Unternehmen sind nicht wehrlos

Immer mehr Unternehmen werden Opfer spektakulärer Fälle von Cyber-Kriminalität. Dabei wäre es ganz einfach, die meisten Angreifer aus dem Internet abzuwehren.

Von Stefan Schatz

Experten gibt es viele, aber nur einen Timo Kob: Kaum jemand anderer kennt sich so gut mit der Abwehr von Gefahren aus dem Internet aus wie der 48jährige Professor aus Deutschland. Schon in den 90ern trieb er mit seinem Unternehmen HiSolutions AG den IT-Grundschutz voran, heute ist er maßgeblich an der Etablierung internationaler Standards für Informationssicherheit und Business Continuity beteiligt. Er berät nicht nur mehr als die Hälfte aller Unternehmen in DAX, zahlreiche Behörden und Organisationen – unter anderem das österreichische Bundeskanzleramt –, sondern unterrichtet auch am FH Campus Wien. Im Interview mit dem Exportjahrbuch spricht er über die Gefahren, die Exportunternehmen aus dem Cyberspace drohen.

Export Jahrbuch: *CEO Fraud, staatliche Spionage, Killerviren … Was sind denn zur Zeit die größten Bedrohungen für Unternehmen, die über die IT kommen können?*
Timo Kob: Der CEO Fraud ist klassischer Betrug, der sich des Vehikels E-Mail bedient. Da muss man keine Server hacken oder in eine IT einbrechen. Was heute die häufigste Bedrohung ist, sind sogenannte Krypto-Trojaner, wie sie zuletzt unter dem Namen „WannaCry" aufgetaucht sind. Die Computer wurden damit verschlüsselt und erst gegen Zahlung eines Erpressergeldes wieder freigegeben. Das war eines der ersten Male, dass man Sabotage zur Gelddruckmaschine machte. Bisher war Sabotage nicht so verbreitet, weil man zwar Schaden anrichtet, aber der Täter hat keinen direkten finanziellen Nutzen davon. Deshalb wird es viele Nachahmer geben, der Aufwand ist ja gering. Beim CEO Fraud geht es zwar um viel größere Summen, aber der Täter muss sich gezielt auf ein Unternehmen vorbereiten.

Wie kommt so ein Krypto-Trojaner ins Unternehmen?
Kob: Das geschieht via E-Mail. Die wird geöffnet, der Rest geht dann automatisch. Meist ist die Schad-Software in PDF-Anhängen versteckt. Nur: Was soll man machen, wenn man Bewerbungsunterlagen als PDF-Anhang kriegt? Ungeöffnet wegwerfen?

Unternehmen sind also ziemlich wehrlos …
Kob: Ganz im Gegenteil. Wenn man die simpelsten Regeln der IT Sicherheit befolgt, wird das Risiko minimiert. Dass man also Sicherheits-Updates einspielt und immer die neuesten Software-Versionen nutzt, am besten gibt es noch ein Backup-System. Dann ist man schon zu 95 bis 98 Prozent sicher. Wir haben mit einer englischen Versicherung eine Cyber-Versicherung aufgebaut, da sind wir Pioniere. Mit dieser Versicherung wird nicht nur der Schaden von Cyber-Angriffen bezahlt, sondern es stehen auch Anwälte, Krisen PR und IT-Profis zur Seite. An den Schadensmeldungen haben gemerkt, dass der WannaCry-Trojaner viel weniger angerichtet hat als im Vorjahr, als solche Krypto Trojaner erstmals massenhaft aufgetaucht sind. Die Unternehmen haben scheinbar daraus gelernt, die Software aktualisiert und Patches eingespielt.

Was sind denn die klassischen IT-Schwachstellen in Unternehmen?
Kob: Wir predigen es zwar seit Jahren, aber die Systeme in vielen Unternehmen werden nicht aktualisiert. Man liest zwar immer von der NSA und sogenannten Zero Day Exploits, das sind frisch entdeckte Software-Schwachstellen, gegen die es noch keine Gegenwehr gibt. Das sind aber nicht die Dinge, die den Schaden anrichten, das sind Werkzeuge, die Geheimdienste nutzen. Angriffe, die Unternehmen wirklich betreffen, sind mit einfachen Maßnahmen zu verhindern: Neben Software-Aktualisierungen und Sicherheits-Updates sind das Back Ups, ausreichend lange Passworte, die Schulung der Nutzer, wie mit Mail-Attachements umzugehen ist, sauber getrennte Zugriffsrechts-Hierarchien. Man schaut immer auf das große Monster und übersieht den kleinen Hund, der dann wirklich zubeißt.

