Wie Cyberkriminalität funktioniert
Milliardenkosten durch Schadsoftware

Maik Leege
Nelly Bösch Computer

Inhalt

Bei fast jeder Malware geht es heute ums Geldverdienen.

Cyberkriminelle haben dazu fantasiereiche Methoden entwickelt.
Allerdings müssen bei ihnen viele Einzelfaktoren nacheinander zusammenspielen, damit der kriminelle Gesamtprozess funktioniert.

Im ersten Schritt suchen die Cyberkriminellen Opfer.

Arglose Benutzer in ihre Netze zu locken und Computer für kriminelle Zwecke zu missbrauchen, gelingt ihnen dabei meist mit den folgenden Methoden:

Spamm:
Durch E-Mail-Spam war es erstmalig möglich, mit Malware direkt Geld zu verdienen. Und das Geschäft mit fragwürdigen Tabletten, gefälschten Uhren und heiratswilligen Russinnen floriert nach wie vor.

Zwar ist das Spamvolumen insgesamt zurückgegangen. Doch noch immer senden Spammer täglich Milliarden von Nachrichten in der Hoffnung, dass ein kleiner Prozentsatz die Spamfilter überwinden und einige Empfänger zum Kauf verlocken kann. Im Anhang von E-Mails kommt außerdem nach wie vor Malware ins Haus, auch wenn der größte Teil der Schadprogramme heute im Web liegt.

Phishing:
Angreifer verwenden E-Mails nicht nur, um per Spam Produkte und Dienstleistungen anzupreisen. Sie führen damit auch Phishing-Angriffe durch. Ihre E-Mails täuschen vor, von Ihrer Bank oder Ihrem E-Mail-Dienstanbieter zu stammen. Das soll Sie dazu bringen, arglos Ihre Zugangsdaten einzugeben. Auf ähnliche Weise bereiten sie auch Angriffe auf unternehmensinterne Dienste vor.

Drive-by-Downloads:
Viele Nutzer infizieren sich schon beim Aufruf einer Webseite, wenn diese bekannte Exploits als „Drive-by-Downloads“ enthält. Die SophosLabs spüren jeden Tag 30.000 neue Seiten im Web auf, die arglose Surfer mit Schadcode bombardieren. Sie wollen damit Schwachstellen in Betriebssystemen, Browsern, Plug-ins und Anwendungen ausbeuten.

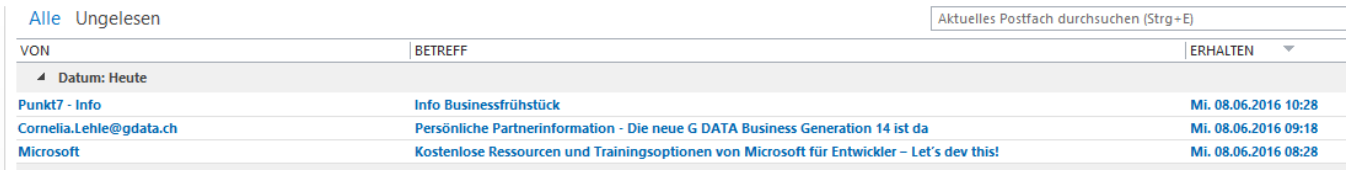
Soziale Medien:
Viele Spammer sind inzwischen von E-Mails auf Spam-Nachrichten in sozialen Medien umgestiegen. Hat ein scheinbarer Freund oder Kollege einen Link gepostet, klicken die Nutzer in Netzwerken wie Facebook oder Twitter sorgloser darauf als sonst. Auch Sensationsberichte und beliebte Funktionen verleiten neugierige Benutzer dazu, auf unsichere Links zu klicken.

Blackhat SEO:
Betrüger versuchen ausserdem, die Suchergebnisse bei Google und Bing zu beeinflussen, was man als Blackhat SEO oder SEO Poisoning bezeichnet. Ziel ist es, die Suchergebnisse bei beliebten Themen so zu manipulieren, dass Treffer auf den ersten Suchergebnisseiten zu gefährlichen Webseiten mit Exploits, Malware oder Phishing führen.

