



Fragen zur „Online-Durchsuchung“

Fragen zur Online-Durchsuchung:

1. Bei der Wohnungsdurchsuchung muss ein Dritter Zeuge hinzugezogen werden, wenn der Inhaber nicht anwesend ist. Außerdem ist eine Wohnraumdurchsuchung zeitlich limitiert und physisch sichtbar. Die Online-Durchsuchung ist durch Dritte nicht zu kontrollieren und damit für den Betroffenen nicht nachvollziehbar. Welche rechtlichen Schlußfolgerungen ziehen Sie daraus?
2. Die Online-Durchsuchung hat eine weitaus größere Eingriffstiefe als die Wohnungsdurchsuchung und umfasst - da es sich um einen Datenspeicher handelt - auch Informationen, die vom Tagebuch, über Briefe, E-Mails, Zeitunglesen, Onlinebanking, Webserver eine Vielzahl an sozialen Tätigkeiten eines Bürgers. Sie ist nicht punktuell wie die Wohnungsdurchsuchung, sondern sie wirkt über Zeitabschnitte und ist damit erheblich intensiver. Wie bewerten Sie die Eingriffstiefe der heimlichen Online-Durchsuchung gegenüber der offen durchzuführenden Wohnungsdurchsuchung und welche rechtlichen Schlußfolgerungen ziehen Sie daraus?
3. Frage zur Beweissicherheit: In der Computerforensik werden heute Festplatten nach der Beschlagnahme "eingefroren", damit sie nicht später verändert werden können (sonst wäre der Beweiswert gleich Null). Die Online-Durchsuchung lässt diese Möglichkeit nicht zu: Sie ist eine Online-Beobachtung des Clients. Die Erkenntnisse lassen sich nicht beweisicher speichern. Welchen Beweiswert soll eine solche Online-Durchsuchung haben und wie soll die Beweissicherheit hergestellt werden?
4. Wenn die Beweissicherheit nicht als notwendig angesehen wird, dann ist die Online-Durchsuchung ein weiterer Schritt zur „Vernachrichtendienstlichung“ der Polizei. Wie bewerten Sie die immer schwierigere Abgrenzung zwischen Nachrichtendienst und Polizei?

5. Wie kann der Kernbereich der privaten Lebensgestaltung der Beschuldigten bzw. anderer betroffener Benutzer des gleichen Systems (bei Multi-User-Systemen) sichergestellt werden?
6. Welche Gefahren für den Kernbereich der privaten Lebensgestaltung eröffnen sich und wie kann ein Missbrauch der Spionagesoftware technisch unterbunden werden? In welcher Weise ist der vom Bundesverfassungsgericht geforderte Schutz des Kernbereichs privater Lebensgestaltung beim Einsatz von Spionagesoftware technisch machbar?
7. Was genau ist mit den "Suchbegriffen" (BKA-Gesetz Art. 20k) gemeint? Woher weiss ein Ermittler, unter welchen Begriffen Terroristen ihre Pläne auf ihrer Festplatte speichern?
8. Sollen Teile der entwickelten Spionagesoftware später wiederbenutzt werden? Wie soll in diesem Fall sichergestellt werden, dass dies nicht zum Aufspüren der Software durch Anti-Viren-Hersteller oder Wirtschaftsspionierende führen wird?
9. Die Online-Durchsuchung setzt ein mehr oder minder „unsicheres“ Netz voraus. Damit einher geht eine Umwertung der bisherigen Sicherheitspolitik. Die Sicherheitsbehörden und das BSI machen das Netz nicht sicherer, sondern im Gegenteil: Es gibt ein staatliches Interesse, „Hintertüren“ in Betriebs- und Anwendungssysteme zu nutzen oder sogar „einzubauen“. Hinzu kommt, dass wenn die deutschen Sicherheitsbehörden heimlich auf Rechner zugreifen können, dass dies dann auch Dienste anderer Staaten können. Wie bewerten Sie diese Tatsache vor dem Hintergrund der weltweiten Wirtschaftsspionage und welche Folgen könnte dies für den Wirtschafts- und Forschungsstandort Deutschland haben? Wer schützt die Zugänge (Ports), die für die Online-Durchsuchung genutzt werden sollen, gegen den Zugriff beispielsweise zu Zwecken der Wirtschaftsspionage oder durch Sicherheitsbehörden und Dienste anderer Staaten?
10. IT-Sicherheit und Datenschutz sind die zentralen Akzeptanzkriterien der sich herausbildenden Informationsgesellschaft und der weltweiten Daten- und Kommunikationsnetze. Eine Folge der heimlichen Online-Durchsuchung wird eine Vertrauenskrise der e-Society sein: Bürgerinnen und Bürger und möglicherweise auch Unternehmen werden beispielsweise auf Updates verzichten, weil sie ihren Systemen nicht mehr vertrauen. Sie werden möglicherweise auch auf Anwendungen wie Online-Banking ver-

zichten. Welche Konsequenzen erwarten Sie aus der heimlichen Online-Durchsuchung für die Akzeptanz der Nutzerinnen und Nutzer und das Vertrauen in die IT-Sicherheitsinfrastruktur?

