

Kripo live | 31.03.2013 | 19:50 Uhr

## Prävention - Internet-Kriminalität

**Ohne Internet geht heute fast nichts mehr. Längst haben auch Kriminelle das Datennetz für sich entdeckt. Sie spähen Daten aus, hacken sich in fremde Computer oder erpressen Ahnungslose mit perfiden Fälschungen. Zum Thema Internet-Kriminalität hat Birgit von Derschau mit Dr. Stefan Köpsell von der TU Dresden gesprochen. Er arbeitet dort am Lehrstuhl Datenschutz und Datensicherheit der Fakultät Informatik.**



**Herr Köpsell, erst vor Kurzem hat es mich zu Hause selbst getroffen: Auf meinem Rechner erschien eine seriös aussehende Seite mit dem Logo der Bundespolizei. Man teilte mir in amtlicher Form mit, ich hätte gegen Gesetze verstoßen und solle eine Geldstrafe zahlen. Wie kommt so etwas auf meinen Computer?**

Vielleicht haben Sie eine kleine Dummheit begangen, auf den Anhang einer E-Mail oder einen Link geklickt. Oder Sie haben sich etwas aus dem Internet heruntergeladen. Oder Sie sind völlig unschuldig und sind auf eine ganz normale Website gegangen, auf der die Täter eine Schadsoftware hinterlassen haben. Und die hat sich dann automatisch auf ihrem PC ausgebreitet und ihn blockiert.

**Bei der aktuellen Variante dieser Schadsoftware werden auf dem Bildschirm des infizierten Computers vier Fotos eingeblendet. Alles wirkt amtlich mit dem Logo der Bundesbehörde. Und diese Fotos zeigen jugendpornografische Darstellungen. Solche Bilder auf seinem PC zu haben, ist tatsächlich strafbar. Was bezwecken die Täter damit?**

Sie wollen bei den Opfern Panik auslösen. Man will die Bilder schnell wieder loswerden und hat Angst. Dadurch ist man schnell bereit, zu bezahlen und das geforderte Geld zu überweisen.

**Die Polizei betont immer, man müsse Anzeige erstatten. Was halten Sie davon?**

Ich finde das gut. Nicht weil man dadurch hoffen kann, dass die Täter geschnappt werden. Denn die sitzen oft im Ausland. Aber durch Anzeigen wird die Statistik auf ein ordentliches Niveau gebracht. Dann reagiert vielleicht die Politik und stellt mehr und besser ausgebildete Polizisten ein.

**Wie kann ich mich am besten schützen, damit mir das**

## Links ins WWW

**Bundesamt für Sicherheit  
in der Informationstechnik**

**Anti-Botnet  
Beratungszentrum**

Der MDR ist nicht für den Inhalt externer Internetseiten verantwortlich!

## nicht wieder passiert?



Dr. Stefan Köpsell arbeitet am Lehrstuhl Datenschutz und Datensicherheit der Fakultät Informatik.

Das ist eine sehr schwer zu beantwortende Frage. Einen hundertprozentigen Schutz gibt es nicht. Aber man sollte sein Betriebssystem, seinen Browser und das Antiviren-Programm auf dem aktuellen Stand halten. Aber auch ein Antiviren-Programm bietet keinen vollständigen Schutz, weil die Täter sehr schnell reagieren und Lücken ausnutzen. Man muss also vorsichtig

sein und immer überlegen, auf welche Website man wirklich gehen will.

## Was wissen Sie über die Täter?

Es sind gut organisierte Banden, die in Osteuropa bzw. oft in Russland zu Hause sind. Sie gehen sehr arbeitsteilig vor. Es gibt Leute, die sehr gut solche Schadsoftware entwickeln können. Andere können sich in Websites einhacken, um dort den Schadcode hinterlegen zu können. Und andere wiederum organisieren die Überweisungen bzw. das Abziehen des Geldes. Es sind gut organisierte Banden – deshalb kann man auch so schnell in deren Fallen tappen.

## Kann man die Spur vom infizierten Computer zurückverfolgen und gleich noch auf die entsprechenden Bankkonten der Täter zugreifen?

Prinzipiell ist das möglich, wenn die Täter ihre Spuren nicht komplett verwischt haben. Allerdings sind die Täter oft im Ausland. Da muss die Polizei über komplizierte Rechtshilfe-Abkommen die anderen Länder um Hilfe bitten. Und bevor da wirklich Informationen vorliegen, was manchmal Monate dauert, ist die Spur längst kalt und die Täter sind über alle Berge verschwunden.

## Für Anzeigen ist ja immer die nächstgelegene Polizeidienststelle zuständig? Wie sind da die Erfahrungen?

In der Großstadt wissen die Polizisten auch mit Internet-Kriminalität umzugehen. Sie nehmen in jedem Fall eine Anzeige auf. Es mag sein, dass im ländlichen Raum der ein oder andere Polizist mit Schlagwörtern wie "Trojaner" nichts anzufangen weiß. Er wird aber eine Anzeige aufnehmen und an die zuständige Behörde weiterleiten.

## Es ist ja nicht nur die Bedrohung. Man will ja auch den PC wieder flott bekommen. Wie schwerwiegend sind denn hier die Schäden? Was kann man tun?

Die Schäden sind i.d.R. nicht sehr schwerwiegend. Das heißt, meine Daten sind nicht gelöscht. Ich kann selber versuchen, das Ganze zu beseitigen. Wenn ich mich aber nicht gut auskenne, frage ich lieber einen guten Freund. Vielleicht gibt es im Ort einen Verein, wie den Chaos-Computer-Club, den ich fragen kann. Oder ich gehe zu einem örtlichen Computerhändler.

## Die Sache hat mich 200 Euro gekostet. An die Täter sollte ich 100 Euro zahlen. Hat das überhaupt Sinn?

Das hat nur für die Täter Sinn, weil die um 100 Euro reicher sind. Ihr Rechner wird aber danach weiterhin gesperrt sein. Also von denen bekommen Sie garantiert keine Hilfe.

**Aber viele werden zahlen, weil sie sich schämen.**

Ja, das ist das clevere Vorgehen: Es ist ein relativ geringer Beitrag. Mancher ist gern bereit, den zu zahlen, damit der Rechner wieder funktioniert. Dadurch werden die Täter sehr reich, aber man selber hat 100 Euro Verlust. Und der Rechner funktioniert nach wie vor nicht!

**Vielen Dank, für die Informationen!**

Zuletzt aktualisiert: 29. März 2013, 12:09 Uhr

© 2013 MITTELDEUTSCHER RUNDFUNK