Special Innovation

Thomas Blaschka: „Firmen sollten darauf achten, welche Informationen ihr Haus verlassen. Derzeit ist es so, dass Mitarbeiter via E-Mail alles wegschicken können. Das stellt ein großes Sicherheitsrisiko dar“, erklärt der Head of Product Management der Kapsch Business Com AG.

Das Pickerl für den Computer

Sonja Gerstl

economy: ***Wie sieht das Bedrohungspotenzial für Unternehmensnetzwerke grundsätzlich aus?***

Thomas Blaschka: Das jeweilige Bedrohungspotenzial ist stark vom Unternehmen und von dessen Umfeld abhängig. Insofern kann man keine verbindlichen Aussagen tätigen. Eindeutig feststellbar ist jedoch, dass die Angriffsszenarien nicht mehr willkürlich sind. Früher hat man gesagt: Da sitzt irgendwo ein junger enthusiastischer Mensch, der mit irgendwelchen Tools irgendwo einzudringen und dort Unruhe zu verbreiten versucht. Mittlerweile agieren Hacker und Co wesentlich zielgerichteter. Vor allem regional abgegrenzte Attacken werden immer häufiger.

Worauf haben Unternehmen in puncto Netzwerksicherheit zu achten? Gibt es spezielle Bereiche, die ganz besonders anfällig sind, wie etwa E-Mail?

E-Mail ist sicher ein großes Thema. Hier stellt sich die Frage, ob es nicht sinnvoll wäre, die private Nutzung von E-Mail – aber auch von Internet – einzuschränken. Eine weitere Frage wäre, inwieweit das Unternehmen darauf achtet, welche internen Informationen das Haus verlassen dürfen. Derzeit ist es so, dass Mitarbeiter via E-Mail alles wegschicken können. Das stellt natürlich ein gewaltiges Sicherheitsrisiko dar.

Zum Beispiel?

Der Mitarbeiter X kann beispielsweise Konstruktionspläne, Vertragsentwürfe und so fort an seine private Mail-Adresse schicken. Der Heim-PC steht aber auch allen anderen Familienmitgliedern zur Verfügung und ist darüber hinaus nicht entsprechend gesichert. Ich denke, es muss einfach gewährleistet sein, dass interne Dokumente da bleiben, wo sie hingehören. Selbiges gilt für Wechselmedien wie USB-Sticks oder externe Festplatten – aber auch iPods. Kaum einer achtet darauf, dass auch in diesem Fall die Daten verschlüsselt sein müssen. So ein USB-Stick geht leicht verloren oder wird irgendwo liegen gelassen. Nachdem diese Medien im Normalfall keinen Schutz haben, kann jeder die Daten, die sich darauf befinden, ganz leicht einlesen.

Welche administrativen Aufgaben und welchen zeitlichen Aufwand erfordert eigentlich eine angemessene IT-Security?

Es ist ein Irrglaube zu meinen: Ich kaufe mir jetzt so ein Teil, lasse es mir implementieren und damit hat sich die Sache erledigt. Natürlich gibt es Möglichkeiten, mit denen man die Administration bis zu einem gewissen Grad automatisieren kann. Regelmäßige Überprüfung ist aber dennoch unumgänglich. Ein Grundmonitoring sollte täglich gemacht werden, eine Re-Auditierung des Netzes sollte zumindest – je nach Größe des Unternehmens – pro Quartal beziehungsweise halbjährlich erfolgen. Mit seinem Auto fährt man ja schließlich auch einmal im Jahr zur Pickerl-Überprüfung.

www.kapsch.net

Das Informationszeitalter birgt eine Menge von Risiken. Sicherheit wird so zu einem wesentlichen Bestandteil von Firmennetzwerken. Foto: Kapsch BusinessCom

Steckbrief

Thomas Blaschka ist Head of Product Management der Kapsch Business Com AG.
Foto: Kapsch BusinessCom