



Technischer Aktionismus reicht im Kampf gegen Cybergangster nicht mehr aus

Immer höhere Budgets für IT-Sicherheit belegen, dass die Sensibilität für die neuen Gefahren steigt. Doch während man sich vielerorts in «technischem Aktionismus» übt, sind im Kampf gegen die immer professionelleren Cybergangster umfassendere Massnahmen organisatorischer und strategischer Art vonnöten. Simon Zaugg

Cyberattacken gegen Weltkonzerne und staatliche Institutionen sind zur offensichtlichen Realität geworden. Spektakuläre Fälle wie Stuxnet oder der Sony-Datenklau haben die Verletzlichkeit selbst mächtigster Institutionen in schmerzhafter Weise zur Schau gestellt. Bei IT-Sicherheitsexperten setzt sich nicht zuletzt aufgrund der zunehmenden Grössendimension der Attacken eine ernüchternde Erkenntnis durch: «Wir müssen verstehen, dass die Cyberkriminellen sehr gut finanziert werden und hochprofessionell arbeiten», sagt Marco Marchesi, CEO der Sicherheitsfirma Ispin.

In der Schweiz bündelt man derzeit auf verschiedenen Ebenen die Kräfte. Einerseits arbeitet der Bund an einer Cyberdefense-Strategie. Man will das Schicksal in die eigenen Hände nehmen. «Es kann nicht sein, dass wir uns über ausländisches, schwer kontrollierbares Personal oder Firmen absichern müssen, um die wichtigsten Funktionen des Staates und unserer kritischen Infrastruktur zu schützen», heisst es im Anfang des Jahres

publizierten Strategiepapier. Andererseits zeichnet sich auch eine verstärkte Zusammenarbeit der IT-Sicherheitsverbände ab. Der jüngste Anlass war die Lancierung der Plattform Swisssecurity.org im Juli, die unter anderem Kollaborationstools und einen gemeinsamen Eventkalender enthält.

Neue Dimension erreicht

Die gravierenden Cyberattacken der letzten Monate sind indes keine Überraschung: Seit Jahren hat sich die Professionalisierung und Kommerzialisierung der Cybercrime-Szene abgezeichnet. Ein neuer Höhepunkt dieser Entwicklung war Anfang August ein Bericht des Anti-Viren-Spezialisten McAfee: Bei der «Operation Shady Rat» geht es um eine neue Dimension der Bedrohung, die Advanced Persistent Threat (APT), hinter der Unternehmen oder gar Staaten stehen und dessen Ziel Spionage oder Sabotageakte sind. Angreifer versuchen mit allen Mitteln für möglichst lange Zeit unerkannt zu bleiben und so viele Informationen wie möglich zu klauen. Beim aktuellen

Fall drangen Hacker über Jahre hinweg in die Datenbanken von insgesamt 72 Regierungen, Firmen und Organisationen ein.

Einen PR-Gau der Sonderklasse lieferte derzeit die US-Sicherheitsfirma HBGary Anfang 2011. Sie hatte sich erst damit gebrüstet, die Hintermänner der Hackergruppe Anonymous identifiziert zu haben. Dann schlugen die Web-Chaoten zurück und hackten die Website von HBGary und das Twitter-Konto von CEO Aaron Barr. Schliesslich stellten sie über 60 000 vertrauliche E-Mails auf die Filesharing-Plattform «The Pirate Bay». «Erschreckend niedrig» sei das Sicherheitsniveau bei HBGary laut einem Artikel des Fachmagazins C'T (Ausgabe 6/11) gewesen. So hätten offensichtliche SQL-Injection-Lücken auf der Website, einfach zu knackende Passwörter, die für viele Dienste erst noch parallel genutzt wurden, sowie ungepatchte Server den Angreifern die Arbeit erleichtert. Der Fall demonstriert eindrücklich, wie verletzlich Unternehmen und deren IT geworden sind.



