

Den Bösen zuvorkommen

Für **SICHERHEIT IM INTERNET** zu sorgen, ist Erwin Markowskys tägliches Brot. Für Erlanger Schüler hält er nun Online-Vorträge.

Um die Gefahren im Internet dreht sich die Veranstaltung „SpardaSurfSafe“ in Erlangen. Erwin Markowsky, professioneller Hacker der IT-Sicherheitsfirma 8com, führt live vor, wie einfach es ist, auf fremde Smartphones oder Computer zuzugreifen. Wir haben mit ihm darüber gesprochen, wie es ist, in fremde Identitäten zu schlüpfen, und was er Leuten rät, die sich im Internet schützen wollen.

Herr Markowsky, Sie sind professioneller Hacker. Könnten Sie mein Konto hacken und für sich Geld abzweigen?

Mit den richtigen Tricks könnte ich das schon machen (*lacht*). Aber man hat sich ja irgendwann mal für eine Seite entschieden.

Sie wollen zu den Guten gehören...

Genau. Es gibt drei verschiedene Arten von Hackern. Einfach gesagt sind Whitehats die Guten, Greyhats der Mittelweg und Blackhats sind die Böartigen, die versuchen, wirklich Schaden anzurichten ohne Rücksicht auf Verluste. Ich bin, wenn Sie so wollen, als Whitehat vor allem im Einsatz gegen Blackhats. Für mich als Familienvater und Fußballtrainer war es wichtig, mit Jugendlichen zu arbeiten. Die kennen sich mit den Geräten zwar meistens super aus, unterschätzen aber die Gefahren im Netz. Und da müssen wir mehr Aufklärungsarbeit leisten. Das mache ich als Referent wie jetzt bei den Vorträgen in Erlangen.

Und Ihre Hacker-Tätigkeit?

Ich bin bei derselben Firma außerdem als Social Engineer tätig. Dabei arbeite ich mit der größten Schwachstelle, die wir im Bereich Cybersicherheit kennen: dem Menschen. Ich lege mir einfach eine vertrauenswürdige Identität zu und gehe zum Beispiel verkleidet als Handwerker oder Techniker in ein Unternehmen und schaue, was ich dort alles anstel-



Foto: 8com

Erwin Markowsky (51) ist Informationssicherheitsexperte und arbeitet als Referent und technischer Prüfer für das Cyber-Security-Unternehmen 8com.

len kann. Da bin ich bisher leider immer in Räumlichkeiten reingekommen, wo ich nichts verloren hatte. Ich nutze dabei menschliche Schwächen aus, um mir Zugriff zu Büros, Serverräumen oder ganzen Produktionsanlagen zu verschaffen.

Was machen Sie, wenn Sie erst mal im Unternehmen drin sind?

Ich könnte zum Beispiel Rooter anschließen und das Netzwerk infiltrieren oder Spyware installieren. Ich muss mich in einen Kriminellen hineinversetzen und versuche dann nicht nur, Unternehmen von außen zu hacken, sondern eben auch vor Ort. Ich muss herausfinden, wie sich die Mitarbeiter verhalten, wenn jemand mit seinem Koffer kommt und behauptet, er sei von der Telekom. Ich richte aber natürlich keinen Schaden an, sondern berichte den Unternehmen anschließend, was möglich gewesen wäre und wo

es Nachholbedarf gibt.

In den USA wurde soeben das Wirtschaftsministerium gehackt. Das ist ein Riesending. Aber was gibt es für Hacker denn zu holen bei Jugendlichen und Erwachsenen, für die Sie Vorträge halten? Müssen die sich wirklich Sorgen um ihre Datensicherheit machen?

Viele Menschen denken, „ich habe nichts zu verbergen“ oder „mir können sie nichts antun“. Aber in diesem Fall geht es um Massenangriffe. Und die finden permanent statt. Die meisten Privatnutzer werden rein zufällig zum Opfer. Immer wieder werden zum Beispiel durch Sicherheitslücken Passwörter im Internet bekannt. Als Hacker ist das für mich ein Jackpot. Ich probiere die Kombination aus Benutzername und Passwort mit einem Programm auch bei anderen Diensten aus. Und da die meisten Nutzer ihre Passwörter mehrfach verwenden, hab ich in

Sekundenschnelle digitale Identitäten gestohlen. Damit kann ich dann zum Beispiel in Ihrem Namen bei Amazon einkaufen. Sie bezahlen, ich liege in der Sonne und kriege die Ware.