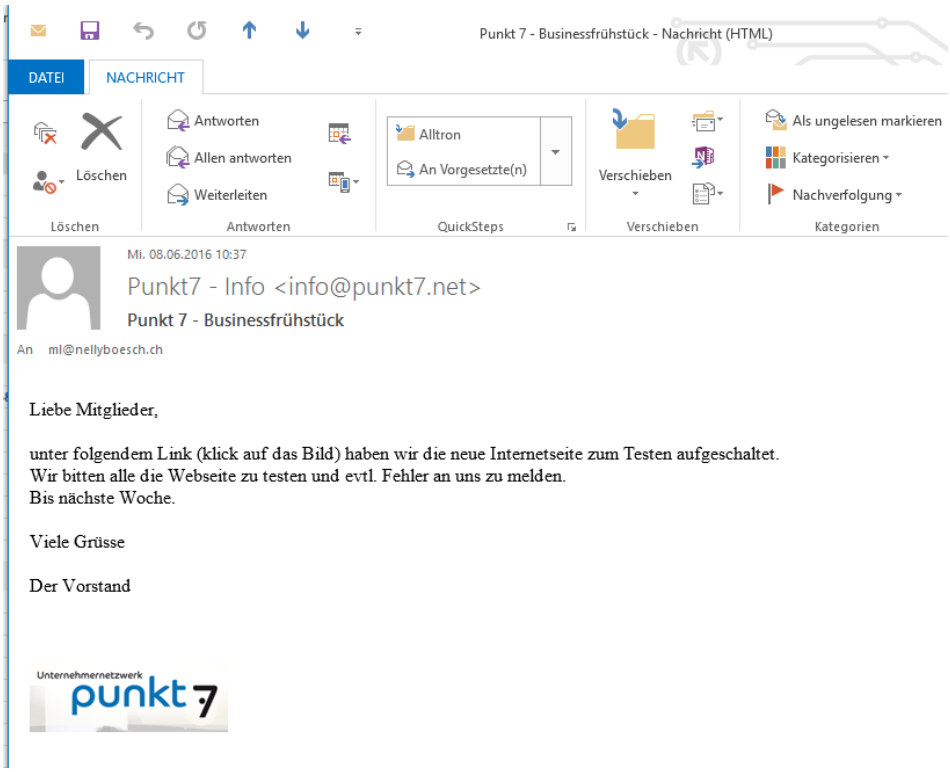
Malware:
Würmer, Viren und andere Malware-Dateien sind noch immer zahlreich im Umlauf. Sie sind heute zwar seltener als noch vor zehn Jahren, doch zur Infektion ungeschützter Systeme und um Computer zu missbrauchen bleiben Sie für die Täter ein wichtiges Mittel.

Identitätsdiebstahl

- Erschleichen von Vertrauen



Im Postausgang sieht die Mail aus, als würde sie von Punkt7 – Info stammen.

