Die bösen Jungs im Dienst der guten Sache: Ethical Hacking.

Hackerangriffe – Tendenz steigend

Ethical Hacking deckt Schwachstellen auf

von Franco Cerminara

Schweizer KMU sind im internationalen Vergleich besonders innovativ, die Dichte an technologisch führenden Unternehmen ist hierzulande überdurchschnittlich gross. Ihr Know-how ist denn auch gutes Geld wert. Damit ein böswillig motivierter Angriff möglichst vermieden wird, können mittels Beauftragung eines «ethischen Hackers» gezielt Schwachstellen ausgelotet und entsprechende Gegenmassnahmen getroffen werden.

Heute muss man kein Computerexperte mehr sein, um sich als Hacker betätigen zu können. Unzählige Websites informieren derzeit umfassend zum besagten Thema, und entsprechende Download-Programme machen diese Tätigkeit zur einfachen Angelegenheit. Leicht zugängliche Hacker-Tools haben den Datendieben neue Türen geöffnet. Befanden sich unter den «Hackern» der ersten Stunde noch Persönlichkeiten wie Steve Wozniak, und Linus Torvalds, welche heute die bedeutendsten Computerunternehmen repräsentieren, sind es heute vor allem kriminelle Personen. Die Hacker der Anfangszeit interessierten sich noch leidenschaftlich für Technologie und wollten diese geistig durchdringen und Programme an die Grenzen ihrer Leistungsfähigkeit zu bringen. Deren Ziele unterscheiden sich denn auch grundlegend von denen der heutigen Generation. Die Motive sind heute mehr und mehr durch Profit und finanziellen Vorteilen, Rache oder Böswilligkeit determiniert.

Wenig Vertrauen in die eigene Sicherheit

Die mit der Führung von KMU betrauten Personen sind sehr stark ins operative Tagesgeschäft eingebunden, zudem verfügen sie häufig über mangelndes oder zu wenig aktuelles Wissen in Informationssicherheitsfragen. Zusätzlich ist vielfach auch kein Budget vorhanden, um Experten anzustellen und somit werden Sicherheitsfragen an die IT-Abteilung delegiert. Diese ist vielfach auch mit Ressourcenproblemen konfrontiert, somit werden oft nur mangelhafte Sicherheitsvorkehrungen getroffen. Oftmals fehlt auch das Know-How, wie die implementierte Sicherheitslösung überhaupt funktioniert und ob sie dies lückenlos tut. Da verwundert es nicht, dass bei den Firmenverantwortlichen ein schlechtes Gefühl bleibt und man der Überzeugung ist, zu wenig für die Informationssicherheit getan zu haben. Wie recht sie haben, zeigen die aktuellen Zahlen auf: Gemäss der Schweizerischen Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBIK wurden hierzulande im Jahr 2013 rund 9200 Meldungen zu gezielten Angriffen auf IT-Systeme von Unternehmen abgegeben, was verglichen zum Vorjahr einem Anstieg von 11 Prozent entspricht

Aus Fehlern lernen

Hackerangriffe und Phishing-Attacken werden von KMU-Führungskräften also aus gutem Grund besonders gefürchtet. Die Angreifer drohen ihnen immer ein paar Schritte voraus zu sein. Grundsätzlich gibt es verschiedene Wege, um in ein «Betriebssystem» sprich Netzwerk eines Unternehmens einzudringen, um dort eine im Hintergrund agierende Schadsoftware zu platzieren; beispielsweise via Mail- oder Webserver. Üblicherweise läuft eine Infektion immer nach den gleichen Schemata ab. Bei fast all diesen Trojanern ist das Zutun eines Anwenders für eine Aktivierung erforderlich. Das heisst, die Programmdatei muss manuell gestartet werden, um gefährlich zu werden. Grundsätzlich gilt: Hacker werden immer skrupelloser und verfügen gleichzeitig über immer hoch entwickeltere Tools. Diese ermöglichen ihnen immer bessere Zugriffsmöglichkeiten auf Unternehmensnetzwerke.

