Hakin9

Ausgabe 1/2012

The best of...

hakin9

Herausgegeben vom Verlag:
Software Press Sp. z o. o. SK

Geschäftsführer:
Paweł Marciniak

Chefredakteurin:
Ewa Strzelczyk
ewa.strzelczyk@software.com.pl

Redaktion:
de@hakin9.org

Produktion:
Andrzej Kuca

DTP:
Marcin Ziółkowski

Umschlagsentwurf:
Marcin Ziółkowski

Werbung: *adv@software.com.pl*

Anschrift:
Software Press Sp. z o.o. SK
ul. Bokserska 1,
02-682 Warszawa,
Poland
Tel. +48 22 427 36 56,
Fax +48 22 244 24 59
www.hakin9.eu

Liebe Hakin9 Leser,

wir präsentieren Ihnen die spezielle Ausgabe **The best of Hakin9**.

Sie umfasst die besten Hakin9-Artikel von den letzten 12 Monaten.
Die Wahl wurde mit Berücksichtigung der Vorschläge unserer Leser und Betatester getroffen.

Die Artikel behandeln unter anderen folgende Themen: *Cloud Computing, IT-Forensik, Linux Rootkits, IT-Compliance, Sicherheit von Webanwendungen, PHP-Security, SPAM-Schutzmechanismen, Wi-Fi Protected Setup, Pentesting, SSL-Zertifikate, Sicherheitsmassnahmen im Online-Banking, Informationssicherheit für die Unternehmen, Mobile-Sicherheit und Malware-Analyse.*

Wir hoffen, dass Sie die Themen interessant finden und die Artikel für Sie nützlich werden, auch wenn die beschriebene Technologie oder die Werkzeuge sich im Laufe der Zeit verändert haben.

Falls Sie Interesse an einer Kooperation oder Themenvorschläge hätten, wenden Sie sich bitte an unsere Redaktion.

Viel Spass bei der Lektüre!
Ewa Strzelczyk

Wirtschaftsspionage, Bedrohungen und Herausforderungen im Bereich der Informationssicherheit für die Unternehmen

Wolfgang Sidler

Aktuelle Studien zeigen auf, dass heute die neuen Bedrohungen durch mobile Endgeräte, Cloud Computing, soziale Netzwerke und unsichere Software-Applikationen stark zugenommen haben. Die grössten Gefahren sind fahrlässiger Datenverlust oder Datendiebstahl durch die eigenen Mitarbeiter. 20 Prozent der europäischen Unternehmen stufen dieses Risiko sogar höher ein als die Wahrscheinlichkeit eines Datenverlustes durch IT-Ausfälle, Cyber-Kriminalität oder Naturkatastrophen.

IN DIESEM ARTIKEL ERFAHREN SIE...

- von den größten Bedrohungen

WAS SIE VORHER WISSEN SOLLTEN...

- wkein spezielles Vorwissen

Die Unternehmenssicherheit stellt sich neuen Herausforderungen, welche durch die stetige Globalisierung, Vernetzung und Komplexität verstärkt wird. Die dynamischen Veränderungen in Wirtschaft und Technik schaffen neue Gefahren und Risiken, welche sich kombiniert mit anderen begleitenden Ereignissen, wie Wirtschafts-Spionage zu einer oft stark unterschätzten Risikoeinschätzung entwickeln können. Die Chancen, die sich aus der Nutzung der Informations- und Kommunikationstechnologie ergeben, stehen aufgrund wachsender Abhängigkeit von der Technologie jedoch auch einer Vielzahl von Risiken gegenüber.

Die eigentliche Herausforderung besteht darin, die unternehmensspezifischen Risiken zu identifizieren, zu bewerten, entsprechende Massnahmen einzuleiten und die Restrisiken zu kennen und zu akzeptieren.

Nachrichtendienste und organisierte Kriminalität führen heute hoch professionelle IT-Angriffe durch, bei denen Informationen und IT-Strukturen von Unternehmen und auch von Privatbenutzern im Mittelpunkt des Interesses stehen. So überrascht es nicht, dass der Informationssicherheit eine immer grössere Bedeutung auf wirtschaftlicher, gesellschaftlicher, politischer und rechtlicher Ebene zukommt.

Sind bereits die meisten Unternehmer vom Virus “Cloud Computing” befallen? Mir scheint, dass genau mit diesem Hype die Risiken in die “Wolke” verschoben werden und so der Betrieb der ganzen IT-Infrastruktur an einen externen Dienstleister delegiert wird. ***Probleme werden nicht behoben, wenn dieses ausgelagert werden!*** Bestimmte Verhaltensmuster, Einstellungen und Ignoranz, vor allem des Managements, führen zu einer erhöhten Risikobereitschaft. Jedoch unterlaufen auch System-Administratoren Fehler und viele Mitarbeitende arbeiten unvorsichtig, weil sie nicht genügend über die Risiken informiert, geschult und sensibilisiert worden sind.

Ein IT-Unternehmen hat im Mai 2010 folgendes errechnet: Die Schweizer Unternehmen geben im Monat durchschnittlich CHF 4.60 pro Mitarbeiter für Klopapier aus. Nur CHF 2.70 kostet hingegen eine minimale E-Mail-Sicherheit. Vielen Firmen ist ihre Sicherheit aber nicht einmal so viel wert! Gemäss einer ETH-Umfrage geben 62 Prozent der Betriebe nicht mehr als CHF 5‘000.00 pro Jahr für die gesamte IT-Sicherheit aus.