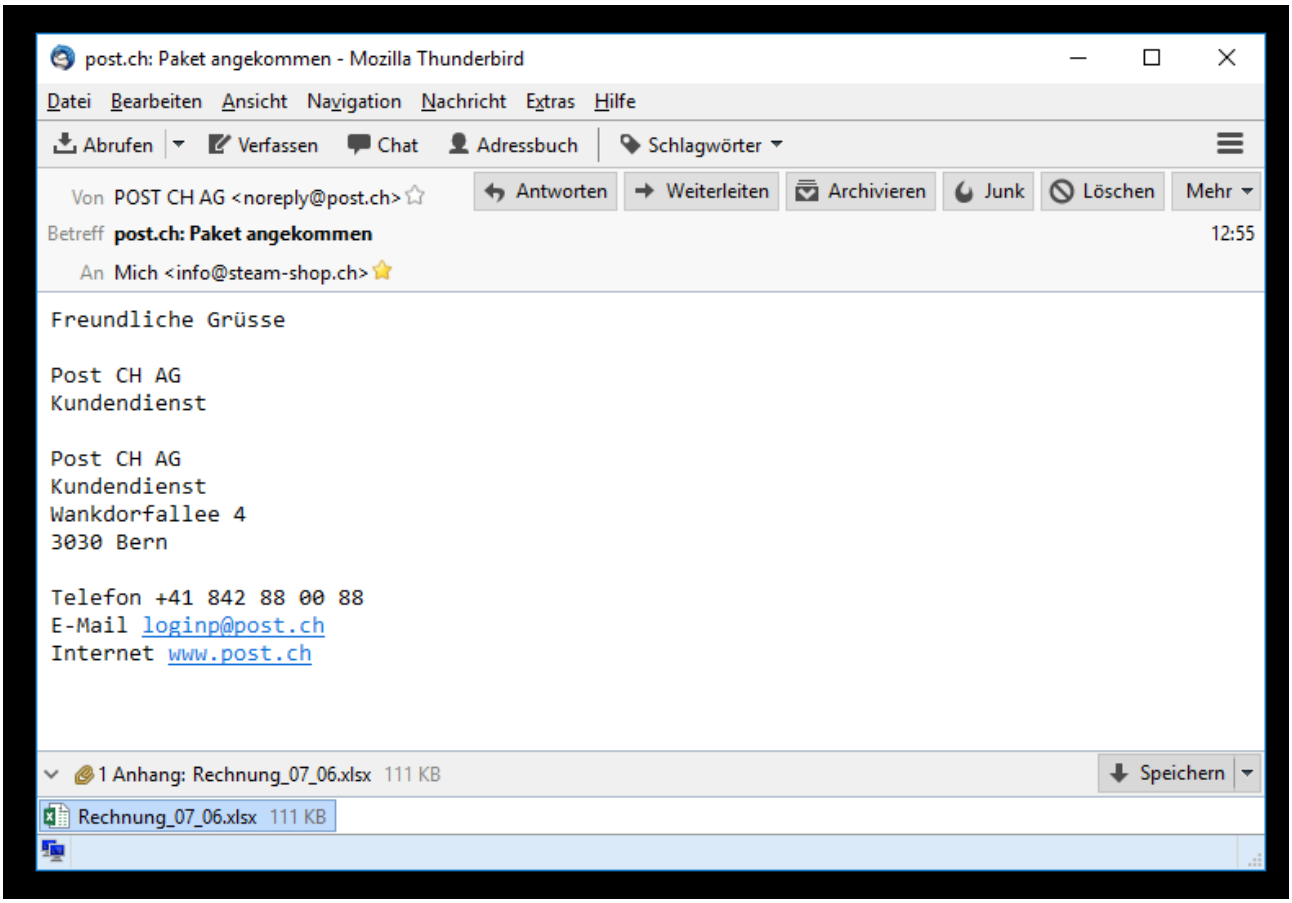


Die Mail macht den Eindruck, als wäre sie von Punkt7 – Info (info@punkt7.net) gesendet worden. Ohne Analyse ist es nicht möglich den Absender zu erkennen, nur im Quelltext kann man ihn „meistens“ aufspüren.

Ein Auszug aus dem Quelltext verrät den Absender:

