Protokoll der Veranstaltung:

Sicherheit in Internet aus Unternehmersicht

Zeit und Ort der Veranstaltung: 22.9.05, Hörsaal 117

Protokoll: Lara M. Pair, JD

Moderator: Wolfgang Golasowski

Vortragende: Dr. S. Streitz, Peter Knapp

Die Veranstaltung begann pünktlich mit einer kurzen Moderation von Herrn Golasowski, der die Höher mit einer kurzen Anekdote wie sich der Umgang mit Daten im Internet in den letzten 20 Jahren verändert hat, begrüßte. Herr Dr. Lapp, der ursprünglich moderieren sollte, ließ sich entschuldigen.

Den ersten Vortag übernahm Dr. Siegfried Streitz. (www.streitz.de) Dr. Streitz ist EDV – Sachverständiger und hat sich mit 3 Themen auseinander gesetzt: dem Internet Shop, dem sog. Dialer, und dem neuen Phänomen des Identity Fishing.

Bezüglich des Internetshops beschrieb Dr. Streitz die Möglichkeiten der Beweisführung. Es wurde angeführt, dass in jedem Internetshop die Profile der Kunden von einem Insider geändert werden können, so dass bei späterem ausscheiden, der Kunde zwar keinen Zugriff mehr hat, aber der Insider diesem Profil administrative Kapazitäten zuordnen kann und damit Zugriff auf viele andere Kunden und deren Bestellungen erhalten kann.

Diese Änderungen werden jedoch von vielen Programmen protokolliert und können später nachvollzogen werden. Als Beispiele nannte Dr. Streitz das Hackerprogramm Brutus (siehe www.hoobie.net/brutus), welches alle Hacks auf dem PC des Täters protokollierte, parallel dazu speicherte auch das benutzte Internetzugangsprogramm (Internet Explorer) alle angewählten Adressen, die Anwahlzeiten usw.

Auf der Seite der betroffenen speichert auch das Programm der Internetseite des Shops Vorgänge, auch die Software des IP Dienstes, der Speicherplatz zur Verfügung stellt, protokolliert die Vorgänge. Mit diesen protokollierten Vorgängen, ist der gestammte Beweis erbracht und auf eine Hauptverhandlung kann möglicherweise verzichtet werden, da alle Vorgänge lückenlos nachvollziehbar klärbar werden.

Bezüglich der sog. Dialer berichtete Dr. Seitz von Programmen die sich als sog. Trojaner im PC einnisteten und teure Vorwahlen zum Internetzugang verwendeten, anstelle der günstigen oder vorher einprogrammierten. Diese meist 0190 Nummern, die sich als Trojaner installierten wurden meist von Zahlservicen wie www.Hausaufgaben.de verwendet. Es gab zwar für solche Nummern Blocker, jedoch war die Installation häufig aufzufrischen.

Jedoch haben zwei neue Gesetze vom November bez. September 03 das Problem weitgehend beseitigt indem z. B. die Zahlungsverpflichtung entfällt. Nähere Informationen gibt es auch auf www.bundesnetzagentur.de

Bezüglich des sog. ID Fishing bezeugte Dr. Streitz, dass dies noch kein Problem der Rechtswissenschaft, doch der zukünftigen Praxis ist. ID Fishing bezeichnet die kriminelle Praxis, unerlaubt Daten von E-Mail Adressen und Passwörtern zu erlangen und damit unbefugt im Internet zu handeln.

Dies geht wie folgt vor sich: Ein Kunde erhält eine E-Mail die einem seiner frequentierten Shops oder Services täuschend ähnlich sieht. Der Kunde wird aufgefordert eine im Link angegebene IP Adresse aufzusuchen und zur Authentisierung Daten einzugeben. So schöpft der Versender Daten ab und benutz sie unbefugt. Solche Möglichkeiten ergeben sich vor allem bei bestimmten Internetbrowsern, die kein Java haben. Noch gibt es für dieses Problem keine Lösung.

Damit beendete Dr. Streitz seinen Vortrag.

Herr. P. Knapp von Interxion Deutschland, GmbH, stellte danach die Nationale Initiative für Internet Sicherheit vor. www.nifis.de. Diese Initiative richtet sich vor allem an Provider und Unternehmen, die Standards und Lösungen für Mitglieder des Vereins anbieten, was alle Arten von Sicherheitsrisiken im Internet für Unternehmer angeht. Dies solle zunächst mit Aufklärung über Gefahren geschehen, dann durch Zusammenarbeit Lösungen erarbeiten und implementieren. Vor allem soll der Verlust von Daten verhindert werden durch Firewall, Spam und Virenschutzsysteme.

Damit endete die Präsentation von Herrn Knapp. Der Moderator sprach noch ein paar Schlussworte.