

Audiopakete zu IT-Kriminalität

- Mitschrift: Radiobeitrag und O-Töne
- Berlin, 8. Oktober 2009
- O-Töne von Prof. Dieter Kempf, Präsidiumsmitglied BITKOM

Sendefertiger Radiobeitrag

+++ Anmoderation +++

Betrug per Internet ist längst nicht mehr ein Sonderfall, wenn es um kriminelle Aktivitäten geht. Im Web finden gut organisierte Betrüger noch zu oft leichte Beute. Das liegt teilweise an der Sorglosigkeit von Internet-Nutzern: jeder fünfte surft zum Beispiel ohne Virenschutz. Der Hightech-Verband BITKOM und das Bundeskriminalamt warnen: Kriminelle brechen in fremde Rechner ein auf der Suche nach persönlichen Daten. Immer mehr Bürger müssen erleben, dass Geld illegal von ihrem Konto abgebucht oder mit ihrer Kreditkarte eingekauft wird. Doch eine Reihe von Vorsichtsmaßnahmen und gesundes Misstrauen bieten Schutz – sagt BITKOM-Präsidiumsmitglied Prof. Dieter Kempf, zugleich Vorstandschef des Vereins „Deutschland sicher im Netz“. Jens Nöller berichtet.

+++ Beitrag mit O-Tönen +++

Kriminalität im Internet ist im Vormarsch. IT-Branche und Bundeskriminalamt warnen: Die Internet-Betrüger werden immer raffinierter. Die Zahl der Phishing-Opfer wächst, aber das ist noch lange nicht die größte Gefahr, wenn Schadprogramme Rechner ausspähen. BITKOM-Vorstandsmitglied Professor Dieter Kempf:

Beim Phishing, da wissen wir, dass der Schaden in dem Jahr zirka 11 Millionen Euro betragen wird. In Wirklichkeit sind die Kriminellen aber auf die Beschaffung der „digitalen Identität“ des Nutzers, weil ich mit der eben eine ganze Reihe krimineller Aktivitäten entfalten kann. (16 Sek.)

Das BKA kennt sogar Fälle von Internetnutzern, die ohne es zu ahnen von internationalen Verbrecherbanden als Geldwäscher benutzt wurden. Viele surfen im Netz, ohne von den Gefahren auch nur etwas zu ahnen – und viele sogar ohne jeden Schutz.

Es ist leider immer noch zirka ein Fünftel der Internetnutzer, das keine Virensoftware nutzt, und es ist ein deutlich größerer Anteil, der keine Firewall-Software benutzt. Ein sehr, sehr großer Anteil derer, die beides nutzen, hält sie nicht ständig up to date. (16 Sek.)

Bundesverband
Informationswirtschaft,
Telekommunikation und
neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel. +49. 30. 27576-0
Fax +49. 30. 27576-400
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner
Christian Spahr
Pressesprecher
Telekommunikation & Recht
Tel. +49. 30. 27576-112
Fax +49. 30. 27576-400
c.spahr@bitkom.org

Präsident
Prof. Dr. Dr. h.c. mult.
August-Wilhelm Scheer

Hauptgeschäftsführer
Dr. Bernhard Rohleder

Aktuelle Sicherheits-Software ist ein Aspekt von Sicherheit. Genau so wichtig ist für Professor Kempf Vorsicht. Passwörter wie der Name der Ehefrau sind für Kriminelle kein Hindernis, vor allem, wenn sie auf dem Rechner abgespeichert sind.

Ideal sind alphanumerische Kombinationen, also Kombinationen aus Buchstaben, Ziffern, vielleicht sogar Sonderzeichen, in gemessener Länge, und wo verwahre ich sie: am besten natürlich im Kopf. (12 Sek.)

Sorgen macht Kempf, wie viel vertrauliche Informationen Nutzer im Internet freiwillig über sich preisgeben – ohne einen Gedanken, dass Kriminelle solche Daten missbrauchen könnten.

Es ist erstaunlich, wie viel Kinder und jugendliche Nutzer sozialer Netzwerke schon einstellen. Letztlich ist es aber ausschließlich die Verantwortung des Nutzers. Das heißt, wenn wir wollen, dass er verantwortungsvoll damit umgeht, müssen wir die Aufklärungsarbeit verstärken. (16 Sek.)

Vorsicht im Netz und aktuelle Rechnerausstattung – das sind Maßnahmen, um die Risiken des Internet im Griff zu halten und an den ständig wachsenden Möglichkeiten teilzuhaben.

Einzelne O-Töne:

1. Ist das Internet heute noch eine Randzone krimineller Aktivität?

Nein, das ist es leider nicht mehr. Ich denke, wir alle müssen uns an den Gedanken gewöhnen, dass das Internet für kriminelle Handlungen genutzt wird, vermutlich auch in größerem Stil für organisierte kriminelle Handlungen. (12 Sek.)

2. Worauf sind Kriminelle im Internet heute aus, und wie viele Menschen werden Opfer solcher Aktivitäten?

Wie viele es erwischt, können wir immer nur an einzelnen Arten von kriminellen Akten festmachen. Zum Beispiel beim Phishing: Da wissen wir, dass der Schaden in dem Jahr ca. 11 Millionen Euro betragen wird, der bekannt gewordene Schaden mit ungefähr 3.000, knapp 3.000

Geschädigten. In Wirklichkeit sind die Kriminellen aber auf die Beschaffung der „digitalen Identität“ des Nutzers, weil ich mit der eben eine ganze Reihe krimineller Aktivitäten entfalten kann. (29 Sek.)

