cebis
Landkreis Neu-Ulm

T-Sicherheit: Existenzbedrohende Risiken richtig vermeiden

Die Vernachlässigung von Sicherheitsaspekten im elektronischen Geschäftsverkehr kostet die Branche jährlich Milliarden von Euro. Zu dieser alarmierenden Schlussfolgerung der Virenschutzprogramm-Hersteller McAfee (http://www.mcafee.com/de/) in einer Studie vom Oktober 2009. Probleme bei der Datensicherheit und der Privatsphäre der Konsumenten sind Ursache dafür, dass Website-Besucher nicht mehr wieder kommen, dass Online-Verkäufe nicht abgeschlossen werden und dass Unternehmen in Foren und Blogs angeprangert werden. Die negative Wirkung des Vertrauensverlustes durch solche Mängel kann, wie die Studie zeigt, durch noch so attraktive Vergünstigungen wie kostenlosen Versand oder Gutscheine nicht aufgefangen werden.

Woher kommen die Risiken?

Die **technischen** Vorkehrungen zur Vermeidung von Risiken sind in vielen Unternehmen unzureichend. In zahlreichen „Show Hacking"-Veranstaltungen kann man beispielsweise miterleben, wie Hacker **in weniger als zehn Minuten** in Firmenrechner eindringen und dort hochsensible Daten wie auf einem Präsentierteller vorfinden. Im ersten Schritt „rootet" der Hacker den anvisierten Firmenrechner, versucht also, bei einem Windows-System die Administrator-Rechte und bei einem Unix-System die Superuser-Rechte zu bekommen. Danach übernimmt er beispielsweise einen Web-Server, um Zugang zu den Daten und den Administrator-Verbindungen zu erhalten. Die entsprechenden Login-Daten könnten auch den Zugang zu anderen firmeninternen Systemen öffnen. Dieser Weg wiederum führt zu den sensibelsten internen Daten des Unternehmens – seien es Konstruktionspläne oder Liquiditätsrechnungen.

Das auf IT-Sicherheitsfragen spezialisierte und international anerkannte amerikanische SANS-Institut (http://www.sans.org) hat im September 2009 ihre **„Top Cyber Security Risks"** veröffentlicht. Danach sind in diesem Jahr die Top-Sicherheitsthemen ungepatchte Client-Software, über die Schadcode eingeschleust werden kann, sowie Schwachstellen in Web-Applikationen. In den vergangenen Jahren sind zwar auch kleine und mittlere Unternehmen im Bereich der Computer-Sicherheit immer besser geworden; andererseits werden die Hacker ebenfalls immer professioneller und von immer besseren **Hacker-Tools** unterstützt (siehe z.B. http://www.hacker-tools.de).

Bei den größten Schwachstellen in Firmennetzwerken denken die meisten übrigens gleich an Viren und Hacker, also an externe Angreifer aus dem Internet. Eine große Gefahr kommt aber **von den Mitarbeitern, also aus dem Unternehmen selbst heraus** - das zeigen unisono und seit langem alle maßgeblichen Statistiken. Das sind zum einen nachlässige und bequeme Mitarbeiter, die der Einfachheit halber ihr Passwort auf die Tastatur, auf den Monitorrand oder auf die Zimmerdecke schreiben. Das sind die ungenügend sensibilisierten Mitarbeiter, die nicht wissen, dass man nicht alle eMail-Anhänge unüberlegt öffnen sollte. Das sind die enttäuschten und verärgerten Mitarbeiter, die aus Rache und Genugtuung dem Unternehmen einen (Sicherheits-)Streich spielen und beispielsweise den Server mit dem Warenwirtschaftssystem lahm legen. Und das sind schließlich die kriminellen Mitarbeiter, die professionellen Datendieben und Industriespionen gegen Geld Hintertüren im System öffnen bzw. geheime Zugangsinformationen zuspielen.

Im Moment erlebt **"Social Engineering"** einen regelrechten Boom; dabei geht es darum, wie man Nachlässigkeit, Bequemlichkeit oder auch Dummheit von Personen ausnutzt, um ihnen geheime Informationen zu entlocken; **Phishing** ist ein verbreitetes Beispiel dafür.

Was steht auf dem Spiel?

Bei Attacken aus dem Internet muss es nicht zwingend um Spionage gehen: "Script Kiddies" beispielsweise knacken im **sportlichen Wettbewerb** Firmen-Rechner und nutzen sie dann vielleicht als preiswertes externes Speichermedium, zum Beispiel für ihre umfangreichen MP3-Files. Größeren Schaden dagegen können jene Hacker anrichten, die Rechner aus reinem **Zerstörungswillen** knacken und über Schadcodes lahm legen oder mit derselben Absicht per E-Mail Trojaner, Würmer oder Viren auf den Rechnern einschleusen. Der Trend geht bei der Internet-Kriminalität jedoch deutlich in Richtung **finanzieller Interessen** - wie auch bei der gewöhnlichen Kriminalität steht zunehmend der materielle Gewinn im Vordergrund. Wobei der Schwerpunkt beim Abgreifen von Kreditkarten-Daten

liegt, die dann über so genannte Underground Economy Server, von denen sich die meisten in den USA befinden, zum Verkauf angeboten werden. Teilweise sind Kreditkartennumer und PIN schon für weniger als 20 US-Dollar erhältlich. Besonders perfide: Der Trend zur **Erpressung** nimmt zu - entweder mit den Daten selbst oder einfach dem Nachweis, dass bei dem erpressten Unternehmen Daten ausgespäht werden konnten.