Bildquelle: Fotolia

Neue Gegenstrategien nötig

Die Managementberater von Ernst & Young beschreiben in ihrer Broschüre «Cyberattacken entgegnetreten» vom vergangenen März die neue Ausgangslage für potenzielle Angriffopfer. Bei der Analyse von Cyberattacken müssten sich IT-Sicherheitspezialisten etwa nicht mehr nach dem Wie fragen, sondern vielmehr nach dem Was und dem Warum. Es gehe darum, den Angreifer zu verstehen und dann ausgefeilte Gegenstrategien zu entwickeln. Das schliesse den Schutz höchster Kader sowie Top-Spezialisten genauso mit ein wie einen gezielten Perimeter-Schutz bei Browsern, Computern und mobilen Geräten.

Für den IT-Sicherheitsexperten und Forensiker Dominique Alessandri (IBM) ist klar geworden, dass vielen Cyberkriminellen mit einfachen Methoden das Handwerk nicht mehr zu legen ist. Auch für die IT-Forensiker hat sich das Tätigkeitsgebiet deutlich verändert, die neuen Technologien erschweren das Arbeitsumfeld. Während sie sich traditionell auf die Sicherung von statischen Informationen, die auf physischen Speichermedien zu finden sind, konzentriert hatten, wird das Forschungsgebiet zusehends komplexer. «Im Hinblick auf den Cloud-Trend hat sich die IT-Forensik stark verändert und bezieht nun auch sogenannte dynamische Informationen wie den Arbeitsspeicher oder Netzwerkdaten mit ein», sagt Alessandri im Interview mit der Netzwoche (siehe Seite 21).

Für die Schweiz stammt die letzte Bilanz zur Cyberkriminalität der Melde- und Ana-

lysestelle Informationssicherung (Melani) vom April dieses Jahres. Demnach zielten die Cyberattacken im zweiten Halbjahr 2010 hierzulande vor allem auf die Verfügbarkeit von Websites oder deren Infektion durch Malware ab. Bei der Motivation sei hingegen eine Verschiebung von reinen Vandalenakten hin zu Racheakten, Konkurrenzschädigung oder politischer Motivation festzustellen. Die Qualität und die damit verbundenen Begleitschäden liessen laut Melani auch in der Schweiz aufhorchen, was sich beispielsweise mit den Attacken auf Schweizer Unternehmen im Zusammenhang mit Wikileaks zeigte. Auch die populären Smartphones dürften zunehmend zum Ziel von Attacken werden. Die zunehmende Verbreitung sowie die Speicherung sensibler Daten auf den Geräten machen diese zu immer attraktiveren Zielobjekten.

Sensibilität steigt

Währenddessen ist in den Chefetagen die Sensibilität für die neuen Gefahren gestiegen. Ein Indiz dafür sind steigende Budgets für IT-Sicherheit. Einer Anfang 2011 veröffentlichten Studie des Marktforschers MSM Research zufolge müssen zwar 66 Prozent der Schweizer CIOs in den kommenden zwei Jahren mit etwa gleich viel Geld für IT-Sicherheit auskommen. Immerhin jedes vierte Unternehmen rechnet jedoch mit einem bis zu 20 Prozent höheren Budget im Vergleich zu 2010. Auch Marchesi, der alljährlich den «ISPIN Security Radar» herausgibt, bestätigt den Trend zu höheren IT-Sicherheitsbudgets. «Insbesondere mittelgrosse Unternehmen

haben in den letzten gut vier Jahren signifikante Verbesserungen bei den Sicherheitsstandards erzielt.» Die Unterschiede zu den Big Players seien kleiner geworden. Das ist auch bitter nötig, denn die Professionalität der Angreifer schliesst verschiedene und bisweilen subtile Angriffsszenarien mit ein. Sind die Hürden bei einem Zielobjekt von der Grösse eines Weltkonzerns zu hoch, sehen sich Angreifer auch schon mal Unternehmen an, die mit dem Konzern zusammenarbeiten. «Dessen Lieferanten sind mögliche Sicherheitslücken, andererseits sind sehr innovative KMUs durchaus selbst mögliche Angriffsziele», gibt Reto C. Zbinden, CEO des Beratungsunternehmens Swiss Infosec, zu bedenken.

