BEILAGE ZUM DSD 3 | 2016

BDSW

INFO
WIRTSCHAFTSSCHUTZ

EINE PUBLIKATION DES ARBEITSKREISES WIRTSCHAFTSSCHUTZ DES BDSW

Spionagetools aus dem Supermarkt

MANCHE MÖGEN SICH NOCH AN DIE FRÜHEN JAMES-BOND-FILME UND AN MAJOR BOOTHROYD ERINNERN. Der Waffenmeister des MI6, besser bekannt unter seinem Dienstnamen „Q", stattete damals den Filmhelden mit immer neuen, wahrhaft phantastischen technischen Finessen aus. Heute hätte Q seine liebe Not, dem Leinwandagenten 007 etwas wirklich Innovatives zu präsentieren, denn viele der futuristischen Gags sind längst von der Gegenwart nicht nur eingeholt, sondern überholt worden. Und nicht nur das: Das heutige Rüstzeug der Spionage muss nicht von einem als AVIS-Mitarbeiter legendierten Major Boothroyd konspirativ auf dem Hamburger Flughafen übergeben werden, wie im Film „Die Welt ist nicht genug". Alles, was der heutige Spion braucht, gibt es im Supermarkt oder im Internethandel.

Nehmen wir als Beispiel einen USB-Speicherstick. Es dürfte wohl kein Büro geben, wo ein solches nützliches Tool nicht zu finden wäre. Noch in den 1970er Jahren wäre vielen Zuschauern ein solcher Massenspeicher im Miniformat selbst in einem Agentenfilm als allzu phantasievoll erschienen. Ein daumengroßer Stick, auf dem sich komplette Aktenwände speichern lassen? Undenkbar zu jener Zeit.

Seit USB-Speichersticks auf dem Markt sind, hat eine rasante technologische Entwicklung Raum gegriffen. Man kann getrost von einer Revolution sprechen. Wurde in den Anfängen dieser neuen Speichertechnik noch mit Megabytes (MB) gerechnet, sind inzwischen Speicherkapazitäten von 128 Gigabyte (GB) keine Seltenheit mehr.

128 Gigabyte, das sollte man sich einmal auf der Zunge zergehen lassen. Etwa 400 unformatierte DIN-A4-Seiten im Word-Format lassen sich mit einem 1-MB-Speicher unterbringen. Ein Gigabyte sind bekanntermaßen 1.024 Megabyte. Und das multipliziert mit 128 – eine unvorstellbare Speicherkapazität.

Das bedeutet: Auf einen Speicherstick, den heute jedermann dabei haben kann, ohne Argwohn zu erregen, lassen sich komplette Festplatteninhalte übertragen. Mussten in früheren Zeiten Berge von Aktenordnern aus einem angegriffenen Unternehmen getragen beziehungsweise tagelang Fotografien angefertigt werden, genügt heute ein wenige Zentimeter großes Gerät, um den gleichen Effekt zu erzielen. Ein Spionagetool, das in jede Tasche passt.

Wirtschaftsspionage und Konkurrenzausspähung sind dadurch für jedermann praktikabel geworden. Deshalb ist es heute wichtiger denn je, betriebsfremden Personen den Zutritt zum Unternehmen zu verwehren. Die gute alte physische Sicherung ist das beste Mittel, auch gegen die Bedrohungen von heute. Denn längst nicht alle Angriffe erfolgen in elektronischer Form über das Netz. „Handarbeit" ist bei Spionen keinesfalls aus der Mode gekommen.

Doch was tun, wenn es dennoch einem Angreifer gelingt, in ein Unternehmen zu gelangen? Was tun, wenn ein Innentäter aktiv wird? Welche Präventivschritte möglich sind, soll unser Hauptbeitrag deutlich machen.