Ethical Hacking in der Praxis

Um dies zu unterbinden und allfällige Lecks zu stopfen, werden vermehrt ethische Hacker engagiert. Solche beschäftigt mein Haus, das Zuger Informationssicherheitsunternehmen InfoGurad AG, welches jüngst von sich reden machte, als es drei Bundesparlamentariern deren IT-Lücken publikumswirksam vor Augen führte. Aber auch immer mehr Unternehmer machen von diesem Angebot Gebrauch. Grundsätzlich hat das Ethical Hacking zum Ziel, Schäden durch semiprofessionelles Verhalten von Mitarbeitern und löchrige Infrastrukturen abzuwenden. Ein «gutes» Eindringen in IT-Systeme und ein Ausloten von Schwachstellen zählt zu den sinnvollsten Services, die man sich als Unternehmen angedeihen lassen kann. In Umkehrung des Märchens dringt – einem Schaf im Wolfspelz gleich – ein gut gesinnter Hacker in ein Unternehmens-Netzwerk ein und erkennt sofort, wo noch Sicherheitsprobleme bestehen und Löcher gestopft werden müssen. Im Gegensatz zu kriminellen Hackern nutzen «gute» Hacker die gefundenen Schwachstellen nicht aus, sondern helfen den Unternehmen, ihre Sicherheit zu verbessern. ■

Sicherheitslücken werden aufgedeckt

InfoGuard-Sicherheitsanalysten umgehen gezielt die Sicherheitsvorkehrungen in Unternehmen und testen so, wie gut diese Massnahmen hochentwickelte Angriffe abwehren. Es werden diejenigen Angriffsarten simuliert, die auch die Cyber-Kriminellen, einsetzen. Das Ziel der Penetration Tests ist dabei, potentielle Eintrittspunkte in das Unternehmensnetzwerk aufzudecken und die Mitarbeiter gegen die raffinierten Tricks der Hacker zu sensibilisieren. Das Ethical Hacking mittels eines Penetration Tests und dessen Auswertung nützt den KMU in vielerlei Hinsicht:

- Der Zustand der IT-Infrastruktur eines Unternehmens wird kritisch durchleuchtet und Schwachstellen werden gezielt gesucht und gefunden. Das gibt den Unternehmen Gelegenheit, ihre Sicherheitslücken gezielt zu stopfen.
- Mängel in Sicherheitskonzepten, Systemen und Anwendungen werden aufgedeckt.
- Fehler in der Organisationsstruktur kommen ans Tageslicht.
- Der Test legt offen, welche Sicherheitsmassnahmen noch getroffen werden müssen, um Integrität, Vertraulichkeit und Verfügbarkeit von Daten und System zu erhöhen.
- Die Awareness gegenüber Phishing-Attacken und Social Engineering wird bei den Mitarbeitern nochmals erhöht.
- Selbst bei wiederholtem Testing stehen sich Kosten und Nutzen immer noch in einem positiveren Verhältnis gegenüber, als wenn ein eigener Informationssicherheitsverantwortlicher im Unternehmen beschäftigt würde.

Mängel in Sicherheitskonzepten und -lücken entdecken.

Franco Cerminara

ist Head of Consulting bei der InfoGuard AG.

www.infoguard.ch

Nicht-Betroffenheitsitis noch weit verbreitet – ein gefährlicher Irrtum!

von Franco Cerminara

Datenklau, Betriebsspionage, Hacking und NSA-Skandal: Längst haben wir uns an die Schlagzeilen zu diesen Schreckensszenarien gewöhnt und klicken gelangweilt zur nächsten Nachricht. «Davon betroffen sind ja sowieso nur börsendotierte Grossunternehmen – warum sollte mein kleines Unternehmen Schaden nehmen – ich schlüpfe unter dem Radar durch», denkt sich manch ein Geschäftsführer eines KMU. Das ist aber falsch.

