Tatort Firma

Die Gefahr, dass jemand ein Unternehmen ausspäht wird unterschätzt. Selbst wenn sie erkannt wird oder Verantwortliche aufmerksam gemacht werden, sind diese selten zu Schutzmaßnahmen bereit.

Die Daten eines Unternehmens liegen in der Regel am Server, geschützt im Hochsicherheitsbereich“, sagte IT-Spezialist DI Markus Schwaiger beim Seminar „Tatort Firma“, veranstaltet von der Fachzeitschrift „Der Detektiv“. „Ausdrucke und USB-Sticks kugeln in den Büros herum – da frage ich mich oft, mit welcher Sorglosigkeit man in manchen Fällen mit Know-how umgeht.“ Selbst wenn Missstände aufgedeckt werden, ist das keine Garantie dafür, dass etwas unternommen werde. Schwaiger, Berufsdetektiv in Wien, überprüft auf Wunsch die Sicherheitszustände von Firmen. „Wir überprüfen dann meistens ein Jahr nach einem Security-Audit, wie unsere Empfehlungen angenommen worden sind. Die Ergebnisse sind für mich jedes Mal ernüchternd: Wenn zehn Prozent der Sicherungsvorschläge dauerhaft umgesetzt werden, ist das schon viel.“ Meist seien es einfache Maßnahmen – und nicht immer die effektivsten.

Sorgloser Umgang mit Daten: Die sicherste Firewall im Netzwerk nützt nichts, wenn Ausdrucke und USB-Sticks herumliegen.

Kleine und mittlere Unternehmen. „Große Unternehmen sind schon sehr oft gewappnet“, sagte Oberst i. R. Reinhard Kohlweg. Er arbeitete 39 Jahre lang im Heeresnachrichtenamt in der Nachrichtenabwehr. „Aber kleine und mittlere Unternehmen sind um nichts weniger gefährdet, etwa was das Ausspionieren geheimer Daten betrifft, zum Beispiel von Firmen-Know-how.“ Bei kleineren Unternehmen kann mitunter der Fortbestand gefährdet sein, wenn wichtige Firmendaten abhanden kommen oder nach außen dringen, etwa eine Geschäftsidee.

„Der Informationsabfluss geht still und leise vor sich“, betonte Kohlweg. Bemerkt werde er mitunter erst dann, wenn jemand anderer Firmen-Know-how am Markt nutze.

„Genau das ist das Tückische am Datendiebstahl“, erklärte Schwaiger. „Im Grunde handelt es sich nicht um einen Diebstahl – die Daten werden ja nur kopiert, und somit gehen sie dem Besitzer nicht ab.“ In den Überwachungsprotokollen der Server sei zwar nachträglich feststellbar, dass Daten kopiert worden seien. „Aber neuerdings kommt es oft vor, dass Daten routinemäßig gelöscht werden, etwa nach einer Woche. Dann ist es nicht einmal mehr möglich festzustellen, ob jemand unerlaubterweise in das System eingedrungen ist.“

Schwachstelle Mensch. Die angreifbarste Schwachstelle ist laut Schwaiger und Kohlweg der Mensch. „Jemand schickt eine präparierte Werbe-CD-Rom – ich möchte nicht wissen, wie viel Prozent der Beschenkten das Präsent nicht in die CD-Lade des Firmen-PCs schieben“, sagte Schwaiger. Auch „Spaßmails“ mit Witzen, Cartoons und hübschen Bildern werden regelmäßig von den Empfängern geöffnet und weiterversandt. „Zwanzig Prozent davon sind mit Viren und Trojanern versetzt“, erläuterte Schwaiger.

Testweise programmierte ein Suchmaschinenbetreiber auf seiner Website den verlockenden Link: „Ihr Rechner ist trojanerfrei – das können Sie ändern, wenn Sie hier klicken“. Der Seitenbetreiber verzeichnete 300 Klicks in einer Woche.

In einem Experiment „verloren“ Studenten 20 USB-Sticks, versetzt mit Trojanern, absichtlich im Umkreis eines Ministeriums. 13 der Sticks wurden an Computern angesteckt. Bei einem Experiment im Umkreis eines US-amerikanischen Konzerns wurden alle 20 USB-Sticks angesteckt und die Firmencomputer verseucht.