Eine nutzbringende Lektüre wünscht Ihnen Ihr

Holger Köster
Vorsitzender
BDSW-Arbeitskreis Wirtschaftsschutz

Nur Sekunden dauert es, einen Keylogger zu installieren, und schon wird jeder Tastenanschlag aufgezeichnet. Foto: I-Vista/pixelio.de

Sind Angreifer erst einmal im Unternehmen, stehen ihnen grandiose Möglichkeiten offen

Von Klaus Henning Glitza

ALCATRAZ, JENE INSEL IN DER BUCHT VON SAN FRANCISCO, GALT ALS EINES DER SICHERSTEN GEFÄNGNISSE DER WELT. Obwohl es niemand für möglich gehalten hatte, ist es dennoch Insassen gelungen, von dort zu fliehen. Daraus ergibt sich im Umkehrschluss, dass auch der umgekehrte Weg nicht gänzlich unmöglich sein kann. Es ist nie völlig auszuschließen, dass in noch so sichere Objekte eingedrungen werden kann. Ein unaufmerksamer, zu leichtgläubiger oder unqualifizierter Mitarbeiter beziehungsweise eine überlistete Technik genügt, und schon spaziert ein Eindringling in das Unternehmen.

Falls er nicht schon da ist. Nicht zu vergessen: Unter den Mitarbeitern können sich schwarze Schafe befinden, die zumindest die Tendenz zu illegalen Handlungen haben. Der „normale" Anteil an Kriminellen macht auch vor Unternehmen nicht Halt.

Beschäftigen wir uns einmal damit, welche wahrhaft traumhaften Möglichkeiten von außen kommende Angreifer oder Innentäter hätten.

Eindringlinge lieben leere Büros. Besonders gute Chancen dort niemanden anzutreffen bestehen frühmorgens, in der Mittagszeit oder am späteren Nachmittag, wenn etliche Mitarbeiter schon Feierabend gemacht haben. Reiche Beute versprechen die Schreibtische. Häufig liegen dort vertrauliche Papiere herum. Sie einzuschließen, darauf haben die Mitarbeiter verzichtet. Denn man wollte ja nur kurz außerhalb des Büros etwas erledigen. Aber dann hat man X und Y getroffen und es ist doch eine Stunde ins Land gegangen. Behördliche und private Sicherheitsexperten können ein Lied davon singen. Büros ähneln oftmals Selbstbedienungsläden, in denen sensible Unterlagen zum Mitnehmen animieren.

Interessante Dokumente wird der Angreifer entweder an sich nehmen, oder aber – die elegantere Lösung – fotografieren. Dazu eignet sich hervorragend ein Smartphone mit Fotofunktion. Die Qualität der eingebauten Technik ist längst mit anderen Digitalkameras vergleichbar. Nach der Aufnahme kann das Fotoergebnis sofort auf dem Display überprüft werden. Der Eindringling kann also immer sicher sein, ein brauchbares Ergebnis zu erzielen. Professionelle Angreifer verschicken die Fotodateien per Smartphone an eine externe E-Mail-Adresse, wobei der Empfänger theoretisch überall auf der Welt sein kann. Selbst beim Ergreifen des Eindringlings kann folglich der Spionageakt nicht mehr ungeschehen gemacht werden. Nach dem Versand werden die Dateien gelöscht. Damit werden dann auch noch die Beweise für die Tat vernichtet.

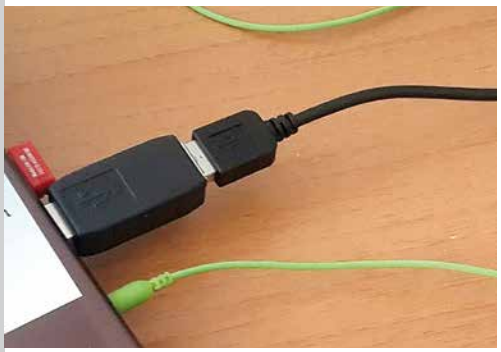
Angreifer-Chance Nr. 2: Obwohl sich niemand im Büro befindet, läuft der Rechner und der Bildschirm ist nicht gesperrt. In solchen Fällen könnte der Eindringling die Festplatte durchstöbern oder gleich den kompletten Inhalt auf einen USB-Speicherstick ziehen.

