

## Mitarbeiter sensibilisieren in österreichischen Unternehmen

*Ob vertrauliche Daten auf einem USB Stick, oder das klassische PostIt mit dem Passwort auf dem Bildschirm. Das Sicherheitsbewußtsein in österreichischen Unternehmen hat Nachholbedarf.*

Österreichische Unternehmen rüsten Ihr Netzwerk mit immer besseren und ausgefeilteren Firewalls auf, es werden mehrstufige Virenschutz-Lösungen realisiert und DMZs eingerichtet. Nun ist diese Tatsache alleine ja nicht schlecht, ganz im Gegenteil. Ich bin froh, dass die Unternehmen endlich erkannt haben, dass Ihr Netzwerk keine Insel ist, sondern mit vielen anderen Netzwerken auf verschiedenste Arten verknüpft ist. Dennoch mache ich mir zuweilen Sorgen um die Sicherheit in einigen österreichischen Unternehmen. Es wird das Hauptaugenmerk eindeutig darauf gelegt, das Netzwerk gegen Angriffe von außen abzusichern, dabei aber vergessen, dass ein "Angriff" ob gewollt oder ungewollt auch von Innen erfolgen kann. So zeigt unsere Recherche in österreichischen KMUs, dass noch immer sehr schwache Passwörter von vielen Mitarbeiter benutzt werden, obwohl es sich mittlerweile bereits herumgesprochen haben sollte, dass man mit etwas Logik und ein paar Regeln sehr gute und auch zu merkende Passwörter gefunden werden können.

Eine weitere Schwachstelle ist unserer Ansicht nach, dass die Mitarbeiter dem geschriebenen Wort mehr vertrauen, als dies berechtigt ist. Wenn Ihnen ein Fremder auf der Straße erzählt, dass Sie gerade von einem Ihnen gänzlich unbekanntem in Nigeria lebenden Onkel etwas geerbt haben, würden die meisten darüber lachen. Wenn der gleiche Fremde, diesen Sachverhalt in einer E-Mail schreibt, beginnen sehr viele darüber nachzudenken, ob das nicht doch möglich wäre. Hier sollten die Mitarbeiter noch viel mehr sensibilisiert werden. Das kann unserer Meinung nach nur über Schulungen Trainings, oder ähnlichen Mitteln erfolgen. Selbst ein strenges Regelwerk wird hier nicht funktionieren.

Viel wird auch über den Schutz persönlicher Daten diskutiert, man redet von verschlüsselter 'Speicherung, und ähnlichen Methoden. Dennoch werden Unmengen von Daten auf simplen USB-Sticks herumgetragen. Aufmerksame Beobachter entdecken sehr viele solcher vergessener Datenträger an PCs, oder Notebooks. Diese Medien sind vermutlich viel zu einfach zu handhaben, als dass der Einsatz von diesen in Unternehmen kontrolliert werden könnte und das schlichte Verbot von solchen Medien wäre wohl eher kontraproduktiv.

Interessant in diesem Zusammenhang ist auch, dass nach der Studie der Hagenberg 70% der Unternehmenangaben einen Sicherheitsverantwortlichen im Unternehmen zu haben, jedoch davon 18% dieser Sicherheitsverantwortlichen keine dementsprechende Ausbildung haben. 57% der Unternehmen haben kritische produktive Maschinen mit dem Firmennetz verbunden, jedoch nur 25% spielen auf diesen Maschinen Sicherheitsupdates ein, wenn es welche gibt. 82% der Befragten Unternehmen gaben an, dass sie das Risiko einer Wirtschaftsspionage als niedrig oder nicht vorhanden einstufen. Sie möchten diese Studie als PDF herunterladen -> Hagenberger Studie März 2008

Wir haben uns hier nur einige offensichtliche Themen herausgepickt, aber wir stellen dieses Thema zu Diskussion, denn wir denken, dass gerade im kommenden Jahr hier viel getan werden sollte, um die österreichischen Unternehmen wieder etwas sicherer zu machen.