

Informationsschutz in Zeiten der elektronischen Kriegsführung

Kampf um die Unverwundbarkeit



Schwachstellen in Schutzmaßnahmen sind eine Realität, mit der wir uns arrangieren müssen. Kein System oder Einzelmaßnahme bietet einen hundertprozentigen Schutz. Daher müssen alle Bausteine der Sicherheitsarchitektur eines Unternehmens so miteinander verknüpft werden, dass etwaige Unzulänglichkeiten an einer Stelle durch eine andere Stelle kompensiert werden. Gerade beim Informationsschutz sieht die Realität jedoch meist anders aus. Das Thema wird häufig nur auf technischer Ebene angegangen und liegt daher in der alleinigen Verantwortung der IT-Abteilung. Dabei kann ein Schutz gegen die zunehmende Bedrohung durch Wirtschaftsspionage der ausländischen Nachrichtendienste nur durch eine interdisziplinäre Zusammenarbeit aller Unternehmensbereiche gewährleistet werden.

Die Risiken eines Know-how-Verlustes sind hoch, weil professionellen Angreifern oftmals nur unzureichende Sicherheitsvorkehrungen auf Firmenseite gegenüberstehen. Dies liegt zum einen an fehlendem Bewusstsein für das Bedrohungsszenario und zum anderen an ungenügender Fachkompetenz zur Abwehr vor gut geplanter Wirtschaftsspionage. Angeregt durch mehrere spektakuläre Angriffe auf bekannte Unternehmen der Informations-, Unterhaltungs- und Rüstungsindustrie in jüngerer Zeit,

über die in den Fachmedien der IT-Sicherheitsbranche ausführlich berichtet wurde, rücken in den Sicherheitsabteilungen vieler Unternehmen vermehrt die Themen Informationsdiebstahl und Wirtschaftsspionage in den Fokus. Das Gespenst des „Advanced Persistent Threat“ (kurz APT) geht um.

Dabei wird der Begriff in den Pressemitteilungen der betroffenen Unternehmen oft als Feigenblatt für alle möglichen Angriffe auf IT-Systeme der Unternehmen ge-

braucht, die im Grunde meist wenig mit der ursprünglichen Bedeutung des Begriffs gemein haben und sich eher durch Nachlässigkeiten in der Sicherheitsorganisation des betroffenen Unternehmens, denn durch ein besonders ausgefuchstes Vorgehen der Angreifer auszeichnen.

Der Begriff APT entstammt ursprünglich dem Militärbereich, wo er für die Aufrechterhaltung geheimdienstlicher Operationen und die Kriegsführung zur Informationsbeschaffung steht. Übertragen auf den Informationssicherheitsbereich kennzeichnet der Begriff Techniken und Vorgehensweisen, die einem Angreifer über einen längeren Zeitraum hinweg das Erheben und Entwerfen von sensiblen Informationen unterhalb des „Sicherheitsradars“ eines Unternehmens erlauben.

In seiner Kernaussage klassifiziert APT eine bestimmte Art von verdeckten Angriffen, bei denen von hochmotivierten Angreifern

ein langfristiges, konkretes Ziel verfolgt wird, welches vom jeweiligen Auftraggeber mit einem hohen Ressourcenaufwand gesponsert wird. Dabei kann es sich entweder um einen gezielten Informationsdiebstahl zur Erlangung von wirtschaftlichen, politischen oder strategischen Vorteilen handeln, oder um die Einrichtung einer dauerhaften „Präsenz“ in der Umgebung des Opfers zum Zweck eines dauerhaften Ausspionierens.

Als Beispiel für einen Angriff, den man Aufgrund des angewandten Vorgehens und der Ergebnisse als APT im ursprünglichen Sinn klassifizieren kann, ist das zweistufige Vorgehen der Angreifer beim Einbruch in die US-Rüstungskonzerne Lockheed Martin und Northrop Grumman. Hierbei wurden im ersten Schritt zuerst durch einen Einbruch bei der Sicherheitsfirma RSA die Seed Codes für alle bisher ausgestellten SecurID-Token der Firma entwendet. Mit Hilfe dieser Codes lassen sich „virtuelle Nachschlüssel“ für die physischen Token erstellen, welche von vielen Unternehmen im Rahmen einer Zwei-Faktor Authentisierung zur Absicherung von Systemzugängen verwendet werden.

Dass es sich bei den gestohlenen Informationen tatsächlich um diese Codes handelte, offenbarte sich jedoch erst einige Wochen später, da RSA zwar den Einbruch als solchen durch eine Kundenmitteilung bestätigte, jedoch darin nur vage Andeutungen zu den entwendeten Informationen machte. Zur Gewissheit wurde dies erst, als einige Wochen später unbekannte Angreifer versuchten, mit Hilfe der von RSA erbeuteten Informationen über die mit SecurID-Authentisierung geschützten Remote-Zugänge der beiden Rüstungsfirmen in deren interne Netze einzudringen. Der Angriff konnte laut Medienberichten nur im letzten Moment durch das Abschalten der Zugangssysteme abgewehrt werden.

