SCHLACHTFELD SOFTWARE

03.11.2009
Bericht VKÖ - RB

Der globale Krieg steht nicht bevor, er hat schon vor Jahren begonnen. Die Gegner werden sich nie sehen, obwohl sie vielleicht Tür an Tür leben oder auf einem anderen Kontinent. Es fließt kein Blut, sondern Daten. Die Kosten und Schäden dieser globalen Auseinandersetzung sind höher als die Militärausgaben im Irak. Im Gegensatz zu physischen Auseinandersetzungen merken die Opfer der digitalen Konfrontation meist nicht einmal dass sie Opfer sind.

Die zunehmende elektronische Vernetzung der Unternehmen bietet ungeahnte Möglichkeiten der Information und Transparenz von Geschäftsprozessen. Die Euphorie über neue Möglichkeiten verdeckt aber meist die Risiken und Gefahren der Manipulation die von dieser neuen Welt ausgehen. Der Zugriff auf wertvolle Unternehmensdaten und personenbezogenen Kundendaten durch Kriminelle kann ein Unternehmen nachhaltig schädigen.

Jeder der einen Computer besitzt weiß es dass es Viren, Würmer, Malware, Datendiebstahl etc. gibt, trotzdem gibt es noch immer Geräte, die ohne jeden Schutz sind. 3% aller Delikte werden weltweit bereits mittels Computer und Internet begangen und trotzdem denken noch immer viele Menschen, mir passiert so etwas nicht, ich passe ja auf. Vor dieser Vogel-Strauß-Perspektive sind nicht einmal Firmen gefeit. Unglaublich, aber ganze Firmennetzwerke liegen offen für jedermann, Grundkenntnisse im Hacken genügen. Heute reicht selbst die routinemäßige Installation von Firewalls oder Intrusion Detection-Systemen nicht mehr aus, es bedarf sowohl technischer, als auch organisatorischer Maßnahmen um Daten zu sichern.

Eine weitere Gefahrenquelle hat sich auf diesem Gebiet aufgetan. In den letzten Monaten hat sich ein Trend von einfachen Standard Mobiltelefonen zu moderne Smartphones ergeben. Diese arbeiten heute wie Computer und verwenden bekannte Technologien, haben daher auch die gleichen Schwachstellen, doch sämtliche Schutzmittel wie Firewalls, Virenscanner, Sicherheitspatch, etc. sind auf diesen Geräten unbekannt. Eine Gefahr der sich kaum ein User dieser Geräte überhaupt nur ansatzweise bewusst ist. Im Gegensatz zu tragbaren Computern wird Geräten dieser Art nur wenig Beachtung in Hinblick auf das Bedrohungspotential geschenkt. Um die Mobilität der Mitarbeiter zu erhöhen, gelangen immer mehr unternehmenskritische Daten auf Smartphons und sind durch ihre geringen Schutzmechanismen leicht zu knacken.

Selbst jene Menschen und Firmen, die sich Gedanken über ihre Datensicherheit machen, können sich nicht der Gefahr Angriffsziel eines Cyberkriminellen zu werden entziehen. Es ist ein ewiger Wettlauf zwischen Angreifern aus dem Cyberspace mit den Verteidigern. Probleme werden zwar temporär gelöst, aber im Grunde ist dieses Wettrüsten nicht zu gewinnen.

Die Wahrnehmung, dass Sicherheitsprobleme im IT-Bereich sowie im Bereich so genannter „kritischer Infrastruktur“ rein technisch bedingt und daher auch nur technisch lösbar wären, führt auf ein Niveau, vor dem ausschließlich der technische Teil der Sicherheit betrachtet wird. Stellt man aber nicht nur das technische Wettrüsten in den Vordergrund, sondern beginnt die Gründe und Ursachen von Sicherheitsproblemen zu analysieren, stellt man fest, dass auch das menschliche Handeln ein Faktor der Unsicherheit ist.

