Aktuelle Situation (Stand 26.10.2011)

Am 8.10.2011 veröffentlicht der Chaos Computer Club (CCC) ein Dossier über einen konkreten Fall eines „Staatstrojaners“, der erhebliche Sicherheits- und Rechtslücken aufweist:

- Eine integrierte „Nachladefunktion“ ermöglicht unbeschränkte Einsatzmöglichkeiten
- Ermittelte Daten werden über einen US-Server geleitet, entziehen sich damit an dieser Stelle deutschem Recht
- Mangelhafte geschützte Verschlüsselung von Daten und Zugangssicherung eröffnen nach Installation dieses Trojaners dem (auch nicht-behördlichen) Missbrauch Tür und Tor
- Eine zur Beweissicherung notwendige Integrität des ausspionierten Systems ist damit nicht mehr gegeben

Im späteren Verlauf stellt sich heraus bzw. müssen die Polizei- und Zollbehörden Stück für Stück zugeben:

- Die Spionagesoftware wurde von Fremdfirmen (Digitask und Syborg) zugekauft, ohne dass man den Quellcode kannte und ohne beurteilen zu können, was diese Software tatsächlich kann und tut und was nicht.
- Fast alle Bundesländer müssen nacheinander zugestehen, dass sie Trojaner wie den des CCC oder ähnliche Wanzen eingesetzt haben und einsetzen. Dabei rechtfertigen sie ihr Tun mit dem Verweis auf den § 100a StPO (siehe Rückseite dieses Blatts).
- In einem Fall wurde der Trojaner im Rahmen einer Zollkontrolle auf den Rechner des Betroffenen eingeschleust, der Zoll stellte „Amtshilfe“ bereit.
- Es stellt sich heraus, dass der konkret beschriebene Trojaner aus Bayern stammt und sich in seiner Ausgestaltung über ein Urteil des LG Landshut vom 20.1.2011 hinwegsetzt.
- Bundesinnenminister Friedrich ignoriert dieses Urteil und begeht mit Aussage aus einem FAZ-Artikel vom 15.10.2011 offenen Rechtsbruch:

  „Das Landgericht Landshut hat zu den Möglichkeiten der Quellen-Telekommunikationsüberwachung eine andere Rechtsauffassung vertreten als die bayerische Staatsregierung. Entscheidend ist: Wir müssen in der Lage sein, Kommunikation zu überwachen. Und wenn Verbrecher über das Internet kommunizieren, muss man die Überwachung auf das Internet übertragen.“
- Die Innenminister kündigen an, „eigene“ Trojaner entwickeln zu wollen.

Unser Standpunkt

Wir verlangen ein grundsätzliches Verbot des Einsatzes von Trojanern sowohl auf Bundes- als auch auf Landesebene.

- Der Einbruch durch staatliche Behörden in Privatcomputer stellt einen derart gewaltigen Eingriff in die Privatsphäre von Menschen dar, der alleine deswegen unzulässig ist, weil das Wissen um die Möglichkeit solcher Maßnahmen eine erhebliche negative Ausstrahlung auf die Bevölkerung und ihr Verhalten hat, selbst wenn die allermeisten Menschen gar nicht davon betroffen sind.
- Es gibt keine staatliche Schadsoftware, die die engen Regeln des Bundesverfassungsgerichts einhalten könnte.
- Es mangelt den Behörden an Fachleuten und -kenntnis, derartige Computerwanzen verfassungskonform einzusetzen geschweige denn überhaupt im Detail zu kennen und zu verstehen.
- Eine ausreichende und vernünftige Kontrolle durch die Datenschutzbehörden ist aus mehreren Gründen nicht möglich: Den meisten dieser Behörden fehlt es an Personal, Kompetenz, Unabhängigkeit und Durchsetzungsvermögen.
- Der Richtervorbehalt ist aufgrund seiner praktischen Umsetzung in seiner Bedeutung als Sicherheitsvorkehrung unwirksam geworden. Es fehlt den zuständigen Richtern an Zeit und Kompetenz.

Hinweise/Erläuterung

Digitask: Hessisches Softwareunternehmen, dessen Geschäftsführer 2002 wegen Bestechung des Zollkriminalamts zu 21 Monaten Haft auf Bewährung und zu 1,5 Millionen Euro Geldbuße verurteilt wurde. Danach Übertragung der Firma auf seine Frau und Fortführung bestehender Geschäfte mit dem Zoll...