Meine Erfahrungen zeigen, dass gewisse Unternehmen ein grösseres Risiko eines Vorfalls betreffend Informationssicherheit eingehen als andere. Die Grösse der Unternehmen und die Nutzung des Internets, um Geschäfte abzuwickeln, spielen dabei eine wichtige Rolle. Neben der Grösse des Unternehmens und ihrer Geschäftstätigkeit können auch andere Faktoren, wie die Art der Internet-Anbindung, der Grad der technischen Innovation, die Bekanntheit der Firma und die Sensibilisierung der Mitarbeitenden im Bereich der Sicherheit das Risiko eines Vorfalls massgebend beeinflussen. Eine Frage bleibt jedoch noch unbeantwortet: Viele Angriffe bleiben unentdeckt und können so in keiner Statistik oder Umfrage erfasst werden. Gerade bei gezielten Angriffen kommt es häufig vor, dass diese lange unentdeckt bleiben oder gar nie entdeckt werden.

Daher dürfen Sie das Thema Informationssicherheit nicht ignorieren. Ein Informationssicherheits-Managementsystem (ISMS) hilft Ihnen, die Vielfalt dieser Herausforderungen systematisch in den Griff zu bekommen. Das systematische und koordinierte Planen, Steuern und Kontrollieren aller auf die Informationssicherheitsziele ausgerichteten Aufgaben bezeichnet man als ISMS und richtet sich nach dem ISO 27001 Standard.

Wirtschaftsspionage und Datenklau

Einerseits haben die letzten Jahre gezeigt, dass selbst bei grossen Firmen wie Amazon, Apple oder Sony es zu schlimmen Pannen mit Kundendaten kommt. Andererseits stellen sich neue Anforderungen in Bezug auf den technologischen Fortschritt und unserer zunehmend selbstverständlicheren Umgang mit den neuen Kommunikationsmitteln. Aktuelle Zeugen dieser Tendenzen sind die schnelle Verbreitung mobiler Geräte mit immer mehr Funktionen und der Einbezug von Social-Media-Plattformen in kommerzielle Prozesse. Die Bedrohungslage hat sich insoweit geändert, dass die Mittel dazu moderner werden, die Bevölkerung immer vernetzter ist und dass ein zu geringes oder gar kein Sicherheitsbewusstsein bzw. Misstrauen vorhanden ist.

Ein Grossteil der Daten, welche in einem Unternehmen ausgetauscht werden, ist schützenswert, was sich auch in gesetzlichen Bestimmungen widerspiegelt. Verfehlungen im Umgang mit Daten gehen in den meisten Fällen mit der Verletzung vertraglicher Pflichten einher. Daten natürlicher und juristischer Personen unterstehen zusätzlich dem Datenschutzgesetz. Zusätzlich wird es für Unternehmen schwieriger, welche grenzüberschreitend oder global Daten austauschen und so eine Vielzahl von landesspezifischen Bestimmungen beachten müssen.

Der Hype um Cloud-Computing verschärft das Thema. Der Nutzer weiss in der public Cloud (z.B. Amazon, Office 365 von Microsoft, etc.) nicht, auf welchen Systemen, in welchem Rechenzentrum und in welchem Land der Provider seine Daten speichert. Seit Juni 2011 ist bekannt, dass die US-Behörden auf europäische Cloud-Daten zugreifen dürfen. Das gilt insbesondere für den Patriot Act, der US-Strafverfolgern weitreichende Zugriffsrechte auf Daten gibt. In den entsprechenden Service Level Agreements (SLA) kann zum Beispiel der folgende Passus stehen “Unter bestimmten Umständen kann (Name des Providers) Daten ohne Ihre vorherige Zustimmung weitergeben. Dazu gehört die Befolgung rechtlicher Anforderungen”. Für ein rechtlich abgesichertes Cloud-Szenario sind dedizierte Anforderungen an den Cloud-Provider sowie wasserdichte Verträge ein Muss.

Kürzlich wurde in der Presse ein interessanter Angriff auf ein Unternehmen mit einer manipulierten Computer-Maus beschrieben. Die Maus wurde einem Mitarbeitenden des Unternehmens als Werbegeschenk getarnt zugeschickt. In das Gehäuse der Maus wurde ein zusätzlicher Mikrocontroller mit USB-Unterstützung eingebaut, welcher eine Tastatur simulierte und das Ganze um einen USB-Speicher ergänzte. Alle Tastatureingaben werden auf der Computer-Maus gespeichert und ein spezielles Programm wird vom Speicher der Maus gestartet. Das Programm sucht dann den von McAfee stammenden Virenscanner und deaktiviert diesen. Auch manipulierte Android-Handys können sich beim Anschluss an den Computer als Keyboard zu erkennen geben und so die Kontrolle übernehmen. Es ist auch bekannt und erwiesen, dass Apps für das iPhone und iPad im Hintergrund heimlich die gespeicherten Kontaktdaten an den Hersteller der Apps sendet.

Die Cyber-Bedrohung entwickelt sich hauptsächlich im Zusammenhang mit den technologischen Fortschritten im Bereich der Informatik. Ein neue Bedrohung sind die mobilen Geräte. Die Vielzahl von Schnittstellen und Sensoren in den modernen mobilen Geräten und die Tatsache, dass diese überall mit dem Besitzer mitgehen, bietet unzählige Möglichkeiten, um ihn und sein Umfeld auszuspionieren (Datendiebstahl, Ortung, Abhören der Gespräche, Ton- und Bildaufnahmen ohne Wissen des Besitzers, usw.). Auch Plattformen, deren Architektur öffentlich weniger bekannt ist wie z.B. Blackberry, dürften durch die Reverse-Engineering Anstrengungen aus der ProfiHacker-Community gegenüber Cyber-Angriffen zunehmend verwundbarer werden.

