum Krisenmanagement bei Großschadensereignissen, bei dem häufig die wichtigste Aufgabe ist, erst einmal die Auswirkungen zu bekämpfen bzw. Schäden zu begrenzen, stellt sich bei einem IT-Vorfall immer die Frage, ob man jetzt „gleich den Stecker ziehen" oder besser noch etwas zuwarten sollte. Ganz wichtig: Bei einem Cyber-Angriff sollte zuerst sichergestellt sein, dass alles entdeckt wurde. Auch wenn die Auswirkungen manchmal schnell identifiziert werden können, bleibt der eigentliche Grund für die Manipulationen oft im Ungewissen. Denn leider kann man bei digitalen Vorfällen nicht immer sofort eindeutig erkennen, welche Systeme betroffen sind.

IT-Systeme müssen dazu gebracht werden, die richtigen Spuren zu erzeugen

Cyber-Angriffe können niemals vollständig verhindert werden. Dies bedeutet, wir müssen akzeptieren lernen, mit diesem Risiko zu leben. Für eine umfangreiche Schadensbegrenzung ist es jedoch wichtig, solche Angriffe schnell und umfassend zu detektieren, um sofort reagieren zu können. Zur Umsetzung dieser Schutzstrategien sind eine gute Vorbereitung, genaue Planung und entsprechende Investitionen notwendig. Die Aufklärungsarbeit hängt maßgeblich von den Spuren ab, die beim Cyber-Angriff hinterlassen wurden. In IT-Systemen fallen diese Spuren jedoch keineswegs automatisch an. Im Regelfall müssen die verschiedenen Systeme erst dazu gebracht werden, die richtigen Spuren zu erzeugen. Daher beginnt richtiges Krisenmanagement für IT-Vorfälle bereits lange im Vorfeld. Für die Vorbereitung auf ein solches Schadensszenario ist es wichtig, die Art und Weise, in der sogenannte Logs erhoben werden, klar zu definieren und transparente Richtlinien für den Umgang mit den erhobenen Daten (Speicherfristen, Zugriffsbeschränkungen etc.) zu erstellen.

Zusammengefasst: Im Bereich des Cyber-Krisenmanagements spielt die Entdeckung und richtige Klassifizierung eines Vorfalls eine außerordentlich wichtige Rolle. Ein Grund dafür ist, dass bei einem Cyber-Sicherheitsvorfall keine offensichtlichen Symptome vorhanden sein müssen – Sie haben eine Unternehmenskrise und wissen es vielleicht noch nicht einmal!

Dies ist beim klassischen Krisenmanagement – sei es bei Entführungen, Erdbeben oder Produktkontaminationen – faktisch nie der Fall. Konsequenz: Effektives Cyber-Krisenmanagement beginnt bereits vor Eintritt eines Cyber-Sicherheitsvorfalls mit der Suche nach Symptomen auf Grundlage intelligent erzeugter Spuren.

An offener Kommunikation führt kein Weg vorbei

Fragt man Unternehmen, was für sie das größte Risiko im Bereich der Cybersecurity ist, dann ist man sich branchen- und größenübergreifend einig: der Reputationsschaden. Und obwohl jedem klar ist, dass es 100-prozentige Sicherheit nicht gibt, ist es für jedes Unternehmen eine große Hürde, zuzugeben, dass man oft seit Tagen, Wochen, Monaten oder sogar Jahren sensible Daten verliert. Und angesichts der Tatsache, dass die IT ja weiterhin funktioniert, ist die Versuchung groß, die Probleme gegenüber Mitarbeitern und externen Stakeholdern totzuschweigen. Dass dabei gesetzliche Meldepflichten im Weg stehen (Datenschutzgesetz und für kritische Infrastrukturen demnächst auch das IT-Sicherheitsgesetz) wird dabei oft geflissentlich „übersehen“. Zudem verliert man in der internen Kommunikation eine wichtige Chance, die Mitarbeiter auf die Reise hin zu einer größeren Sicherheit mitzunehmen. Es sollte ihnen gegenüber mindestens von einer abstrakten Gefahr gesprochen werden, um sie für die Umsetzung neuer Schutzstrategien zu motivieren.

