

Sonntag, 27. November 2011

Datendiebe im Firmennetzwerk (Handelsblatt, Sonntag, 27. November 2011)

Die schwere Eisentür des Containers knarrt, als die Beamten des Hamburger Zolls sie aufstemmen.

Dahinter kommen Hunderte Plattenspieler zum Vorschein. Die Ware stammt aus China. Robert

Suchy, einer der Geschäftsführer des Plattenspielerherstellers Clearaudio aus Erlangen bei Nürnberg

mit 44 Mitarbeitern, sieht seinen Verdacht bestätigt: Dreist hat ein chinesischer Hersteller

seine Audiogeräte kopiert. "Dass die Entwürfe wahrscheinlich aus unserem Computersystem geklaut

wurden, haben wir nur durch Zufall bemerkt", sagt Suchy. Wenige Monate zuvor: Auf einer Messe in München stellt Clearaudio Geräte mit einem neuen High-Tech-Magnetlager aus, gefertigt in penibler Handarbeit und nach zweijähriger Entwicklung gerade erst patentiert. Mit dem Magnetlager lassen sich die Platten vibrationsfrei abspielen; das sorgt für einen besseren Klang. Etwa 2.500 Euro kosten damals die Geräte im Handel. Ein paar Stände weiter, bei einem Importeur chinesischer Produkte,

entdeckt Suchy durch Zufall genau das gleiche Magnetlager - millimetergenau kopiert. Zuvor hatten die Chinesen wahrscheinlich mithilfe von Schadsoftware Clearaudios Computersystem ausgespäht,

vermutet Suchy. Zu der Zeit seien viele Angriffe auf das Firmennetzwerk registriert worden.

Der Unternehmer reagiert, macht den chinesischen Hersteller ausfindig, schafft es sogar, dort einen Spion im Versand einzuschleusen. Mit Erfolg: Der V-Mann findet die Containernummern für die Fracht nach Deutschland heraus. Der Hamburger Zoll greift ein, beschlagnahmt und zerstört die Fälschungen

- noch bevor sie in den deutschen Handel gelangen. Was klingt wie ein Agentenkrimi ist häufig bittere Realität. "Die meisten mittelständischen Unternehmen sind sich der Bedrohung durch Datendiebstahl gar nicht bewusst", sagt Mathilde Koller, Leiterin des Verfassungsschutzes Nordrhein-Westfalen. Bei den Datendieben ist alles beliebt, was in Forschung und Entwicklung teuer ist:

Patente,

Baupläne und Designideen. Viele Mittelständler glauben, dass lediglich Konzerne wie Siemens und BMW vom Technologiediebstahl betroffen sind. Dabei sind in etwa 96 Prozent der Fälle kleine und mittlere Betriebe das Ziel von Spionageattacken, schätzt Verfassungsschutz-Chefin Koller. Für Mittelständler

ist der Datenklau besonders gefährlich: Ihr Erfolg basiert oft auf nur einem Patent. Stiehlt jemand diese Informationen, kann das den wirtschaftlichen Ruin bedeuten.

2010 hatte nicht einmal jedes zehnte mittelständische Unternehmen eine umfassende Sicherung eingerichtet, ergab eine Umfrage des Bundesministeriums für Wirtschaft und Technologie. Und nur etwa die Hälfte derjenigen, die Computerspionage als Bedrohung für sich erkannt hatten, haben Gegenmaßnahmen

ergriffen. "Kleine und mittelständische Unternehmen haben in der Regel keinen ITVerantwortlichen, das macht der Chef mit", sagt Berthold Stoppelkamp, Geschäftsführer der Arbeitsgemeinschaft für Sicherheit der Wirtschaft. Und der habe meist keine Zeit, sich intensiv um Sicherheit zu kümmern. Jährlich entstehe deutschen Betrieben durch Datenspionage ein Schaden von mindestens

20 Milliarden Euro, sagt Stoppelkamp. Die Dunkelziffer dürfte viel höher liegen. Viele Vorfälle werden gar nicht als Spionagefälle erkannt, wie ein Praxis-Beispiel des Verfassungsschutzes zeigt: Am Morgen stellt der Geschäftsführer eines Mittelständlers einen Einbruch fest. Doch außer einem alten Computer fehlt nichts. Trotzdem behandelt es die Polizei als normalen Einbruch. Allerdings

wurde genau dieser Rechner am Vortag für die Präsentation eines neuen Produkts benutzt. In welchem

Unternehmen das passiert ist, mag der Verfassungsschutz nicht verraten. Viele Betriebe befürchten Imageschäden, wenn sie sich zu einer Sicherheitslücke bekennen. Clearaudio ist eines der wenigen Unternehmen, die öffentlich reden: "Wir wollen anderen vermitteln, wie wichtig das Thema ist", sagt Suchy.

