Stephan Gemke

Maßnahmen gegen Cyber-Crime und Social Engineering

Nr. 9/2019

Maßnahmen gegen Cyber-Crime und Social Engineering

Dies ist eine mit konkreten Beispielen aus der Praxis gefütterte Liste von Abwehrmaßnahmen gegen Hackerangriffe und Spionage. Technischer Schutz allein reicht nicht, solange das gesamte Personal eines Betriebes arg- und sorglos agiert. Informationssicherheit ist Chefsache!

Das größte Einfallstor um in die Systeme von Unternehmen zu gelangen ist menschliches Versagen vom Zeitarbeiter bis zum Chef. Gleichzeitig liegt auch die Lösung vor dem Gehackt werden im gesamten Personal einer Firma.

Doch der Reihe nach:

Wer seine Software aktuell hält (Stichwort: Patchen), wer Firewalls und Antivirenprogramme installiert hat und auch seinen Systemadministratoren nicht jedes Zugangs- bzw. Zugriffsrecht einräumt, der ist technisch alles andere als gefährdet. Schwächen liegen dann nur noch in menschlicher Form vor, z.B. in Form von Naivität, Unachtsamkeit, Vergesslichkeit, Rache oder Reziprozität (tust du mir einen Gefallen, tu ich dir auch einen). Wobei „nur noch“ in diesem Zusammenhang sehr beschönigt ist, denn man kann technisch noch so sehr aufrüsten, menschliche Schwächen wie die obigen lassen sich noch schwerer und erst recht nicht gänzlich eliminieren.

Und weil die größte Gefahr im Zuge von Cyberattacken und Wirtschaftsspionage vom Menschen selbst herrührt, heißt es auch „Social Engineering“. Es ist der Mensch, oder besser gesagt, das soziales Wesen, das angegangen und so beeinflusst wird, dass es vertrauliche Informationen weitergibt oder anderen den Zugang zu ebendiesen ermöglicht.

Wie gehen Cyber-Kriminelle vor?

Die Methoden reichen von fingierten, täuschend echt aussehenden und vertrauensweckenden E-Mails und Webseiten über infizierte USB-Sticks bis hin zu geheuchelten und gefälschten Umfragen, Studieninterviews, Bewerbungen und Dergleichen. Man gibt sich als Mitarbeiter und Kollege aus, sagt, dass es dringend sei und man von ganz oben geschickt wurde. Man schmeichelt und bändelt an,

nutzt die ausgelassene Stimmung und das viele Bier in After Hour-Partys schamlos aus, offenbart etwas Falsches (bzw. etwas für Außenstehende nicht leicht zu durchschauendes) und ermuntert so seine Gegenüber es ihm gleich zu tun. Man bittet um kleine Gefallen, die sukzessive mehr werden oder, kein Witz, stiehlt unbemerkt das Fahrrad der Zielperson, bringt es tags darauf ebenfalls unbemerkt zurück, jedoch versehen mit einem Kinoticket und dem Begleitschreiben „Tut mir Leid, war in Not und Eile. Als Wiedergutmachung liegt ein Kinoticket bei". Und während die Zielperson abends freudig ins Kino geht, bricht man in sein Haus ein, weil man ja weiß, dass der Bewohner für mindestens zwei Stunden nichtsahnend im Kino sitzt. Die Einbrecher können ungeniert die Räume inspizieren, die Schränke und den Schreibtisch durchwühlen, den Arbeits-PC und den Aktenkoffer mitnehmen, Passwörter knacken und vieles mehr.

Die Methoden sich das Vertrauen der Zielpersonen zu erschleichen, zu täuschen und sein Verhalten zu manipulieren sind mannigfaltig: Beginnend mit Schadsoftware gespickte USB-Sticks, die getarnt als Werbegeschenke auf Branchenmessen verteilt werden, über Drohnen, die über das Betriebsgelände und an die Fenster der Büros fliegen bis zu tadellos auf deutsch formulierte Erpressermails a la „Ich habe Videoaufnahmen von dir beim Porno gucken. Damit ich sie nicht veröffentliche, klicke hier und bezahle".
Dies sind ganz typische Formen der Ausspähung und Bedrohung.