Erster Schritt ist natürlich, das eigene Management korrekt und richtig zu informieren. Eine herausfordernde Situation, denn im Gegensatz zu greifbaren Krisen ist ein Cyber-Angriff nicht sofort mit dem gesunden Menschenverstand einschätzbar – die IT funktioniert nämlich augenscheinlich wie immer. Hier gilt es für die IT-Verantwortlichen, richtige Analogien und klare, einfach verständliche Erklärungen zu finden.

Was Unternehmen präventiv tun können

Im Zeitalter des Cyberwars – d. h. der systematischen und von langer Hand geplanten Angriffe, verübt von gut ausgerüsteten Angriffseinheiten – geht es bei der Verteidigung der eigenen IT-Infrastruktur nicht mehr um das „ob“, sondern um das „wann“ und „wie lange“. Die Zahl der Angreifer ist so vielfältig wie ihre Motive, und Unternehmen aller Größen stellen fest, dass sie selbst jederzeit und unvermittelt zum Ziel eines Angriffs werden können. In einem aktuellen Fall IT-gestützter Industriespionage konnten sich die Angreifer nach dem Eindringen über mehrere Monate unbemerkt in der IT-Infrastruktur des Unternehmens bewegen und durch gezielte Manipulation von Schlüsselsystemen (Applikationsserver, Domain Controller) eine dauerhafte Präsenz etablieren. Dadurch waren sie in der Lage, sich einen umfassenden Überblick über alle vorhandenen Informationen im Unternehmen zu

verschaffen. Der eigentliche Datendiebstahl erfolgte erst am Ende dieser Spähphase und dauerte nur wenige Stunden.

Eine professionelle IT-Sicherheitsstruktur muss die Möglichkeit von erfolgreichen Angriffen daher nicht nur theoretisch akzeptieren, sondern ganz konkrete Vorkehrungen treffen, um sie möglichst schnell zu erkennen. Hier hilft nur ein Zusammenspiel aus Mensch und Technik. Die Überwachung von sich ständig verändernden Systemen, die zielgerichtete Reaktion auf intelligente Attacken und die Aufklärung komplexer Angriffsmuster können nicht allein mit maschinellen Systemen bewältigt werden, sondern bedürfen trotz aller technische Vorkehrungen auch menschlicher Aufmerksamkeit. In jedem der uns bekannten Fälle lag die Hauptursache für die meist zu späte Entdeckung dieser Aktivitäten darin, dass nicht regelmäßig und gezielt durch erfahrene Spezialisten nach einer möglichen Präsenz von Angreifern im eigenen Netz gesucht wurde. Dabei fehlt es in der Regel nicht an den nötigen Indikatoren, sondern es war schlicht und einfach keine „Wachmannschaft“ vorhanden, die regelmäßig sucht und nach Auffälligkeiten Ausschau hält.

Ein gelungenes Krisenmanagement für IT-Vorfälle erfordert heutzutage, dass das IT-Security Budget verstärkt in eine gut ausgebildete IT-Wachmannschaft investiert werden sollte, anstatt in noch mehr technische Systeme. Das Know-how dieser Spezialisten ist unabdingbar: Einerseits für die erfolgreiche Suche nach Auffälligkeiten in der Unternehmens-IT, andererseits für eine praxisnahe Beratung der IT-Fachabteilungen, was die Planung und Implementierung geeigneter Verteidigungsstrategien betrifft.

Christian Schaaf ist Gründer der Corporate Trust Business Risk & Crisis Management GmbH und geschäftsführender Gesellschafter. Die Unternehmensberatung für Sicherheitsdienstleistungen unterstützt als strategischer Partner im Risiko- und Krisenmanagement Unternehmen, Organisationen und Privatpersonen im High-Level-Security-Bereich.
www.corporate-trust.de