11. Wie möchte das BSI der abzusehenden Vertrauenskrise, der sich auch eine erneute BSI-Debatte anschließen wird, begegnen?
12. Wer berät sachverständig die Sicherheitsbehörden und das BMI bei der Konfiguration von Online-Durchsuchungen?
13. Welche staatlichen Stellen beraten Bürgerinnen und Bürger, Forschungseinrichtungen und Unternehmen oder Verwaltung, um Schutzlücken ihrer technischen Systeme aufzudecken und sich vor unberechtigten Zugriff zu schützen?
14. Wenn keine Softwareteile wiederverbenutzt werden, wie hoch schätzen Sie den Mehraufwand für die jeweilige komplette Neuentwicklung?
15. Mit welchen Kosten rechnet das BMI / das BKA pro ausgespähter Person, bei Wiederverwendung von Teilen der Software für die Durchführung von Online-Durchsuchungen bzw. bei kompletter Neuentwicklung?
16. Wie hoch ist nach Einschätzung des BMI / BKA die Entdeckungsfahr beim Einsatz des bzw. der Tools der Online-Durchsuchung? Wie soll sichergestellt werden, dass Kriminelle oder Wirtschaftsspionierende keinen Zugriff auf den mit der Spionagesoftware infizierten Rechner bekommen und darüber in andere mit dem Rechner verbundene Netzwerke (VPN-Netzwerke etwa in Firmen und Behörden o. ä.) gelangen?
17. Eine Schwachstelle in einem Computersystem, die ausgenutzt wird, lässt ein Tor offen für andere Spionageprogramme - sehen Sie eine Gefahr möglicher Schadensersatzforderungen betroffener Unternehmen?
18. Was ist vorgesehen, um die Software zu steuern oder abzuschalten, wenn der Port für die Kommunikation beispielsweise mittels einer Firewall gesperrt ist?
19. Wie soll sichergestellt werden, dass die Online-Durchsuchungssoftware unbemerkt bleibt, vor allem beim Einsatz von Firewalls und Systemüberwachungssoftware? Sollen diese evtl. durch die Online-Durchsuchungssoftware ausgeschaltet werden?

Wenn ja, wie sehen Sie die dann erhöhte Anfälligkeit des Systems gegenüber anderen Angreifern?

20. Wie soll verfahren werden, wenn gängige Anti-Viren-Programme oder Firewalls die Tools bzw. die Online-Durchsuchungssoftware entdeckt haben?
21. Wie sollen Instabilitäten bei sich oft ändernden Bedingungen auf dem Zielrechner (Neuinstallation oder Updates von Software oder Betriebssystem) verhindert werden?
22. Wie soll die automatische Löschung der Software nach dem vorgeschriebenen Zeitrahmen realisiert werden? Auf welchen Zeitgeber stützt sich die Löschung und was geschieht, wenn dieser nicht verfügbar ist bzw. verändert wird?
23. Sollen die technischen Möglichkeiten der Onlinedurchsuchung auch zu einer dauerhaften akustischen und visuellen Raumüberwachung verwendet werden?
24. Trojaner können Daten eines ausspionierten Rechners manipulieren sowie Daten platzieren. Können die mittels Online-Durchsuchung gewonnenen Informationen vor Gericht zweifelsfrei als echt angesehen werden? Welchen Beweiswert und Aussagegehalt haben die mit der Online-Durchsuchung erlangten Daten und Informationen?
25. Informatiker und IT-Sicherheitsfachleute sind übereinstimmend der Meinung, dass es technisch nicht möglich ist, während der Durchführung der Online-Durchsuchung zu verhindern a) privateste Daten des durchsuchten PCs einzusehen und b) Daten auf dem PC zu manipulieren oder hochzuladen, bspw. um Beweise für eine Straftat zu fälschen. Ein "digitales Richterband" in Form eines Logs lässt sich so manipulieren, dass dieser Missbrauch für einen überprüfenden Richter nicht nachweisbar ist. Wie wollen Sie einen solchen Missbrauch verhindern?
26. Das BKA argumentiert, dass man den Quellcode der Durchsuchungs-Software bei Gericht vorlegen werde, wenn die Maßnahme beantragt wird. Sind sie der Meinung, dass Gerichte in Deutschland tatsächlich in der Lage sind, anhand des Quellcodes einer Software deren korrekte Funktion zu beurteilen?
27. Was ist unter einem informationstechnischem System in abschließender Definition zu verstehen? Sind unter "informationstechnischen Systemen" auch Mobilgeräte wie

Handys, Smartphones, Blackberries etc. zu verstehen? Sind unter "informationstechnischen Systemen" auch Infrastrukturkomponenten untergeordneter Netzebenen zu verstehen (Router, Switches, aber auch DE-CIX-Einrichtungen ...)?