Sich als Student ausgeben, der ein paar Fragen für seine Bachelorarbeit hat, oder als fremder Steuerberater, der nach Durchsicht der Bilanz im Bundesanzeiger finanzielle Verbesserungsvorschläge anzubieten hat, oder als Mitarbeiter diverser Behörden, die unangekündigte Prüfungen durchführen, die Palette an Täuschungsmanövern ist ellenlang.
Hinzu kommen Besucher, externe Projektmitarbeiter, Putzdienste und Handwerker, die die Unterlagen auf den Schreibtischen oder im Kopierraum abfotografieren bzw. direkt einstecken. Zu berücksichtigen sind ebenfalls Leute auf Montage, die sich frei auf dem Gelände und in den Firmenhallen bewegen dürfen, weil sie in einem der Appartements der Firma übernachten und daher einen Schlüssel haben sowie ehemalige Mitarbeiter, denen man die Zugangskarten nicht abnahm und die, selbst wenn die Zugangsberechtigung deaktiviert wurde, allein durch das Vorzeigen der Karte vom Pförtner hineingelassen werden könnten.
Das geschickte über die Schulter schauen, das Stellen von auf dem ersten Blick unverfänglichen, aber auf dem zweiten Blick sehr suggestiven Fragen und das immer weiter Nachbohren, das Wühlen in den Papierkörben und Abfallcontainern,

das heimliche Mitschneiden von Gesprächen und Präsentationen in Meetings und von Telefonaten sowohl innerhalb des Unternehmens, als auch außerhalb in Hotel-Lobbys, im Bus, in der Bahn oder im Flugzeug gehören ebenfalls dazu.

Informationssicherheit ist Chefsache

Und ein Opfer von Social Engineering kann jeder werden, vom Vorstand über die Abteilungsleiter bis zu Lageristen.
Insbesondere die Geschäftsführung stellt aus folgenden Gründen eine Gefährdung dar:

1) Behandelt sie die Mitarbeiter schlecht, sei es von der Bezahlung oder der Arbeitsbelastung her, mangelt es an Zuspruch und Verständnis für die Angestellten oder wird gemobbt, belästigt, beschönigt und vertröstet, dann sinnen nicht wenige Mitarbeiter auf Rache. Ihre Unzufriedenheit, Enttäuschung und Wut münden in geschäftsschädigendem Verhalten indem sie z.B. diverse Dateien (u.a. Budgetplanungen, technische Pläne, Preiskalkulationen, Gehaltslisten, Kundendaten, Zugangsdaten und Forschungsergebnisse) auf private USB-Sticks kopieren, über Clouddienste versenden oder direkt einstecken. Oder sie installieren selbst Schadsoftware. Vertrauensunwürdiges, cholerisches, arrogantes oder gleichgültiges Verhalten auf der Leitungsebene birgt entsprechend sehr gefährliches Potential in sich.

2) Auf die Chefs kommt auch deswegen die größte Bedeutung in Sachen Cyberkriminalität und Informationssicherheit zu, weil Sicherheit grundsätzlich Chefsache ist. Wenn die Vorgesetzten diese Vorbildfunktion vernachlässigen und Sicherheit predigen, aber, um im Bild zu bleiben, Unsicherheit trinken, kann man es von vornhinein vergessen. Wer als Chef unbedingt Dropbox installiert haben und seine IT-Infrastruktur mittels AWS von Amazon laufen lassen möchte und wenn der Chef eine „Clean Desk Policy“ ausruft, aber selbst unaufgeräumt bleibt, der kann nicht erwarten, dass dieses Fehlverhalten nicht Schule macht und keine Nachahmer findet. Ohne Disziplin und Rigorosität geht es einfach nicht. Wohingegen eine Ausnahme von der Regel zur nächsten Ausnahme und von dort wieder zur nächsten Ausnahme führt und man nachher mehr einen Flickenteppich als ein kohärentes und sicherndes Regelwerk besitzt.