Unter Wirtschaftsspionage versteht man die Gesamtheit von Handlungen zu Gunsten eines Staates, einer Firma oder einer Person, zwecks Beschaffung von geschützten oder geheimen Informationen aus den Bereichen Militär, Politik, Wirtschaft, Wissenschaft und Technologie, die zum Nachteil eines Landes oder einer Firma führt. KMUs und wissenschaftliche Institute stellen wegen ihrer innovativen Forschungs- und Entwicklungsvorhaben und ihres Know-hows häufig interessante Ausspähungsziele dar. Besonders beliebt sind auch Messen, wie beispielsweise die CeBIT in Hannover. Hier sind Spione gezielt am Werk und greifen offen auf Informationen zu, die nicht selten in Joint Ventures münden.

Wir unterscheiden die folgenden externen Bedrohungen:

- Delikte durch Einzelpersonen an der Firma
  Einbruch, Drohung, Nötigung, Betrug, Erpressung durch Kunden als „Verhandlungsstrategie“
- Wirtschaftsspionage
  Konkurrenzausspähung, abhören, kopieren, fotografieren an Messen, etc.
- Cybercrime
  Diebstahl geistigen Eigentums von Produktions- und Marketingplänen, Geschäftsstrategien, Rezepten, Patenten durch spezielle Trojaner und Spyware, welche durch E-Mails (SPAM) unbemerkt auf den Firmen-Computern installiert werden.

Firmen im Visier

Folgende Methoden sind üblich im Bereich der Wirtschaftsspionage:

- Unternehmensbesuche von ausländischen Delegationen mit oder ohne Begleitung durch einen Botschaftsvertreter.
- Angebote von Dienstleistungen an Forschungsunternehmen, Universitäten und Rüstungsbetriebe.
- Teilnahme an gemeinsamen Unternehmen (Joint Ventures) und Forschungsprojekten.
- Erwerb von Technologien und Unternehmen zwecks Platzierung neuer Mitarbeiter in sensiblen Bereichen.
- Abschöpfung ehemaliger Mitarbeiter, die Zugang zu sensiblen Informationen hatten.

Beispiele einiger Spionage-Fälle:

- 2005: Grossunternehmen in Israel horchten sich mit individualisierten trojanischen Pferden aus (Mobilefunkprovider, Satelliten-TV-Anbieter, Auto-Importeure)
- 2007: Angriff auf interne E-Mails der PNOS-Parteileitung.
- 2005: Ein französischer Automobilteile-Hersteller entdeckte, dass eine chinesische Praktikantin namens Li Whuang in ihr Computersystem eingedrungen war und dort Daten über neue Konzepte kopiert hatte. Seit 3 Jahren in Frankreich, galt sie als brillant und hatte Universitätsdiplome in Mathematik und Physik. Die Polizei fand bei ihr zuhause mehrere Computer und Festplatten mit enormen Speicherkapazitäten, die sie angeblich nur für ihre Arbeit beim französischen Automobile-Hersteller benutzte.
- 2007: Eine Delegation liess sich in einem deutschen Unternehmen eine neue Anlage vorführen. Die Steuerung des Verfahrens erfolgte über ein älteres Notebook. Dies bewahrte der zuständige Ingenieur in seinem Büro im Schreibtisch auf. Die Täter drangen wenige Tage nach der Präsentation in das Gebäude ein und entwendeten das ältere Notebook aus dem Schreibtisch. Hierbei liessen sie ein neues Notebook samt Netzgerät ausser Acht, das auf dem Schreibtisch stand.

Es ist also zu erwarten, dass sich heute Spione (Studenten) aus China und anderen Staaten unter dem Denkmantel „Praktikant oder Trainee“ von Firmen anstellen lassen, damit sie an die vertraulichen Daten gelangen. In vielen Fällen wurde zunächst nur wegen Einbruch oder Einbruchdiebstahls ermittelt und erst nach einer Sensibilisierung durch die Sicherheits-Spezialisten die tatsächliche Zielrichtung - der Angriff auf das Firmen-Know-how - erkannt. Die Beteiligung fremder Nachrichtendienste an solchen Sachverhalten ist zwar oft schwierig zu belegen, vor allem dann, wenn bereits einige Zeit seit der Tat vergangen ist. Aber gerade deshalb ist es wichtig, einen Sicherheits-Spezialisten so früh wie möglich beizuziehen. Denn häufig sind an diesen Straftaten auch so genannte Innentäter beteiligt, so dass weitere Verluste von sensiblem Firmen-Know-how zu befürchten sind.

Wie wird heute spioniert? Fremde Staaten können E-Mails, Faxe, Telefone durch Satelliten abhören und Wanzen installieren oder können durch IT-Angriffe via individueller Trojaner in ein IT-System eindringen und dort meistens unbemerkt Informationen sammeln und weiterleiten (z.B. unbemerktes Weiterleiten aller E-Mails).

Wer kennt es nicht? Sie besuchen eine Messe und bekommen auf den Unternehmensständen nach Abschluss eines Gesprächs kleine Werbegeschenke angeboten. Darunter ist auch ein USB-Speicherstick mit einer Kapazität von einigen Gigabytes. Obwohl gerade ein USB-Speicherstick ein hochwertiges „Give-away“ ist, ist bei solchen Geschenken Vorsicht geboten! USB-Speichermedien dieser Art gelten nur sekundär als Werbegeschenke. Primär verfolgen die

Absender das Ausspionieren der Adressaten. In einigen Fällen ist ein solches Speichermedium mit einem Trojaner infiziert, der den Datenverkehr ausspioniert und diesen kontinuierlich an den Verursacher leitet.]

