BILD: ISTOCKPHOTO.COM/NYCSHOOTER

Vorbereitung für den Ernstfall

Im September 2011 musste DigiNotar, ein niederländischer Anbieter digitaler Zertifikate, aufgrund einer erfolgreichen Hackerattacke – und dem unglücklichen Versuch, diese zu vertuschen – Konkurs anmelden. Damit Ihr Unternehmen besser vorbereitet ist, sollten Sie einige Grundregeln beachten.

→ VON CHRISTOPH BAUMGARTNER & YVES KRAFT

Digitale Zertifikate sind die elektronischen Identitätskarten im Internet. So können sich beispielsweise Onlineshops oder Internetbanking-Portale gegenüber ihren Besuchern und Kunden identifizieren, indem sie ihre Identität von einer Zertifizierungsstelle (Certification Authority, CA) überprüfen lassen. Nach erfolgreicher Überprüfung stellt die CA ein SSL-Zertifikat aus, das der Onlineshop oder die Bank auf ihrem Webserver installiert. Besucher des Onlineshops oder der Internetbanking-Website können ab diesem Zeitpunkt die Identität des Anbieters verifizieren, indem der Browser das Zertifikat bei der zuständigen CA auf seine Gültigkeit hin verifiziert. Die Sicherheit steht und fällt somit mit der Vertrauenswürdigkeit der Gültigkeitsbestätigung der CA.

STÖRFALL MIT SCHWEREN KONSEQUENZEN

Der Fall DigiNotar ist ein negativer Meilenstein in der Geschichte des E-Business' im Internet. Dort ist es einem oder mehreren Hackern gelungen, trotz implementierten Sicherheitsmechanismen, in die CA-Systeme einzudringen und mehr als 500 vermeintlich gültige Zertifikate auszustellen. Unfreiwillig betroffen waren auch namhafte Organisationen wie die CIA, Google, Facebook, Microsoft, Skype, Twitter und mehr. Der Teufel liegt hier im Detail: Im Gegensatz zu Falschgeld oder gefälschten Pässen, die mehr oder weniger echt aussehen, sind die falschen digitalen Zertifikate nicht von echten zu unterscheiden. Für den Anwender sieht das Zertifikat legitim aus, da es von einer offiziell anerkannten CA signiert ist und im Browser keine Sicherheitswarnung auslöst. Damit wurde das auf anerkannten Zertifizierungsstellen basierende Vertrauensmodell im Internet erstmals empfindlich getroffen. In der Folge mussten die Software-Hersteller in Windeseile Patches oder neue Versionen veröffentlichen, um die von DigiNotar herausgegebenen Zertifikate zu blockieren bzw. als ungültig zu erkennen.

Dieser besonders eklatante Fall zeigt, dass Hackerattacken eine Organisation durchaus in ihrer Existenz bedrohen können. Zwar ist der Fall DigiNotar zugegebenermassen ein Extrembeispiel, weil der Angriff die Kernkompetenz des Unternehmens zerstörte. Das Unternehmen würde aber wohl noch existieren, wenn die Verantwortlichen zeitnah nach Erkennen der – laut Aussage des untersuchenden Auditors – über mehrere Tage laufenden Hackerattacke richtig reagiert hätten, anstatt den Vorfall zu ignorieren und nach öffentlichem Bekanntwerden herunterzuspielen.

WAS TUN, WENN DER ERNSTFALL EINTRITT?

Doch wie reagiert man richtig auf eine Hackerattacke? Unmittelbar nach Erkennen eines Angriffs ist der IT-Sicherheitsverantwortliche der Organisation zu informieren. Dann gilt es, einige Fragen zu klären: Wie hoch ist der zu erwartende direkte und indirekte Schaden? Soll nur direkte Schadensbegrenzung betrieben werden oder möchte man sich die Option offenhalten, den Verursacher auf juristischem Weg zu belangen? Im zweiten Fall sollten Computer-Forensik-Spezialisten beigezogen werden, weil betreffend der Beweissicherung, der Analyse und der Dokumentation strikte Regeln eingehalten werden müssen, um eine gerichtliche Verwertbarkeit zu gewährleisten. Bei laufenden Hackerattacken ist zu überlegen, ob ein System temporär vom Netz genommen werden soll, bis die letzte Datensicherung zurückgespielt und das System anschliessend gehärtet wurde, oder ob externe Hilfe in Betracht kommt.