Mehr Gefahren auf der einen, gleich viele oder nur geringfügig mehr finanzielle Mittel auf der anderen Seite, um diese abzuwehren – das ist heute die Ausgangslage für CIOs und IT-Sicherheitsverantwortliche. Das führt dazu, dass sich diese neue Strategien ausdenken mussten. Risikomanagementberater Urs Fischer kennt eine solche. Er hat einen Trend in Richtung eines «qualitativen Risikomanagements» erkannt: «Im Gegensatz zu früher ergreift man nicht immer wieder neue Security-Massnahmen um jeden Preis, sondern stuft die Risiken ein.» Das führe aber auf der anderen Seite auch dazu, dass man bewusst bestimmte Risiken in Kauf nehmen müsse, so Fischer.

Die Rechnung «Schadensausmass mal Eintretenswahrscheinlichkeit» – also eine der Grundweisheiten des Risikomanage- ▶

Security Framework – das sichere Fundament Ihrer Security Organisation

- Mit dem Security Framework wird die Grundlage für ein einheitliches Sicherheitsmanagement innerhalb Ihres Unternehmens gelegt.



Experten raten wegen der zunehmend professionelleren Cyberattacken zu umfassenden Strategien zum Schutz der IT. Bildquelle: Swiss Infosec

► ments – reiche nicht mehr, sagte auch Uwe Müller-Gauss anlässlich des Fachevents Ito-day von Swisscom IT Services zum Thema Business Continuity Management (BCM) im Juni. Vielmehr sollten die Unternehmen laut Müller-Gauss mit gezielten Investitionen die Widerstandsfähigkeit bei den lebenswichtigen Kernprozessen erhöhen. Wie beim Menschen, bei dem das Herz, die Lunge und das Hirn überlebensnotwendig sind, müssten auch in Unternehmen die absolut kritischsten Prozesse identifiziert und sichergestellt werden.

Hohe technische Verletzlichkeit

Die lange Zeit gültige Devise nach möglichst 100-prozentiger IT-Sicherheit dürfte somit zur überflüssigen Floskel verkommen: Bisher delegierten Geschäftsleitungen die Verantwortung für die IT-Sicherheit an den CIO oder IT-Sicherheitsverantwortlichen. Wurden neue Risiken identifiziert, löste dieser das Problem nicht selten mit dem Einkauf einer neuen Sicherheitslösung. Für den Informationssicherheitsspezialisten Zbinden greift dieser «technische Aktionismus» jedoch zu kurz: «Es reicht nicht, nur Lösungen einzukaufen, wenn man das Darumherum vergisst. Das heisst, dass die Massnahmen beispielsweise mit Schulungen, der Awareness-Bildung oder Veränderungen in der Personalführung einhergehen sollten.»

Nicht nur auf der strategischen, sondern insbesondere auch auf der technischen Ebene müsste man stärker ansetzen, um die IT-Risiken einzudämmen, macht Thomas Dübendorfer, Präsident des IT-Sicherheits-

verbands ISSS im Interview mit der Netzwoche klar (siehe Seite 44). «Die heutigen Computersysteme sind viel zu komplex und zu offen vorkonfiguriert, als dass ein ungeschulter Benutzer die Systemsicherheit gewährleisten könnte.» Allerdings seien diese mit vielen Funktionen ausgestatteten Geräte heute ein Marktbedürfnis. Dennoch plädiert er für einfacher kontrollierbare Thin Clients. Das altbewährte Konzept – schlanke Endgeräte und alle komplexen Funktionalitäten auf Mainframes oder Servern – könnte, der Cloud sei Dank, in Zukunft womöglich wieder zum Modell werden, so Dübendorfer.

Zur hohen Komplexität kommt ein weiteres systemisches Problem dazu: Noch sind viele veraltete Systeme im Einsatz, die gar nie dafür konzipiert waren, ans Internet angeschlossen zu werden. Ein Beispiel sind SCADA-Systeme (Supervisory Control and Data Acquisition), die bei der Steuerung von Industrieanlagen zum Einsatz kommen und deren Schwachstellen die vielbeachtete Schadsoftware Stuxnet ausgenutzt hatte. «Es ist eine Tatsache, dass immer mehr SCADA, also speicherprogrammierbare Steuerungen, mit Leitsystemen kombiniert werden und dafür auch immer stärker das Internet zum Einsatz kommt», sagte IT-Sicherheitsexperte Markus Martinides anlässlich eines Medienanlasses des Sicherheitslösungsanbieters Norman Ende Mai. Derweil ist für Dübendorfer klar: «Die Betreiber müssten die Systeme eigentlich komplett erneuern, um auch sicherheitstechnisch auf dem neusten Stand zu bleiben. Das ist aber teuer.»

