

## **Interview: Abgefischt! Antiviren-Software schützt vor Datenklau im Netz.**

*Interview mit Ildiko Bruhns, ESET Deutschland GmbH*

### **|Anmoderationsvorschlag:|**

Ach ja, und täglich grüßt... – nein, nicht das Murmeltier, sondern das Bundesamt für Sicherheit in der Informationstechnik mit Warnungen vor aktuellen Schadprogrammen im Netz. Da wimmelt es ja nur so von Viren und Würmern und momentan haben wir es mal wieder mit einer Phishing-Welle zu tun. Ständig kommen neue, raffinierte Schädlinge hinzu und sie alle haben das Ziel, an die Daten und das Geld von uns Internetnutzern zu gelangen. Ich spreche dazu mit Ildiko Bruhns von ESET Deutschland:

### **|Begrüßung Moderator/in:|**

Guten Tag Frau Bruhns, ich grüße Sie.

### **|Begrüßung Ildiko Bruhns:|**

Hallo, ich grüße Sie!

**0:01“**

### **1. Frage: Wie riskant ist es, sich im Internet zu bewegen?**

**0:13“**

Ja, wie im realen Leben sollte man auch in der virtuellen Welt Vorsichtsmaßnahmen treffen, um sich vor Betrügern zu schützen. Denn wer hier unbedarft seine Daten preisgibt, der macht es Cyberkriminellen ziemlich einfach, persönliche Informationen zu stehlen.

### **2. Frage: Welche Gefahren lauern im Netz?**

**0:30“**

Eine ganze Menge. Neben unerwünschten Spam, also den Werbemüll, den Sie wahrscheinlich alle kennen, gibt es eben gefährliche Schadsoftware, wie Viren, Trojaner oder Schnüffelsoftware. Die verstecken sich dann in E-Mails, Links oder Anwendungen und schleusen sich unbemerkt auf Ihrem Computer ein. Phishing-Mails zum Beispiel sind eine sehr beliebte Masche, die dann angeblich von einer Bank oder einem Warenanbieter kommen und die Nutzer auffordern, Daten zu bestätigen. Oder auf Facebook und Twitter, da gibt auch täglich neue Hoaxes, also brisante Falschmeldungen, um User zu ködern.

### **3. Frage: Worauf haben es Cyberkriminelle in erster Linie abgesehen?**

**0:18“**

Online-Betrüger wollen zunächst nur an Ihre Daten. Die können sie dann auf dem Schwarzmarkt verkaufen oder sie räumen damit die Konten ihrer Opfer leer. Und ganz ehrlich, wir reden hier schon lange nicht mehr über Einzeltäter, die irgendwo einsam im Hinterzimmerchen Schadprogramme entwickeln, sondern es geht in den meisten Fällen um organisierte und vernetzte Cyberkriminelle.

### **4. Frage: Warum ist die Vorweihnachtszeit auch für Online-Betrüger so interessant?**

**0:14“**

Naja, wenn Sie bedenken, dass jeder zweite Deutsche seine Weihnachtseinkäufe im Internet erledigt, da gibt es natürlich für Online-Betrüger viel zu holen. Da ist das wahre „Datenparadies“ für sie. Sie kennen auch die Tricks, mit denen sie am schnellsten an Daten und Konten ahnungsloser Online-Shopper kommen.

### **5. Frage: Welche Betrugsmaschen setzen Cyberkriminelle vermehrt in der Vorweihnachtszeit ein?**

**0:27“**

Ja, gerade zum Beispiel gefälschte Webseiten für elektronische Weihnachtsgrüßkarten. Doch anstatt der netten Geste, bekommt man Viren und Trojaner geschenkt. Und von besonders günstigen Online-Schnäppchen, vor allem bei Markenprodukten, sollte man auch die Finger lassen. Denn in diesem Fall kauft der Nutzer im Internet Ware per Vorkasse, bekommt sie aber auch nie geliefert. Also, er hat nicht nur Geld ausgegeben, sondern auch jede Menge persönlicher Daten hinterlassen. Und Phishing-Mails zum Beispiel stehen auch ganz, ganz oben auf der Beliebtheitskala von Netz-Betrügern.