Insgesamt weist die Statistik des Bundeskriminalamtes (http://www.bka.de) im Jahr 2008 **43.642 Fälle von Computer-Kriminalität** aus - und das mit jährlich sinkender Aufklärungsquote (2008: lediglich 40,2 %). Dabei ist mit einer **sehr hohen Dunkelziffer** zu rechnen: Die Furcht vor Image-Schaden ist sicherlich einer der Gründe. Ein anderer ist, interne Nachlässigkeiten und internes Fehlverhalten nicht in die Öffentlichkeit zu tragen.

Was tun?

Das größte Sicherheitsproblem bei den meisten kleinen und mittleren Unternehmen dürfte sein, dass diese Unternehmen gar **nicht wissen**, dass sie erheblichen Nachholbedarf in Punkto IT-Sicherheit haben - und zwar nicht einmal dann, wenn tatsächlich etwas passiert ist. Wenn Daten gestohlen werden, dann sind sie ja im Unternehmen nicht physisch weg, sondern nur kopiert. Und das erste, was ein Hacker lernt, ist, bei einem Einbruch in ein System seine Spuren zu verwischen. Und das erste, was ein nachlässiger Mitarbeiter beim Auftauchen von Problemen machen wird, ist, sie zu vertuschen. Viele Unternehmen, die denken, sie seien sicher, wissen nicht, dass sie bereits geschädigt wurden.

Wenn sich ein Unternehmen dazu entschließt, IT-Sicherheits-Maßnahmen zu ergreifen, dann stellen **technische Lösungen** wie Firewall und Antivirus-Software eine wichtige Basis dar, reichen aber keinesfalls aus. **Sicherheitsrisiken durch Mitarbeiter** kann man durch technische Lösungen nicht eliminieren; man muss kriminelle Absicht, Nachlässigkeit, Bequemlichkeit und Dummheit verhindern. Das aber zu schaffen, ist schwierig. **Sensibilisierung** ist in jedem Fall angebracht, wirkt aber beispielsweise nicht bei kriminellen oder rachewilligen Mitarbeitern. **Verhaltensregeln und Kontrollen** schränken die Arbeit und die Motivation der "gutwilligen" Mitarbeiter unzumutbar ein. Und ein Klima des gegenseitigen Misstrauens und der Denunziation trägt sicher nicht zum Unternehmenserfolg bei.

Klar ist damit: Unternehmen müssen beim Streben nach mehr Sicherheit sowohl bei der Technik als auch beim "Faktor Mensch" ansetzen. Klar ist auch, dass ein Unternehmen nicht in einem Schritt die 100-Prozent-Sicherheitsmarke erreicht. Vielmehr fängt es in überschaubaren Schritten an, um sich mit der Zeit zu einem sicheren Unternehmen zu entwickeln; eingesetzte Maßnahmen dürfen das Unternehmen weder in finanzieller, noch in organisatorischer Hinsicht überfordern:

Nötig ist zunächst einmal ein/e MitarbeiterIn im Unternehmen als "Kümmerer" für Sicherheitsangelegenheiten.

Diese Person kümmert sich zuerst darum, dass ein funktionsfähiges Backup-System eingerichtet wird,damit bei Problemen der Schaden begrenzt werden kann.

Dann muss mit regelmäßig aktualisierter Antivirus-Software und richtig konfigurierter Firewall die technische Basis für ein sicheres Unternehmen geschaffen werden.

Ist die Technik vorhanden, dann kann bei den Mitarbeitern durch Sensibilisierung und Schulung die adäquate Nutzung der Technik motiviert werden.

Die nächste Stufe stellt die Absicherung der Kommunikation mit Externen und Außendienst dar.

An dieses dann schon recht hohe Sicherheitsniveau können sich - je nach Finanzkraft und Personalkapazität - nahezu beliebig viele weitere Stufen wie die Einführung von Intrusion Detection Systemen oder regelmäßige Penetration Tests anschließen.

Viele Unternehmen haben inzwischen **Handlungsbedarf erkannt**. Laut einer Studie des Marktforschungsunternehmens Gartner (http://www.gartner.com/technology/home.jsp) vom September 2009 werden die Ausgaben für IT-Sicherheit die anderen Kostenfaktoren der eingesetzten Informations- und Kommunikationstechnologien in der nächsten Zukunft deutlich übersteigen. Dies betrifft sowohl Sicherheits-Software als auch Sicherheitsdienstleistungen, also Wartungs-Service oder Schulungen. Gardner empfiehlt daher dringend, dass die Unternehmen ihre finanziellen Spielräume möglichst für **gezielte, auf die betreffende Firma zugeschnittene Maßnahmen** einsetzen. Das oben dargestellte Stufenmodell hat sich in dieser Hinsicht gerade bei kleinen und mittleren Unternehmen bewährt.