Zeichen der Zeit erkannt

Als ob das alles nicht schon genug wäre, kommen auch ständig neue Risiken hinzu. Social Media, Smartphones und die Cloud lassen grüssen. Für Risikomanagementberater Fischer ist ohnehin klar: «Neue Technologien werden das Sicherheitsdenken bei Unternehmen nachhaltig verändern. Sie brauchen eine klare Strategie, klare Richtlinien und Benutzungs-Policies.» Er empfiehlt Tools und Methoden wie Governance Frameworks, wie zum Beispiel Cobit und Risk IT. Insbesondere auch, um ein seiner Meinung nach weiteres gravierendes Problem der IT zu lösen: Das oft schwache Zusammenspiel zwischen Business und IT. Denn dieses führt laut Fischer auch zu neuen Sicherheitsproblemen, wie er anhand eines Beispiels erläutert: «Eine Marketing- oder Verkaufsabteilung kann irgendwo ihre Facebook-Sites machen, ohne dass die IT weiss, wie genau das Ganze gesichert ist.»

Trotz aller neuen Risiken sehen die von der Netzwoche befragten Experten die Schweiz insgesamt jedoch gut gerüstet für die Zukunft. Zwar seien die Finanzindustrie und innovative Weltkonzerne beispielsweise im Pharmabereich lukrative Angriffsziele. Doch die Sicherheitsstandards seien hierzulande um einiges höher als anderswo, was die Attraktivität eines Angriffs wiederum deutlich verringere. Zudem werde auch die Vernetzung unter den Akteuren der IT-Sicherheit immer besser. «Die Zusammenarbeit zwischen Experten von Bund sowie Unternehmen ist sehr gut», sagt Marchesi. <

«Vielen Cyberkriminellen ist mit einfachen Methoden das Handwerk nicht mehr zu legen»

Nach einer kriminellen Tat die Spuren zu untersuchen – das ist der Job der Forensiker. Das gilt auch für die IT und für Cybercrime. Derzeit verkompliziert sich deren Arbeit massgeblich, wie Dominique Alessandri, IT-Sicherheitsexperte und Forensiker bei IBM, im Gespräch mit der Netzwoche erläutert. Interview: Simon Zaugg

Herr Alessandri, was beschäftigt Sie im Moment am meisten im Zusammenhang mit dem Thema Cybercrime?

Vieles, was unter Cybercrime-Experten bisher Theorie war, ist Realität geworden beziehungsweise an die breite Öffentlichkeit gelangt. Die Anzahl und das Ausmass der uns bekannten Fälle der letzten 12 Monate ist erschreckend. Die Angreifer sind viel professioneller geworden und kommerziell ausgerichtet. Insbesondere haben auch Staaten erkannt, dass man die IT nutzen kann, um Organisationen und andere Staaten im Mark zu treffen. Es geht beispielsweise um kritische Infrastrukturen und Industriespionage. Viele Attacken werden dabei so ausgeführt, dass sie «unter dem Radar» bleiben und kaum je oder erst sehr spät entdeckt werden.

Was können Sie als IT-Forensiker dagegen tun?

Ein Forensiker untersucht das Geschehene, das heisst die Forensik ist reaktiv. Im Zusammenhang mit Cybercrime können dann basierend auf den gefunden Erkenntnissen proaktive Massnahmen ergriffen werden. Klar ist, dass vielen Cyberkriminellen mit einfachen Methoden das Handwerk nicht mehr zu legen ist. Der Aufwand der forensischen Analyse steigt entsprechend stark an.

Wer das Wort «Forensiker» hört, denkt mitunter an die klischeehafte Darstellung in Kriminalfilmen. Was steckt wirklich dahinter, insbesondere in der IT?