**6. Frage: Was sind Phishing-Mails?****0:29“**

Mit Phishing-Mails versuchen Kriminelle über gefälschte Webseiten oder E-Mails oder Instant Messaging persönliche Daten eines Nutzers abzugreifen. Das ist zwar keine neue Masche, aber sehr, sehr effektiv. Und die Online-Betrüger werden immer gewiefter und professioneller. Denn früher war es viel, viel leichter, eine Phishing-Mail zu erkennen. Und heute kommen die mit persönlicher Anrede, korrektem Namen und in fehlerfreiem Deutsch in Ihr Postfach geflattert. Und auch der Inhalt selbst wirkt täuschend echt. Angebliche Nachrichten von Amazon oder Pay-Pal sind hier die Klassiker.

**7. Frage: Was bedeutet Phishing?****0:27“**

Der Begriff setzt sich zusammen aus ‚Password‘ und ‚fishing‘ und bedeutet im übertragenen Sinne so viel wie ‚nach Passwörtern‘ angeln. Und genau darum geht’s auch: Die Kriminellen klauen Passwörter und Identitäten, um ans Geld ihrer Opfer zu gelangen. Phishing ist auch eine Form von Social Engineering, wo eben gezielt versucht wird, Leute zu manipulieren. Zum Beispiel gibt man sich als einen Verwandten am Telefon aus, um an bestimmte Informationen zu kommen. Den Enkeltrick dürfte hier fast jeder kennen.

**8. Frage: Wie können sich Internetnutzer schützen?****0:22“**

Ganz wichtig: Öffnen Sie zum Beispiel keine Anhänge von unbekanntem Absendern oder laden Sie auch nichts von unseriösen Quellen herunter. Und bei Rechnungen oder Mahnungen fragen Sie sich erstmal, ob Sie überhaupt was von dem Anbieter bestellt haben. Ja, und denken Sie immer daran, keine Bank oder kein Warenanbieter verschickt E-Mails an Sie, um Daten bestätigen zu lassen. Und am Besten schützen Sie sich mit einer Antiviren-Software.

**9. Frage: Warum ist Anti-Viren-Software so wichtig?****0:25“**

Ja, weil auch Online-Betrüger immer raffinierter und ausgefeilter werden und Methoden entwickeln, um ihre Opfer zu täuschen. Es gibt immer mehr Banden von Internetkriminellen, die versuchen, über Schadprogramme wie Viren, Würmer oder Trojaner an Ihr Geld zu kommen. Unsere Produkte zum Beispiel enthalten von Haus aus Spam-Filter oder Anti-Phishing-Module, die gefälschte Webseiten oder gefährliche Anhänge erkennen. Und damit surfen sie weitaus sicherer im Netz.

**10. Frage: Welche Lösungen bietet ESET?****0:40“**

Jeden Tag tauchen neue Schadprogramme im Internet auf, die irgendwie auf so viele Rechner, wie möglich eingeschleust werden soll. Und deswegen bieten wir effektive Sicherheitssoftware, die Viren und Co erkennt und auch abwehrt. Unsere Produkte sind zum Beispiel mit einer Firewall, Spam-Filter oder Anti-Phishing-Modulen ausgestattet, die Sie vor Angriffen von außen schützen. Und auch mit Sicherem Online Banking und Bezahlen bleiben eben Ihre Finanzen im Netz sicher. Und dabei setzen wir bei unseren Produkten auf einfaches Handling für den Nutzer und ganz wenig Ressourcenbedarf, damit Ihre Hardware nicht ausgebremst wird. Und so sorgen wir dafür, dass Sie mit gutem Gewissen surfen, shoppen oder spielen können – und das mit maximaler Rechenpower.

**|Verabschiedung Moderator/in:|**

Frau Bruhns, haben Sie vielen Dank für das Gespräch.

**|Verabschiedung Ildiko Bruhns:|****0:02“**

Ich danke Ihnen auch, tschüß.