„Man muss aber nicht einmal zu solch gefinkelten Tricks greifen“, betonte Schwaiger. „Meistens reicht es, mit entsprechendem Selbstvertrauen durch die Eingangstür einer Firma zu gehen.“ Trotz technisch ausgeklügelter Zutrittssysteme, ausgestattet mit biometrischen Merkmalstechniken oder komplexer Sperrsysteme gelinge es immer wieder, dass „einem jemand höflich und zuvorkommend die Tür aufhält und man in eine Firma gelangt“, sagte Schwaiger. Innerhalb des Unternehmens stünden Eindringlingen Tür und Tor offen – „im wahrsten Sinn des Wortes. Oder versperren Sie Ihre Bürotür jedes Mal, wenn sie auf die Toilette gehen?“

Unzufriedene Mitarbeiter. Ist ein Eindringen in ein Firmenareal dann doch zu schwierig, führe ein zuverlässiger Weg zum Beispiel über unzufriedene Mitarbeiter. „Das ist um ein Vielfaches leichter, als irgendwelche Tricks anzuwenden“, sagte Markus Schwaiger. Mitarbeiter kennen den Hausgebrauch, wissen, wie die Securitysysteme eines Unternehmens aufgebaut sind und seien selbst nach Kündigung eine Bedrohung. „Sie würden nicht glauben, wie viele gekündigte Mitarbeiter immer noch einen Passwortzugang zum Computersystem ihrer Ex-Firma haben.“ Besonderer Schwachpunkt seien Mitarbeiter, die sich in Geldschwierigkeiten befänden, etwa weil sie Spielschulden hätten oder in Scheidung lebten. Auch Mitarbeitern ist der Datendiebstahl oft schwer nachzuweisen, etwa weil die Datenbestände regelmäßig überschrieben werden. Nach Schwai-

FOTO: GERHARD BRENNER

gers Erfahrungen landet einer unter 30 Fällen, in denen Mitarbeiter Daten nach außen gereicht hätten, vor Gericht.

Die Täter sind laut Schwaiger neben Mitarbeitern eines betroffenen Unternehmens professionelle Hacker, „Script-Kiddys“ oder Unbedarfte, deren Computer in Botnets von Kriminellen missbraucht werden. Das größte Bedrohungspotenzial liege in Hackern aus Russland und China. „Sehen Sie China in Bezug auf die Informationstechnologie nicht als Entwicklungsland“, betonte Schwaiger. „Dort gibt es mehr Universitäten als in Europa. Das Personal dort verdient einen Bruchteil.“ Bestimmte „Leistungen“ seien dort leicht zu kaufen.

Die Dimensionen der Bedrohung seien im Internet laut Schwaiger andere als in der „wirklichen Welt draußen“. „Nehmen Sie als Beispiel den Internetshop Amazon“, sagte Schwaiger, „ein Unternehmen, das jede Sekunde zwanzig Bestellungen abwickelt. Ein Angriff über ein Botnet würde ein solches Unternehmen existenziell bedrohen. Das öffnet zum Beispiel Erpressungen Tür und Tor.“

FOTOS: GERHARD BRENNER

Markus Schwaiger: „Meist reichen einfache Tricks, um in eine Firma zu gelangen.“

Reinhard Kohlweg: „Es ist ungemein leichter geworden, jemanden auszuspähen.“

Späh- und Lauschangriffe. Für jemanden, der die Manager eines Unternehmens abhören oder ausspähen möchte, ist es laut Reinhard Kohlweg „ungemein leichter geworden“, zum Ziel zu kommen. War es vor zehn, fünfzehn Jahren noch Agenten und Spionen vorbehalten, Späh- und Lauschangriffe zu starten, sei die dazu nötige Technik für Laien kein Mirakel mehr. „Top-Mikrofone, Minikameras und nahezu grenzenlose Speichermedien sind heutzutage für jedermann erhältlich“, sagte Kohlweg. Die Technik sei noch dazu mit Gegenständen aus dem Alltag getarnt. „Wenn ich heute meinen Laptop irgendwo aufstelle, würde niemand vermuten, dass darin ein Aufnahmegerät versteckt ist. Hinzu kämen Spezialgeräte, wie Keylogger, die die Tastendrucke mitschrieben.

„Wenn Sie bedenken, dass eine Million Tastendrucke ein Megabyte Datenvolumen verursachen, können Sie sich vorstellen, wie lange ein solcher Keylogger aktiv sein und Schaden anrichten kann“, sagte Markus Schwaiger. Den Keylogger zwischen Computer und Tastatur anzuschließen, stelle kaum ein Problem dar: „Wenn ich heute in ein Büro komme, wird mir in der Regel ein Kaffee angeboten. Falls die Sekretärin nicht ohnehin den Raum verlassen muss, damit sie den Kaffee macht, bitte ich sie um Süßstoff statt Zucker. Dann muss sie meist in die Kaffeeküche oder den Sozialraum. Das gibt mir die Zeit, den Keylogger anzubringen.“ Das Risiko, dass jemand einen Keylogger entdeckt, ist laut Schwaiger gering. „Oder sehen Sie ständig hinter dem Tisch, ob die Computerkabel noch so liegen wie zuvor, als sie das Zimmer verlassen haben?“

Gerhard Brenner