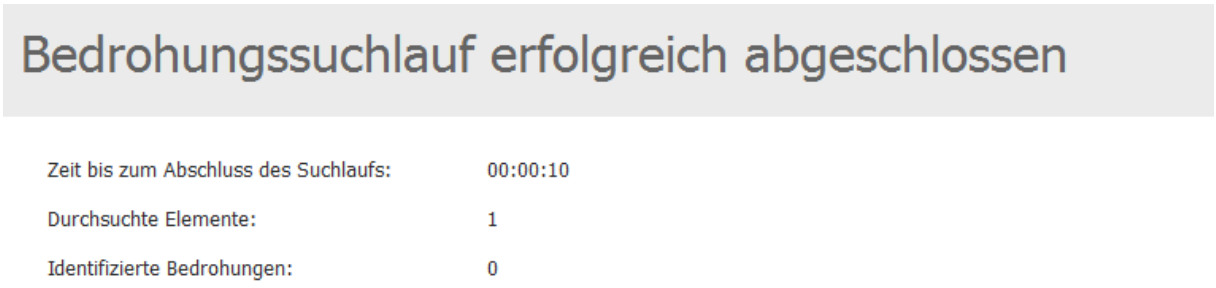
Return-Path: info@punkt7.net
(envelope-from <info@punkt7.net>)
Wed, 08 Jun 2016 10:36:58 +0200
X-Authenticated-Sender-Id: maik@steam-shop.ch
Reply-To: info@punkt7.net

Ein weiteres Beispiel:



Der Betreff recht einfach: Paket angekommen.

Scan mit Virenschutzsoftware – keine Bedrohung



Auch hier ein Blick in den Quelltext:

```
Return-Path: <noreply@post.ch>
Delivered-To: info@steam-shop.ch
Received: from zrh-lb2.core.hostpoint.net ([10.0.0.100])
    by popimap004.mail.hostpoint.ch (Dovecot) with LMTP id 1spCLuanVlch2QAAN/QmnA
    for <info@steam-shop.ch>; Tue, 07 Jun 2016 12:55:19 +0200
Received: from mxin015.mail.hostpoint.ch ([10.0.2.42])
    (using TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits))
    by zrh-lb2.core.hostpoint.net (Dovecot) with LMTP id UzYhD+6nVldFfAAAVs719w
    ; Tue, 07 Jun 2016 12:55:19 +0200
Received: from mailnull by mxin015.mail.hostpoint.ch with local_accounts_spamscanned (Exim 4.84 (FreeBSD))
    (envelope-from <noreply@post.ch>)
    id 1bAEfF-0003zc-IE
    for info@steam-shop.ch; Tue, 07 Jun 2016 12:55:19 +0200
X-Spam-Checker-Version: SpamAssassin 3.4.0 (2014-02-07) on
    mxin015.mail.hostpoint.ch
X-Spam-Level: *
X-Spam-Status: No, score=1.1 required=4.0 tests=BAYES_40,DCC_CHECK,
    FSL_BULK_SIG autolearn=no autolearn_force=no version=3.4.0
Received: from world-of-pandora.org ([93.170.168.181] helo=post.ch)
    by mxin015.mail.hostpoint.ch with smtp (Exim 4.84 (FreeBSD))
    (envelope-from <noreply@post.ch>)
    id 1bAEfF-0003zF-Bv
    for info@steam-shop.ch; Tue, 07 Jun 2016 12:55:17 +0200
Message-ID: <CCC97F2C27F3DD6EB2B7FE4397FA22F6@post.ch>
Reply-To: "POST CH AG" <noreply@post.ch>
From: "POST CH AG" <noreply@post.ch>
To: <info@steam-shop.ch>
Subject: post.ch: Paket angekommen
Date: Tue, 7 Jun 2016 13:55:16 +0300
Organization: post.ch
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="316068f0677386870ac16ef7af80"

This is a multi-part message in MIME format.

--316068f0677386870ac16ef7af80
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: 8bit

Freundliche GrÃ¼sse

Post CH AG
Kundendienst
```

Der tatsächliche Absender wird verschleiert, die Mail ist von world-of-pandora.org gesendet worden. Eine Domain registriert in einem Inselstaat ohne Möglichkeit der Nachverfolgung.