3) Vorstände haben die größte Entscheidungsmacht im Unternehmen und zumeist auch die meisten Informationen über ihre Firma sowie ebenfalls weitgehendste Zugriffsrechte innerhalb des Unternehmensnetzwerkes. Ein Hack dieser Personengruppe ist daher besonders lohnend. Und weil sie das favorisierte Angriffsziel sind, müssen die Vorstände Sicherheit und Sorgsamkeit vorleben.

Wie kann man sich schützen?

Nun, es fängt mit der Sensibilisierung an. Denn wenn einem die Bedrohungslage bewusster ist, nimmt man so etwas wie die obigen Beispiele perfider Verhaltensweisen überhaupt erst wahr und agiert ganz grundsätzlich skeptisch und zurückhaltend.

Zurückhaltung und Verschwiegenheit ist der nächste Punkt.
Im öffentlichen Raum sollte man so wenig wie möglich mit Firmeninterna hantieren und zwar mündlich und schriftlich gleichermaßen. Eine Sichtschutzfolie ist ohnehin unerlässlich und lassen Sie sich auch nicht bei Ihrem Stolz packen. Sprich, widerstehen Sie ausführlich von Ihren Erfolgen zu sprechen.
Sensibilisierung und Diskretion gelten zudem für alle Mitarbeiter. Es kann jeden treffen und nicht allein die Geschäftsführung, das Sekretariat und die Assistenten, die IT-Abteilung oder die Forschungsabteilung sind im Visier der Hacker. Der Reiz des Hackings, bzw. der Kern von Wirtschaftsspionage besteht ja nicht darin, möglichst schnell an wichtige Informationen zu kommen, sondern überhaupt an diese Unterlagen heran zu kommen. Und wenn dies besser gelingt, in dem man über einen Sachbearbeiter geht und sollte es auch 200 Tage dauern, dann geht man eben diesen Weg.
Geben Sie daher nie Ihre vollständigen E-Mailadressen oder Ihre Durchwahl heraus, auch nicht in Präsentationen. Schränken Sie Ihre Profile auf LinkedIn, Xing, Facebook, Instagram, Twitter und Co. ein, so dass nicht jeder alles von Ihnen erfahren kann. Bestätigen Sie auch nicht jede Kontaktanfrage und registrieren Sie sich möglichst selten mit Ihrer beruflichen E-Mailadresse, sondern mit einer generischen oder zweckgebundenen Unternehmensmailadresse. Ändern Sie regelmäßig Ihr mindestens 8-stelliges Passwort und verwenden Sie niemals dasselbe Passwort mehrfach. Zumindest sollte das Passwort für Ihren Client, d.h. um auf Ihren Computer zugreifen zu können, ein anderes sein, als Ihr E-Mail-Passwort oder Ihr Passwort für einen Clouddienst.
Veranlassen Sie, dass nur Mitarbeitern der IT Zugang zum Serverraum gewährt wird.

Besonders hilfreich ist es, sein Personal regelmäßig zu testen, z.B. über selbst fingierte E-Mails und Webseiten. Hierzu ein weiteres Beispiel eines börsennotierten Unternehmens: Allen Mitarbeitern wurde eine E-Mail vom Vorstand zugestellt in der es hieß, dass man wegen der neuen Datengrundschutzverordnung ein aktualisiertes Einverständnis zur Übermittlung persönlicher Daten an den Finanzdienstleister für die Gehaltsauszahlungen bräuchte. In der E-Mail fand sich ein Link auf eine spezielle Eingabemaske dieses Finanzdienstleisters mit der Bitte, sich dort mit denselben Logindaten, wie man sie auch für seinen Bürorechner benutzt, einzuloggen und die Datenfreigabe zu bestätigen. Andernfalls könne es in der Gehaltsauszahlung Probleme geben und wer will das schon? Glücklicherweise waren die Mitarbeiter aufgrund früherer Vorfälle und Sensibilisierungsmaßnahmen schon so weit geschult, dass nur sehr wenige tatsächlich Ihre Logindaten mitteilten.
Dies waren nahezu ausnahmslos neue Mitarbeiter, die entsprechend wohlgefälliger, da neu, und auch unsensibilisierter waren.
Nun könnte man sagen, es sei ein Erfolg, dass immer weniger Mitarbeiter darauf hereinfallen, dass es aber immer noch welche gibt und vor allem laufend hinzukommen, da neue Mitarbeiter, besteht keineswegs Anlass zur Freude. Solche Tests regelmäßig durchzuführen ist daher sehr empfehlenswert. Denn, wenn schon ein gewisser Sockel an informationsfreudigen Mitarbeitern bleibt, sollte dieser doch wenigstens so gering wie nur möglich ausfallen.

