cebis
Landkreis Neu-Ulm

Datenschutz und Datensicherheit: Die Lebensversicherung für Unternehmen

„Wenn Sie glauben, dass Ihre Daten sicher sind, dann gehe ich davon aus, dass Sie nur nicht wissen, dass sie unsicher sind - und bereits in anderen Händen“. Dieser Ausspruch des bekannten Datenschutz- und Datensicherheits-Experten Volker Birk (http://fdik.org) beschreibt plastisch das Problem: Wenn im Unternehmen Produkte gestohlen werden, dann fällt das auf - spätestens bei der Inventur. Wenn Daten gestohlen werden, dann sind sie ja nicht (physisch) weg, sondern nur kopiert - und unter Umständen bemerkt das niemand im Unternehmen, denn Hacker sind Meister im Spurenverwischen. Auch wenn Daten verändert werden, fällt das in der Regel nicht auf. Und dabei geht es nicht nur um Betriebsspionage und deren Folgen, sondern strafrechtliche Sachverhalte: Das Bundesdatenschutzgesetz enthält in den Paragrafen 43 und 44 Straf- und Bußgeldvorschriften; auch wer „nur“ fahrlässig gegen Datenschutzrichtlinien verstößt, kann mit bis zu 300.000 Euro zur Kasse gebeten werden.

Das Internet als Gefahrenquelle

Das Internet ist ein offenes Netz, an dem jeder teilnehmen kann. Eine große Herausforderung ist dabei die Richtigkeit und vor allem die Vertraulichkeit der im Unternehmen gespeicherten Daten; mögliche Gefahren sind **Sabotage** (Zerstörung von Daten, Programmen und Geräten), **Spionage**, **Betrug** (beispielsweise bei Käufen in Online-Shops), **Lahmlegen** des eigenen Internet-Angebotes und - in jüngster Zeit vermehr - **Erpressung**.

Jeder Internet-Nutzer ist selbst für Datenschutz und Datensicherheit verantwortlich und muss sich gegen Gefährdungen aus dem Internet schützen. Dies setzt voraus, dass sich Unternehmen intensiv mit diesem Thema beschäftigen und das Feld nicht den Angreifern überlassen.

Gefährdungen können folgende Ursachen haben:

- **Computer-Viren**: Computerviren sind Programme die per E-Mail, Download oder Austausch von Datenträgern (z.B. USB-Sticks) auf einen Computer gelangen. Sie bereiten sich selbständig auf dem befallenen System aus. Ihr Schadenspotential reicht von einfachen Hinweisen auf ihre Existenz über eine Verlangsamung des Computers bis zur kompletten Zerstörung von Daten und Programmen.
- **Trojanische Pferde**: Trojaner sind Programme, die außer den vom Nutzer vermuteten Funktionen (z.B. Bildschirmschoner) unerwartete und unerkannte Funktionen ausführen. Sie sammeln beispielsweise Passwörter und geben diese unbemerkt weiter oder sie konfigurieren das System um. Wie Viren erhält man diese Programme auch über E-Mails und Downloads, z.B. von Freeware.
- **Unerwünschte aktive Inhalte**: Aktive Inhalte sind z. B. als Active-X-, Java- oder Javascript-Anweisungen in der Internetseite enthalten und werden bei einem Aufruf der Seite auf dem eigenen Computer ausgeführt - i.d.R. ohne, dass es der Benutzer sofort merkt. Sie stellen ein Sicherheitsrisiko dar, wenn sie im Browser generell aktiviert sind. Auch diese Programme können u. a. vertrauliche Daten ausspionieren.
- **Ungeschützte Kommunikation**: Die E-Mail wird immer noch wie ein (verschlossener) Brief eingesetzt. Sie ist jedoch mit dem Versenden einer (offenen) Postkarte gleichzusetzen. Werden vertrauliche Daten unverschlüsselt per E-Mail übertragen, können diese leicht in unberechtigte Hände gelangen.
- **Angriffe von Hackern**: Jedes Unternehmen, das im Internet aktiv ist, ist prinzipiell von Hackern bedroht; Hacker sind Personen, die unerlaubt in ein System eindringen und dort unerlaubte Aktivitäten betreiben. Hacker können u. a. folgende Schäden anrichten: Das eigene Web-Angebot manipulieren, Daten wie beispielsweise Kundendaten oder Konstruktionsdaten unberechtigt lesen und weiter geben oder Dienstleistungen (z.B. Speicherplatz) unberechtigt in Anspruch nehmen. Durch geschicktes Manipulieren mehrerer anderer Computer kann der eigene Computer dadurch außer Kraft gesetzt werden, dass er mit Anfragen regelrecht bombardiert wird.