Die Forensik als solche ist eine naturwissenschaftliche Disziplin, in der man beispielsweise untersucht, wie jemand ums Leben gekommen ist. Anstatt um Haare und DNA-Spuren geht es in der IT jedoch um Bits und Bytes und dabei insbesondere um die Sicherung virtueller Spuren. Den Tatort zu sichern ist auch in der IT-Forensik eine wichtige Basis, um danach Daten untersuchen zu können.

Wie wird sich die IT-Forensik Ihrer Ansicht nach in den nächsten Jahren entwickeln?

Die IT-Forensik ist im Kontext der Kinderpornografie gross geworden. Dabei ging es in den meisten Fällen darum, eine überschaubare



Nicht zuletzt wegen der Cloud und der Smartphones dürfte Dominique Alessandri, IT-Sicherheitsexperte und Forensiker, die Arbeit kaum ausgehen.

Anzahl von Rechnern zu untersuchen. Durch die weitreichende Vernetzung sind forensische Untersuchungen entsprechend komplexer geworden. Stuxnet ist ein gutes Beispiel dafür, was eine Cyberattacke heutzutage alles beinhalten kann. Ein spezielles Augenmerk gilt auch der starken Verbreitung von mobilen Geräten, kombiniert mit den mittlerweile immer stärker verbreiteten Cloud-Services. Analog zur gesellschaftlichen Entwicklung eröffnet dies aus der Sicht der Forensik eine neue Dimension der Komplexität.

Welchen Stellenwert hat die Forensik innerhalb der IT-Sicherheit heute?

Das ist unterschiedlich und hängt stark vom Geschäftsfeld der jeweiligen Organisation ab. Bei weitem nicht alle Firmen betreiben ihre eigene Forensik. In einigen Firmen ist die Forensik ein Teil der Rechtsabteilung, bei anderen ist sie der IT angegliedert. Es gibt viele externe Anbieter, die IT-Forensik als Service anbieten.

Welche Branchen fragen diese besonders nach?

Mit Sicherheit gehören die Finanzbranche wie auch andere reglementierte Branchen dazu. Die IT-Forensik kann aus verschiedensten

Gründen zum Einsatz gelangen. Dazu gehören Szenarien wie Hacking, Wirtschaftskriminalität, Industriespionage. Mit der Grösse einer Firma wächst die Wahrscheinlichkeit von Angriffen und kriminellen Handlungen.

In Unternehmen wird ja derzeit intensiv darüber diskutiert, wie man mit Social Media umgehen soll.

Social Media haben für ein Unternehmen positive wie auch negative Seiten. Bevor auf der IT-Ebene Massnahmen ergriffen werden, sollte eine Strategie zum Umgang mit Social Media definiert werden. Gewisse Risiken, wie die Verbreitung von Malware, betreffen jedoch Nutzer von Social Media. Gegen solche Risiken existieren etablierte Mittel, jedoch verbleibt ein nicht zu unterschätzendes Restrisiko. Ein spezielles Augenmerk sollte auch auf die ausgetauschten Informationen gelegt werden. Social Media erlauben es Menschen, sich mit möglichst vielen anderen zu verknüpfen und sich untereinander auszutauschen. Die Informationen, die da ausgetauscht werden, betreffen in den wenigsten Fällen nur die Person selbst. Aus der Sicht der IT- und Informationssicherheit ist dies gewissermassen ein «soziales Problem». So spielen Social Media unter anderem dem Social Engineering in die Hände.

Wie beurteilen Sie aus forensischer Sicht die Auswirkungen des Cloud-Trends?

Die IT-Forensik hat sich traditionell stark auf die Sicherung von statischen Informationen, die auf physischen Speichermedien zu finden sind, konzentriert. Dies hat sich nicht zuletzt im Hinblick auf den Cloud-Trend stark verändert und bezieht nun auch sogenannte dynamische Informationen wie den Arbeitsspeicher oder Netzwerkdaten mit ein. Bei Cloud-Services stellt sich denn auch die Frage nach den relevanten Daten und wo diese zu finden und zu sichern sind. Dies hängt stark von der eingesetzten Technologie und den Betriebsprozessen ab. Was die IT-Forensik betrifft, wird die Cloud sicherlich noch einige Innovationen auf der technologischen, wie auch auf der Ebene der Methoden erfordern und hervorbringen. <