

„Größter Risikofaktor ist in vielen Fällen der Mensch“

Hacker-Angriffe: Interview mit Sebastian Feld vom Institut für Internet-Sicherheit an der Fachhochschule Gelsenkirchen

Auf Veranstaltungen, die Sie Live-Hacking-Vorfürungen nennen, weisen Sie anschaulich auf IT-Risiken hin. Wie reagieren Unternehmer auf die gezeigten Bedrohungsszenarien?

Im Allgemeinen sind sie „baff“. Sie sind oft erstaunt, was alles möglich ist, wie schnell und einfach ein Hacker Angriffe durchführt. Vielen im Publikum werden die Konsequenzen von verschiedenen Vorfällen zum ersten Mal klar. Eine typische Reaktion lautet: „Natürlich habe ich schon so oft gehört, dass ein Passwort lang und kryptisch sein soll, aber jetzt erst verstehe ich es.“

Apropos Passwörter: Die Algorithmen und Rechnerleistungen zum Knacken werden immer leistungsfähiger. Was zeichnet ein sicheres Passwort im Jahr 2011 aus?

Wenn ein Dokument oder ein Dienst durch ein Passwort geschützt wird, so empfehlen wir mittlerweile mindestens zwölf Stellen, besser 14. Die Zeichen sollten aus Groß- und Kleinbuchstaben bestehen, sowie aus Ziffern und Sonderzeichen. Ein gutes Beispiel ist „lbgg123F,da\$ggs!“. Sieht kompliziert aus, ist es auch. Aber es ist gut merkbar. Denn ich habe mir einfach einen Satz ausgedacht und nehme daraus die Anfangsbuchstaben und Satzzeichen, außerdem habe ich an einer Stelle einen Buchstaben durch ein Sonderzeichen ersetzt: „Ich beantworte gerade gefühlte 123 Fragen, die aber \$ehr gut gestellt sind!“

Was halten Sie von zentralen Passwortspeichern, die mit einem Masterpasswort die restlichen verwalten?

Grundsätzlich empfehlen wir solche „Passwortsafes“. Enorm wichtig ist aber ein sehr gutes Masterpasswort.

Der Anstieg der Sicherheit im Vergleich zu einem schlechten Passwort, was womöglich noch mehrfach genutzt wird, ist sehr hoch. Andererseits sagen wir auch, dass wichtige Passwörter im Kopf gespeichert werden sollten. Wir sagen beispielsweise, dass das Passwort für alles, was mit Geld zu tun hat – etwa Online-Banking oder Amazon –, besser nicht der Technik anvertraut werden sollte. Denn man kann nie sicher sein, ob der Rechner, auf dem man den Safe öffnet, wirklich sauber ist.

Mit einer präparierten USB-Maus ist es Sicherheitsforschern jüngst gelungen, Schadsoftware in ein >>

Zur Person

Sebastian Feld ist wissenschaftlicher Mitarbeiter des Instituts für Internet-Sicherheit. Er schloss sein Studium der Angewandten Informatik an der Fachhochschule Gelsenkirchen im Jahr 2010 mit einem Master ab. Derzeit beschäftigt er sich mit der Generierung von Kennzahlen für das Internet, Identity Management (und insbesondere dem neuen Personalausweis), Web-Service-Sicherheit, Intrusion Detection, Awareness Performance und Penetrationstests.



Firmennetz einzuschleusen. Ein Mitarbeiter hatte das Gerät als Werbegeschenk erhalten und im Büro angeschlossen. Wie funktioniert so ein Angriff technisch?

In eine normale Computermaus wurde ein Micro-Controller eingebaut, der so programmiert war, dass er ein bestimmtes Programm ausführt, sobald er Strom bekommt, die Maus also angeschlossen wird. Dieses Programm hat dann den eigentlichen Schadcode aus dem Internet geladen und ausgeführt. Auf dem angegriffenen Rechner war sogar ein Anti-Viren-Programm installiert, doch es wurde meines Wissens eine sehr „junge“ Schwachstelle ausgenutzt, sodass der Basischutz nicht angeschlagen hat.

