

31.10.08, 16:13, Von FOCUS-Redakteurin [Ruth Henke](#)

|
Spam-Welle

„Die Gangster haben Kunden weltweit“

Seit einigen Tagen rollt eine gigantische Welle gefährlicher Mails durch das Internet. Der Sicherheitsspezialist Achim Kraus von der Firma IronPort Systems erläutert im Interview die aktuellen Trends.



Sicherheitsspezialist Achim Kraus von der Firma Ironport Systems

Seit einigen Tagen rollt eine gigantische Welle gefährlicher Mails durch das Internet. Auf einem Anti-Spam-Gipfel in Wiesbaden berieten Sicherheitshersteller, Polizei und Behörden, wie sie länderübergreifend intensiver zusammenarbeiten können, um die global agierenden Kriminellen aufzuspüren. Der Sicherheitsspezialist Achim Kraus von der Firma IronPort Systems erläutert die aktuellen Trends.

FOCUS Online: Seit einigen Tagen finden Internetnutzer häufig fingierte Rechnungs-Mails in ihrem Postfach. Mal kommen sie angeblich von einer Techinkasso Forderungsmanagement GmbH, vom Amtsgericht oder vom Energieversorger Vattenfall. Stets wird der Empfänger aufgefordert, die vermeintliche Rechnung im Anhang zu öffnen. Sonst werde ein bestimmter Betrag von seinem Konto abgebucht. Was verbirgt sich hinter solch einer Mail?

Kraus: Man nennt solche speziellen Mails auch Scareware (englisch: scare = erschrecken). Der Absender der Nachricht versucht, jemanden so zu erschrecken, dass er handelt. In diesem Fall soll er auf den Mail-Anhang klicken, um zu verhindern, dass von seinem Konto Geld verschwindet. In dem Anhang wie zum Beispiel der Datei „rechnung.zip“ verbirgt sich jedoch ein gefährlicher Trojaner oder Virus. Ein Klick, und schon ist der Computer infiziert.

FOCUS Online: In welcher Art und Weise ist dann mein Rechner infiziert?

Kraus: Es gibt verschiedene Varianten. Die aktuellste sind Programme, die heimlich Informationen von Ihrem PC nach draußen an versteckte Drahtzieher senden, die für diese Informationen bezahlen. So werden beispielsweise E-Mail-Anschriften aus Ihrem Adressbuch oder Bankdaten an Dritte verkauft. Manche Kriminelle verkaufen E-Mail-Adressen an Firmen, die dann Reklame für gefährliche oder nutzlose Pillen versenden, für dubiose Finanzprodukte werben oder Aktienpreise in die Höhe treiben wollen. Gleichzeitig kann auch ein Programm auf Ihrem Computer installiert werden, um Ihren Rechner fremdgesteuert ohne Ihr Wissen in eine Spam-Schleuder zu verwandeln. Dadurch

verwischen die Cyber-Kriminellen ihre Spuren und können über Zehntausende Computer Millionen Mails gleichzeitig versenden. Gangster, die solche Informationen besitzen und ein großes Netz von Computern fernsteuern können, haben viele Kunden weltweit.

FOCUS Online: Immer wieder kursieren auch Mails, die mich auf den ersten Blick erfreuen, weil ich etwas gewonnen habe oder etwas besonders günstig erwerben kann. Ich muss lediglich vorab eine gewisse Gebühr bezahlen oder soll eine bestimmte Website besuchen. Hat dieser sogenannte Lotterie-Spam eine hohe Relevanz?

Kraus: Gerade in der Vorweihnachtszeit werden solche Mails sicherlich wieder häufig in unseren digitalen Postfächern landen. Es ist eine der vielen Methoden, die verwendet wird, um die Empfänger von Spam zu einer Aktion zu bewegen.

FOCUS Online: Diese Form der Kriminalität ist ein internationales Geschäft, das sich auf nationaler Ebene nicht ausreichend bekämpfen lässt. So sitzt vielleicht derjenige, der sich Zugriff auf meinen Computer verschafft hat, in Russland und verkauft seine Dienstleistung an Pillenversender in den USA. Den Text für die Spam-Mail oder gefährliche Websites wiederum könnte jemand aus Deutschland liefern. Wie sind diese Leute überhaupt aufzuspüren?

Kraus: Das ist in der Tat extrem schwer. Außerdem fehlt ein einheitliches Vorgehen der Länder. So kann beispielsweise ein Betrüger, der von Russland aus auf US-amerikanische PCs zugreift, nicht von den Vereinigten Staaten verklagt und vor Gericht gestellt werden. Solch eine Tat ist in Russland selbst nicht einmal strafbar. Umso wichtiger ist der Zusammenschluss der zuständigen Behörden weltweit, beispielsweise durch den deutsche Anti-Spam-Kongress.

FOCUS Online: Diese Woche berieten auf dem Anti-Spam-Kongress in Wiesbaden Vertreter von Branchenfirmen, Verbände, Polizei- und Justizbehörden aus mehreren Ländern, wie sie diesen gigantischen, verbrecherischen Sumpf austrocknen können. Wie sehen die Pläne aus?

Kraus: Internetfirmen, Banken und Behörden wollen noch enger und verstärkt länderübergreifend kooperieren. Auch wir arbeiten mit deutschen Behörden und Internet-Providern zusammen. Mit unseren Lösungen können Unternehmen ihre Internetanbindung und die E-Mail-Kommunikation übergreifend an den Außenstellen absichern und steuern. Dadurch kann beispielsweise verhindert werden, dass vertrauliche Daten per E-Mail versandt werden. Eine Überwachung der ausgehenden E-Mail-Kommunikation kann zum Beispiel auch dem Bundeskriminalamt helfen, die Spur eines Spammers aufzunehmen.

FOCUS Online: Werden Sie diese Gefahr künftig auch technisch besser bannen können?

Kraus: Die Verbrecher sind technologisch extrem fit und sehr professionell. In diesem Jahr hat sich das Spam-Volumen im Gegensatz zu 2007 sogar verdoppelt. Es bleibt wohl ein ständiger Wettlauf. Wir rüsten auf, die Gegenseite rüstet nach.

FOCUS Online: Viele Mails sind mittlerweile so perfekt gestaltet und überzeugend getextet, dass selbst Vorsichtige hin und wieder auf die Tricks der Ganoven hereinfallen. Wie kann man das verhindern?

Kraus: Zum einen immer wieder prüfen, ob ich den Absender kenne. Dann den E-Mail-Text daraufhin studieren, ob er sich persönlich auf mich bezieht, zum Beispiel mich namentlich anspricht. Handelt es sich nicht um eine personalisierte E-Mail, dann ist es mit hoher Wahrscheinlichkeit Spam, den man sofort löschen sollte. Im Zweifelsfall sollte man immer davon absehen, einen enthaltenen Web-Link anzuklicken oder eine enthaltene Datei zu öffnen.