Chance Nr. 3: Der Rechner ist ausgeschaltet oder der Bildschirm ist gesperrt. Eine Reaktivierung wäre folglich nur per Kennwort möglich. In vielen Fällen bedeutet dies aber keine wirkliche Sicherheit, da in mehr als 50 Prozent der Fälle das Kennwort sehr einfach herausgefunden werden kann. „Ich suche unter der Schreibtischunterlage, in der obersten Schublade oder an den Innenseiten der anderen Schubladen und werde sehr oft fündig. Manchmal wird das Kennwort auch mit einem Post-it an den Bildschirm geklebt", berichtet ein Profi, der im Unternehmensauftrag Arbeitsplätze auf Sicherheit überprüft.

Ein Innentäter kann das Kennwort eventuell erraten. Der eigene Name, der Name des Ehepartners, der Kinder oder des Haustiers, das bevorzugte Automodell respektive „abc123" und „12345", das klappt in etlichen Fällen. Viele Nutzer haben eine panische Angst, das Passwort zu vergessen, und wählen deshalb eine Kombination, die so schlicht ist, dass sie sie auf keinen Fall vergessen.

Abwehrmöglichkeiten

Ein sicheres Kennwort, das unbedingt öfter gewechselt werden sollte, ist entscheidend. Ein guter Weg ist die „Eselsbrücke". Bilden Sie einen Satz. Beispiel: „Es heißt, über sieben Brücken sollst Du gehen, dabei reicht doch eine". Aus dem ü machen wir ein ue, die Mengenangaben sieben und eine wandeln wir in die Ziffern 7 und 1 um und die Kommata lassen wir weg. Daraus ergibt sich Ehue7BsDgdrd1. Wenn Sie auf Nummer sicher gehen wollen, hängen Sie noch ein Sonderzeichen (@, %; & etc.) an. Denken Sie sich einen Satz aus, den Sie nicht vergessen. Ein Satz gerät nicht so schnell in Vergessenheit wie eine Buchstaben-Zahlen-Kombination.



Erkennbar ist ein Keylogger daran, dass sich zwischen USB-Anschluss und Tastaturkabel ein Zusatzteil befindet. Das Spionagetool gibt es auch für den runden PS/2-Anschluss. Bei einigen Keyloggermodellen befindet sich das Zusatzteil nicht direkt in der Buchse, sondern am Anschlusskabel. Foto: Archiv G.

Der beste Virenschutz nützt nichts, wenn es externen Angreifern oder Innentätern im Direktzugriff gelingt, Spionagetools zu installieren.
Foto: Martina Taylor/pixelio.de

Mit einem sicheren Kennwort ist auch eine Bildschirmsperre eine sichere Angelegenheit. Ist eine Bildschirmsperre eingerichtet, kann der Bildschirm nur durch Eingabe des Kennworts wieder aktiviert werden.

Wie kann eine solche Sperre eingerichtet werden?

Im einfachsten Fall drücken Sie die Taste mit dem Windowssymbol (auf der Tastatur im unteren linken Bereich) zugleich mit dem Buchstaben L. Er erscheint die Anmeldemaske. Der Bildschirm kann dann erst wieder durch Eingabe des Passworts aktiviert werden. Alternativ: Den so genannten Klammer- oder Affengriff (Tastenkombination STRG + ALT + ENTF) verwenden und danach Button „Computer sperren" wählen. Der Bildschirmschoner kann auch standardmäßig eingestellt werden, wodurch er nach einer voreingestellten Wartezeit automatisch aktiviert wird. Steuern Sie den Bildschirmschoner über Systemsteuerung an oder geben Sie im Suchfeld (Taskleiste) Bildschirmschoner oder Bildschirmschonereinstellungen ein. Wählen Sie dann die Art des Bildschirmschoners (z. B. 3D-Text, Fotos aus der Fotogalerie oder Seifenblasen) aus und stellen Sie die Wartezeit (z. B. eine Minute) ein. Machen Sie dann bei „Anmeldeseite bei Reaktivierung" ein Häkchen und drücken Sie auf OK. Der automatische Bildschirmschoner hat allerdings den Nachteil, dass Sie sich bei Schreibpausen, beispielsweise Telefonaten, jedes Mal neu anmelden müssen. Vorteil ist aber, dass die Bildschirmsperre selbst dann greift, wenn Sie die Aktivierung einmal vergessen haben.