An Daten zu gelangen ist wesentlich einfacher, als es viele Mittelständler wahrhaben wollen. In Deutschland überprüfen zum Beispiel viele Firmen die persönlichen Angaben ihrer Mitarbeiter nicht, kritisieren Sicherheitsexperten, es herrsche eine unglaubliche Gutgläubigkeit. Häufig wäre schon viel damit gewonnen, die Mitarbeiter für Gefahren zu sensibilisieren. Die Anfrage des potenziellen Kunden

aus dem Ausland klingt gut, die Verhandlungen laufen vielversprechend. Gerade, als es im Gespräch mit dem Chef um die Details geht, steht einer der Gäste auf und fragt nach der Toilette. Im Vorzimmer wendet er sich an die Sekretärin. Sie weiß, um welche Summen es geht, und ist dem Kunden

gegenüber besonders zuvorkommend. Der Gast bittet, schnell ein wichtiges Dokument ausdrucken zu dürfen. Höflich überlässt die Sekretärin ihm ihren Platz. Der Kunde steckt seinen USB-Stick in den Computer, druckt das Dokument aus und geht wieder zurück in die Besprechung. Die Kunden waren zwar am Produktdesign der Firma interessiert, jedoch nicht daran, es zu kaufen. Der Ausdruck war nur ein Vorwand. Denn was die Sekretärin nicht wusste: Im Hintergrund hatte der programmierbare

USB-Stick unbemerkt die Entwürfe von der Festplatte kopiert. Damit war es ein Leichtes für die vermeintlichen Kunden, die Gespräche abzubrechen und das Design heimlich zu nutzen. "Social Engineering"

heißt das Erschleichen der Daten von innen im Fachjargon. Die Täter setzen auf das mangelnde Problembewusstsein der Mitarbeiter. Konkurrenten oder staatliche Nachrichtendienste schleusen Personen unter Vorspiegelung falscher Tatsachen in Unternehmen - von der Putzfrau bis zum Praktikanten. So verschaffen sie sich Zugang zu sensiblen Daten. Bei kleinen und mittelständischen

Betrieben haben sie oft leichtes Spiel. "Manchmal reicht es schon, sich am Telefon als Mitarbeiter einer Telefongesellschaft auszugeben, um an Zugangsdaten zum Firmennetzwerk zu gelangen", sagt Heiko Oberlies, IT-Spezialist der Industrie- und Handelskammer Bonn/Rhein-Sieg.

Am gefürchtetsten sind indes immer noch Hacker, die IT-Sicherheitsschranken wie etwa Firewalls von außen knacken. Auch hier geht es darum, die eigenen Mitarbeiter für die Gefahren zu sensibilisieren. Jeden Morgen muss die Angestellte die Newsletter verschiedener Unternehmen durchgehen, zusammenfassen

und an den Chef weiterleiten. Dass an diesem Tag eines der angehängten Dokumente leer ist, wundert sie nicht. So etwas kann schon mal passieren. Erst später schlägt ein ITVerantwortlicher

Alarm. Eine Schadsoftware greift das Firmennetzwerk an, ausgehend vom Computer der Angestellten. Schnell ist der Träger des Schädlings gefunden: der vermeintlich leere Anhang. Auf der weißen Seite steht in weißer Schrift der Schadcode. Clearaudio wurde damals durch so eine Schadsoftware angegriffen. Das Unternehmen hat aus dem Vorfall gelernt und rund 25.000 Euro in neue Schutzmechanismen investiert. Das ist günstig im Verhältnis zum Umsatz von mehr als fünf Millionen Euro und zu dem Schaden, der durch Spionage entstehen kann. Allein die Entwicklung des Magnetlagers hat etwa 350.000 Euro gekostet. Und einen Versicherungsschutz gegen Datendiebstahl gibt es nicht. "Man muss einmal Arbeit in die IT-Sicherheit investieren, und dann hat man fünf Jahre Ruhe", sagt Suchy. Seine Mitarbeiter sind jetzt geschult und aufmerksam. Kunden steht ein gesonderter

Computer ohne Zugang zum Firmennetzwerk zur Verfügung. Nicht jeder Angestellte hat volle Zugriffsrechte auf alle Daten. Für externe Speichermedien wie USB-Sticks steht ein separater Rechner bereit, bei allen Computern der Mitarbeiter sind USB-Anschlüsse gesperrt. Sensible Interna sind auf einem vom Internet abgekoppelten Computer gespeichert. "Wir sind bis an die Zähne bewaffnet",

sagt Suchy. Bei der Erstellung des Konzepts hat er sich vom Verfassungsschutz beraten lassen.
Clearaudio

ist noch einmal davongekommen. "Wir haben den Chinesen einen Schlag versetzt", sagt Suchy stolz, "die haben unser Patent nicht mehr angefasst." Die Plattenspieler kommen jetzt ausschließlich aus Erlangen. Nichtsdestotrotz produziert das chinesische Unternehmen munter weiter - nur eben nicht mehr kopierte Teile von Clearaudio.