

## Online-Überwachung gefährdet IT-Security und Datenschutz in Unternehmen



**Nicht nur Privatanutzer geraten ins Visier der Online-Durchsuchung. Auch Unternehmen sehen sich einem verstärkten Interesse der Behörden bei der Verbrechensbekämpfung ausgesetzt, mahnten Datenschützer auf der Sommerakademie in Kiel. Deshalb ist eine sachliche Diskussion mit Blick auf sinnvolle technische und wirtschaftliche Szenarien unbedingt notwendig.**

cirosec GmbH  
Edisonstraße 21  
74076 Heilbronn  
Tel: 07131 / 59455-0  
Fax: 07131 / 59455-99  
info@cirosec.de  
[www.cirosec.de](http://www.cirosec.de)

20.09.2007 | Autor: Lothar Lochmaier

Wie sehr das Thema IT-Sicherheit in die Mühlen der politischen Justiz geraten ist, verdeutlicht der Umstand der jüngst verhinderten Terroranschläge in Deutschland. Bereits einen Tag nach der erfolgreichen Festnahme dreier Verdächtiger, die Sprengstoffanschläge auf amerikanische Einrichtungen in Deutschland planten, entzündete sich die Diskussion um die Online-Durchsuchung von neuem. Der baden-württembergische Innenminister Heribert Rech etwa stellte gleich seine eigenwillige Interpretation der Dinge dar.

Mithilfe der Online-Überwachung, so Heribert Rech, wären die Behörden in dieser Sache wesentlich schneller vorangekommen. Auf diese Weise hätten Ressourcen und Aufwand bei der Ermittlung eingespart werden können.

Dabei rückt allerdings in den Hintergrund, dass die erfolgreiche Polizeiarbeit auch in diesem Fall mehr auf klassischen Methoden fußte, denn auf einer technischen Überwachung. Im Zuge der aufgeheizten Diskussion droht somit auch die Rolle der Informationstechnologie in der Gesellschaft und Wirtschaft unter die Räder zu geraten.

Eine Diskussion über deren Chancen und Grenzen ist dementsprechend unausweichlich. „IT-Überwachungstechnologien sind nicht in der Lage, den Terrorismus abzuschaffen“, bilanzierte nüchtern der Datenschützer Thilo Weichert, Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD), auf der Kieler Sommerakademie: „Auch die lückenloseste Überwachung kann nicht in die Köpfe der Menschen schauen und lässt sich – insbesondere von professionellen Kriminellen – mit technischen Mitteln austricksen“, so das Fazit des Experten.

### **Diskussion über die staatliche Überwachung nimmt Fahrt auf**

Die Riege der bundesdeutschen Datenschutzbeauftragten aus zahlreichen Konzernen und mittelständischen Unternehmen traf sich in diesem Jahr in Kiel nicht ganz routinemäßig zur Sommerakademie. Denn derzeit diskutieren nicht nur die Datenschutzexperten kontrovers über aktuelle Trends in der staatlich verordneten Datenüberwachung.

Auch unter Bürgerrechtlern sei die irreführende These verbreitet, die Informationstechnologie würde als Überwachungsinstrument die Freiheit zerstören, relativierte Thilo Weichert das Schreckgespenst einer allumfassenden staatlichen Überwachungspraxis.

„IT ist Kommunikationstechnologie und fördert damit Transparenz und freiheitliche Diskussion“, stellte der Experte klar. Der Datenschützer sieht durchaus positive Begleiterscheinungen, denn die IT erlaube es nicht nur Kriminellen, sich der Überwachung zu entziehen, sondern auch freien

Menschen, ihre Privatsphäre zu verteidigen.

Eine effektive Gewährleistung der Sicherheit dürfe aber nicht dazu benutzt werden, das Grundgesetz auszublenden. „Hierzu gehört, dass Wirtschaftsunternehmen nicht systematisch zu staatlichen Hilfsdiensten verpflichtet werden dürfen“, kritisiert Weichert.

### **Pannen im Rahmen der Online-Durchsuchung**

Eben jene Verpflichtungen stellen die Zulässigkeit rechtlicher Verfahren generell auf eine harte Probe. Das zeigt auch eine Affäre beim Bundesnachrichtendienst (BND): Ein in Berlin tätiger Mitarbeiter des Geheimdienstes, der mit der Überwachung der elektronischen Kommunikation betraut war, soll seine technischen Möglichkeiten im Rahmen der Online-Durchsuchung auch privat genutzt haben, berichtet die Berliner Zeitung. Dem Beamten werde vorgeworfen, während seines Dienstes den E-Mail-Verkehr eines Deutschen ausgespäht zu haben, weil dieser angeblich ein Verhältnis mit seiner Frau hatte.

Weitere Informationspannen heizen die öffentliche Diskussion an und erschweren den sachlichen Überblick, welche technischen Maßnahmen sinnvoll wären. So gelangte der 78-seitige „Entwurf eines Gesetzes zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundeskriminalamt“, datiert vom 11. Juli 2007, in die Hände des Chaos-Computer-Clubs (CCC).