Die Donau-Universität-Krems hat das Studium über Sicherheitsprobleme seit Beginn an in ihrem portfolio und bietet seit 2001 auch einen Lehrgang Informations-Security an. Begleitend wird

seit dieser Zeit auch jährlich eine Informations-Sicherheitskonferenz abgehalten. Die 7. Information Security Konferenz dieser Serie fand heuer unter dem Leitthema „Critical Infrastructures“ am 29. Oktober statt. Im Programm fanden sich rein theoretische, hoch akademische Betrachtungen bis zu praxisorientierten Lösungen und Anwendungen.
Mag. Dr.Walter Seböck, Leiter des Zentrums für Praxisorientierte Informatik, zeichnete in seinem Einführungsvortrag eine düsteres Bild der Cyperwelt. Während man vor wenigen Jahren der Informationssicherheit kaum Bedeutung beigemessen hat, kann heute niemand mehr an dem Thema vorbei. Der Datendiebstahl hat um 100% zugenommen, Terroristen finden über das Internet eine Propagandaplattform, Erpressungen, dass man Firmennetzwerke lahm legt, nehmen rasant zu und Spammails mit betrügerischem Inhalt überschwemmen millionenfach Server, Leitungen und Endgeräte.
DI. Martin Pirker von der Technischen Universität Graz erläuterte dem Fachpublikum, dass Computersicherheit weitgehend Software abhängig und dies auf Dauer unbefriedigend ist. „Software passt auf Software auf“ hat seine Grenzen. Niemand finde beim Starten seines Computers Anhaltspunkte, ob der Rechner in einem befriedigenden Zustand ist. Die Lösung sieht er in der Bindung von geheimen Daten an einen bestimmten Systemzustand. Erreichbar ist dies mit Trusted Plattform Modulen (TPM) einem zusätzlichen Baustein im PC. Der Vorteil: Hardware lässt sich nicht so leicht manipulieren wie Software.
Die Gefahr ultramobiler Geräte zeigte DI Peter Teufl, ebenfalls von der TU-Graz auf. Vor allem zum Zwecke der Spionage werden Smartphones angezapft und hier weiß man, im Gegensatz zu einem Computerstandort, wo sich das Gerät befindet. Für Hacker heute kein Problem ein Smartphone zu einem trojanischen Pferd für den Besitzer zu machen.
Ein Duo der Fachhochschule St.Pölten erklärte den Konferenzteilnehmern die Bedrohungslage durch s.g. Botnetze

(Verbund infizierter Computer). Bereits 1991 als mögliche Zukunftsaussicht vorgestellt, wurde 1993 der erste IRC-Bot (Eggdrop) veröffentlicht. 1999 ginge das erste bösartige Botnetz in Betrieb, das einen Trojaner ins System einschleuste. Im Jänner 2009 wurden bereits 9 Millionen Infektionen durch den Wurm „Conficker“ der über Botnetze verschickt wurde, festgestellt. Botnetze, so wurde festgestellt, bestehen aus bis zu 50.000 Geräten. Die zu „Computer-Zombies“ degenerierten Geräte werden vor allem zur Versendung von Malware missbraucht. 2008 registrierte man bereits 62.000.000.000.000 Spams im Netz, 85% davon liefen über Botnetze. 400.000 Spams für nur 55 Euro sind derzeit der Diskontpreise der angeboten wird.

Eine interessante Gegenstrategie gegen die Infizierung eines Computernetzwerkes wurde von Emanuel Klein vorgestellt – Honeypots. Im Prinzip werden in ein Netzwerk Geräte eingebaut, die keine produktive Aufgabe haben. Jede Aktivität zu diesen Geräten ist daher verdächtig und lässt einen Angriff von außen möglich erscheinen.

Spams könnte man ja noch als lästig, aber nicht gefährlich bezeichnen, aber die kriminelle Intensität endet damit nicht. Es sind bereits Erpressungsfälle bekannt, dass man Firmen androhte, ihre Netzwerke und Informationszugänge zu kappen, wenn es nicht zu Zahlungen kommt. Politisch motiviert dagegen der erste Cyberwar gegen Litauen, tagelang ging in dem kleinen baltischen Staat nichts mehr was über Computer lief oder der Angriff auf das Bankensystem in Südkorea.

Je stärker unternehmerische und staatliche Wertschöpfungsprozesse und die damit verbundenen Informationen ausgebaut werden, desto höhere Priorität muss dem Thema der Informationssicherung gewidmet werden. Vor allem aber muss aber das Bewusstsein

geschaffen werden, dass das Internet ein Einfallstor für kriminelle Aktivität ist und man sich zum unfreiwilligen Helfer macht, wenn man keine Abwehrmaßnahmen beachtet.

R.B.

Zitat:

„Das Abschneiden von Information ist genauso gefährlich wie das Niederbrennen eines Hauses“ – Mag. Dr. Walter Seböck