Humanistische Union

Techniken der Online-Durchsuchung: Gebrauch, Missbrauch, Empfehlungen

Andreas Pfitzmann

Fehlerquellen der heimlichen Infiltration - Szenarien der Technikentwicklung - Zukunft des Selbstdatenschutzes.

Dokumentation des Vortrags vom 28. April 2008

Techniken der Online-Durchsuchung: Gebrauch, Missbrauch, Empfehlungen

Andreas Pfitzmann wies in seinem Vortrag über "Gebrauch, Missbrauch und Empfehlungen" aus der Sicht des Informatiker darauf hin, dass die Diskussion um Online-Durchsuchung einem klassischen Muster von Technikdiskursen folgt: Man nehme ein soziales Problem und behaupte, es mit technischen Mitteln lösen zu können. Diesmal soll uns das heimliche Ausforschen von Computern vor den Gefahren terroristischer Anschläge schützen. Paradoxerweise bringen dabei diejenigen Akteuere, die öffentlich mit ihrem technischen Unverständnis kokettieren - etwa Wolfgang Schäuble oder Jörg Ziercke -, das größte Vertrauen in die Zielsicherheit und Fehlerfreiheit einer Software auf, mit der heimliche Online-Durchsuchungen durchgeführt werden. Als Informatiker sehe er - Pfitzmann - erhebliche Probleme bei einer heimlichen Infiltration von Computern und könne deshalb nur zu nicht-manipulierenden Beobachtungsmethoden raten.

Sie können den Vortrag von Prof. Dr. Andreas Pfitzmann hier vollständig nachhören:

Die Durchführbarkeit heimlicher Online-Durchsuchungen steht und fällt mit der Frage, ob und wie den Ermittlern der unerkannte Zugriff auf den gewünschten Computern gelingt. Das "offizielle", dem BKA-Gesetzentwurf zugrundeliegende Zugangsszenario sieht so aus: Die Schadsoftware soll von außen aufgespielt werden. Das kann durch infizierte Webseiten, verseuchte E-Mail-Anhänge oder einen zugespielten Datenträger erfolgen, ebenso wäre ein Einbruch während einer bestehenden Internetverbindung denkbar. Neben der Tatsache, dass bei den meisten dieser Zugriffsmethoden von außen die Zielperson mithelfen muss, damit die Infiltration gelingt, weisen diese Zugriffsszenarien nach Einschätzung von Andreas Pfitzmann erhebliche Nachteile auf, die eine rechtsstaatliche Verwendung der so gewonnenen Informationen weitgehend ausschließen. Dazu zählt er vor allem eine erhöhte Gefahr, dass die Ermittler den falschen Computer durchsuchen und völlig unverdächtige Personen zum Ziel einer Online-Durchsuchung werden: Pfitzmann verwies hier auf die mündliche Verhandlung vor dem Bundesverfassungsgericht, in der ein Mitarbeiter des BKA zugeben musste, dass man erst dann, wenn man die durchsuchten Daten auswerte, wissen könne, ob man den richtigen Computer durchsucht habe. Im Unterschied zu Lauschangriffen bestehe bei einer von außen gestarteten heimlichen Online-Durchsuchung ein stärkeres Verwechslungsrisiko. Zu Verwechslungen könne es durch eine sich kurzfristig ändernde IP-Adresse nach einer Unterbrechung des Internetzugangs kommen; oder die infizierte Webseite werde zufällig von anderen Personen besucht, der infizierte Mailanhang versehentlich an Dritte weitergeleitet, die zugespielte CD mit der Schadsoftware von jemand anderem gestartet... Pfitzmann sprach sich deshalb dafür aus, im Zweifelsfall das BKA zur Verantwortung zu ziehen, schließlich habe man das Risiko der Ausforschung Unbeteiligter wohl wissend in Kauf genommen.

Welchen Zugang die Ermittler auch immer wählen, teilen alle Methoden der heimlichen Infiltration eines Rechners nach Andreas Pfitzmann ein weiteres Manko: Die durch sie gewonnenen Daten eignen sich nur sehr eingeschränkt als Beweismittel. Die Daten könnten (unbeabsichtigt) durch die Schadsoftware verändert worden sein oder gar von Dritten stammen, die sich auf vergleichbare Weise Zugang zu dem Rechner verschafft haben - eine strafprozessuale Anwendung von Online-Durchsuchungen wäre deshalb noch schwieriger als im Präventionsbereich. Alternativ schlägt Pfitzmann deshalb vor, bei der heimlichen Überwachung auf eine Aufzeichnung von Abstrahlungen (des Monitors, der Tastatur o.a. Schnittstellen) zu setzen.

Andreas Pfitzmann hob hervor, dass das neue Computer-Grundrecht ein deutliches Signal gegen immer wieder genährte Spekulationen um ein Verbot kryptografischer Programme (Verschlüsselung) bzw. von Anonymisierungsdiensten sei. Die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme setze das Recht des Einzelnen voraus, geeignete Methoden des Selbstdatenschutzes bei seinen eigenen IT-Systemen anzuwenden. Aus dem Gewährleistungscharakter des neuen Grundrecht ergebe sich auch, dass der Staat nicht nur den Selbstdatenschutz (bereits IT-mündiger) Bürgerinnen und Bürger achten müsse, sondern auch einen Bildungsauftrag habe, um den Bürgern einen kompetenten Umgang mit IT-Systemen zu ermöglichen.

Bericht: Sven Lüders

Das hier wiedergegebene Referat war ein Beitrag auf der Fachtagung "Online-Durchsuchungen. Konsequenzen des Karlsruher Richterspruchs", die die Humanistische Union gemeinsam mit der Friedrich-Naumann-Stiftung am 28. April 2008 in Berlin veranstaltete. Die weiteren Referate der Fachtagung finden Sie hier dokumentiert.

Kategorie: Veranstaltungsberichte: Audio