Um der Gefahr zu begegnen, dass sensible Unterlagen herumliegen oder nicht sachgerecht behandelt werden, sollten die Dokumente klassifiziert, das heißt ähnlich wie bei amtlichen Verschlusssachen in Geheimhaltungsgrade eingestuft werden. Klassifizierte Unterlagen sind grundsätzlich Verschlusssachen und müssen auch beim kurzzeitigen Verlassen des Büros ausnahmslos eingeschlossen werden.

Bewährt haben sich folgende Einstufungen: Intern, Vertraulich, Streng vertraulich.

Intern bedeutet, das Dokument darf nur innerhalb des Unternehmens verwendet werden. Einschließen in Schreibtische oder Aktenschränke.

Vertraulich heißt, es wird namentlich festgelegt, wer von der Unterlage Kenntnis haben darf (Vorgesetzte, Projektleiter, am Projekt mitarbeitende Kollegen). Einschließen in Tresor.

Streng vertraulich ist eine Klassifizierung, die besondere Ansprüche an die Zugangsberechtigten (bekannt zuverlässige Personen) und an das Handling stellt (beispielsweise Zuklappen der Unterlage, wenn ein nichtberechtigter Kollege das Büro betritt). Einschließen in Tresor einer besonders gesicherten Stelle.

Gefahrenbild Keylogger

Nur ein paar Sekunden braucht ein professioneller Angreifer, um einen Hardware-Keylogger zu installieren. Das ungefähr USB-Stick-große Spionagetool wird einfach zwischen Tastaturbuchse des Zielrechners (PS/2 oder USB) und Keyboardstecker gesteckt. Es bedarf weder einer Software noch eines Treibers. Hardware-Keylogger bleiben für Virenscanner unsichtbar. Die „abgegriffenen" Speicherinhalte können effektiv verschlüsselt werden, so dass selbst beim Auffinden des illegal angebrachten Geräts nicht festgestellt werden kann, seit wann es in Betrieb ist und welche Textdateien gespeichert wurden.

Das Überwachungstool zeichnet unabhängig vom verwendeten Betriebsprogramm sämtliche Tastenanschläge auf und speichert sie. Bessere Modelle haben eine Speicherkapazität von über einer Million Anschlägen und mehr. Angeboten werden aber auch Keylogger, die nicht Tastenanschläge, sondern Bildschirminhalte protokollieren. Dabei wird alle paar Sekunden ein Screenshot im JPEG-Format aufgezeichnet und gespeichert.

Um an die gespeicherten Daten zu kommen, bieten sich den Angreifern zwei Wege an:

1. Der Eindringling (es könnte sich auch um einen Innentäter handeln) tritt nochmals in Aktion und entfernt den Hardware-Keylogger. Die Textdateien können dann an einem anderen Rechner ausgelesen werden.
2. Die Funklösung: Ein WiFi-Keylogger ist in der Lage, einmal täglich über den nächstgelegenen WLAN-Router den Speicherinhalt zu verschicken.

Achtlos herumliegende Unterlagen in zeitweise verlassenen Büros lassen Unternehmen zu Selbstbedienungsläden für Know-how-Diebe werden. Als Abwehroption ist eine abgestufte Klassifizierung der betrieblichen Dokumente als Verschlusssachen denkbar.
Foto: Timo Klostermeier/pixelio.de

Bürokommunikation gestern und heute. Jeder Innovationsschritt brachte eine Erleichterung, aber auch neue Risiken mit sich. Bei Schreibmaschinen verriet das Farbband, was geschrieben wurde, bei Tastaturen erledigt dies der Keylogger. Foto: Rainer Sturm/pixelio.de

Es kann ein Keylogger aber auch fest in einer Tastatur verbaut werden. Der Aufwand ist allerdings ungleich größer als bei einem üblichen Keylogger. Unter anderem müssen neue Verbindungen gelötet werden. Der Vorteil aber ist, dass der Logger nicht so einfach detektiert werden kann.