28. Wie wird die Zugriffsmöglichkeit für Ermittler technisch installiert und realisiert? Wie wird die Datenübertragung realisiert? Wie wird die Revisionsfähigkeit der Online-Durchsicht technisch sichergestellt, so dass die Methode und die Authentizität der gewonnenen Informationen der Prüfung durch einen unabhängigen Gutachter standhält?
29. Wie wird technisch sicher ausgeschlossen, dass der für eine Online-Durchsicht verwendete Zugang nicht von Dritten mißbraucht wird?
30. Wie wird bei Beendigung der Maßnahme technisch sichergestellt, dass das untersuchte informationstechnische System wieder in den ursprünglichen Zustand versetzt wird? Wie wird technisch sichergestellt, dass nicht z.B. durch ein während der Maßnahme erzeugtes Backup der kompromittierte Zustand wieder hergestellt wird?
31. Wie wird während der einzelnen Phasen von Infiltration, Überwachung/Kommunikation und Beendigung der Maßnahme technisch sichergestellt, dass die Maßnahme nicht aufgedeckt und mit Gegenmaßnahmen beantwortet wird?
32. Mit welchen Gegenmaßnahmen gegen Online-Durchsicht und -Überwachung wird gerechnet und wie soll diesen technisch wie organisatorisch begegnet werden?
33. Wie soll verschlüsselte Internettelefonie überwacht werden, wenn die Nutzer die Verschlüsselung nicht durch einen PC durchführen lassen, sondern durch ein Hardware-VoIP-Telefon, das sichere Verschlüsselung unterstützt?
34. Warum ist diese Methode nicht auch für das Abfangen PC-verschlüsselter VoIP-Kommunikation geeignet?

35. Welche Stellen sind aus Gründen der Einleitung der Maßnahme ggf. zu kontaktieren (z.B. Provider)?
36. Welche genauen technischen Möglichkeiten gibt es und welche davon sollen genutzt werden, um die Maßnahmen umzusetzen differenziert nach
- a) dem Aufbringen der Überwachungssoftware auf das informationstechnische System,
 - b) der Identifizierung (Dateien) und Erfassung (Tastatureingaben etc.) von Inhalten unter Sicherstellung des Schutzes des Kernbereichs privater Lebensgestaltung,
 - c) der Ausleitung von Inhalten aus dem informationstechnischen System,
 - d) der jederzeitigen Beendigung der Maßnahme unter Sicherstellung, dass keine Beeinträchtigung der Systemsicherheit resultiert.
37. Wie wird technisch sicher ausgeschlossen, dass vom Aufbringen der Überwachungssoftware versehentlich Unbeteiligte betroffen werden?
38. Ist auch geplant, zur Installation eines Trojanischen Pferdes E-Mail-Kommunikation zwischen Verdächtigen zu manipulieren (z.B. durch Infizierung eines erwarteten Dateianhangs) oder vorzutäuschen? Falls ja: Wie soll dies technisch realisiert werden? Wie wird technisch sicher ausgeschlossen, dass sich Dritte dieser Möglichkeit bemächtigen?
39. Ist geplant, dass eine Softwarekomponente auf dem Zielsystem auch bei Nichtbestehen einer Online-Verbindung Informationen sammelt (Tastatureingaben, etc.), diese auf dem Rechner zwischenspeichert und dann zeitversetzt übermittelt?
40. Soll eine Installation eines Trojanischen Pferdes Änderungen an der Systemkonfiguration vornehmen? Falls ja: Zu welchem Zweck? Wie wird sichergestellt, dass nach Beendigung der Maßnahme die Systemkonfiguration bereinigt wird?

41. Soll eine Identifizierung relevanter Inhalte vor der Übertragung auf dem Zielsystem oder erst nach einer Übertragung auf einem Ermittlersystem erfolgen?
42. Wie wird im Falle fremdsprachlicher Datenbestände die Analyse von Daten realisiert?
43. Ist geplant, für die Infiltration von Zielsystem Informationen über Sicherheitslücken in Software, die den jeweiligen Herstellern noch nicht bekannt sind (sog. Zero-Day-Exploits) auf entsprechend von Kriminellen angebotenen Märkten zu erwerben? Falls nein: Wie sollen diese Informationen dann beschafft werden?
44. Wie wird bei einem Zielsystem, das keine Internet-Verbindung mit dem Ermittlungssystem mehr aufbauen kann, sichergestellt, dass das Trojanische Pferd nach Ablauf einer befristeten Anordnung deaktiviert und vom System ohne Zurücklassen von Sicherheitslücken deaktiviert wird?
45. Welche Software wurde bei den bereits ohne Rechtsgrundlage durchgeführten Online-Durchsuchungen verwendet, wer hat sie hergestellt, wer unabhängig die Funktionsweise geprüft?

Vorschlag für Sachverständige:

Dr. Johann Bizer / Markus Hansen, Unabhängiges Landeszentrum für den Datenschutz Schleswig-Holstein (ULD)

Andreas Pfitzmann, TU Dresden

Dr. Alexander Dix, Landesbeauftragter für den Datenschutz, Berlin

Constanze Kurz, Chaos Computer Club

Prof. Dr. Jörg Schwenk und **Dr. Christoph Wegener**, Ruhr-Universität Bochum, Horst Görtz Institut für IT-Sicherheit

Peter Schaar, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit.