2007/50 Lifestyle

https://jungle.world/artikel/2007/50/dont-believe-skype

Don’t believe the Skype

Von **Burkhard Schröder**

Skype ist der bekannteste Voice-over-IP-Dienst. Die Software ist einfach zu installieren, flexibel und vor allem weit verbreitet. Wie das proprietäre Skype-Protokoll funktioniert, ist nicht bekannt. Und niemand weiß genau, wie sicher beziehungsweise unsicher das »Skypen« ist. Was die meisten Nutzer auch nicht wissen: Es gibt Alternativen, um über das Netz zu kommunizieren. von burkhard schröder

Die spannende Frage ist: Können Sie abhören, oder können Sie nicht? Beim Thema Skype werden alle Ingredienzien zusammengerührt, die den Plot für einen zweitklassigen Agentenkrimi tauglich machen. Da benutzen Leute das Internet, um zu telefonieren, nutzen dafür eine Software, über deren geheimnisvolles Inneres man wenig weiß, und die Schnüffler und Schlapphüte haben das Nachsehen. Haben die Guten also gewonnen?

Jörg Ziercke, Chef des Bundeskriminalamts, jammerte auf einer Tagung im November wie gewohnt darüber, dass seine Leute die VoIP-Software nicht mehr entschlüsseln könnten. Das ist wahr und falsch zugleich. Falls ruchbar würde, dass sich die Betreiberfirma auf eine Hintertür für die Sicherheitskräfte einließe, könnte man den Laden vermutlich schließen. Skype wird weder einen »Bundestrojaner« noch ähnliche Dinge implementieren lassen. Skype gehört heute Ebay, und das Unternehmen hat nicht vor zwei Jahren mehr als drei Milliarden Dollar für Skype bezahlt, um beim Thema Sicherheit seinen guten Ruf zu verlieren. Falsch ist aber die suggestive These Zierckes, das BKA oder die üblichen Verdächtigen, nämlich Mossad, NSA und CIA, könnten überhaupt irgendetwas abhören.

Wenn die Opfer des Lauschangriffs sich der Gefahr bewusst wären, der große Bruder schnitte alles mit, wäre das Rennen gelaufen. Seit Erfindung der asymmetrischen Kryptografie haben die Codebreaker verloren, die Codemaker gewonnen. Die Untertanen können sich also jederzeit, kommunizieren sie nur digital, vor der informationellen Begehrlichkeit der Obrigkeit schützen. Das Problem ist: Die Untertanen tun das nicht. Sie sind meistens sorglos und glauben jedem, der ihnen sagt: »Meine Software ist sicher.« Zierckes Statement könnte auch eine Nebelkerze sein. Vielleicht soll sein Lamentieren die Nutzer nur in Sicherheit wiegen, sie können den nächsten Bankraub, die nächste militante Demo oder den Handel mit schweinischen Dateien jetzt sicher über Sykpe abwickeln, ohne dass jemand davon erführe? Skype verweigert jede Angabe darüber, ob man mit irgendjemandem zusammenarbeite, und verrät auch nicht das geringste Detail über die Technik, die man benutzt.

Angeblich soll es möglich sein, schon auf die Inhalte der Telefonate zuzugreifen, bevor diese in der Datenleitung verschwinden. Im Oktober berichteten deutsche Medien, es habe mehrere Fälle von »Quellen-Telekommunikationsüberwachung« gegeben. Der Zollfahndungsdienst hätte unbemerkt auf den Rechnern einer verdächtigen Person eine Software implementiert, die die Internet-Telefonate abhört, bevor diese verschlüsselt werden. Das geschah nicht »online«, sondern durch Eindringen in die Wohnung, während der Betroffene nicht zu Hause war.

Ludwig Waldinger, der Sprecher des bayerischen Landeskriminalamts, bestritt jedoch in einem Interview mit der Tagesschau, dass diese Methode angewendet werde: »Das würde technisch auch keinen Sinn machen.«

Das Schweizer Sicherheitsunternehmen ERA IT Solutions verkauft eine Software »ausschließlich an Sicherheitsbehörden«, eine Art Wanze, die Skype angeblich abhören kann – bevor die Daten kodiert werden. Das Schweizer Departement für Umwelt, Verkehr und Kommunikation soll das Programm testen, berichteten die Medien vor gut einem Jahr. Wenn es so etwas prinzipiell geben kann, dann sind auch andere Entwickler in der Lage, so etwas nachzubauen.