Der Keylogger kann sogar installiert werden, während Sie anwesend sind. Ein „IT-Servicetechniker" könnte unvermittelt auftauchen, etwas von einem Check murmeln und das Spionagetool installieren. Da sich die Anschlussbuchsen im Regelfall ja an der Hinterseite Ihres Rechners befinden, würde die Manipulation auf den ersten Blick nicht auffallen. Ebenso könnte dieser „Techniker" die Tastatur gegen eine präparierte austauschen.

Abwehrmöglichkeiten:

Kontrollieren Sie regelmäßig die Tastaturbuchse. Befindet sich zwischen Buchse und Keyboardstecker ein Zwischenstück, handelt es sich mit größter Wahrscheinlichkeit um einen Keylogger. Bei einigen Überwachungstools ist der Logger als Kabel-Zwischenstück getarnt. Deshalb sollte nicht nur gecheckt werden, ob sich im Verlauf des Anschlusskabels ein Fremdkörper befindet. Merken Sie sich unbedingt den ursprünglichen Zustand der Buchsen, der Stecker und der Verbindungskabel. Alles, was vorher nicht da war, deutet auf eine Manipulation hin.

Analysen und Hilfestellungen zum Wirtschaftsschutz

Von Dr. Berthold Stoppelkamp
Leiter des Hauptstadtbüros des BDSW und zuständiges Geschäftsführungsmitglied für den Arbeitskreis Wirtschaftsschutz

KPMG-Studie: Wirtschaftskriminalität in Deutschland 2016

Laut dieser Studie, bei der 500 Unternehmen befragt wurden, ist jedes dritte deutsche Unternehmen Opfer von wirtschaftskriminellen Handlungen geworden. Bei großen Unternehmen ist es sogar die Hälfte. Auffällig ist, dass über ein Viertel der betroffenen Unternehmen keine Angaben zu den entstandenen Schäden machen kann. Besonders gefürchtet ist der Diebstahl und/oder Missbrauch von Daten. 87 Prozent der Befragten stufen dieses Risiko als hoch bis sehr hoch ein. **www.kpmg.com**

BKA-Analyse: Wirtschaftsspionage und Konkurrenzausspähung

Im Fokus der Analyse standen Beiträge aus Fachliteratur sowie empirische Studien, in denen Unternehmensbefragungen durchgeführt wurden. Die Ergebnisse der Studien zeigen, dass Unternehmen bei der Abwehr von Ausforschung häufiger mit privaten Akteuren zusammenarbeiten als mit Behörden. So nutzten zwei Drittel der Unternehmen Beratungs- und Informationsangebote privater Akteure. **www.wirtschaftsschutz.info**

PwC-Studie: Wirtschaftskriminalität in der analogen und digitalen Wirtschaft 2016

Im Rahmen dieser Studie wurden deutschlandweit 720 Unternehmen mit mindestens 500 Beschäftigten befragt. Es überwiegen nach wie vor Delikte der klassischen Wirtschaftskriminalität. 51 Prozent der Unternehmen waren davon betroffen. 34 Prozent der Unternehmen sind Opfer von Cyberattacken geworden. Am häufigsten handelt es sich um Computerbetrug, Manipulation von Konto- und Finanzdaten sowie das Ausspähen und Abfangen von Passwörtern. **www.pwc.de**

NIFIS: Cyber-Attacken meist Insider-Jobs

60 Prozent aller Cyberattacken werden weltweit von Personen ausgeführt, die eine Zugriffsberechtigung zum angegriffenen IT-System besitzen. Die Angriffe erfolgen entweder durch Angestellte oder Externe, die Systemzugriff haben. **www.nifis.de**

BDSW

BDSW BUNDESVERBAND DER SICHERHEITSWIRTSCHAFT

Verantwortlich: Dr. Berthold Stoppelkamp
Redaktion: Henning Glitza

Norsk-Data-Straße 3 · 61352 Bad Homburg
Fon: +49 6172 948050 · Fax: +49 6172 458580

Mail: mail@bdsw.de
Web: www.bdsw.de