3. Was sind typische Maschen der IT-Kriminellen?

Wenn ich die digitale Identität eines Internetnutzers habe, dann kann ich sowohl versuchen, zum Beispiel sein Konto abzugreifen, indem ich mir eine PIN-TAN-Kombination abgreife, um dann eine Überweisung umzuleiten, zu tätigen. Ich kann ihn aber auch als – wie im Fachjargon – „man in the middle“, also als den Mann, der gar nicht weiß, dass er benutzt wird, nutzen, indem ich mir einfach seine digitale Identität zunutze mache, z.B. indem ich in seinem Namen Waren kaufe oder ihn als Mittelsmann illegaler Geldtransfers, Geldtransaktionen nutze. (39 Sek.)

4. Geben Sie uns ein Beispiel für einen solchen Fall?

Es gibt zu diesem Fall „man in the middle“, oder „money donkey“, wie man auch dazu sagt, eine schöne Beispielgeschichte, eines Mittfünfzigers, der sich in einem sozialen Netzwerk in eine junge hübsche Frau verliebt hat – dass sie jung und hübsch war, wusste er, weil sie ihm Bilder geschickt hat –, die ihm dann erzählt hat, sie würde ihn eigentlich gern besuchen, habe aber hierfür kein Geld; sie wolle aber gar kein Geld von ihm direkt überwiesen, sondern ihre Schwester schulde ihr noch Geld, und dieses Geld würde ihre Schwester auf sein Konto überweisen, und er möge dies doch dann weiter überweisen, in dem Fall nach Petersburg, damit sie die Reise bezahlen könne. In dem Beispielfall war der Mann sogar relativ vorsichtig, hat dabei aber nicht gemerkt, dass er in Wirklichkeit als Geldbote benutzt wurde für illegale Geldtransfers. Das Ende vom Lied war, dass er beim letzten Transfer, dessen Summe über der Aufgriffsgrenze oder Meldegrenze des Geldwäschegesetzes lag, erwischt wurde. Der Betrag, der ursprünglich von einem Schweizer Bankkonto auf sein Bankkonto überwiesen wurde, wurde zurückgezogen, er hatte dummerweise aber schon nach Petersburg überwiesen, blieb also auf dem finanziellen Schaden in sechsstelliger Euro-Höhe hängen. (1 Min. 12 Sek.)

5. Wie ernst nehmen die Nutzer das Thema Sicherheit im Internet?

Ja, das ist leider sehr schade, dass viele Internet-Nutzer sich dieser Gefahren noch nicht wirklich bewusst sind. Es ist leider immer noch ca. ein Fünftel der Internet-Nutzer, der keine Virus-Software nutzt, und es ist ein deutlich größerer Anteil, der keine Firewall-Software benutzt. Und was noch schlimmer kommt: ein sehr, sehr großer Anteil derer, die beides nutzen, Viren-Erkennungssoftware und Firewall-Software, hält sie nicht ständig up to date. All diese drei Aktionen wären notwendig, um hardware- und systemesoftwareseitig einen einigermaßen brauchbaren Schutz zu gewährleisten. Dazu kommen muss aber noch der verständige Umgang mit dem Internet. (45 Sek.)

6. Welche Regeln gibt es für sichere Passwörter, und wo bewahre ich sie am besten auf?

Also: Das Wichtigste beim Passwort ist natürlich, dass es keine Trivial-Passworte geben darf, geben soll. Also: Die berühmte 1-2-3-4-5-6, der Vorname der Ehefrau, der Vorname der Kinder, der eigene Kosenamen sind völlig ungeeignet. Ideal sind alphanumerische Kombinationen, also Kombinationen aus Buchstaben, Ziffern, vielleicht sogar Sonderzeichen, in angemessener Länge, und wo verwahre ich sie: am besten natürlich im Kopf. Das ist etwas schwierig, wenn es sehr viele Passwörter sind, es gibt am Markt hierfür aber Lösungsangebote, die einem helfen, das eigene Passwort zu verwalten, bzw. die Summe der eigenen Passwörter, die man ja für unterschiedliche Applikationen hat, zu verwahren. (48 Sek)

7. Was kann man tun, um das Sicherheitsbewusstsein zu stärken?

Die Veröffentlichung privater Daten im Internet, insbesondere in den so genannten sozialen Netzwerken, und die nicht bedachten Folgen dieser Veröffentlichungen sind in der Tat etwas, was uns in der Branche sehr beschäftigt. Was können wir tun? Das Allererste und Allerwichtigste ist Aufklärung, das muss bei den Kindern, bei den Jugendlichen beginnen. Es ist erstaunlich, wie viele Kinder und jugendliche Nutzer sozialer Netzwerke schon reinstellen. Man kann natürlich auch in den sozialen Netzwerken ein bisschen was tun, indem man an geeigneter Stelle, nämlich beim Input, den Nutzer darauf hinweist: „Willst Du dies wirklich einstellen?“ Letztlich ist es aber ausschließlich die Verantwortung des Nutzers, was er ins Netz stellt. Das heißt, wenn wir also wollen, dass er verantwortungsvoll damit umgeht, müssen wir die Aufklärungsarbeit verstärken. (49 Sek.)