Im Internet kursieren aber detaillierte Analysen, die die Schwachstellen der Software auseinander nehmen. Zum Beispiel die Studie »Silver Needle in the Skype«, die 2006 von Philippe Biondi und Fabrice Desclaux für die European Aeronautic Defence and Space Company verfasst wurde. »Smart guys« und natürlich auch girls könnten das gesamte lokale Rechnernetz angreifen und kompromittieren, während jemand Skype benutzt, so das Fazit der beiden Verfasser. Doch nicht mal das wird für die meisten Benutzer ein Argument sein, die Finger von Skype zu lassen, genau so wie Millionen auch die bekannte Software aus dem Hause Bill Gates nutzen, obwohl die teurer und unsicherer ist als Open-Source-Alternativen.

Skype geht ähnlich wie Peer-to-Peer-Software vor. Im Security-Forum des Heise-Verlags spricht man vom »Albtraum eines Netzwerk-Admins«. Skype macht sich im Prinzip zunutze, dass der Aufbau einer Verbindung zwischen Rechnern im Internet und das Gespräch selbst technisch zwei ganz verschiedene Vorgänge sind. Die Methode, Firewalls zu umgehen, beruht auf einem technischen Täuschungsmanöver: Der Datenstrom der Internet-Telefonie gaukelt den digitalen Schutzwällen vor, es handele sich um ein ganz normales Datenpaket mit Sender und Empfänger, etwa wie bei einer E-Mail, und schmuggelt sich dort vorbei, wo eine ganz andere Art der Datenübertragung vorgesehen ist.

Ist Skype sicher genug? Es gibt immer wieder Berichte über kritische Lücken und Software-Fehler. Das ist nicht unbedingt ein Nachteil, denn ein absolut sicheres Programm existiert nicht, zumal wenn die relativ schlicht konstruierte Art der Datenübertragung genutzt werden muss, auf der das Internet basiert. Die Wirtschaft geht mit Sykpe aus Sicherheitsgründen nur zögerlich um, in vielen Untenehmen ist es schlicht verboten. Das European Organization for Nuclear Research rät sogar dringend davon ab, diese Art von Internet-Telefonie zu nutzen. Skype ist schon deswegen »unsicher« weil niemand genau weiß, wie sicher es ist. Diese Methode nennt man in Hackerkreisen »Security by obscurity«, meistens entpuppt sich die Sicherheit dann als mehr oder weniger obskur. Skype läuft auf jedem Betriebssystem. Die Installation ist jedoch auf Open-Source-Plattformen wie den Linux-Derivaten nicht immer so einfach, wie es versprochen wird.

Es existieren aber zahlreiche Alternativen: Digg (digg.com/software/Open_Source_Skype_-Alternative) ist zum Beispiel eine, inklusive SMS und Videofunktion, für Windows und Linux. Die

meisten klassischen Instant-Messaging-Programme haben heute eine Audio- und Video-Funktion eingebaut, mit der sich Online-Konferenzen abhalten lassen und mit denen man so gut telefonieren kann wie mit Skype, vorausgesetzt, man hat Headset und Kamera. Jabber (**www.jabber.org/**) ist vermutlich das bekannteste Beispiel. Viele Benutzer der populären Linux-Distribution Ubuntu schwören auf Ekiga (**www.ekiga.org/**), das auch mit Microsofts Netmeeting kompatibel ist. OpenMoko (openmoko.org/) arbeitet an einem offenen Standard für Mobiltelefone, ist aber über das Stadium der Entwicklung noch nicht wesentlich hinausgekommen.

Skype hat einen gravierenden Nachteil: Es ist nicht kompatibel mit den zahlreichen anderen Methoden, über das Netz zu kommunizieren – per Audio- oder Videoübertragung. Es verwendet ein so genanntes proprietäres Protokoll, also eine Eigenentwicklung, deren Zweck die kommerzielle Verwertung ist. Das ermöglicht der Firma auch, ähnlich wie Google, mit Diktaturen eng zu kooperieren. Nutzer von Skype aus China bekommen einen Textfilter vorgesetzt, der bestimmt Worte nicht durchlässt. »Falun Gong« und »Dalai Lama« sind nur zwei Beispiele. Diese Zensur funktioniert natürlich nur, wenn die Betreiberfirma die Möglichkeit ab Werk eingebaut hat, die Gespräche mitzuprotokollieren und zu belauschen. Aber auch das wird die breite Masse nicht hindern, Skype weiter zu benutzen. Google Mail gibt sogar offen zu, dass den Nutzern die zum Inhalt ihrer E-Mails passende Werbung eingeblendet wird. So etwas benutzen auch kritisch denkende und aufgeklärte Menschen. Das sind aber vermutlich große Ausnahmen.