Können multinationale Konzerne mit Niederlassungen in schwach entwickelten gebieten diese Sicherheitsstandards überhaupt weltweit durchsetzen?
Kob: Prinzipiell schon, es ist nur eine Herausforderung, das auch gesetzeskonform zu machen. In China etwa ist die Verschlüsselung verboten. Dann muss man eben nach regional tauglichen Lösungen suchen. Das ist aber eher ein Problem von französischen Konzernen, die sehr zentra-

listisch geführt werden. Aus meiner Erfahrung lassen deutsche und österreichische Unternehmen viel mehr lokale Lösungen und Eigenständigkeiten zu. Das macht auch in der IT Sinn, dass man Richtlinien herausgibt. Mit welchen Mitteln sie umgesetzt werden, wird vor Ort entschieden. Gibt es keine Möglichkeit, kann ich sensible Bereiche immer noch dadurch schützen, in dem diese regionalen Niederlassungen keinen Zugriff auf wertvolle Daten haben. Es ist eigentlich nur eine Frage der Planung. Man muss alles einmal durchdenken.

Das heißt, gute Planung entwaffnet schon die meisten Cyber-Kriminellen.
Kob: Die zu klärende Frage ist: Wer braucht Zugriff auf was? Das Problem ist: Ich kann diesen Job nicht der IT umhängen. Das muss schon organisatorisch in der Leitung überlegt werden, die IT setzt die Vorgaben dann um. Das Problem sind fehlende Prozess-Definitionen, oft sind die Organisationen einfach wild gewachsen, ohne dass sich jemand genau die Rollen und Zugriffsrechte überlegt hat. Und das sind dann die Einfallstore für Kriminelle.

„Die Hoffnung auf eine Software, in die man nicht einbrechen kann, ist irreal."

Timo Kob
Cybersecurity-Experte, CEO HiSolutions AG

Wer ist für diese Strukturen zuständig? Die Geschäftsführung oder ist es besser, einen externen IT-Berater damit zu beauftragen?
Kob: Früher wurde das gerne möglichst weit weggeschoben, man holte Berater und sagte: „Nun macht mal schön." Das hat nicht funktioniert und hat sich Gott sei Dank geändert, jetzt ist das Bewusstsein in den Führungsetagen angekommen. Auch ich bin IT-Berater und sage

meinen Kunden: Ich kann Euch bei den letzten 20 Prozent helfen, die Grundstrukturen müsst ihr selber ausarbeiten, dafür fehlt mir der Einblick in Euer Geschäft und ich wäre dafür auch zu teuer.

Haben Softwarehersteller überhaupt eine Chance, Sicherheit zu schaffen? Jede neue Software von jeder noch so großen Firma ruft doch sofort Millionen von Hackern auf den Plan, die nichts anderes zu tun haben, als die Schwachstellen zu suchen.
Kob: Nein. Ein Knackpunkt ist: Es gibt keine Haftung für Software. Wenn an Ihrem Auto ohne Fremdeinwirkung die Achse bricht, haftet der Hersteller für die Schäden. Bei Software ist das anders. Man geht davon aus, dass Software so komplex ist, weshalb sie nicht fehlerfrei zu bauen ist. Deshalb sind die Hersteller von der Haftung befreit. Das wiederum gibt ihnen die Möglichkeit, auch erst sehr spät auf Schwachstellen zu reagieren. Das ist von Anbieter zu Anbieter unterschiedlich. Aber die Hoffnung auf eine Software, in die man nicht einbrechen kann, ist irreal.

Was ja auch den staatlichen Geheimdiensten nutzt, wenn man Medienberichten glaubt. Brechen staatliche Stellen tatsächlich bei Unternehmen ein?
Kob: Ja, das ist bekannt und das ist ein komplexes Thema. Teilweise wird dies sehr aggressiv von Ländern betrieben, die ihre Volkswirtschaft damit stärken und Innovationsrückstände ausgleichen wollen. Da müssen wir sicher Richtung Osten schauen. Aber auch der Blick in andere Himmelsrichtungen lohnt sich. Hier geht es staatlichen Stellen teilweise weniger um Forschungsergebnisse, sondern es wird als Ansatz gesehen, um z.B. Korruption oder illegale Aktivitäten wie Embargoverstößen bei ausländischen Unternehmen aufzudecken. Aber auch in diesem Fall ist das auch für gesetzestreue Unternehmen in Deutschland und Österreich ein Problem. Wenn es zu einer Gemengelage aus privaten und öffentlichen Interessen kommt, etwa weil staatliche Sicherheitsaufgaben an private Unternehmen ausgelagert werden, wer soll dann sicherstellen, dass Firmengeheimnisse quasi als „Beifang" solcher Ermittlungen doch an Mitbewerber verkauft werden? Die meisten glauben ja, das betrifft nur große Unternehmen. Dabei haben die Großen viel mehr Mittel, in Sicherheit zu investieren, und die tun das auch. Aber der mittelständische Hidden Champion mit der Schlüsseltechnologie, der ist bei weitem schlechter geschützt. Und der ist mindestens so interessant für solche Aktivitäten wie ein Großkonzern.

