Sicherheit im E-Business

Dank neuer Technologien sind Einkaufen und Bankgeschäfte zunehmend auch per Internet möglich. Bei der Speicherung, Übermittlung und Verarbeitung der für E-Commerce und E-Business relevanten Daten bestehen aber erhebliche Sicherheitsrisiken. Sie gilt es zu erkennen und zu bekämpfen.

VON KURT BAUKNECHT

Die Möglichkeiten für den Umgang mit Daten und Informationen haben sich dank technischen Entwicklungen in den letzten Jahren drastisch verändert. Es sind dadurch viele neue Anwendungspotenziale und -möglichkeiten entstanden. Im Vordergrund stehen Begriffe und Schlagworte wie E-Commerce, E-Business, E-Government, E-Voting und viele andere. Gemeinsam ist ihnen, dass dank technischer Entwicklungen Arbeitsabläufe neu gestaltet werden und diese dann Anlass für eine völlig neue betriebliche Orientierung sein können.

Wesentliche Einflussgrössen hierfür sind die weltweit intensive Vernetzung und der vereinfachte Zugang zu Personen, Informationen und Rechnerleistung rund um die Uhr und rund um den Globus. Ebenso bedeutend ist die zunehmende Digitalisierung von klassischen physischen Prozessen wie dem Einkauf von Gütern und der Gestaltung von Bankgeschäften und deren Abwicklung über Internet. Bei der dank neuer Technologien möglichen, neuartigen Speicherung, Übermittlung und Verarbeitung relevanter Daten bestehen neben dem Innovationspotenzial aber auch erhebliche Risiken. In dieser Situation darf man keinesfalls die Augen schliessen angesichts verlockender Novität und der Möglichkeiten für neuartige Lösungen, wenn man nicht mit unsicheren Lösungen und mit nicht vertretbarem Gefahrenpotenzial die Prosperität unserer Wirtschaft, das Wohlergehen unserer Gesellschaft oder das Vertrauen von Partnern aufs Spiel setzen will.

Dr. Kurt Bauknecht ist ordentlicher Professor für Informatik an der Universität Zürich.

Vielseitige Herausforderung

Die Realisierung von E-Business-Anwendungen und deren geeigneter Einsatz in betrieblicher Umgebung bedeuten eine vielschichtige Herausforderung sowohl für diejenigen, die mit der Erarbeitung von geeigneten Lösungen beauftragt sind, als auch für die künftigen Betreiber und Benutzer. E-Business-Lösungen können nur dann verantwortet und dürfen nur dann betrieben werden, wenn ein umfassendes, aufgabengerechtes Informationssicherheitskonzept besteht und die geeigneten technischen Lösungen implementiert sind und von den Benutzern auch respektiert werden. Dies setzt umfassende Kenntnisse der zweckmässigen Sicherheitsmassnahmen und das Verständnis für deren oft auch unangenehmen Einsatz voraus.

Setzt man sich mit der Sicherheit von E-Business-Anwendungen auseinander und geht es darum, die für bestimmte Umgebungen und Bedrohungsarten bestmögliche Lösung zu finden, hat man sich zuerst mit der Art der Bedrohung, den potenziellen Zielen und Objekten von Angriffen und dem möglichen Vorgehen der Angreifer auseinander zu setzen. Grundbedrohungen sind solche, welche die Verletzung der Vertraulichkeit, der Integrität und der Verfügbarkeit von Daten zum Ziel haben. Sogenannte abgeleitete Bedrohungen richten sich auf die Verletzung der Authenzität, der Verbindlichkeit und der Zweckbindung von Informationen. Schliesslich sind die zu erwartenden Auswirkungen von Angriffen der entsprechenden Ebene im sogenannten Netzwerk-Referenzmodell zuzuordnen, damit die geeigneten Schutzmassnahmen bestimmt und wirkungsgerecht realisiert werden können. Aus der Vielzahl von möglichen Aufgaben und Konzepten seien hier nur einige wenige genannt:

- Schutz vor Angriffen aus dem Internet durch Firewalls in unterschiedlicher Ausprägung
- Verschlüsselung der Passwörter auf verschiedenen Ebenen
- Aufteilung des internen Netzes in Netze unterschiedlicher Vertrauenswürdigkeit
- Private Adressräume im lokalen Netz
- Teilung des Netzes in verschiedene physische Netze
- Aufteilung von Mail- und Webserver auf getrennte Maschinen

Die Gewährleistung der geforderten Sicherheit ergibt sich nicht durch den Einsatz von punktuellen Einzelmassnahmen; sie muss sich immer auf eine den spezifischen Sicherheitsbedrohungen entsprechende Sicherheitspolitik und deren aufgabengerechte Umsetzung abstützen (wesentliche Komponenten einer solchen Sicherheitspolitik sind im Kasten Seite 33 skizziert).