Das kann also jeden treffen...

Klar, das erwischt letztendlich jeden, der sich nicht um den Schutz seiner Geräte und Benutzeraccounts kümmert. Nehmen wir ganz aktuell das Beispiel Homeoffice: Firmen stellen ihren Mitarbeitern Laptops zur Verfügung, aber keiner macht sich Gedanken darüber, welchen Router die Mitarbeiter zuhause haben. Viele Leute benutzen das voreingestellte Passwort nach zehn Jahren immer noch. Der Router ist eine Schwachstelle, über die Kriminelle in ein Netzwerk eindringen können.

Das heißt, Sie empfehlen starke, komplizierte Passwörter?

Definitiv. Aber was kompliziert aussieht, muss nicht kompliziert sein – man muss sie sich ja noch merken können. Man sollte aber auch wissen, dass zum Beispiel alles, was im Duden steht, innerhalb von Sekunden gehackt wird. Wenn Sie jedoch Dialekt einsetzen, im Fränkischen etwa „Bradwürschdla2018“, dann haben Sie etwas, wo ein normaler Rechner Jahrhunderte braucht, das zu rechnen. Die Leute müssen sich etwas überlegen, um die Angriffsfläche zu verkleinern, denn in der Corona-Zeit greifen die Kriminellen Privatleute noch mehr an als bisher.

Stichwort Corona: Gehen Sie auf Datensicherheit im schulischen Bereich ein?

Mit Blick auf Homeschooling sehe ich da vor allem die Länder in der Pflicht, endlich eine gute digitale Lösung für alle Beteiligten zu finden, die auch den Anforderungen an den Datenschutz entspricht. In puncto Digitalisierung hinken wir noch massiv hinterher.

Die Digitalisierung wird durch Corona beschleunigt. Gleichzeitig nimmt auch Cybermobbing zu. Für Sie ein Thema?

Auf jeden Fall. Ich muss auch die Eltern ein bisschen wachrütteln. Wir begegnen Jugendlichen, die gemobbt werden und von den Eltern hören „stell' dich nicht so an“. Dabei ist Mobbing eine wirklich üble Geschichte. Und das endet heute nicht mehr mit der letzten Schulstunde, sondern geht im Netz einfach weiter. Eltern sollten also sehr sensible Antennen haben. Natürlich geben wir Hilfestellung dazu und ermutigen die Jugendlichen, nicht zum Mitläufer zu werden und sich für andere stark zu machen.

INTERVIEW: EVA KETTLER

ZUR SACHE

„SurfSafe“: Am Sonntag kann sich jeder zuschalten

ERLANGEN - Die Corona-Krise hat es ganz deutlich gezeigt: Es gibt Nachholbedarf in Sachen Medienkompetenz. Inhalte kritisch zu hinterfragen, seriöse Nachrichten von Fake News zu unterscheiden, vertrauenswürdige Quellen erkennen – all das will gelernt sein. Die SpardaBank Nürnberg holt dafür, in Kooperation mit

der Stadt, das Medienkompetenz-Projekt „SurfSafe“ bereits zum zweiten Mal nach Erlangen: In diesen Tagen werden insgesamt bis zu 5000 Schüler ab der fünften Jahrgangsstufe in Online-Schulungen für die Gefahren im Internet sensibilisiert und über wichtige Themenbereiche der digitalen Welt aufgeklärt. Das umfangreiche

Angebot, das in diesem Jahr coronabedingt ausschließlich virtuell stattfindet, ist dank des Engagements der Sparda-Bank Nürnberg für alle Schüler kostenlos.

Am Sonntag, 20. Dezember, 18.30 bis 20 Uhr, schließt sich eine Infoveranstaltung für Eltern, Lehrer und alle anderen Interessierten an, die

sich und ihre Kinder für den verantwortungsvollen, sicheren Umgang mit dem Internet wappnen möchten. Jeder kann sich zuschalten. Zugang zur virtuellen Veranstaltung erhalten Interessierte unter www.spardasurfsafe.de/live. Die Teilnahme ist kostenfrei und ohne Registrierungs- oder Anmeldeverfahren möglich. **en**