Wie können Sie feststellen, ob Ihr Unternehmen ausgehorcht wird? Erhalten Sie zum Beispiel auf Ihre Offerten über Monate hinweg keine Aufträge mehr - sondern Ihr Mitbewerber gewinnt die Aufträge - könnte es sein, dass Ihre E-Mails mit den Offerten unbemerkt an Ihren Mitbewerber gesendet werden.

Wie können Sie sich schützen?

In Anbetracht der weltweit verschärften Konkurrenzsituation und einer steigenden Abhängigkeit von modernen Informations- und Kommunikationssystemen wird es immer wichtiger, sich gegen illegale Nutzung des eigenen Wissens zu schützen. Mit zunehmender Vernetzung kommt der Sicherheit der IT-Infrastruktur Priorität zu. Informationssicherheit darf nicht an Firmen- oder Landesgrenzen Halt machen. International tätige Firmen müssen sich bewusst sein, dass Informationsverluste bei ausländischen Niederlassungen, Konzerngesellschaften oder Geschäftspartnern möglich sind. Einen vollständigen Schutz gegen Informationsabfluss gibt es nicht, doch geeignete Massnahmen können wirkungsvollen und finanziell tragbaren Schutz bieten.

Folgende präventiven Massnahmen können unter anderem ergriffen werden:

- Personensicherheit: Vor jeder Neuanstellung, speziell für sensible Bereiche, empfehle ich Ihnen die Identität und Referenzen des Bewerbers zu überprüfen. Achten Sie aber auch darauf, wenn Sie Hilfskräfte (z.B. Reinigungspersonal) einstellen.
  In einem Unternehmen sollten alle Mitarbeiter inkl. Management sichtbar einen Ausweis (Badge) tragen. Nur so können die Mitarbeiter in einem grösseren Unternehmen interne von externen Mitarbeitern unterscheiden. Externe Mitarbeiter (Handwerker, temporäre Mitarbeiter) müssen einen speziell markierten Ausweis sichtbar tragen. Begleiten Sie Handwerker in die Räumlichkeiten. Verfügt Ihr Unternehmen über eine Entwicklungsabteilung, verbieten Sie digitale Kameras oder andere Mobilgeräte mit einer eingebauten Kamera während einer Führung durch diese Räumlichkeiten.
- Verschlüsselung: Schützen Sie Ihr Firmen-Knowhow durch eine geeignete Verschlüsselung der Notebook-Festplatte. Wenn Sie vertrauliche Dokumente via E-Mail versenden, verschlüsseln Sie das E-Mail und dessen Inhalt. Nur mit einer angemessenen Verschlüsselung können Sie die Vertraulichkeit wahren.
- Passwörter: Verwenden Sie jeweils starke Passwörter und geben Sie Ihr Passwort nie bekannt. Keine Passwortliste unverschlüsselt speichern oder ausdrucken.
- USB-Sticks: Schliessen Sie keine USB-Sticks mit unbekannter Herkunft an Ihr Notebook an. Überprüfen Sie Ihnen vertraute USB-Sticks und CDs nach Viren, bevor Sie diese verwenden. Speichern Sie vertrauliche Firmen-Daten nur verschlüsselt auf einem USB-Stick. Schliessen Sie Ihren USB-Stick an keinen unbekannten PC oder Notebook an, denn die Daten auf dem USB-Stick können schnell, unbemerkt und ohne Spuren zu hinterlassen auf den PC kopiert werden.
- Handy und PDA: Vorsicht mit dem Umgang der PDAs (iPhone, Blackberry etc.). Nehmen Sie solche elektronische Geräte bei wichtigen und vertraulichen Verhandlungen nicht ins Sitzungszimmer. Auch ein angeblich ausgeschaltetes Handy kann mit einem speziellen Handy-Trojaner alles im Raum aufnehmen oder das Gespräch live übertragen.
- Öffentlichkeit: Behandeln Sie geschäftliche Themen und Informationen in der Öffentlichkeit vertraulich während einer Bahn- oder Flugreise oder im Restaurant. Lassen Sie andere nicht mithören und lassen Sie sich nicht aushorchen.
- Büro: Schliessen Sie vertrauliche Unterlagen weg. Verlassen Sie Ihren Arbeitsplatz jeweils aufgeräumt (Clear Desk). Werfen Sie keine Datenträger (CDs) und Dokumente mit sensiblem Inhalt ungeschreddert in den Papierkorb. Wenn Sie Ihren Arbeitsplatz auch nur für kurze Zeit verlassen, aktivieren Sie Ihren Bildschirmschoner.
- E-Mail: Versenden Sie vertrauliche E-Mails nur verschlüsselt und überprüfen Sie den oder die Empfänger vor dem Senden genau. Senden Sie wenn möglich keine Word-Dokumente (DOC) in einem E-Mail. Senden Sie nur PDF-Dokumente als Anhang in einem E-Mail. Denn Word-Dokumente beinhalten viele Informationen (Meta-Daten), welche Sie in kompromittierende Situationen bringen könnten.
- Software: Installieren Sie keine unbekannte Software. Vorsicht bei Freeware-Software. Stellen Sie sicher, dass die Quelle vertrauenswürdig ist. Es gab Fälle, wo Spyware in den Gratis-Programmen eingebaut war. Halten Sie Ihren Virenschutz und Ihre Programme inkl. Betriebssystem auf dem aktuellsten Stand.
- Informatik: Vor der Entsorgung von Computern ist die Festplatte „sicher zu löschen“. Dasselbe gilt vor dem Verschenken oder Verkaufen von Computern. Löschen oder deaktivieren Sie alle Benutzer-IDs von Mitarbeitern, welche Ihr Unternehmen verlassen haben.