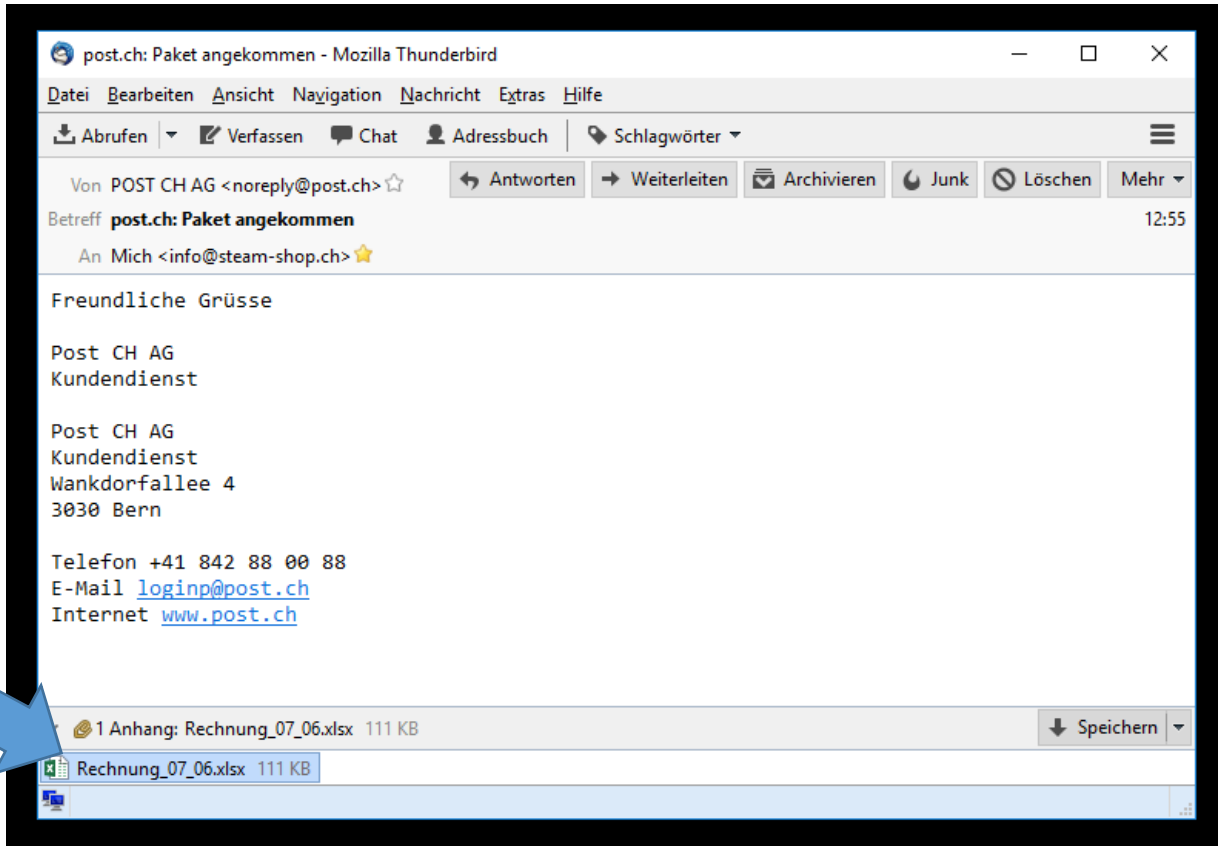
Zurück zur Mail

Die Mail selbst ist recht ungefährlich, die Anlage bringt die Gefahr mit.

In der Anlage befindet sich eine Excel Datei und hier drin ist Schad – Script versteckt.
Beim Öffnen wird dieser aktiv.