«Ein einfaches Zonenkonzept schützt bereits vor der Ausbreitung von Angriffen oder unkontrollierter Malware»

Yves Kraft

Obwohl es in solchen Situationen keine einzig richtige Lösung gibt, ist vor Hyperaktivismus abzuraten. Die Gefahr ist gross, dass entweder ungewollt Spuren verwischt, das Firmenimage wegen nicht erreichbarer Systeme geschädigt oder gar unbeteiligte Dritte attackiert werden. Kosten-Nutzen-Überlegungen sollten auch nicht ausser Acht gelassen werden. So kann eine erstattete Anzeige dem geplagten Systemadministrator zwar persönliche Genugtuung verschaffen, andererseits kann aber auch eine daraufhin vom Beschuldigten angezettelte Medienschlacht die von der eigenen Marketingabteilung über Jahre realisierte kostspielige Imagekampagne über Nacht zunichtemachen. In manchen Situationen ist die Flucht nach vorn angebracht. Denn nur so lässt sich die Berichterstattung zumindest teilweise steuern.

WIRKSAME VORSICHTSMASSNAHMEN

Firewalls und Malware-Schutz sollten heute selbstverständlich sein. Ergänzend dazu sind Security-Awareness-Schulungen der Mitarbeiter die wirkungsvollste Massnahme. Denn wer weiss, wie man sich in bestimmten Situationen verhalten soll, handelt höchstwahrscheinlich richtig. Eine weitere Massnahme auf der organisatorischen Seite ist die Dokumentation der Security Policy und des IT-Nutzungsreglements, in der die Mitarbeiter auf die Meldepflicht bei Sicherheitsvorfällen und auch auf den Verantwortlichen hingewiesen werden, an den Meldungen zu erfolgen haben. In Stellenbeschreibungen für sicherheitsrelevante Rollen, wie beispielsweise Systemadministratoren, sollten die Aufgaben für den Normal- und Notfallbetrieb berücksichtigt werden.

Auf technischer Ebene können verschiedene Netzwerkzonen definiert werden, die voneinander mittels restriktiv eingestellten Firewalls getrennt werden. So kann ein einfaches Zonenkonzept bereits gewissen Schutz vor dem Eindringen von Angreifern in andere Netzwerksegmente oder die unkontrollierte Ausbreitung von Malware bieten. Die simple Separierung von PC/Client- und Server-Zone im internen Netzwerk, einer DMZ für den öffentlichen Webserver und das Internet reicht für kleinere Organisationen oft schon aus. Weitergehende Zonenkonzepte berücksichtigen beispielsweise den Schutzbedarf der Daten und Systeme, die Zugriffsprozesse, die Applikationsarchitektur und/oder physische und virtualisierte Systeme.

«In manchen Situationen ist die Flucht nach vorn angebracht»

Christoph Baumgartner

Ein vordefinierter und konsequent gelebter Change-Management-Prozess sichert das regelmässige Security Patching und den Systemwechsel bei von den Herstellern nicht mehr gepflegten Systemen. Die Aktivierung der Logging-Funktion auf Firewalls und kritischen Systemen und die regelmässige Auswertung der Einträge macht die Aktivitäten im Netzwerk nachvollziehbar. Dabei sind aber die einschlägigen gesetzlichen Auflagen zum Datenschutz zu berücksichtigen. Netzwerkkomponenten wie Intrusion-Prevention-Systeme (IPS) und Web Application Firewalls (WAF) bieten neben gängigen Firewalls zusätzlichen Schutz auf Netzwerk- und Applikationsebene. Mittels technischer Sicherheitsüberprüfungen, wie (Web-)Application Security Audits, Penetration Tests oder Ethical Hacking, wird die Infrastruktur systematisch, gründlich und möglichst realitätsnah auf Sicherheitslücken untersucht, bevor diese von einem Angreifer ausgenutzt werden können.

Erfolgreiche Hackerattacken können einer Organisation ernsthaften Schaden zufügen. Wer sich neben den klassischen Werkzeugen zusätzlich mit einem Zonenkonzept und entsprechenden Prozessen im Unternehmen schützt, kann das Risiko deutlich verringern und handelt im Ernstfall schneller und vor allem richtig. ←

Christoph Baumgartner ist CEO und Inhaber der auf Security Consulting und anspruchsvolle Security Audits spezialisierten OneConsult GmbH

Yves Kraft ist Senior Security Consultant im selben Unternehmen. Seine Spezialgebiete sind Security Audits, Netzwerk-Design und Systemhärtung
→ **www.oneconsult.com**