Das geht Unternehmen etwas an

Cyber-Kriminalität auf dem Vormarsch

von Andreas Wisler

Aktuell können wir in jeder Tageszeitung über Datenskandale und Cyberangriffe von Geheimdiensten lesen. Nicht wenige Unternehmensverantwortliche wagen die These, dass sie davon nicht betroffenen sind. Diese hält der Realität jedoch nicht stand.

Die vergangenen Wochen haben gezeigt, dass die Überwachung von Regierungen schon länger Tatsache ist. Im grossen Stil wurden (und werden) Regierungen, Firmen, aber auch Bürgerinnen und Bürger überwacht. Auch in der Schweiz ist die Cyber-Kriminalität auf dem Vormarsch. Die Melde- und Analysestelle MELANI des Bundes zeigt in ihren halbjährlichen Lageberichten, dass die Schweiz immer mehr ins Visier von Kriminellen kommt. Der Bundesrat hat daher reagiert und am 27. Juni 2012 die «Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken» verabschiedet. Mit dieser Strategie will der Bundesrat in Zusammenarbeit mit Behörden, Wirtschaft und den Betreibern gefährdeter Infrastrukturen die Cyber-Risiken minimieren, welchen sie täglich ausgesetzt sind.

Informationen sind Geld

Aber auch «normale» Firmen sind davon betroffen. Die Schweiz gilt nicht umsonst als ein sehr innovatives Land mit guten Ideen und weltweit den meisten neu angemeldeten Patenten. Mit Ideen und Erfindungen lässt sich viel Geld verdienen. Zudem sind die technischen Infrastrukturen von kleineren Unternehmen im Normalfall nicht so gut geschützt wie bei Firmen mit eigenen IT-Abteilungen. Oft heisst es «an meinen Daten hat niemand Interesse» oder «wir sind ja keine Bank». Doch beide Aussagen sind heutzutage falsch. Daten und Informationen bedeuten Geld. Eine geschickte Verknüpfung von verschiedenen Informationsquellen und das Profil für einen Menschen sind schnell erstellt. Ein Beispiel dafür ist die Suchmaschine von Google. Die Suchresultate werden im Lauf der Zeit immer besser den persönlichen Vorlieben angepasst und damit die freie Meinungsbildung beeinflusst. Nicht vergessen werden darf, dass diese Angaben «freiwillig» zur Verfügung gestellt werden, wie dies auch bei den verschiedenen Kundenkarten der Fall ist. Auch hier wird ein Profil erstellt und personalisierte Werbung verschickt.

Auf der anderen Seite sind die Informationen, die nicht freiwillig oder bewusst preisgegeben werden. Eine Methode an solche Informationen zu gelangen ist Phishing. Der Halbjahresbericht 2012.2 von MELANI zeigt, dass die Schweiz auch hier im Visier der Cyber-Verbrecher steht. Beim klassischen Phishing per E-Mail wird versucht, das Opfer auf eine manipulierte Seite zu locken, auf welcher persönliche Daten abgefragt werden. Oft sehen diese Seiten einem Original täuschend ähnlich und es ist schwierig zu erkennen, wo sich der Nutzer effektiv befindet. Beliebt sind dabei Abfragen nach Kreditkarteninformationen. Obwohl sehr viel über Phishing und den zugehörigen Methoden berichtet wird, ist es erstaunlich, wie erfolgreich solche Angriffe immer noch sind. Bei unseren gezielten Phishing-Angriffen, selbstverständlich in Absprache mit unserem Kunden, ist die Erfolgsrate sehr hoch, oft zwischen 50 bis 70 Prozent der angeschriebenen Personen fallen auf den Angriff herein.

Perfide Kombinationen

Das klassische Phishing wird aber vermehrt mit anderen Methoden kombiniert. Ende 2012 waren Schweizer E-Banking-Kunden Angriffsziel eines so genannten Voice-Phishing. Dabei werden Phishing-E-Mails verschickt, mit dem Hinweis, dass ein neues Sicherheitssystem installiert wurde und sich ein Bankmitarbeiter telefonisch melden werde. Dazu müsse nur die Telefonnummer angegeben werden. Anschliessend werden die Opfer tatsächlich von den Betrügern angerufen. Aus «Sicherheitsgründen» muss nun das Login inklusive dem zweiten Merkmal (SMS, Token) angegeben werden. Wie MELANI zeigt, erfolgen die Anrufe sehr professionell und teilweise sogar auf Schweizerdeutsch. Daher gilt auch hier, sehr vorsichtig zu sein und nie persönliche Angaben weiterzugeben. Wie bereits erwähnt, sind aber auch Firmen direkt ein Angriffsziel. Dabei über eine Firewall und ein Antivirenprogramm zu verfügen, reicht nicht mehr aus. Verschiedene Tools sind auf dem Markt verfügbar, mit welchen innert weniger Minuten eine Schadsoftware (Malware) erstellt werden kann, die von heutigen Antivirenprogrammen nicht erkannt wird. Gelangt es einem Verbrecher diese in eine Firma einzuschleusen, sind keine Hindernisse mehr vorhanden und er kann sich im Netzwerk frei bewegen und nach interessanten Daten suchen. Um diese Hürde so hoch wie möglich zu setzen, ist es wichtig, die Systeme, das heisst das Betriebssystem und die installierten Programme, immer auf einem aktuellsten Stand zu halten. Auch hier gilt es, E-Mails genau anzuschauen, bevor ein mitgeschicktes Programm ausgeführt wird. Auch der vermeintlich gewonnene USB-Sticks gilt es erst nach einer genauen Prüfung mit dem Computer zu verbinden.

Verschiedene Statistiken zeigen, auch Schweizer Firmen und Personen sind ins Visier der Cyber-Kriminellen geraten. Mit der notwendigen Vor- und Umsicht ist es aber möglich, die Sicherheitshürde so hoch wie möglich anzusetzen. Aktuelle Systeme und gesunde Skepsis helfen, nicht selber Opfer eines (erfolgreichen) Angriffs zu werden. ■

Andreas Wisler

ist IT-Spezialist bei GO OUT Production GmbH, welche sich mit umfassenden Security-Audits, Penetration-Tests und Sicherheitsberatungen auseinandersetzt.

Geschickte Verknüpfung von Informationsquellen ist das Mittel.