Mangelnde Sensibilisierung

Der Information kommt heute eine gleiche Bedeutung wie den klassischen Produktionsfaktoren Arbeit, Kapital und Boden zu. Sie muss deshalb bezüglich Sicherheit mit gleichem Massstab und in ihren Auswirkungen vergleichba-

ren Konzepten und Massnahmen behandelt werden. Diese Forderung ist zurzeit nur teilweise und nicht alle Bereiche umfassend erfüllt. Neben der Wahl und dem Einsatz von geeigneten Schutzmassnahmen fehlen auch in weiten Kreisen die Sensibilisierung und das Verständnis für die Verletzbarkeit von Daten. Die Einsicht fehlt, dass Information sehr leicht kopiert, gestohlen und auch verändert werden kann; dies oft für längere Zeit unbemerkt, für den Dieb mit wenig Aufwand und Kosten, für den Betroffenen aber mit katastrophalen Folgen.

Informationssicherheit verlangt heute einen gesamtheitlichen Schutz der Information mit ihren Bausteinen und Verarbeitungsmöglichkeiten. Sie umfasst deshalb wesentlich mehr als die in der Vergangenheit angewandten klassischen Sicherungsverfahren beim Umgang mit Computerdaten. Es geht hier um die Sicherstellung der längerfristigen Geschäftstätigkeiten und um den Schutz des Wissens der Mitarbeiterinnen und Mitarbeiter im Unternehmen. Informationssicherheit ist daher eine strategische und sicher nicht nur eine technische Frage.

Durch den Fortschritt im IT-Bereich wächst die Bedeutung der Informationssicherheit sowie die Abhängigkeit der Unternehmen und Organisationen von Daten, Informationen und Wissen. Ihre Wettbewerbsfähigkeit und Wirtschaftlichkeit, die Einhaltung von gesetzlichen Vorschriften und nicht zuletzt ihr Image werden unmittelbar von der Verfügbarkeit, Verlässlichkeit und Vertraulichkeit der Information beeinflusst. Erfolg und Misserfolg des E-Business werden zweifellos vom situationsgerechten Umgang mit den geeigneten Sicherheitsmassnahmen abhängen.

Komponenten einer Sicherheitspolitik im E-Business

Strategische Ebene – Informationssicherheitspolitik
- beinhaltet Grundsatzentscheidungen basierend auf der Unternehmenspolitik
- legt die Rahmenbedingungen fest für die Gewährleistung der Informationssicherheit und der damit verbundenen Informationsverarbeitungsprozesse (was erreicht werden soll und warum)
- definiert organisatorische Elemente (z. B. wer die Erreichung der Ziele vertreten soll)

Informationssicherheitspolitik

Inhalte einer Informationssicherheitspolitik:
- Allgemeine Grundsätze: Bezugsrahmen, Geltungsbereich, Sicherheitsziele, Grundbedrohungen…
- Erfüllung diverser Gesetze und der Erhalt der Handlungsfähigkeit, z. B. Datenschutzgesetz, Urheberrecht…
- Voraussetzungen für die interne Revision
- Möglichkeiten, im Schadensfall allfällige rechtliche Schritte abzustützen

Mögliche Aussagen in einer Informationssicherheitspolitik:
- Es ist alles erlaubt, was gemäss Organisationshandbuch erlaubt ist, aber nicht mehr
- Jeder soll nur so viel wissen, wie zur Ausführung der jeweiligen Arbeiten benötigt wird (Need-to-know-Prinzip)
- Bestimmte Arbeiten müssen von mehr als einer Person verantwortet werden (Mehr-Augen-Prinzip)

Taktische Ebene – Sicherheitskonzeption
- Anwendung Grundschutz
- Feststellung der momentanen Bedrohungssituation
- Identifikation der Schutzobjekte
- sorgfältige Risikoanalyse durch Antizipation gefährlicher Ereignisse und Situationen
- Bewertung der Risiken (Schadenswert und -häufigkeit)
- Suche nach adäquaten Massnahmen
- Bewertung dieser Massnahmen (Kosten/Nutzen)
- Auswahl und Realisierung durch Management (Restrisikobestimmung)
- Kontrolle

Personelle und organisatorische Massnahmen
- Ausbildung/Bewusstseinsbildung
- geprüftes aktuelles Organisationshandbuch
- strenges und unumgehbares Rollenkonzept
- Beachtung von Interessens- und Befugniskonflikten
- Protokollierung
- Mehr-Augen-Prinzip
- Auditing/Revision

Technische Massnahmen
- Zugriffskontrolle
- Verschlüsselung
- digitale Unterschriften
- Integritätssicherung
- Authentisierung
- Verkehrserzeugung
- Routingkontrolle
- Notarisierung

Das geeignete Vorgehen und die entsprechenden Massnahmen sind immer situations- und aufgabengerecht zu wählen, um den notwendigen und für die Benutzer von E-Business-Lösungen auch verständlichen Schutz gewährleisten zu können.

QUELLE

Leitfaden zur Informationssicherheit für Führungskräfte, Stiftung InfoSurance, http://www.infosurance.org