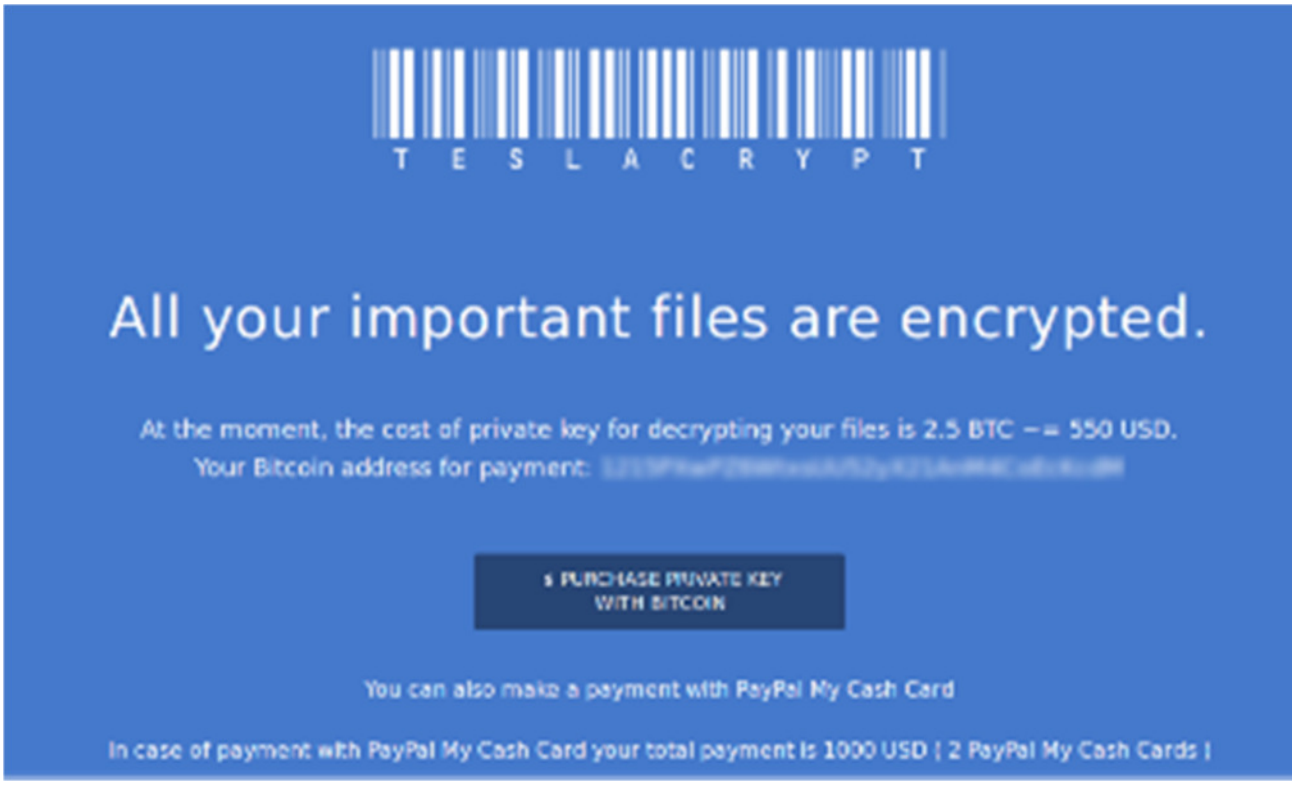
Um kein Risiko einzugehen habe ich es in diesem Fall nicht geöffnet.

Gefährlich sind in diesem Zusammenhang:
.exe, .com, .dll, .bat, .cmd, .vbs, .scr, .scf, .wfs, .jse, .shs, .shb, .lnk, .pif, .src



Churerstrasse 160a · 8808 Pfäffikon/SZ · Telefon 055 415 62 52 · Telefax 055 415 62 58 · E-Mail info@nellyboesch.ch

Und dann könnte der Bildschirm wie folgt aussehen:



Aktuell sind immer mehr Verschlüsselungsprogramme in den Anlagen / Skripten versteckt.

Zahlen 100 Opfer die geforderte Summe, kommen rund 55.000$ zusammen.