- **Gefährdung durch Interne**: Mangelndes Sicherheitsbewusstsein der eigenen Mitarbeiter stellt mit die größte Gefahr für die Datensicherheit dar. So werden z. B. Passworte leichtfertig am Telefon weitergegeben, PCs beim verlassen des Raums nicht abgeschaltet oder der Zettel mit dem Passwort leicht sichtbar am Monitor befestigt. Inzwischen hat sich mit **Social Engineering** eine eigenständige Angriffsmethode herausgebildet; dabei wird die Unbedarftheit, Sorglosigkeit oder aber auch Dummheit von Geheimnisträgern ausgenutzt, deren geheime Daten auszuspionieren. Ein Beispiel dafür ist **Phishing**; hierbei klicken Leser einer Mail auf Links, die auf betrügerische Webseiten führen. Dies Webseiten gleichen anderen Seiten (z.B. der Zugangsseite zum Online-Banking einer Bank), werden mit diesen verwechselt und dienen nur dazu, TANs, Passworte und Benutzernamen einzusammeln.

  Neben diesem fahrlässigen Verhalten kommt es auch häufig vor, dass eigene Mitarbeiter Daten mit kriminellem Vorsatz ausspionieren und weitergeben. Die Gründe sind vielfältig; sei es aus Rache für die Entlassung oder Nichtbeförderung oder um sich persönliche Vorteile zu verschaffen. 70 Prozent der befragten 500 Unternehmen sehen in einer Studie des Emnid-Instituts vom September 2010 (http://www.emnid.de/) die Täter von Computerkriminalität im eigenen Haus, also bei Mitarbeitern, ehemaligen Mitarbeitern oder sonstigen Insidern; 48 Prozent sagen konkret, dass die Verstöße aus Habgier oder persönlicher Rachsucht erfolgten. Denn: Um an die wirklich interessanten Firmendaten heran zu kommen, sei ist fast immer Insider-Wissen notwendig.

Etwa 43 Prozent der Internet-Nutzer berichten in einer Studie von Forsa (http://www.forsa.de) vom September 2010, dass ihr Computer schon einmal oder mehrfach infiziert wurde. Rechner wurden lahm gelegt und digitale Identitäten und Daten ausgespäht. 3,5 Millionen Deutschen wurden bereits persönliche Zugangsdaten für Shops und Auktionshäuser, Communities, Foren und E-Mail-Konten gestohlen. 2,5 Millionen Deutsche haben der Studie zufolge bereits einmal einen finanziellen Schaden durch Datendiebstähle oder Schadprogramme erlitten.

Über ein Drittel der befragten Unternehmen hat innerhalb der letzten zwölf Monate über den E-Mail-Versand vertrauliche oder urheberrechtlich geschützte Daten verloren, dies zeigte eine jährliche Studie zum Thema E-Mail-Sicherheit und -Datenverlust des Dienstleisters Proofpoint im September 2010 (http://www.proofpoint.com/news-events/localized/Proofpoint-DLP-Outbound-Survey-GERMAN.pdf). Gleichzeitig belegte die Studie immer mehr Vorfälle, bei denen Daten über Social Media-Kanäle nach außen dringen. Mitarbeiter missbrauchen dabei E-Mail, firmeneigene, mobile Geräte und beliebte Social Media-Tools wie Facebook, LinkedIn, Twitter, Video-Plattformen, Foren und Blogs. Jedes vierte Unternehmen in Deutschland ist innerhalb der letzten drei Jahre schon mindestens ein Mal Ziel eines Betrugsversuchs im Netz geworden, so die genannte Emnid-Studie.