- Recht: Bestehen Sie darauf, dass Ihre Mitarbeiter bei der Anstellung eine Vertraulichkeitsvereinbarung (Geheimhaltungs-, Sorgfaltspflicht- und Treuepflicht) unterschreiben, welche auch nach dem Austritt Gültigkeit hat.
- Weisungen: Stellen Sie sicher, dass alle Mitarbeiter die internen Firmen-Weisungen in Bezug auf die Nutzung der Informatik-Mittel kennen. Ich empfehle Ihnen, eine Sicherheitspolitik erstellen zu lassen, welche die generellen Ziele der Informationssicherheit und die Informationssicherheits-Organisation definiert.
- Sensibilisierung: Sensibilisieren Sie Ihre Mitarbeiter mit einfachen aber wirkungsvollen Präsentationen und Publikationen. Besonders Mitarbeiter im Verkauf, Marketing, in der Entwicklung und Filialleiter im In- und Ausland.
- Zutritt: Schützen Sie Ihre Büro-Räumlichkeiten und Computer-Räume vor unbefugtem Zutritt.
- Risiko-Analyse: Führen Sie mit Hilfe eines Sicherheitsspezialisten eine **IT-Risiko-Analyse** in Ihrem Unternehmen durch. Dabei geht es darum, die Unternehmenswerte zu identifizieren, damit die Risiken und Gefahren explizit richtig eingeschätzt werden können. Ermitteln Sie die möglichen Szenarien mit den entsprechenden Gegenmassnahmen.
- Geschäftsführung: Erstellung eines Informationssicherheitskonzepts (ISMS) und Ernennung einer dafür verantwortlichen Person, die mit Unterstützung der Geschäftsleitung Kontrollen durchführt und die Sicherheit durchsetzt.

Verhaltenstipps bei Geschäftsreisen

- Vor Reiseantritt möglichst genaues Bild vom Gastland erarbeiten, allgemeine Gefährdungs- und Sicherheitslage eruieren und mit den Gebräuchen und Gesetzen des Landes vertraut machen.
- Lassen Sie Ihr Notebook, Handy, PDA und sensible Firmenunterlagen nie unbeaufsichtigt liegen. Dies gilt insbesondere auch für die Aufbewahrung in Fahrzeugen, Seminar-Räumen und Hotelzimmern.
- Vermeiden Sie Ihr mobiles Gerät auf irgendeine Weise mit Ihrer Firma in Verbindung zu bringen und verzichten Sie auf das Anbringen von Logos, Klebern etc., sowie auf die Aktivierung entsprechender, eindeutiger Bildschirmschoner.
- Tragen Sie Ihr Notebook und andere Mobilgeräte bei Flugreisen ausschliesslich im Handgepäck. Dies gilt auch für wichtige Unterlagen. Verstauen Sie alle Geräte, wenn immer möglich und für Sie gut einsehbar, unter dem vorderen Sitz.
- Setzen Sie Passwörter, Virenschutz- und Verschlüsselungsprogramme zum Schutz Ihres PCs und Notebooks ein.
- Seien Sie besonders aufmerksam, wenn Sie Ihr Notebook am Flughafen durchleuchten lassen müssen. Legen Sie es erst auf das Förderband, wenn Sie selbst durch den Metalldetektor gehen. Sollten Sie durch Anstehen aufgehalten werden, dann behalten Sie Ihr Notebook im Auge und achten Sie dabei auf verdächtige Personen, die es in der Zwischenzeit vom Band nehmen können.
- Nutzen Sie für sensible Kommunikation nur gesicherte Wege (Vorsicht insbesondere bei Fax-, E-Mail- und Telefonverkehr von unterwegs).
- Berücksichtigen Sie bei Telefongesprächen vom Mobiltelefon, dass diese ohne grossen technischen Aufwand abzuhören sind.
- Vernichten Sie nicht mehr benötigte Unterlagen. Ihr Abfall kann für andere wertvolle Informationen enthalten.
- Seien Sie misstrauisch, wenn Sie sich ungewöhnlich stark ausgefragt fühlen – nicht jeder Gesprächspartner hat das gemeinsame Geschäft im Sinn. Niemals Gespräche mit Fremden über Reisezweck und Arbeitgeber führen.
- Analysieren Sie in der Gesprächsvorbereitung, welche Informationen Ihre Gesprächspartner zu Ihrem Nachteil verwenden könnten.
- Sitzen Sie in der Bahn oder in einem Flugzeug, verwenden Sie für Ihr Notebook einen speziellen Sichtschutzfilter. So kann der Nachbar nicht mitlesen.
- Sind Sie vorsichtig beim Eröffnen von Filialen und Produktionsstätten in allen Ländern, die den Patent- und Markenschutz nicht respektieren oder nicht durchsetzen.
- Wenn Sie Ihre neuen Produkte auf internationalen Ausstellungen präsentieren, achten Sie darauf, dass während der Ausstellung kein Firmen-Know-how gestohlen wird.

Social Engineering - Angriffsziel Mensch

Der Mensch ist das schwächste Glied in der Informationssicherheitskette. Dieser Tatsache bedienen sich so genannte „Social-Engineering-Angriffe". Technische Sicherheits-Massnahmen bieten keinen Schutz vor nichttechnischen Angriffen!

Mit Social-Engineering können zwischenmenschliche Beziehungen zur Manipulation genutzt werden, um unerlaubt an Informationen zu gelangen. Das Ziel ist das ausspionieren des persönlichen Umfeldes eines ausgewählten Opfers. Dies geschieht vielfach mit der Vortäuschung falscher Identitäten oder der Nutzung von Verhaltensweisen, um an geheime Informationen oder gewinnbringende Daten zu gelangen. Meist wird dies über den Einstieg in ein fremdes Computersystem erreicht, das vertrauliche Daten beherbergt. Diesen Vorgang nennt man auch Social-Hacking.