Wie lässt sich die Bedrohung speziell durch ein USB-Gerät abwehren?

Angriffe mittels Autostart-Funktion sind mittlerweile bekannt. Eine neue Dimension kommt nun durch verschiedene USB-Geräte hinzu, die sich nicht als Speichermedium melden, sondern beispielsweise als Maus oder Tastatur. Im Unternehmen wird oft das sogenannte „Schnittstellenmanagement“ genutzt. Hierbei wird jede Schnittstelle im Rechner – wie CD-Rom-Laufwerk oder USB-Port – deaktiviert. Oder es wird definiert, dass lediglich Geräte mit bestimmten Seriennummern genutzt werden dürfen.

Ist die „Trojaner-Maus“ nur ein extremes Beispiel oder steht grundsätzlich jedes USB-Gerät unter Generalverdacht?

Beides. Diese Trojanermaus war schon neuartig. Aber wie so oft, war es einfach nur der erste Angriff, dieser kann nun verfeinert werden und „gebräuchlich“ werden. Aus diesem Grund kann man sagen, dass jedes Medium unter Generalverdacht steht. Aber wie schon erwähnt: Die Trojanermaus-Angreifer haben eine Schwachstelle ausgenutzt, die entweder sehr jung war oder noch nicht bekannt. Das ist dann kein Werk mehr von 16-jährigen, gelangweilten „Hackern“.

Neben manipulierter Hardware spielen bei Hacker-Angriffen immer wieder auch E-Mails eine Rolle, die Kriminelle sogar gezielt an Mitarbeiter senden. Wie kann ich sicher sein, dass der Absender nicht gefälscht ist?

Diese Frage ist sehr schwierig bzw. sehr technisch zu beantworten. Technisch kann man natürlich schauen, ob der einliefernde Mail-Server auch zur entsprechenden Domain gehört. Sprich, ob der Bote/Kurier, der mir den Brief eigenhändig gibt, wirklich der Angestellte desjenigen ist, der mir einen Brief schreibt. Aber auch das ist nicht hundertprozentig wasserdicht. Im Unternehmensumfeld würde ich die Verantwortung

vom Anwender auf die IT-Abteilung verlagern. Diese sollte sicherstellen, dass über die eingesetzten Mailserver kein Missbrauch stattfinden kann. Wenn aber ein Angreifer in das Postfach des Chefs gelangt und in dessen Namen eine E-Mail verschickt – ist diese Mail dann gefälscht?

Wie sollte man mit E-Mail-Anhängen wie PDF- oder Excel-Dateien umgehen, die ja durchaus üblich sind?

Anhänge sollten Sie nur öffnen, wenn Sie sich sicher sind, dass Sie den Absender kennen und wenn Sie den Anhang erwarten – oder wenn es Sinn macht, dass Sie etwas geschickt bekommen. Den weiteren Verlauf sollte eigentlich der installierte und per Updates auf dem aktuellen Stand gehaltene Basisschutz erledigen, also eine Anti-Viren-Software und eine Personal-Firewall.

Links in einer Mail anzuklicken, ist unter Sicherheitsaspekten nie eine gute Idee?

In E-Mail-Clients kann man schauen, wo mich ein Link hinführt. Ein Link besteht ja aus zwei Teilen: dem verlinkten Text – zum Beispiel „finden Sie hier“ – und der eigentlichen Zieladresse. Diese sollte ich überprüfen, bevor ich auf den Link klicke. Problematisch wird es bei den heute viel genutzten Link-Verkürzungsdiensten wie „bit.ly“. Da kann man nicht vorab erkennen, wo der Link hinführt. Links von Fremden bitte grundsätzlich nicht anklicken, aus folgendem Grund: Die Angreifer schicken an jede mögliche Adresse eine Mail und wollen schauen, welcher Account aktiv ist. Wenn ich nun auf diesen Link klicke, der in gewisser Weise präpariert ist, dann merkt der Angreifer das und weiß, dass dieser Account aktiv ist – und zum Beispiel noch mehr Spam-Mails empfangen kann.