Beispiele:

Rund 2000 $ müssen Cyberkriminelle investieren, wollen sie sich eine Schadsoftware zulegen, die stationäre Rechner oder Laptops verschlüsselt. Doch auch hier lohnt sich die Investition, denn mit 20 bis 500$ pro Entschlüsselung sind die Ausgaben schnell wieder eingespielt.
Zahlen 100 Opfer die geforderte Summe, kommen rund 55.000$ zusammen

Im Dezember 2013 schaffte es der IT Dienst ZDNet, Zuwächse auf vier BTC - Konten einer Gruppe, die einen Cryptolocker (Verschlüsselungssoftware) nutzen, einzusehen. Die vier geprüften Adressen haben in der Zeit vom 15 Oktober bis 18 Dezember einen Zuwachs von:

41.928 BTC (Bitcoin)

Umgerechnet ca. **27.000.000 $**

Das Netzwerk der Cyberkriminellen

Malware-Schreiber:
„Entwickler“ das Herzstück der Cyberkriminalität.
Dabei verbreiten die meisten Malware-Entwickler ihre Produkte offenbar nicht direkt, sondern verkaufen ihre Dienste an Netzwerke organisierter Cyberkriminalität.

Übersetzer:
Die sprachliche Qualität vieler Spam-E-Mails, Lockmittel und Social-Engineering-Angriffe hat sich in den vergangenen Jahren deutlich verbessert.

Bot-Hirten:
Ein Bot-Hirte infiziert Computer, damit Kriminelle es zur Verbreitung von Spam und für andere kriminelle Cloud-Computing-Anwendungen verwenden können.

Exploit-Schreiber:
Hacker spezialisieren sich darauf, Sicherheitslücken in Software aufzuspüren und in sogenannten „Exploit Packs“ zu sammeln. Die Exploit-Schreiber verkaufen ihre Packs.

Geldesel & Mule Manager:
Helfer, die für sie zu Banken gehen, Gelder überweisen oder Schecks einlösen. Mule Manager sind auf die Rekrutierung solcher Personen spezialisiert. Money Mules werden sehr häufig mit angeblichen Home-Office-Angeboten geködert.

Tool-Provider:
Software zu entwickeln, ist an sich nicht kriminell.
Cyberkriminelle können für Beträge zwischen 20 und mehreren Tausend Dollar zahlreiche Tools kaufen, darunter Trojaner, Spam-Werkzeuge, etc.

Churerstrasse 160a · 8808 Pfäffikon/SZ · Telefon 055 415 62 52 · Telefax 055 415 62 58 · E-Mail info@nellyboesch.ch

Schäden in Milliardenhöhe

Erkenntnisse Forcepoint Global Threat Report 2016

- Anstieg infizierter Emails um 250% seit 2014
- Ransomware hat weltweit finanziellen Schaden in Höhe von über 325 Mil. $ verursacht
- In den USA gibt es mehr Phishing-Webseiten als in allen anderen Ländern zusammen. Deutschland liegt an dritter Stelle
- Angriffe konzentrieren sich zunehmend auf Länder, Wirtschaftsräume und Industrien
- Die größte Bedrohung für die Sicherheit – absichtlich oder unbeabsichtigt – geht von Mitarbeitern aus.

Wie können wir gewinnen

An dieser Stelle ist nicht gemeint wie wir Gewinne machen können – das überlassen wir den „Kriminellen“.

Wir wollen gegen die Kriminellen gewinnen!

- VORSICHT / Mistrauen
  Geben Sie keinesfalls irgendwie Ihre Zugangsdaten und Passwörter bekannt
- Kein Mitarbeiter einer seriösen Firma fragt Sie nach Ihren Zugangsdaten (PIN, TAN, Passwort)
- Starten (Doppelklick) Sie keinerlei fremde Software unbekannter Herkunft
- Seien Sie vorsichtig mit E-Mail-Anhängen
- Installieren Sie ein Virenschutz - Programm
- Aktualisieren Sie regelmäßig Ihr Virenschutz - Programm

Churerstrasse 160a · 8808 Pfäffikon/SZ · Telefon 055 415 62 52 · Telefax 055 415 62 58 · E-Mail info@nellyboesch.ch