

Skype abhören oder wie sich deutsche Richter das E-Mail-Schreiben vorstellen



- 4 -

Der Beschluss wurde im Auftrag der Staatsanwaltschaft Landshut von den Polizeibehörden vollzogen. Hierzu hat das Bayerische Landeskriminalamt zum Zwecke der Ausleitung der verschlüsselten Telekommunikation auf dem Computer des Beschuldigten [REDACTED] eine Software aufgebracht, welche über zwei Überwachungsfunktionen verfügt: Die Überwachung und Ausleitung der verschlüsselten Skype-Kommunikation (Voice-over-IP sowie Chat) vor der Ver- bzw. nach der Entschlüsselung sowie das Erstellen von Screenshots der Skype-Software sowie des Internet-Browsers Firefox im Intervall von 30 Sekunden zur Überwachung der über https geführten Telekommunikation. Diese Maßnahmen wurden sodann auch umgesetzt.

Der Beschuldigte wurde von den durchgeführten Telekommunikationsmaßnahmen nicht unterrichtet.

Beschluss des Landgerichts Landshut: „Zwar muss der Beschuldigte um eine E-Mail verfassen zu können, eine Verbindung zu einem Server aufbauen, der ihm die erforderliche Maske zur Verfügung stellt. Der Vorgang des Schreibens der E-Mail findet dann aber ohne Datenaustausch statt, da die einzelnen Buchstaben nicht sofort an den Server weiter übertragen werden. Die E-Mail wird erst dann zum Server und damit in die Außenwelt transportiert, wenn der Beschuldigte den IIVersenden-Button“ betätigt. Hält man sich diese technischen Vorgänge vor Augen, kann nach Auffassung der Kammer – auch im Lichte der Entscheidung des Bundesverfassungsgerichts zur Unzulässigkeit der Online-Durchsuchung (NJW 2008, 822) – beim Schreiben einer E-Mail noch nicht von einem Vorgang der Telekommunikation gesprochen werden.“ (via [law blog](#), mehr dazu bei [ijure.org](#))

Bruhahahah. Das ist ja wieder ein gefundenes Fressen für unsere Verschwörungstheoretiker zum Thema „Online-Durchsuchung“. Hier geht es aber um Skype (vgl. auch den [Beschluss](#) des LG Landshut dazu.) Der Beschuldigte kommunizierte via Skype und benachrichtigte die Gesprächspartner vorher durch eine SMS.

Frage: Wie kam der so genannte „Trojaner“ (der keiner ist) auf den Rechner des beschuldigten? (Es ging übrigens um die pöhsen Drogen.) Was wäre gewesen, wenn der Beschuldigte *nicht* den Internet-Explorer für Windows, sondern [Galeon](#) für Linux benutzt hätte?

Zum Thema habe ich am [09.20.2010](#) ausführlich gebloggt – „Skype: Heimlich auf den Rechner spielen“:

Udo Vetter scheint vergessen zu haben, dass er [zum Thema Skype](#) schon am 17.8.2010 gebloggt hat. Er verwies damals auf den [Wikipedia-Eintrag zu Skype](#), wo man lesen kann, worum es eigentlich geht. Natürlich kann man Skype anhören, aber nicht mit Methoden, die der real gar nicht existierenden „Online-Durchsuchung“ irgendwie ähneln. Man kann also mitnichten, wie Spiegel offline suggiert, einfach so „heimlich“ ein Programm auf fremde Computer „spielen.“ Nein, das kann man nur, wenn man den physikalischen Zugriff hat und Software installieren darf (der Besitzer des Rechner muss also ein DAU sein.)

Installation der Skype Capture Unit auf dem Zielsystem

Für die Installation der Skype Capture Unit wird eine ausführbare Datei mitgeliefert die zum Beispiel als Anhang an eine E-Mail versendet werden kann oder aber direkt auf dem Zielsystem installiert werden kann.. Weitere Installationsroutinen können jederzeit integriert werden. Diese werden dann nach dem entstandenen Aufwand berechnet.

Eine ausführbare Datei, die per E-Mail-Anhang verschickt werden kann? Da lachen ja die Hühner!. Und die installiert das Zielobjekt nichtsahnend? Und der Verdächtige hat auch weder einen Mac noch Linux? Ich zitiere mich selbst vom [27.08.2009](#):

In der [Heise-Meldung](#) von gestern heisst es: „Ein Schweizer

Software-Entwickler hat auf seinen Seiten den Quelltext zu einem Programm [veröffentlicht](#), das verschlüsselte Kommunikation über Skype heimlich belauschen kann. Das Programm ist dazu vorgesehen, als Trojanisches Pferd auf einem PC eingeschmuggelt zu werden. Dort klinkt es sich nach Angaben des Autors in den laufenden Skype-Prozess ein, schneidet die Audio-Daten der Gespräche heimlich mit und lädt sie dann als MP3-Dateien auf einen externen Server.“

Das habe ich mir genauer angesehen. Das Trojanische Pferd ist mitnichten ein „Bundestrojaner“, den es bekanntlich nicht gibt, sondern das Programm [Minipanzer](#): „Minipanzer is a trojan horse that disguises as any kind of file type and when executed on a victims system it collects all sensitive data like account information etc. and sends it to an email address owned by the attacker. It is a one-shot-trojan. It doesn't install on a target system but only executes its payload and removes itself afterwards.“

Im [dazugehörigen Blog](#) heisst es: „The code is simple and straightforward. You have know malware development is no rocket science and if you expect big magic you are at the wrong place.“ Am besten hat mir der Kommentar „Giovannis“ gefallen: „Despite what some people say, Skype has never been secure. It is relatively easy to hack skype accounts, skype does not even check if the same user logs in simultaneously on different machines and what is worst, the second user can get a copy of all the chats. Skype is good for housewives that want to chat a bit with their kids, but for confidential conversations the use of strong voice encryption is required. In our company we tested many of them, we now keep with [PhoneCrypt from securstar](#) as it proved to be very good, stable, and with an excellent voice quality.“

Ich verweise auf mein hiesiges Posting „[„Bayerntrojaner“ zum Abhören von Internet-Telefonie?](#)“ sowie auf meinen Artikel in der [Netzeitung](#): „Wenn der Laptop zweimal klingelt“.

Auf law blog gab es einen interessanten Kommentar: „@mark: es geht um einen einfachen Audio-Capture-Client mit Streamingfunktion der sich fernwarten lässt. Der Programmieraufwand dafür beträgt ca. 20-30 h. Dazu kommt dann die Sonderfunktionalität für Skype die man noch mal mit der gleichen Zeit veranschlagen kann. Dazu noch Tests sowie der Server. Alles in allem ein Projekt, dass sich mit nur einem Mann-Monat stemmen lässt. Selbst bei einem Stundenpreis von vollkommen utopischen 500€ für den Entwickler reden wir hier von Entwicklungskosten im sehr niedrigen 5stelligen Bereich. Bei den Preisen muss die Software nur ein einziges Mal zum Einsatz kommen, damit sie sich für die entwickelnde Firma rechnet. Ich bleibe dabei: hier wird über den Tisch gezogen.“

Nach mal langsam zum Mitschreiben: Man kann nichts heimlich auf fremde Rechner spielen, wenn der Besitzer das nicht will. Kapiert?