Sicherheitskonzept notwendig

Eine hundertprozentige Sicherheit gibt es nicht! Ein Computersystem ist vielmehr dann als sicher einzustufen, wenn der Aufwand zum Überwinden der Sicherheitsvorkehrungen für einen Angreifer größer ist, als der Nutzen, den er daraus ziehen kann. Auf der anderen Seite sollte jedes Unternehmen nur solche Sicherheitsmaßnahmen einsetzen, deren Kosten den Nutzen, also den vermiedenen Schaden, nicht übersteigen. Um dies entscheiden zu können, sollte jedes Unternehmen eine **Sicherheitskonzeption** haben. Sie dient dazu, systematisch alle sicherheitsrelevanten Faktoren zu analysieren, notwendige Sicherheitsmaßnahmen auch unter wirtschaftlichen Gesichtspunkten festzulegen und diese Maßnahmen für das Unternehmen verbindlich festzuschreiben.

Die Erstellung der Konzeption beginnt mit einer **Bestandsaufnahme**: Welche Hard- und Software wird im Unternehmen eingesetzt? Gibt es dort bereits Sicherheitseinrichtungen wie z. B. Werksschutz, Firewall oder Antivirus-Software? Gibt es einen Sicherheitsbeauftragten oder zumindest einen Datenschutzbeauftragten? Was konkret ist zu sichern (Hardware, Software, Daten, Betriebsmittel)?

In einer anschließenden **Bedrohungsanalyse** wird in unterschiedlichen Szenarien durchgespielt, welche Schäden überhaupt auftreten können. Mögliche Schäden sind der Verlust von Daten, die Nichterreichbarkeit des Systems, Zerstörung der Server durch Wasser oder Feuer usw. Die darauf folgende **Risikoanalyse** dient dazu, die möglichen Schäden nach ihrer Eintrittswahrscheinlichkeit zu bewerten. Dazu dienen z. B. eigene Erfahrungen, Polizeistatistiken, Daten von Versicherern oder Herstellern von Sicherheitsprodukten.

Voraussetzung für eine anschließende wirtschaftliche Festlegung der Sicherheitsmaßnahmen ist die **Schadensanalyse**. Der Schaden kann in steigenden Kosten wie z. B. für die Wiederherstellung der Daten, oder in Erlöseinbußen wie z.B. Auftragsausfällen durch die Nichterreichbarkeit des Internetshops liegen.

Abgeleitet aus der aufgeführten Analyse sind **Sicherheitsmaßnahmen** konkret festzulegen. Diese können **vorbeugend** sein wie beispielsweise die Absicherung des Unternehmensnetzes durch eine Firewall. Es müssen Maßnahmen getroffen werden, um Gefährdungen zu **erkennen** wie beispielsweise durch Viren-Scanner. Es müssen Möglichkeiten existieren, um die Folgen von Schädigungen zu **reparieren** wie beispielsweise durch Restaurieren beschädigter Daten mittels regelmäßig erstellter Sicherungskopien. Schließlich sind Gefährdungen, die sehr selten eintreten, deren Schadensausmaß aber sehr hoch ist wie beispielsweise die Zerstörung der Hardware durch Wasser oder Feuer, über eine **Versicherung** abzudecken.

Sicherheitskonzepte für KMU

Viele gängige Sicherheitskonzepte sehen auch für kleine und mittlere Unternehmen ein Sicherheitsniveau vor, das sich finanziell und organisatorisch nur Großunternehmen leisten können. Sicherheitskonzepte für KMU sollten daher an die jeweilige Situation angepasst sein; Datenschutz und Datensicherheit sollten nicht „von 0 auf 100“, sondern in Stufen eingeführt werden.

