I T – Services

Das Thema IT-Security ist heutzutage, sowohl für den privaten, als auch für den öffentlichen und wirtschaftlichen Sektor, von herausragender Be-deutung, Ziel ist die Vertraulichkeit, Verfügbarkeit und Integrität von Systemen und Daten zu gewähr-leisten. Durch die voranschreitende Entwicklung und Verbreitung neuer Technologien (Web 2.0, mobile Internet und Voice over IP (VoIP) und dem ver-mehrten Einsatz von mobilen Endgeräten (Note-books, Smart-Phones, und PDAs) steht die e-Community vor immer größer werdenden Heraus-forderungen.

Maßnahmen um sich gegen Angriffe zu schützen und die Vertraulichkeit, Verfügbarkeit und Integrität zu gewährleisten lassen sich in infrastrukturelle Maßnahmen und organisatorische Maßnahmen unterteilen, die wichtigsten seien hier genannt:

Organisatorisch:

Sicherheitsaudits und Security Awareness Trainings, Erstellen von Security-Policies

Infrastrukturell:

Firewalls, Intrusion Prevention Systeme (IPS), Content Scanner, Antiviren Lösungen und Verschlüsselung von Systemen und Kommunikation um durch Virtual Private Networks (VPN) oder der eMails selber.

Im privaten Bereich bedeutet das den Schutz der privaten Daten durch den Einsatz von verschiedenen Technologien vor fremden Zugriff, das können u.a. Bank Daten, persönliche Korres-pondenz in Form von eMails, elektronische Tagebücher und Intellectual Property sein.

Wenn das nicht geschieht, können private Daten abgegriffen, missbraucht und / oder veröffentlicht werden oder sonst wie verwendet werden - so kann finanzieller Schaden entstehen, und privates der Öffentlichkeit zugänglich gemacht werden.

Dem öffentlichen Sektor (Verwaltung) obliegt ein ganz wesentlicher Schutzauftrag, oder gar -zwang. Auftrag der Verwaltung ist den Bürger, und alle ihn persönlich betreffende Daten und Informationen die für ihn von (wesentlichem) Belang sind, zu schütz-en. Dies sind zum einen Information über den einzelnen Bürger selbst zum anderen Informationen die dem Bürger zugänglich gemacht werden (müssen). Für EoE ist insbesondere der Bildungsbe-reich von Relevanz.

Das bedeutet, dass das Wissen jedem Bürger zugänglich gemacht werden muss. Wissensarchi-vierung, (berufliche) Interessensausrichtungen in Bildung und Ausbildung müssen individuell und privat bleiben, damit sich soziale Verantwortung im Sinne des Gemeinwohls frei entwickeln kann, es ist unbedingte Aufgabe der Lehre, das zu vermitteln

Es muss immer gewährleistet sein, dass die privaten Daten der Bürger sicher und unantastbar sind. Der Bürger muss sich stets seiner Privatsphäre sicher sein. (Freiheit des Geistes)
Nur ein Bürger der sich dessen sicher sein kann, ist ein freier Bürger, nur ein freier Bürger wird seine Potenziale entwickeln können und dem Gemein-wohl zur Verfügung stellen wollen.

Im wirtschaftlichen Sektor hat IT Sicherheit vor allem folgende Relevanz:

- Schutz der firmeneigenen Intellectual Property vor internen und externen Gefahren. (Datendiebstahl/-missbrauch).
- Schutz vor (System-)Angriffen von intern und extern.
- Entstehende Rationaliserungspotenziale wg eingesetzter Sicherheitstechnologien

In der jährlich vom CSI/FBI herausgegebenen Studie „CSI Computer Crime and Security Survey[1]“ lässt sich ein Trend zu sinkenden Verlusten durch Cyberkriminalität durch den Einsatz von Sicherheits-technologien erkennen.
EoE arbeitet mit allen drei Sektoren zusammen und setzt die modernsten IT-Sicherheitstechnologien ein um die eigene Infrastruktur und Daten zu schützen, als auch die Kommunikation und die Anbindung von Partnern aus der Wirtschaft, sowie die Anbindung von dem öffentlichen Sektor (Schulen) als auch den Bürger/Schüler selbst.

[1] CSI Computer Crime and Security Survey 2008 by Robert Richardson, CSI Director