Das meist verwendete Grundmuster des Social-Engineerings wird in Form von Telefonanrufen gehandhabt. Der Social-Engineer ruft einen Mitarbeiter eines Unternehmens an und gibt sich fälschlicherweise z.B. als Techniker aus. Mit Hilfe dieses Deckmantels gelangt er an vertrauliche Zugangsdaten, weil er unmissverständlich kundtut, dass er seine Arbeit sonst nicht abschliessen könne. Gelingt ihm dies auf Anhieb nicht, wird er es wieder und wieder versuchen und wird in Kombination von vorgängig konsultierten öffentlichen Quellen und mit Informationsfetzen und Teilen der gescheiterten Anrufe sein Ziel der Manipulation früher oder später erreichen. Der Angreifer beeindruckt sein Opfer, das ihm meist technisch unterlegen ist, einerseits mit Charme und andrerseits mit Fachjargon und erntet Sympathie und Autorität. Wer wird da nicht weich? Zudem kann es schwierig sein, der Androhung, dass der Chef kontaktiert wird, wenn die Information nicht gegeben wird, zu widerstehen. Und vielleicht liegt tatsächlich ein technisches Problem vor und man wartet auf einen Anruf.

Eine andere Form des Social-Engineerings ist das Phishing. Das Prinzip ist dasselbe, wie herkömmliches Social-Engineering über fingierte Telefonanrufe, mit dem Unterschied, dass es sich um eine unpersönliche Variante via Email handelt. Die Emails operieren mit dem Schein einer vertrauenswürdigen Seite und lassen den Benutzer glauben, dass es zwingend notwendig ist, das Mail zu beantworten. So wird der Empfänger aufgefordert seine geheimen Zugangsdaten wie Passwörter etc. zu erfassen. Der Angreifer braucht in diesem Fall nichts mehr als die Email-Adresse des Empfängers, ein bisschen Glück und Geduld. Durch die unpersönliche Form des Phishings ist die Wirksamkeit zwar begrenzt, aber nicht minder gefährlich.

Social-Engineering kann grob in zwei unterschiedliche Angriffsarten gegliedert werden:

Computer Based Social Engineering basiert, wie der Name schon sagt, auf die Verwendung des Computers, um an die gewünschten Informationen zu gelangen. Dazu ein Beispiel: Ein Social-Engineer verschickt Massenmails, gibt sich als Mitarbeiter des Online-Auktionshauses eBay aus und versucht so, an Kreditkartennummern und andere persönliche Daten heranzukommen. In seiner Massenmail bestätigt er den Kauf eines erfundenen Artikels und gibt als Stornierungsseite www.ebay.com.rr.nu an. Auf dieser gefälschten Seite kann der Kauf mit der Eingabe der Kreditkartennummer storniert werden.

Mittels Human Based Social Engineering wird versucht, die gewünschten Informationen direkt von den Opfern zu erhalten, indem der Social-Engineer mehr oder weniger geschickt danach fragt. Dazu ein Beispiel: Ein Angreifer gibt sich am Telefon als Mitarbeiter der Informatikabteilung aus und fragt das Opfer nach seinen Passwörtern. Subtiler ist folgende Angriffsart: Der Social-Engineer verursacht dem Opfer ein Problem und tritt als Retter in der Not auf. Er verschafft sich so das Vertrauen des Opfers und erhält die gewünschten Informationen. Ein weiteres lohnenswertes Ziel der Social-Engineers ist das Durchwühlen von Mülltonnen. Studien zeigen immer wieder, wie sorglos Firmen mit ihrem Müll umgehen. Oft können in Mülltonnen interne Telefonbücher, Kalender, Notizen, Ausdrucke von vertraulichen Dokumenten, Systemhandbücher, Ausdrucke von Benutzernamen mit Passwörtern, Ausdrucke von Source-Code, Disketten, Backup Tapes oder alte Hardware

gefunden werden. Informationen dieser Art sind für einen Social-Engineer äusserst wertvoll und erleichtern ihm den Weg ins System erheblich.

Der Mensch als Tor zu sensiblen Informationen. Die 6 typischen Schritte einer Social-Engineering-Attacke:

- Informationen beschaffen (z.B. im Internet, Google, Adressverzeichnisse, etc.)
- Aufbauen eines vermeintlichen Vertrauens (Insider, Gewohnheiten, etc.)
- Gezielte Manipulation von Personen, um an die gewünschten Informationen zu gelangen (Lieferanten, Techniker, Journalist, etc.)
- Ausnutzen von menschlichen Eigenschaften, um das Opfer zu bestimmten Aktionen zu verleiten (um Hilfe fragen, Auskunft verlangen, etc.)
- Angriffe auf IT-Systeme oder Diebstahl von Daten und Passwörtern über Menschen (Bestechung, Erpressung, etc.)
- Personen ohne Fachwissen zu Sicherheitsgefährdenden Aktionen bewegen.

