Das weltweite Netz vergisst nicht ...

Über Schwachstellen von Software informiert Erwin Markowsky Erwachsene und Jugendliche

Wer hat nicht schon mal einen Fehler in einer Anleitung oder einem Text gemacht? Richtig. Niemand ...

Aufmerksam folgen die Schüler dem Vortrag von Erwin Markowsky über Risiken des Internets. Fotos: Waldecker Bank

Korbach. Erwin Markowsky von der 8com GmbH und Co. KG zeigt, dass jede Software kleine, tückische „Fehler" und Sicherheitslücken enthalten kann, die Kriminelle ausnutzen könnten, um persönliche Daten aller Art abzugreifen. Die Veranstaltung, die von der Waldecker Bank eG und der Stadt Korbach initiiert wurde, war Teil der Korbacher Präventionswoche.

Während die knapp 450 Schüler sowie deren Lehrkräfte noch einen Platz in der Korbacher Stadthalle suchen, lässt Referent Markowsky bereits einen Scan laufen, um herauszufinden, wer denn so alles im Publikum sitzt. In kürzester Zeit tauchen dabei Gerätenamen wie meli, discoqueen, Kitty, alphatier oder Amazone auf. „Relativ harmlos", meint der Referent.

Manipulieren kinderleicht

Doch die Bezeichnung ist nicht die einzige Information, die eine aktive Bluetooth-Schnittstelle preisgibt. Markowsky findet von einem Testhandy beispielsweise die Versionsnummer und noch einiges mehr heraus. „Ein Handy ist so einfach zu manipulieren und Daten herunterzuladen", sagt er. Umgehen und abändern von Softwarebefehlen sei bei manipulierten Geräten kinderleicht.

Auch das Mithören von Gesprächen, wenn das Handy in der Hosentasche steckt, konnte das Publikum live miterleben. Dazu schickte Markowsky einen Schüler und eine Schülerin aus dem Raum, um zu „flirten". Alle im Raum Verbliebenen konnten dann das Gespräch über Lautsprecher mithören.

Nicht nur beim Handy, auch beim Umgang mit Laptop und PC gibt es viele Dinge zu beachten. So sollte man aktuelle Softwareupdates nicht ignorieren, da mit ihnen meistens Sicherheitslücken geschlossen werden. Ein aktueller Virenscanner, eine Firewall und ein gesundes Misstrauen gegenüber allem Unbekannten können zudem folgenschwere Situationen verhindern.

Gemeinsam mit Schüler Erik führte Markowsky vor, wie wichtig ein kryptisches Passwort doch sein kann. Das zunächst gewählte Kennwort „Heike" knackte die Software innerhalb weniger Sekunden. Erik sollte sich ein neues Kennwort für den Administratorbenutzer des Testrechners ausdenken, doch prompt erschien das eingegebene Kennwort auf den Bildschirm des Referenten. Der hatte den ungeschützten Rechner zuvor mit einem Keylogger infiziert, welcher es ihm gestattete, alle Tastatureingaben zu verfolgen. Markowsky konnte den Rechner über wenige Befehle in kürzester Zeit fernsteuern.

Löschen fast unmöglich

Als weiteres Thema vermittelte der Referent seinen jungen Zuhörern die Gefahren der sozialen Netzwerke und der ungeschützten Informationsweitergabe im Netz. Vor allem in Facebook und Co. könne sehr vieles mitgelesen und verwertet werden.

Durch peinliche Informationen war beispielsweise die Traumkarriere einer Klientin in weite Ferne gerückt. Auch vor ungewollter Verbreitung von Fotos und Videos warnte Markowsky. In einem Fall sei seine Firma bereits seit fünf Jahren bemüht, ein Nacktfoto für eine weitere Klientin aus dem Netz zu löschen, doch das Netz vergisst nicht. Bis nach Japan sei man dem Bild gefolgt – und alles nur, weil sich die Freundin der damals 14-Jährigen einen Scherz erlauben wollte.

Der Referent mahnte auch, im Umgang mit Tauschbörsen achtsam zu sein, und führte als Beispiel den Fall eines 17-Jährigen auf, der angeblich 400 Songs heruntergeladen haben sollte. Eine Anwaltskanzlei verlangte nach einem Widerspruch bis zu 250 000 Euro Schadensersatz, da der Junge die Songs unwissentlich auch zur Weitergabe bereitgestellt hatte. Vor allem das Verbreiten ließ die Summe in die Höhe schnellen. „Auch das Anschauen von abgefilmten und bereitgestellten Filmen ist nicht legal und kann hohe Bußen nach sich ziehen", ermahnte Markowsky die Schüler, die den Referenten mit kräftigem Applaus nach einer spannenden und anschaulichen Vorführung verabschiedeten.

Am Abend begrüßten Bank-Vorstand Karl Oppermann und Erwin Markowsky das etwas ältere Publikum. Rund 220 Interessierte hatten den Weg in die Stadthalle gefunden und waren gespannt, was der Referent zu präsentieren hatte. Wie bereits am Vormittag bezog er sein Publikum ein und zeigte an diversen Beispielen, wie einfach der Datenklau sein kann.

Vertraue keinem

Als zusätzliche Programmpunkte nahm Markowsky die Bereiche Phishing und Online-Banking in sein Repertoire auf. Er verriet, wie Kriminelle das mittlerweile veraltete PIN/TAN-Verfahren überlisten konnten und dass das heutige Sm@rt-TAN Verfahren bisher allen Attacken standgehalten habe.

Markowsky warnte, jeder E-Mail zu vertrauen. Auch wenn der angebliche Absender bekannt sei, könne sich eine ganz andere Person dahinter verbergen. So schrieb der Referent eine angebliche Mail vom Bundeskanzleramt an die Parteispitze der SPD mit einer Spendenbitte, die in der angehängten PDF-Datei erklärt werden sollte. Sobald der Empfänger die Datei geöffnet hatte, bekam er jedoch nur eine Fehlermeldung, während im Hintergrund unbemerkt Schadsoftware ausgeführt wurde. Ohne es zu wissen, hätte ein unbedarfter Benutzer nun auf seinem Rechner für einen Hacker Tür und Tor geöffnet.

Auch an diesem Abend begeisterte Markowsky sein Publikum und verabschiedete sich nach zwei interessanten Stunden mit dem Ratschlag, sich über die zehn Gebote der Internetsicherheit zu informieren (z. B. unter http://www.waldecker-bank.de). (r)