Warum investieren die Unternehmen sehr viel in Gebäudeschutz, aber so wenig in die IT-Sicherheit?
Kob: Es geht um Risikowahrnehmung. Das ist zutiefst menschlich. Man fürchtet sich im Flugzeug aber fährt im Auto viel zu schnell, obwohl die Statistik sehr genau zeigt, dass zweiteres viel gefährlicher ist. Das Schwierigste ist der Eigentümer, der Techniker ist, tief im Produkt seines Unternehmens drinnen ist: Dem zu sagen, gib mal 50.000 Euro aus, und am Ende siehst Du nichts, es ist genau so wie vorher, und Du bist zwar sicherer aber Dir kann immer noch etwas passieren – der investiert die 50.000 Euro lieber in eine neue Maschine, mit der er schneller produzieren kann.

Unter KMUs hält sich auch die Auffassung, mit exotischeren Betriebssystemen sei man sicherer. Stimmt das?
Kob: Es ist nicht so, dass die Betriebssysteme von dem einen oder anderen Hersteller sicherer oder besser sind. Aber: Je größer die Monokultur, desto größer die Gefahr. Wenn ich der einzige Weizenhalm in einem Maisfeld bin, ist die Wahrscheinlichkeit gering, dass ausgerechnet hier der Schädling auf mich wartet. Das gilt übrigens auch für PDFs: Wenn ich ein solches PDF mit einem exotischen Tool öffne, ist das nicht per se besser oder schlechter als die von der Masse genützten Reader, aber ein Angreifer muss sich erst einmal die Arbeit machen, für so wenige potentielle Opfer eine Schadsoftware zu schreiben. Die Wahrscheinlichkeit ist für ihn doch viel größer, mit einem Angriff via Massenprogramm sein Ziel zu erreichen.

Mit den Millenials kommen auch die Smart Phones in viel mehr Unternehmen zur Anwendung. Ist das sicherheitsrelevant?
Kob: Problematisch ist der Umgang mit Privatgeräten. Unter dem Schlagwort „Bring Your Own Device ", weil jeder sein Lieblingshandy hat und man Mitarbeiter nicht mit Vorschriften für ein Firmenhandy nerven will, öffnet man natürlich Tür und Tor für Angreifer. Aber auch davor kann man sich wieder einfach schützen, wenn man via Smartphone eben nur auf bestimmte Informationen zugreifen kann.

Das wird mit dem Internet of Things und Industrie 4.0 wahrscheinlich schon schwieriger.
Kob: Da kommt eine richtige Cybercrime-Welle auf uns zu. Bei der Office-IT haben wir gelernt: Updates machen, Patches einspielen, dann ist man relativ sicher. Aber das geht bei den Maschinen nicht so einfach. Wir vermischen Systeme miteinander, die nicht zur Vermischung gedacht sind. Wir binden begeistert an, was sich anbinden lässt und stellen dann verblüfft fest: „Oh, das läuft noch mit Windows 95." Da sind riesige Scheunentore von Einfallsmöglichkeiten.

Es wäre also möglich, dass ein Cyberkrimineller damit droht, die vernetzten Maschinen abzuschalten.
Kob: Das ist ein durchaus realistisches Szenario geworden. Aber wenn man mal von der Erpressung weggeht: Was sind denn die geheimen Informationen in einem Unternehmen? Ist es das Ur-Rezept, das wie bei Coca Cola im Safe liegt? Oder wäre es für einen Mitbewerber nicht auch sehr spannend zu erfahren, wie denn die Maschineneinstellungen sind und die Prozesse, dass man so günstig oder qualitativ produzieren kann?

Herzlichen Dank für das Gespräch. «