Die Social-Engineering-Attacken werden immer raffinierter und nehmen zu. Ein gekonntes und autoritäres Auftreten mit der richtigen *Ver*-kleidung macht es möglich. Besonders so genannte kommerzielle Spionage-Software (Spyware, Trojaner) bzw. Überwachungs-Programme werden heute in Kombination mit Social-Engineering Attacken eingesetzt. Viele dieser Spionage-Programme werden von den Antiviren-Scannern nicht erkannt. Einige Beispiele aus der Praxis:

- Mitlaufen mit einer Gruppe Mitarbeiter, welche das Gebäude betreten.
- Beschäftigt telefonierend in den Aufzug marschieren und warten bis dieser von jemandem in ein oberes Stockwerk gerufen wird.
- Beschäftigt telefonierend an anderen Zu- oder Ausgängen wartend bis jemand die Tür öffnet und diese dann für den unberechtigten Zutritt benutzt.
- Als Getränke-Lieferant getarnter Mitarbeiter verschaffen sie sich Zugang.

- Guten Tag Herr Muster, hier ist Frau Meier von der IT-Abteilung. Wir haben gerade ein Systemproblem und brauchen unbedingt Ihre Hilfe. Wie lautet ihre User-ID und Passwort?
- Beim Personaleingang: Ein Mitarbeiter der Reinigungsfirma reinigt den Personaleingang. Entschuldigen Sie, ich habe meinen Badge vergessen.
- Ein Social-Engineer wartet in der Toilette, bis die Mitarbeiter in den Feierabend gehen.
- Reinigungspersonal: Entschuldigen Sie, ich habe meine Aktenkoffer im Büro liegen gelassen.
- Durchsuchen von Altpapier und Müll (Dumpster Diving)

Erfahrungen aus der Praxis zeigen, dass Social-Engineering-Attacken sehr erfolgreich bei ungenügender Sensibilisierung der Mitarbeitenden sind. Bei Passwort-Phishing per E-Mail liegt die Erfolgsquote zwischen 30 und 50%. Bei Passwort-Klau per Telefon bei 50-80%. Und Zutritt in gesicherte Räume bei 50%.

Tipps:

Seien Sie kritisch und haben Sie ein gesundes Mass an Misstrauen.

- Begleiten Sie eine externe Person an den Bestimmungsort.
- Fragen Sie eine Ihnen nicht bekannte Person freundlich nach Name, Kontaktperson und Auftrag.
- Alle Mitarbeiter und Besucher sollen einen Badge sichtbar tragen.
- Achten Sie darauf, dass Sie keine vertraulichen Dokumente auf Ihrem Arbeitsplatz unbeaufsichtigt liegen lassen (Clear Desk).
- Speichern Sie vertrauliche Informationen auf mobilen Geräten immer verschlüsselt ab.
- Transportieren Sie vertrauliche Daten nur geschützt.
- Senden Sie vertrauliche e-Mails nur verschlüsselt.
- Wählen Sie ein komplexes Passwort von mind. 8 Zeichen und behalten Sie es für sich.
- Sprechen Sie nie in der Öffentlichkeit (Zug, Tram, Bus, Restaurant, Raucherecke, Toilette) über geschäftsinterne und vertrauliche Angelegenheiten. Lassen Sie andere nicht mithören!
- Schliessen Sie keine USB-Sticks mit unbekannter Herkunft an Ihren Computer an.
- Schliessen Sie Ihren USB-Stick nicht an einen Ihnen unbekannten Computer an.
- Legen Sie keine CD-Rom ein, von der Sie nicht wissen, woher sie stammt.
- Installieren Sie keine Gratissoftware mit unbekannter Herkunft. Viele Gratis-Programme sind getarnte Spionage-Programme.
- Lassen Sie Notebook, Handy oder PDA nie unbeaufsichtigt. Das gilt auch für Aktentaschen oder Papier-Agenden.
- Lassen Sie keine vertraulichen Dokumente auf dem zentralen Drucker/Fax/Kopierer liegen.
- Entsorgen Sie Datenträger und vertrauliche Dokumente sicher (Schredder).
- Entfernen Sie nach jeder Sitzung die Skizzen und Notizen auf dem Whiteboard bzw. entfernen Sie die Flip-Chart-Notizen.

Den wichtigsten Beitrag zur Bekämpfung von Social-Engineering-Attacken liefert das Opfer selbst, indem es Identität und Berechtigung des Ansprechenden zweifellos sicherstellt, bevor es weitere Handlungen vornimmt. Bereits die Rückfrage nach Name und Telefonnummer des Anrufers kann schlecht informierte Angreifer enttarnen. Auch scheinbar geringfügige und nutzlose Informationen sollten Unbekannten nicht offen gelegt werden, denn sie könnten in folgenden Kontaktaufnahmen zum Aushorchen anderer missbraucht werden oder zusammen mit vielen anderen für sich genommen nutzlosen Angaben zum Abgrenzen eines grösseren Sachverhalts dienen. Wichtig ist eine schnelle Warnung aller potenziellen weiteren Opfer; erste Ansprechpartner sind die Sicherheitsabteilung des Unternehmens, die Kontaktadresse des E-Mail-Providers und Mitmenschen und Institutionen, deren Angaben zur Vorspiegelung falscher Tatsachen missbraucht wurden.

Ein „Social-Engineering-Audit“ ist eine sehr gute Methode das Sicherheitsbewusstein in einer Unternehmung effektiv zu messen.

Im Rahmen eines Social-Engineering-Audit stellt man fest, wie es um das Sicherheitsbewusstsein der Mitarbeiter steht. Durch den persönlichen Kontakt werden dem Mitarbeiter vertrauliche Informationen entlockt – meist eine User ID und ein Passwort. Der Social-Engineer als Angreifer täuscht dem Mitarbeiter eine bestimmte glaubwürdige Identität vor, um an die gewünschten Informationen zu gelangen. Ein solches Audit basiert auf den bekannten Angriffsmethoden des Social-Engineerings, welche vorher beschrieben wurden. Die einzelnen Angriffsarten können je nach Kundenbedürfnis beliebig kombiniert werden. Folgende Ziele werden in einem solchen Audit verfolgt:

- Überprüft effektiv das Sicherheitsbewusstsein der Mitarbeiter.
- Erkennt Schwachstellen im Sicherheitsverständnis und Sicherheitsdispositiv.
- Liefert erprobte und praxisnahe Ansätze zur Risikominimierung.