Demnach räumt der Bundesinnenminister dem Bundeskriminalamt (BKA) deutlich mehr Befugnisse zur heimlichen Überwachung der Bevölkerung ein als bislang bekannt. So sollen nicht nur unmittelbar Terrorverdächtige überwacht werden, sondern auch Kontakt- und Begleitpersonen, wenn dadurch die Verhütung dieser Straftaten aussichtslos oder wesentlich erschwert sei.

### **Unikat: Was leistet RFC?**

Im Kern entzündet sich die Debatte an der öffentlichen Diskussion um die Online-Überwachung. Im Fachjargon ist der im Volksjargon genannte „Bundestrojaner“, der die technische Basis für die Online-Durchsuchung darstellt, bereits mit dem eleganteren Begriff „Remote Forensic Software“ ersetzt worden. Auf der Kieler Konferenz bezog der Chef des Bundeskriminalamts Jörg Ziercke in einem Videointerview Stellung und verteidigte die staatlichen Bemühungen, diesen Schritt rechtlich durchzusetzen bzw. zu legalisieren.

„Meiner Meinung nach können wir Instrumente entwickeln, die es uns ermöglichen, vor oder nach der Verschlüsselung an diese verschlüsselten Daten heranzukommen“, bekräftigte Ziercke. Er zeigte sich zuversichtlich, dass die eingesetzte Software als Unikat unentdeckt bleibe. Das Programm solle auch herkömmliche Firewalls und Antivirus-Lösungen umgehen, wenn sich das Durchsuchungsprogramm installiert habe.

Die Gefahr der Entdeckung des Trojaners sei indes minimal, da sich das Programm nach einer gewissen Zeit selbst lösche. Ziercke betonte jedoch auch, dass jede Maßnahme eine richterliche Erlaubnis voraussetze. Auch die umfassende Vorratsdatenspeicherung verteidigt der BKA-Chef weiterhin. Sie ist nach Auffassung von Ziercke unerlässlich, um Straftaten bis zu deren Planung rekonstruieren zu können.

## **Welche Gefahren birgt der Bundestrojaner?**

IT-Experten stehen der „Unikat-Theorie“ zur Online-Untersuchung durch ein leistungsfähiges Individualprogramm indes kritisch gegenüber: Wirkungsvolle Schutzprogramme gegen Spionage-Software und Viren-Attacken würden längst nicht mehr ausschließlich nach bekannten Codemustern fahnden. Mittlerweile versuchen sie das gesamte System zu analysieren, um das Verhalten von Keyloggern und Spyware zu erkennen. Dieser Umstand allein könne bereits zur vorzeitigen Enttarnung derartiger Tools führen.

Aus Sicht der IT-Industrie besteht dadurch auch die Gefahr, dass sich die Grenzfällen zwischen „Gut und Böse“ weiterhin verschieben bzw. gänzlich verschwiegen. Allerdings mangelt es bisher an eindeutigen Stellungnahmen. Gefragt sind nämlich auch die Anbieter von IT-Sicherheitslösungen, sich zu positionieren. „Wenn ein Sicherheitsanbieter den Key seiner Festplattenverschlüsselung von den Behörden dekodieren lässt, dann stellt sich für Anwender generell die Frage, ob sie einer derartigen Software noch vertrauen können“, sagt Security-Experte Stefan Strobel, Geschäftsführer der Cirosec GmbH in Heilbronn. In die Mühlen der Justiz geraten auch die Unternehmen, die das Restrisiko von Hintertüren bereits erkannt haben. Auf keinen Fall dürften aber Soft- und Hardwarehersteller entsprechende Hintertüren erlauben, so Strobel. Der Experte zeigt sich entsetzt über die Art und Weise, wie die aktuelle Diskussion geführt werde. „Die Maßnahmen der Online-Untersuchung bringen überhaupt keinen Fortschritt. Sie dienen nur dazu, die Rechte ahnungsloser Privatpersonen und Internetnutzer über Bord zu werfen“, bringt Strobel auf den Punkt.

Aus seiner Sicht dienen die erhobenen Daten nämlich weit weniger der Aufklärung von Straftaten. Vielmehr unterstützen sie verstärkt die Interessen der Musikindustrie, um mit Hilfe des gläsernen Internetnutzers Urheberrechtsverstöße transparent zu machen.

So gesehen sei der Bundestrojaner nur ein erster Schritt, ergänzt Sicherheitsexperte Sebastian Schreiber, Geschäftsführer des IT-Sicherheitsspezialisten Syss GmbH in Tübingen: „Wenn Hersteller damit beginnen, Hintertüren in Betriebssysteme einzubauen, wird der Überwachungsstaat viel stärker als bisher in die Unternehmen hinein getragen“.

Redakteur: Stephan Augsten

***searchsecurity.de 20.09.07***