Schweizer KMU machen über 90 Prozent der Unternehmen hierzulande aus und sie gelten im europäischen Umfeld als sehr innovativ. Warum also sollte die Betriebsspionage vor ihnen Halt machen. Studien des Beratungsunternehmens PricewaterhouseCoopers AG PWC belegen jedoch, dass kleine und mittlere Unternehmen auf Hackerangriffe, Datendiebstahl und andere Formen der Cyber-Kriminalität nur unzureichend vorbereitet sind.[1]) Was wir bestätigen können: Wie wir aus unserer täglichen Arbeit feststellen, sind es zwei Schwachstellen, durch welche Kriminelle hauptsächlich ihren Weg in ein Unternehmensnetzwerk finden, um dort entweder ein Optimum an Daten zu entwenden oder ein Maximum an Schaden anzurichten. Gefahrenquelle Nummer 1 ist und bleibt der Mensch – der mittels Phishing-Attacken, Social Engineering, dem leichtfertigen Preisgeben von Interna auf Social Media oder dem Auspionieren am Telefon vielfach elegant umdribbelt und dann aufs Kreuz gelegt wird.

Eine weitere Gefahr lauert im BYOD-Trend: Die zunehmende betriebliche Nutzung privater Endgeräte und der externe Zugriff auf die Unternehmens-IT via Smartphone und Tablet birgt enorme Sicherheitsrisiken. Konnte ein Angreifer einmal die Hürden knacken und in ein Netzwerk eindringen, befindet er sich im Paradies. Vielfach sind die Hierarchien im Netzwerk so flach, dass die Informationen einfach abgesogen werden könnten. Bei den geschäftskritischen IT-Sicherheitsprozessen – dem Umgang mit Sicherheitsvorfällen, dem Notfallmanagement und der Bewertung der Gefahrenbereiche – zeigen sich bei den KMU ebenfalls deutliche Schwächen.

Jedes fünfte Unternehmen war laut PWC-Studie schon mindestens einmal Ziel einer Cyber-Attacke. Allerdings kann mehr als die Hälfte der Betroffenen (58 Prozent) nicht genau angeben, welche Bereiche beziehungsweise Daten angegriffen wurden und welche Folgen dies hatte. Es ist davon auszugehen, dass etliche Attacken von den Unternehmen gar nicht bemerkt werden, weil erforderliche Monitoring- und Kontrollverfahren fehlen. Und was viele Unternehmer nicht wissen: Sie können rechtlich belangt werden, wenn Daten ihrer Mitarbeiter von Hackern ausspioniert werden. Das gilt als Verstoss gegen das Datenschutzgesetz.

Gelegenheit schafft Diebe gilt auch beim Datenklau bei KMU. Aber resignieren Sie nicht. Sie können durch Sicherheitsmassnahmen eine erfolgreiche Attacke in eine nicht mehr lohnenswerte verwandeln. Zu Ihrem Schutz empfehlen wir Ihnen folgende Massnahmen:

- *Schulung: Regelmässige Weiterbildung der Mitarbeiter in IT-Sicherheitsfragen und Aufklärung über die neusten Trends im Bereich Phishing, Social Engineering und Social Media Attacken.*
- *Dreistufiges Login-Verfahren: Nur User-Identifikation und Passwort reichen für ein Login in ein Unternehmensnetzwerk nicht, es braucht noch ein Token oder SMS mit zusätzlicher Identifikation.*
- *Sicherheitssysteme aktualisieren und auf ihre Wirksamkeit überprüfen, beispielsweise mittels Ethical Hacking, respektive Penetration Tests.*
- *Sicherheitskonzept für BOYD-Thematik: Reglementierter Umgang mit den Mitarbeiter eigenen Geräten, beispielsweise sollen sie ein gesondertes WLAN benutzen und verlangen Sie spezifische Authentifizierungsmechanismen.*
- *Melden von sicherheitsrelevanten Vorfällen: Scheuen Sie sich nicht, wenn Sie bemerken, dass Sie gehackt wurden. Melden Sie es der Melde- und Analysestelle des Bundes, damit diese Muster erkennen und frühzeitig wieder warnen können.*
- *Definition eines IT-Sicherheitsprozesses nach ISO 27001 auf der Basis einer entsprechenden Risikobewertung.*

Quelle
1) Pricewaterhouse Coopers AG: Disclose Dezember 2013.

Franco Cerminara

ist Head of Consulting bei der InfoGurad AG.

www.infoguard.ch