- Eine wirkungsvolle Art die Effektivität einer Awareness-Kampagne zu messen.
- Sinnvoll ist ein Audit vor und nach einer Awareness-Kampagne.

Unsere 10 Management und Sicherheits-Grundregeln

Die Erkennung und Festlegung der kritischen Informationen für ein Unternehmen und die anschliessende Auswahl der geeigneten Massnahmen zur Verbesserung der Informationssicherheit sind Führungsaufgaben, die sich nur eingeschränkt delegieren lassen. Damit die Informationssicherheit erfolgreich umgesetzt werden kann, ist die volle Unterstützung des Managements unerlässlich. Die Verantwortung für die Informationssicherheit trägt das Management, welches die notwendigen Massnahmen initiieren und deren Umsetzung kontrollieren muss. Achten Sie darauf, dass technische Massnahmen zur Verbesserung der IT-Sicherheit immer mit organisatorischen Massnahmen kombiniert werden müssen.

Dabei gelten unsere folgenden 10 Management Grundregeln:

- Die Verantwortung für die Informationssicherheit liegt beim Management und kann nicht vollumfänglich delegiert werden. Es entscheidet über den Umgang mit den Risiken, stellt die notwendigen Mittel zur Verfügung und trägt das verbleibende Restrisiko.
- Informationssicherheit muss in alle Prozesse und Projekte im Unternehmen integriert werden, bei denen Informationen verarbeitet und genutzt werden.
- Der Informationssicherheits-Prozess muss vom Management überwacht werden.
- Für den IT-Betrieb und die Informationssicherheit müssen ausreichende Ressourcen bereitgestellt werden.
- Es müssen organisatorischen Rahmenbedingungen für die Informationssicherheit geschaffen werden.
- Die Umsetzung muss wirtschaftlich sein. Informationssicherheit darf nicht mehr kosten als die damit erreichte Risikominderung.
- Die Informationssicherheit muss in sinnvoller Relation zum Schutzbedarf stehen (Angemessenheit).
- Die Schutzmassnahmen müssen realisierbar sein und dürfen die Sicherheitslage nicht verschärfen (Praktikabilität). Sie müssen nachweisbar Bedrohungen abwehren bzw. Risiken mindern (Wirksamkeit).
- Informationssicherheit darf nicht behindern und muss von allen als Notwendigkeit verstanden werden (Akzeptanz).
- Die IT-Sicherheitspolitik(-Strategie) muss regelmässig überprüft werden.

Mehr über das Thema IT-Sicherheit und Informationssicherheit finden Sie auf unserer Webseite *www.sidler-security.ch*

Fazit

Wirtschaftsspionage, Datenabfluss und Social-Engineering ist eine Realität! Durch die wachsende Komplexität und Vernetzung der IT-Systeme und die Globalisierung ergeben sich neue Herausforderungen an den Schutz der Daten und Informationen. Schützen Sie Ihr Firmen-Know-how mit Ihren Möglichkeiten und lassen Sie sich wenn nötig von einem Sicherheitsspezialisten beraten. Befolgen Sie die hier beschrieben Tipps und Empfehlungen, die dazu beitragen werden, Ihr Firmen-Know-how und somit Ihr Unternehmen angemessen zu schützen.

Diverse Rezepte haben in der Praxis gezeigt, dass die Sicherheitskultur durchaus positiv beeinflusst werden kann. So genannte Aha-Effekte bei Zuhörern sind langen Erklärungen über Sinn und Zweck vorzuziehen, da sie wesentlich besser und nachhaltiger aufgenommen werden. Beispielsweise das Knacken eines Passwortes, eines Notebooks oder das Fälschen eines e-Mails während einer Sensibilisierungs-Präsentation z.B. in Form eines Info-Lunch zeigen die Risiken eindrücklich auf. Der Hinweis auf eine mögliche, ja sogar sinnvolle Nutzung der Verhaltenshinweise auch im Umgang mit dem privaten PC, erhöht die Aufmerksamkeit des Publikums merklich. So hat sich die Verknüpfung der Informationen mit privatem Nutzen als erfolgsversprechend erwiesen: Im Rahmen einer unternehmensweiten Informationssicherheit Awareness Aktion wurde eine CD «Vertrauen ist gut, Kontrolle ist besser! Wie Sie Ihren Home-PC schützen können» mit einem Virus-Scanner und anderen Tools inkl. Booklet mit Internet-Tipps allen Mitarbeitern abgegeben, damit sie zu Hause ihren PC sicher und kontrolliert betreiben können. Besonders heute mit der Verwendung von USB Memory-Sticks ist das Risiko einen Virus oder andere schädliche Programme einzuschleusen sehr hoch. Das Feedback der Mitarbeiter war durchwegs positiv, zumal sie einen aktuellen Viren-Scanner mit Update-Abo und Tipps für das korrekte Verhalten im Internet kostenlos bekommen haben. Ziel ist, das Verhalten aller Mitarbeiter nachhaltig in Bezug auf die Informationssicherheit zu ändern.

WOLFGANG SIDLER

Wolfgang Sidler, Inhaber SIDLER Information Security GmbH www.sidler-security.ch, Master of Advanced Studies in Information Security, Certified ISO 27001 Lead Auditor und Mitautor des «IT-Sicherheitshandbuches für die Praxis»