Die IT-Abteilung nicht vernachlässigen

Schutz erhält man auch durch technische Aufrüstung. Wenn eine IT-Abteilung in finanzieller, personeller wie technisch-funktioneller Hinsicht über mehr Ressourcen verfügt, kann sie deutlich wirkungsvoller und präventiver agieren. IT-Sicherheit eignet sich nun wahrlich nicht dafür, mal nebenbei erledigt zu werden. Es braucht schon mindestens einen, je nach Unternehmensgröße auch ein Dutzend und mehr Vollzeitmitarbeiter, die das Unternehmensnetzwerk überwachen und nach verdächtigem Muster Ausschau halten. Ein solch verdächtiges Muster kann beispielsweise sein, dass es auf einem Computer mehrere gescheiterte Loginversuche, oder dass es Loginversuche zu ungewöhnlichen Uhrzeiten gab. Überdies erschwert eine aktuelle IT-Umgebung sowie eine gut ausstattete IT-Abteilung den Informationsabfluss und Hacker könnten entnervt ausgeben. Es ist nämlich nicht so wie im Film, wo sich binnen weniger Augenblicke ins Firmennetz gehackt wird, sondern es dauert viele Stunden, Tagen und Wochen. Ein Hacker muss sehr viele Versuche unternehmen, bis er mal eine erste Sicherheitslücke gefunden hat. Dann vergeht wiederum einiges an Zeit und an Knobelarbeit, bis er endgültig drin. Und dann muss er wieder warten, bis er vom infizierten Rechner in

die jeweiligen Dateiordner und Programme gelangt. Dem Hacker auf seinem Weg zum Ziel so viele Steine in den Weg zu legen, kann daher dazu führen, dass er resigniert. Ständig muss er sich einen neuen Weg suchen und weil sich all die entwickelten Exploits regelmäßig als unnütz herausstellen, steigt sein Frust und er gibt auf. Daher gehen Informationssicherheit und IT-Sicherheit Hand in Hand.

Zu empfehlen sind überdies regelmäßige Pentests (kurz für Penetrationstests), vorzugsweise von externen IT-Firmen. Ich kenne Logistiker, die mindestens jeden Monat einen Pentest durchführen und zudem immer, wenn eine neue Applikation eingesetzt oder entwickelt wurde.
Seinen Betrieb nach der ISO 27001 zertifizieren zu lassen, wäre ebenfalls nicht verkehrt und stelle zudem ein aussagekräftiges Qualitätsmerkmal für Kunden und Lieferanten dar. Getreu dem Motto: Wir achten auf unsere und damit auf ihre Sicherheit.

Jährlich oder sogar noch unterjährig alle USB-Sticks auszutauschen und auf Geschäftsreisen in die USA, nach China oder Saudi-Arabien einen separaten Laptop mitzunehmen auf dem nur unbedingt notwendige Dokumente und Dateien gespeichert sind, sind zwei weitere Tipps. Schließlich erlaubt die Rechtslage in einigen Ländern den gezielten Zugriff auf Ihre Daten, z.B. durch Verschlüsselungsverbote, weitreichende Befugnisse für staatliche Behörden und Geheimdienste im Zuge der Ein- und Ausreise.

Und das Wichtigste nochmal zum Schluss:

Leben Sie eine Sicherheitskultur im Unternehmen und achten Sie auf die Zufriedenheit, Motivation und persönliche Notlagen Ihrer Mitarbeiter und Kollegen.