Im Rahmen dieser Vorfälle wurde durch Beiträge im RSA-Blog bekannt, dass der Einbruch bei RSA mit Hilfe eines geschickt vorbereiteten Social Engineering Angriffs

eingeleitet wurde. Hierbei wurden einzelne Mitarbeiter per Email gezielt auf ein laufendes Recruiting-Programm angesprochen, mit der Bitte, sich das angefügte Excel-Dokument anzusehen. In diesem Dokument verborgen war Schadcode, der eine bis dahin unbekannte Schwachstelle im Adobe Flash Player ausnutzte. Von den Mitarbeitern unbemerkt wurde auf deren Rechnern ein Programm installiert, welches für die Angreifer fortan verdeckt als „Brückenkopf“ für den Zugriff auf die internen Netze der Firma diente. Von dort aus konnten sie sich über einen längeren Zeitraum über die Kompromittierung weiterer Systeme unbemerkt bis zu ihrem Ziel vorarbeiten.

Ähnliche Vorgehensweisen wurden in der jüngeren Vergangenheit schon bei vergleichbaren Fällen von Spionage - beispielsweise bei Google - beobachtet. Dabei gibt es einen gemeinsamen Aspekt, der bei jedem dieser Angriffe eine essentielle Rolle spielt: Die Zero-day Vulnerability, also die bis dahin unbekannte Schwachstelle in einem Programm oder System. Angreifer, deren Ziele im Bereich moderner und oft (vermeintlich) gut gesicherter Infrastrukturen liegen, sind auf einen konstanten Nachschub an neuen Informationen zu Schwachstellen angewiesen, die möglichst zuverlässig und verdeckt funktionieren und gleichzeitig in ihrem exklusiven Besitz sein sollten.

Neuer Markt für unbekannte Sicherheitslücken

Im Bereich der Schwachstellenanalyse hat sich daher im Laufe der letzten Jahre ein lukrativer und vielschichtiger Markt für neue, unbekannte Sicherheitslücken in Softwareprodukten entwickelt. Neben unabhängigen Forschern und spezialisierten Firmen wie beispielsweise Vupen bauen auch immer mehr „klassische“ Sicherheitsfirmen wie HBGary auf das Geschäft mit Schwachstellen. Dabei verfolgen die Akteure verschiedene Strategien, die sich grob in drei Bereiche gliedern lassen.

Auf der einen Seite gibt es den sogenannten „White Hat“ Bereich. Hier versuchen

Forscher, die von ihnen entdeckten Informationen über neue Schwachstellen entweder unentgeltlich oder gegen Bezahlung an die jeweiligen Produkthersteller zu verkaufen. Manche Hersteller wie Google oder Mozilla offerieren hierzu eigene „Bug Bounty“ Programme, die je nach Schweregrad der entdeckten Lücke gestaffelte Festbeträge zahlen. Andere Hersteller wie Adobe oder Oracle haben sich statt dessen zentralen Initiativen angeschlossen, beispielsweise der „Zero Day Initiative“ von Tipping Point oder dem „Vulnerability Contributor Program“ der iDefense Labs. Diese fungieren wie eine Art zentraler Einkauf und bieten ebenfalls nach Schweregrad gestaffelte Honorare für die Meldung unbekannter Schwachstellen. Alle Teilnehmer verpflichten sich dabei, dem Kredo der „verantwortungsvollen Veröffentlichung“, bei der eine Schwachstelle erst publik gemacht werden darf, nachdem der betroffene Hersteller diese über eine Aktualisierung seiner Produkte beheben konnte.

Das Gegenstück dazu bildet der „Black Hat“ Bereich, ein Schwarzmarkt für Sicherheitslücken. Hier kaufen Kriminelle entsprechende Informationen zu Schwachstellen, idealerweise mit fertigen Codebeispielen, die sie für gezielte Angriffe oder die Erweiterung ihrer Botnetze nutzen können. Der erzielbare Preis richtet sich hier vor allem nach zwei Aspekten: Die Zuverlässigkeit der Schwachstelle (funktioniert der Angriff bei jedem Versuch oder nur unter bestimmten Rahmenbedingungen) und deren Sichtbarkeit (ist eine Benutzerinteraktion erforderlich oder kann die Schwachstelle unbemerkt ausgenutzt werden). Die Anbahnung eines Verkaufs gestaltet sich in diesem Bereich schwieriger, weil es naturgemäß keinen öffentlichen Markt gibt. Stattdessen laufen die Geschäfte meist über persönliche Kontakte oder einschlägige Untergrund-Foren. Die erzielbaren Verkaufserlöse können hier ungleich höher liegen als im White Hat Bereich, unterliegen jedoch mangels öffentlicher Vergleichbarkeit starken Schwankungen.