"Der erste Schritt einer Sicherheitsstrategie muss die Bestimmung eines **Verantwortlichen** sein, der sich um Datenschutz und IT-Sicherheit kümmert ", so der Sicherheitsspezialist Stephan Rogge vom Ulmer IT-Sicherheits-Dienstleister Certerius GmbH (http://www.certerius.biz). Dieser Sicherheitsbeauftragte muss alle weiteren Schritte koordinieren. Da in vielen Unternehmen noch keine geeigneten Sicherheitsmechanismen existieren, besteht der zweite Schritt einer Sicherheitsstrategie aus einem **Backup-Konzept** mit regelmäßigen kontrollierten und vor allem zentralen Datensicherungen, um geschädigte Daten gegebenenfalls rekonstruieren zu können. 32,5 Prozent der Unternehmen überlassen es noch immer jedem Mitarbeiter selbst, Sicherungskopien sensibler Daten anzulegen, so eine Studie von IDC (http://www.idc.com/germany/) vom Januar 2010; damit ist kein sicheres Backup-Konzept möglich.

Der dritte Schritt ist die Einrichtung eines wirksamen **Virenschutzes**, der sich automatisch selbst aktualisiert. Dabei ist es wichtig, alle Systeme zu schützen, also auch Außendienst-PCs. Der vierte Schritt besteht in der Einrichtung einer speziell angepassten **Firewall**, um das Ausspionieren von Daten zu verhindern. Ein weiterer Schritt besteht in der **Absicherung der Kommunikation zwischen Außendienstmitarbeitern und zentralen DV-Systemen** beispielsweise über Virtual Private Networks (VPN).

Wenn die grundsätzlichen technischen Voraussetzungen geschaffen sind, besteht der weitere Schritt im Aufbau einer **Sicherheitskultur**; alle Mitarbeiter im Unternehmen sind mit den Sicherheits-Mechanismen vertraut zu machen und im Einhalten von Sicherheitsprinzipien zu schulen.

Bereits mit diesen Maßnahmen ist ein grundsätzlicher Schutz auch im Mittelstandsunternehmen erreicht. Je nach Unternehmen kann es sinnvoll sein, weitere Sicherheitssysteme einzuführen.

CEBIS hilft weiter

Mit der Erstellung eines derartigen Sicherheitskonzeptes sehen sich viele, vor allem kleinere Unternehmen organisatorisch und technisch überfordert. Hier bieten sich zahlreiche **Dienstleister** an; lassen Sie sich bei CEBIS oder auch den Kammern (IHK, Handwerkskammer) beraten, worauf bei der Auswahl von Dienstleistern zu achten ist.

Ein kostenloses Marketing- und Datenschutz-**Whitepaper** des International Advertising Bureau (IAB) (http://www.iab.net/media/file/data-primer-final.pdf) klärt darüber auf, wie man Marketing-Daten schützen muss, was man mit ihnen machen darf und was nicht.

Eine **Veranstaltung von CEBIS am 14. Oktober 2010**, und dabei insbesondere der Vortrag über „**Datenschutz und Datensicherheit: Fallstricke bei der Speicherung und Verwendung von sensiblen Kundendaten vermeiden**“ gibt Ihnen praxisorientierte und bewährte Tipps an die Hand, wie Kundendaten effizient und sicher gespeichert und gepflegt werden können. Bitte melden Sie sich bis spätestens **07. Oktober 2010** zur Veranstaltung an (info@cebis-neu-ulm.de).

Unternehmen, die Informations- und Beratungsbedarf zu Chancen und Risiken von IT und Internet haben, können sich an CEBIS wenden. In Veranstaltungen und an Beratertagen können Unternehmen Hilfestellung durch kompetente Berater erhalten. Informieren Sie sich auf der CEBIS-Website über die entsprechenden Termine und melden Sie sich möglichst frühzeitig an.