Syborg: Saarländisches Software-Tochterunternehmen der israelischen Firma Syborg (vormals: Comverse Infosystems), die Teil eines handfesten Skandals mit an US-Behörden gelieferte Spionagesoftware war, zu der sie sich unerlaubt Zugriff verschaffen konnte.

Herausgeber dieses Blattes:

AK Vorrat, Ortsgruppe Hannover
Stand: Oktober 2011
http://wiki.vorratsdatenspeicherung.de/Hannover

Mehr Infos zum Arbeitskreis Vorratsdatenspeicherung:
www.vorratsdatenspeicherung.de

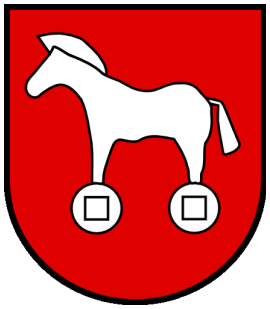
V.i.S.d.P.
Michael Ebeling, Kochstraße 6, 30451 Hannover,
micha_ebeling@gmx.de

AK VORRAT hannover

Staatstrojaner und Online-Durchsuchung

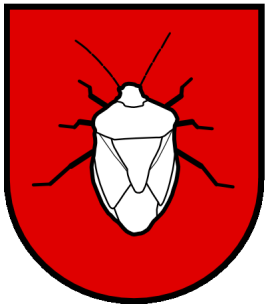
Informationen über Behörden-Trojaner, polizeiliche Computerwanzen und andere Ungehörigkeiten

Was ist ein Trojaner?



Als „Computer-Trojaner“ oder auch „Trojanisches Pferd“ bezeichnet man ein Computerprogramm, das sich als harmlose Datei oder Teil einer ansonsten nützlichen Software ausgibt, tatsächlich allerdings andere, vom Betroffenen unbemerkte und unerwünschte Aufgaben erfüllt.

Der Name entstammt der griechischen Mythologie. Als nützliches und interessantes Holzpferd getarnt holten die Einwohner der belagerten Stadt Troja dieses Pferd in das Innere ihrer geschützten Festung. Dort konnten die im Inneren des Pferdes versteckten Soldaten in einem günstigen Moment entweichen und die Stadt erobern, indem sie die Festungstore von innen öffneten.



Dieser Begriff lässt sich nicht trennscharf vom Bild der „Computerwanze“ abgrenzen. Eine Wanze versteckt sich und möchte in seiner Existenz unentdeckt bleiben, während sich der Trojaner als nützliches Computerprogramm oder Teil eines solchen ausgibt und Harmlosigkeit vortäuscht.

Gemeinsam ist sowohl der „Wanze“ als auch dem „Trojaner“, dass sie ein vom Besitzer des Computer unerkanntes Eigenleben führen, indem Sie beispielsweise den Inhalt des Computers oder das Verhalten, Tun und Lassen des Benutzers ausspähen und diese Informationen an Dritte außerhalb des Computers übertragen, ohne dass dieses (für den normalen Menschen) erkennbar wäre.

Wie kommt ein Trojaner auf meinen Computer?

- Durch Phishing-Attacken, also mit Hilfe gefälschter E-Mails, dem Öffnen befallener Dateien, Programme oder Internetseiten mit unzureichend gesicherten Browsern oder Computern.
- Während der Kontrolle des Rechners durch Polizei oder Zoll (z.B. Flughafen, Beschlagnahme auf Demos …)
- Unbemerkter Einbruch in die Wohnung bzw. in die Räume, in denen sich der Computer befindet.

Online-Durchsuchung und „Quellen-TKÜ“

Aus rechtlicher Sicht ist zwischen einer „Online-Durchsuchung“ und einer „Quellen-Telekommunikations-Überwachung“ (Quellen-TKÜ) zu unterscheiden. Ob und inwiefern sich diese beiden unterschiedlichen Ermittlungsmaßnahmen in der Praxis überhaupt trennen lassen, ist heftig umstritten.