Zwischen beiden Extremen liegt ein Graubereich, der von manchen Firmen recht offen, von anderen eher verdeckt bedient wird. Vupen etwa tritt hier sehr offen und aggressiv auf. Unter dem Label „Vupen Exploits for Offensive Security“ wird Kunden aus dem Strafverfolgungs- und Geheim-



Für Abonnenten ist dieser Artikel auch digital auf www.datakontext.com verfügbar



Weitere Artikel/News zum Schwerpunkt unter www.datakontext.com/sap



dienstbereich die Erstellung von „maßgeschneiderten, individuellen Lösungen“ für „offensive Missionen“ angeboten. Der Großteil der Anbieter geht dagegen lieber verdeckt vor, meist werden diesbezügliche Aktivitäten nur durch Zufall entdeckt. Beim Einbruch in den Webserver des US-Dienstleisters HBGary Federal Anfang dieses Jahres wurden beispielsweise unter den dabei entwendeten und später veröffentlichten Emails verschiedene diesbezügliche Informationen entdeckt. Im Rahmen eines Auftrags der Firma General Dynamics, einem US-Rüstungsunternehmen, wurden verschiedene Rootkits entwickelt, bei denen die Unterstützung des verdeckten Informationsdiebstahls im Vordergrund stand.

Behördliche Elite-Hacker

Auch europäische Unternehmen beteiligen sich unter dem Deckmantel der „Lawful Interception“, also Überwachungsmaßnahmen durch Behörden, mehr oder weniger offensichtlich an diesem lukrativen Geschäft. Im Rahmen der sogenannten „Amn Dawla Leaks“, in deren Verlauf verschiedene brisante Dokumente der ägyptischen Behörde für Staatsicherheit von Aktivisten im Internet veröffentlicht wurden, wurde auch ein Angebot der britischen Firma „Gamma International UK Limited“ an den ägyptischen Geheimdienst publik. Inhalt dieses Angebots war die Lieferung verschiedener Produkte zur Kommunikationsüberwachung und zum Einbruch in IT-Systeme - inklusive Vor-Ort Einweisung und Training in deren Anwendung. Das Unternehmen ist Teil der Gamma Firmengruppe,

mit der unter anderem auch die Münchner Elaman verbunden ist, die als Lizenznehmer der „Finfisher IT Intrusion“ Produktlinie mit dem Verkauf an europäische Behörden betraut ist.

Die Veröffentlichung der Angebotsunterlagen rief schnell ein reges öffentliches Interesse hervor. Selbst das rasche Einschalten mehrerer Anwaltskanzleien durch Elaman beziehungsweise deren Muttergesellschaft Gamma konnte nicht verhindern, dass verschiedene Medien (zum Beispiel der Spiegel und die Tagesschau) ausführlich darüber berichteten. Die Darstellung der angebotenen Produkte ist inzwischen von der Firmenwebseite verschwunden, der frühere Zustand der Webseite kann jedoch noch über verschiedene alternative Wege eingesehen werden.

Im Zuge der immer schnelleren Abfolge dieser „high profile“ Angriffe und des gesteigerten Medieninteresses werden auch ständig mehr Details über entsprechende Aufrüstungsmaßnahmen staatlicher Akteure bekannt. Während das chinesische Verteidigungsministerium vor kurzem erstmals im Rahmen eines Interviews mit der „Times“ öffentlich die Existenz einer Einheit von sogenannten „Elite-Hackern“ eingeräumt hat, wird auch bei anderen Staaten, allen voran in Amerika, aber zum Beispiel auch in Israel und dem Iran, fieberhaft am Aufbau entsprechender Einrichtungen gearbeitet. Von offizieller Seite her dienen diese natürlich nur der Abwehr von Angriffen der jeweiligen „Gegner“. Die be-

kannt gewordenen Indizien rund um die jüngsten Angriffe auf Unternehmen aus den Bereichen Wirtschaft, Informationstechnologie und Rüstung, vor allem zu deren vermuteten Ausgangspunkten, legen jedoch den Schluss nahe, dass einige Seiten hier durchaus auch nicht-militärische Ziele verfolgen.

Während staatliche Stellen sich hauptsächlich auf den Aufbau entsprechender Angriffsmittel konzentrieren, überlassen sie derzeit den Aufbau einer angemessenen Verteidigung weitestgehend den Unternehmen selbst. Während beispielsweise in den USA zumindest Planungen existieren, einzelne „kritische Unternehmen“ (etwa Energieversorger) in entsprechende Unterstützungsprogramme der Regierung aufzunehmen, gibt es in Deutschland diesbezüglich derzeit noch keine konkreten Pläne.

Um mit den Entwicklungen der staatlichen Behörden im offensiven Bereich Schritt halten zu können, müssen Wirtschaftsunternehmen mit ihren Maßnahmen auf der defensiven Seite ein vergleichbares Niveau erreichen. Der Informationsschutz darf nicht mehr als reines Thema der IT-Sicherheit angesehen werden, vor allem deswegen, weil technische und einzelne organisatorische Maßnahmen alleine nicht mehr ausreichend sind, um gegen diese neue Qualität der Angriffe einen ausreichenden Schutz zu bieten. Wichtig ist eine interdisziplinäre Zusammenarbeit aller sicherheitsrelevanten Unternehmensbereiche, um das Ziel der „Mehrschichtigen Sicherheit“ zu erreichen. ■



Martin Huber,
Leiter Netzwerk- und Clientsicherheit bei Corporate Trust Business Risk & Crisis Management GmbH