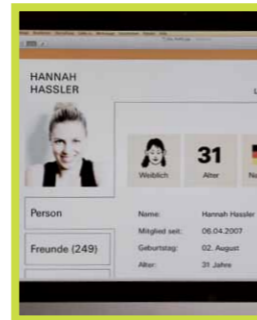
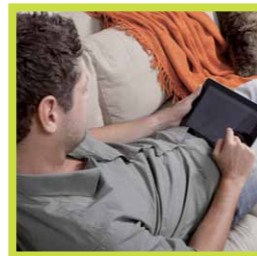


Problematik

Schadsoftware (Malware) zielt darauf ab, auf einem fremden Computersystem unerwünschte Aktionen auszuführen und dadurch Schaden anzurichten. Grundsätzlich kann sich diese Software in jeder Art von Datei- oder Programmbestandteilen verbergen und sich sozusagen im Vorbei-Surfen auf einem fremden System einnisten. Schadprogramme können auch mit jedem Download, jedem Dateianhang aus einer E-Mail oder schlicht über E-Mails auf das System gelangen.

So genannte Bots installieren sich auf einem Rechner meist so, dass es dem PC-Besitzer nicht auffällt. Betrüger schließen „befallene“ Rechner später zu Bot-Netzen zusammen und nutzen sie zum Beispiel für den

massenhaften Versand von Spam-Mails. Der Rechner ist mit dem Anschluss an ein Bot-Netz nicht mehr nur geschädigt, sondern führt auch gleichzeitig Straftaten aus. Der Bot-Netz-Betreiber ist in der Lage den Rechner vollständig und für den Computerbesitzer nahezu unerkannt fern zu steuern.



Tipps

- Schützen Sie Ihren PC durch einen Virens Scanner. Halten Sie alle Programme und das Betriebssystem aktuell. Nutzen Sie auch automatische Update-funktionen. Eine Firewall ist in den modernen Betriebssystemen vorhanden oder wird oft durch Antivirensoftware zusätzlich bereitgestellt.
- Gehen Sie nie mit Administrator-Rechten online. Da ein Angreifer über dieselben Rechte verfügt, wie Sie als angemeldeter Benutzer, kann er das System übernehmen – und Sie selbst von der Nutzung ausschließen. Legen Sie für die Internetnutzung ein Benutzerkonto mit eingeschränkten Rechten an.
- Öffnen Sie niemals ungeprüft Dateianhänge. Löschen Sie verdächtige E-Mails schon im Posteingang ohne sie zu öffnen. Viele Antivirenprogramme kontrollieren ein- und ausgehende Mails ebenfalls.
- Stellen Sie Ihren E-Mail-Account auf das „Nur-Text“-Format um, denn E-Mails im HTML-Format können Schadsoftware enthalten.
- Seien Sie kritisch bei ausführbaren Programm-Dateien mit den Endungen .exe, aber auch .bat, .com oder .vbs. Ändern Sie die Standardkonfiguration Ihres Rechners, um den Dateityp sehen zu können (im Windows-Explorer unter „Extras – Ordneroptionen – Ansicht – Erweiterte Einstellungen – Dateien und Ordner“ das Häkchen vor „Erweiterungen bei bekannten Dateitypen ausblenden“ entfernen).
- Wird Ihr PC gesperrt und Sie am Monitor aufgrund angeblich strafbarer Handlungen Ihrerseits zu Zahlungen aufgefordert, kommen Sie dieser Aufforderung nicht nach – dabei handelt es sich um so genannte Ransomware. Informieren Sie sich darüber auf www.botfrei.de bei Ihrer Polizei und erstatten gegebenenfalls Strafanzeige.
- Überprüfen Sie Ihren Computer regelmäßig auf Schadsoftware. Nicht jede Schadsoftware wird sofort durch die Scanner erkannt und beseitigt. Nutzen Sie dazu zusätzlich zu Ihrer Anti-Viren-Software beispielsweise ein Programm unter <https://www.botfrei.de/decleaner.html>

Linkempfehlungen

www.polizei-beratung.de/viren-und-trojaner
www.polizei-beratung.de/bot-netze
www.botfrei.de
www.bsi-fuer-buerger.de
www.verbraucher-sicher-online.de



Schad-
Schadsoftware und Bot-Netze
software



Rechtliche Aspekte

§ 202a Strafgesetzbuch (StGB)

Ausspähen von Daten

„(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft. [...]“

OSCAR CHARLIE



THEMA Schadsoftware und Bot-Netze

Klicks-Momente

(00V)150.2013.03

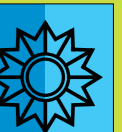
Wir wollen,
dass Sie
sicher leben.



Ihre Polizei

www.polizei-beratung.de

Wir wollen,
dass Sie
sicher leben.



Ihre Polizei

Kompetent. Kostenlos. Neutral.