Welche Bedeutung haben für Hacker Sicherheitslücken im Betriebssystem oder in Anwendungssoftware?

Sicherheitslücken sind die bevorzugte Eingangstür für einen Angreifer in ein System. Man kann natürlich die Zugangsdaten eines Anwenders erraten oder knacken, aber eine Sicherheitslücke ist da „bequemer“. Software wird von Menschen gemacht – und Menschen machen Fehler. Diese Fehler lassen verschiedene Aktionen zu, die so nicht gedacht sind. Programm-Updates bieten neue Funktionalität, aber auch den Vorteil, dass Sicherheitslücken geschlossen werden. Aus diesem Grund ist es enorm wichtig, Updates zeitnah einzuspielen.

Mit der zunehmenden mobilen Internetnutzung wird auch der Mobilfunk für Hacker interessant.



Welche Bedrohungen lauern in diesem Bereich?

Wir erleben gerade eine Art Déjà-vu im Bereich der mobilen Endgeräte. Ein Handy ist kein Mobiltelefon mehr, sondern ein Smartphone, ein kleiner Computer. Alles, was wir auf einem Desktop-PC kennen, haben wir jetzt auch auf den mobilen Geräten – oder werden wir bald haben: Festplattenverschlüsselung zum Schutz der Informationen bei Diebstahl und Verlust, Zugriffsschutz per PIN, ähnlich dem kennwortgeschützten Bildschirmschoner am PC, Anti-Viren-Software, Betriebssystem-Updates ... Bei den mobilen Endgeräten scheint die Sensibilisierung allerdings noch weniger vorhanden zu sein als bei „starrten“ Geräten. Man installiert eine App, bei der man Klopapier abrollen muss, und gibt gleichzeitig den Zugriff auf das Adressbuch frei. Das macht keinen Sinn!

Wie schütze ich mich vor Missbrauch?

Insbesondere im Geschäftsumfeld sind die Daten auf meinem Smartphone schützenswert. Ich sollte da Gerät auf keinen Fall unbeaufsichtigt lassen. Ich sollte einen Zugriffsschutz verwenden, als PIN oder Muster, immer alle Updates einspielen, nur Software aus seriösen Quellen installieren, keine ominösen Links anklicken und keine fragwürdigen Webseiten besuchen. Es gilt eben alles das, was man auch von der „normalen IT“ her kennt.

Bleibt letztlich der Mensch der größte Risikofaktor für gut geschützte Firmennetzwerke?

Eine Kette ist so stark wie ihr schwächstes Glied. Und in vielen Fällen ist tatsächlich der Mensch der größte Risikofaktor. Stichwort Social Engineering: Einer mit Akten vollbeladenen jungen Dame halte ich die Tür auf, obwohl wir eine Zugangsschleuse haben – das kann schon ein Angriff sein. Oder Redseligkeit, Höflichkeit, Hilfsbereitschaft. Alles das kann ausgenutzt, aber schwer durch Technik geschützt werden. Hier hilft nur Sensibilisierung.

Was raten Sie, um im Umgang mit IT nicht allzu paranoid zu werden?

Ich rate immer dazu, dass man das mit der „realen Welt“ vergleichen soll. Klar kann ich auf der Autobahn sehr leicht den Tod finden. Oder als Fußgänger im Straßenverkehr. Aber man darf sich von so etwas nicht abschrecken lassen und sollte sich nicht verstecken. Um wieder zurückzukommen zur IT: Wie auch mit dem Immunsystem ist man mit einem Basisschutz vor vielen Angriffen geschützt.



*Die Fragen stellte Michael Milewski.
Kontakt: milewski@gestaltmanufaktur.de*

Creditreform

■ Das Unternehmernmagazin aus der Verlagsgruppe Handelsblatt ■

*Der Inhalt dieser PDF-Datei ist ein Zusatzbeitrag des Unternehmernmagazins „Creditreform“ aus dem Fachverlag der Verlagsgruppe Handelsblatt, Ausgabe 09/11.
Alle Rechte vorbehalten.*

© Copyright 2011
www.creditreform-magazin.de