Online-Durchsuchung

Eine Online-Durchsuchung ist die staatliche Durchsuchung von Computern oder Computernetzen. Nach höchstrichterlicher Klärung darf eine solche Maßnahme nur zur Strafverfolgung, zur Gefahrenabwehr und für geheimdienstliche Zwecke eingesetzt werden.

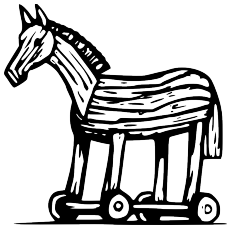
Nachdem Nordrhein-Westfalen unter einem FDP-geführten Innenministerium in 2006 als erstes eine Gesetzesregelung für so einen Eingriff eingeführt hatte, führte eine von mehreren Einzelpersonen initiierte Verfassungsbeschwerde zum dem Urteil vom 27.2.2008, dass das konkrete Gesetz für verfassungswidrig erklärte und strenge Vorgaben für den Einsatz einer Online-Durchsuchung aufstellte.

Gleichzeitig entwickelte das Bundesverfassungsgericht das neue **Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme**, das u.a. der Tatsache gerecht wird, dass viele Menschen ihre Computer in einer Weise benutzen, wie man es zum Teil von Tagebüchern kennt. Dieses lässt den eigenen Computer zum Raum der Persönlichkeitsentwicklung und damit zum besonders geschützten Kernbereich eines jeden Menschen werden.

Das Gericht stellte dabei u.a. fest:

„Die heimliche Infiltration eines informationstechnischen Systems, mittels derer die Nutzung des Systems überwacht und seine Speichermedien ausgelesen werden können, ist verfassungsrechtlich nur zulässig, wenn tatsächliche Anhaltspunkte einer konkreten Gefahr für ein überragend wichtiges Rechtsgut bestehen. (...)
Das Gesetz, das zu einem solchen Eingriff ermächtigt, muss Vorkehrungen enthalten, um den Kernbereich privater Lebensgestaltung zu schützen.“

Nach der Änderung des BKA-Gesetzes darf das Bundeskriminalamt Online-Durchsuchungen durchführen. Für den Einsatz durch die Geheimdienste fehlt zwar eine explizite Rechtsgrundlage, dennoch geht das Bundesinnenministerium davon aus, dass der Einsatz dieser Spionagetechniken den Nachrichtendiensten zustehe. Von allen Bundesländern hat nur Bayern hat einen rechtlich umstrittenen Paragrafen zum Einsatz heimlicher Online-Durchsuchungen in seinem Polizeigesetz integriert.



Von fast allen anderen Bundesländern ist aufgrund der neuesten Entwicklung zugegeben worden, Trojaner-Software einzusetzen, dann allerdings angeblich „nur“ zum Zwecke der Quellen-TKÜ, was nach Ansicht der verantwortlichen nichts mit einer Online-Durchsuchung zu tun habe.

Die Quellen-TKÜ

In der Begründung zum Einsatz von Computerwanzen und Spionagesoftware ziehen sich die Politiker auf die Bestimmungen des § 100a StPO zurück.

Dieser Paragraf erlaubt den Ermittlungsbehörden die Überwachung der Telekommunikation, also das Abhören von Telefon- und Handytelefonaten inkl. SMS und wird in diesem Zusammenhang von den Landeskriminalämtern fleissig beansprucht.

Mit dem Verweis darauf, dass einige Menschen heutzutage den Internet-Dienst Skype zum Telefonieren benutzen würden und dass Skype-Telefonieren gemäß § 100a StPO abgehört werden dürfte, sei also auch ein Trojaner-Einsatz zulässig.

Was dabei übersehen/verschwiegen wird:

- Es gibt eine anerkannte, wenn auch kritikwürdige, offizielle Zusammenarbeit von Skype und Polizeibehörden, die das Skype-Abhören ohne Trojaner-Einsatz ermöglicht. Warum dann also Computerwanzen einsetzen?
- Skype bietet nicht nur einen Audio, sondern auch einen Video-Stream. Damit offenbaren die Benutzer viel mehr als nur das gesprochene Wort. Ob dieses nach § 100a StPO zulässig ist, ist mehr als fraglich.
- Installation und Betrieb eines Trojaners in einem privaten Computer erfordert derart schwere Eingriffe, dass die Integrität des Systems und die Echtheit der angeblichen Beweisdaten nicht mehr gewährleistet werden kann.