SÜDWESTRUNDFUNK
SWR2 Wissen – Manuskriptdienst

Tatort Internet: Der Computer als Ermittler

Autor: Kai Laufen
Redaktion: Detlef Clas
Regie: Eigenproduktion des Autors
Sendung: Montag, 20. April 2009, 8.30 Uhr, SWR 2

Dieses Manuskript enthält Textpassagen in [Klammern], die in der ausgestrahlten Sendung aus Zeitgründen gekürzt wurden.

MANUSKRIPT

Autor:
Das Internet ist ins Gerede gekommen – die Schattenseiten der weltweiten Vernetzung treten auf allen Ebenen zu Tage, kulturell, gesellschaftlich, politisch und: Schon „einige hunderttausend Menschen“ seien Opfer von Computerkriminalität geworden, warnte Jörg Ziercke, der Präsident des Bundeskriminalamtes, im Herbst 2008 auf einer Fachtagung in Berlin. Jewgeni Kaspersky, ein anerkannter Fachmann für alles, was Computern und dem Internet schädlich werden kann, weiß auch warum die Computerkriminalität so rasant zunimmt und immer raffinierter wird:

Cut 1 (Kaspersky):
There are three factors, which define and stimulate cybercriminals …

Übersetzer:
Drei Dinge motivieren die Computerkriminellen:
Einmal ist es profitabel – Computerkriminalität bringt viel Geld ein, zweitens: Diese Art Kriminalität ist sehr leicht umzusetzen und drittens ist es ein Geschäft mit sehr geringem Risiko.

Ansage:
Tatort Internet: Der Computer als Ermittler. Eine Sendung von Kai Laufen

Autor:
Hinter den Zahlen, mit denen Sicherheitsexperten und Polizei die Schäden und Opfer ermessen, liegt ein weites Feld ganz unterschiedlicher Delikte: Noch nie war es so leicht, Kinderpornografie zu verbreiten. Bankkunden werden immer öfter ausgeraubt, weil ihre Kundendaten abgefischt wurden. Die Infrastruktur von Firmen, Politischen Gruppen oder ganzen Staaten werden digitalisiert angegriffen. Die Unterhaltungsbranche beziffert ihre Verluste durch sogenannte Raubkopien in Milliardensummen. In manchen Internetforen wird gemobbt, gelogen und beleidigt, in anderen tauschen sich Kriminelle über neue Angriffsmethoden und -ziele aus. Terroristen versuchen Mittäter über Webseiten zu rekrutieren. So unterschiedlich die Delikte auch sind: Computer und das Internet taugen als Tatort und als Tatwaffe. Aber auch die Ermittler und Sicherheitsexperten rüsten nach, fasst der IT-Forscher Thorsten Holz von der Universität Mannheim zusammen:

Cut 2 (Holz):
Im Bereich der IT-Sicherheit ist es eben so, dass man dauernd so einen Wettlauf hat zwischen den Angreifern und den Verteidigern. Mal ist der eine ein Stück weiter, mal der andere. Es gibt da dauernd Weiterentwicklungen in diesem ganzen Bereich, deshalb muss man auch aktiv dabei bleiben und ich denk, Automatisierung ist eben so einer der Schlüssel. Dadurch dass das Problem so groß geworden ist und die Angreifer viel Automatisierung benutzen, dass wir aus Verteidigersicht eben auch schauen müssen, wie kann man Sachen automatisieren, wie kann man wirklich schnell an neue Infos kommen.

Autor:

Der typische Bankraub findet heute nicht mehr mit übergezogener Maske und vorgehaltener Waffe in einer abgelegenen Filiale statt, sondern inmitten der Datenströme, die zwischen Banken, Privatkunden, Firmen und Kreditkartenanbietern ausgetauscht werden.

Cut 3 (Laufen):
Am 12. hab ich zufällig bei meiner Visakarte mir den Kontoauszug angesehen und festgestellt, dass zu dem Zeitpunkt schon über 2.400 Euro von diesem Visa-Konto in bar von diversen Banken in Sao Paolo, Brasilien abgebucht worden sind.

Autor:
... wo der Bankkunde Michael Laufen noch nie war – leider, fügt er mit einem Schmunzeln hinzu, denn nach dem ersten Schrecken hat er den Humor wieder gefunden; die Bank hat das Geld zurückerstattet. Wie die Täter an die Daten seiner Kreditkarte gekommen waren ist nicht geklärt. Es gibt verschiedene Vorgehensweisen, von denen die Mannheimer Computerforscher um Thorsten Holz einige genauer betrachtet haben. Ausgangspunkt der Forschung sind PCs, die bewusst ohne jeglichen Virenschutz mit dem Internet verbunden sind. Nach der Devise „Mit Honig fängt man Bären“ soll der Honeypot ganz bewusst Schadsoftware einfangen, die im Internet verbreitet wird.

Cut 4 (Holz):
Wir machen die Honeypots um Kopien von der Schadsoftware zu bekommen und im zweiten Schritt machen wir dann eine automatische Analyse in der wir die Schadsoftware, die wir gefangen haben in einer speziellen Umgebung starten. Das ist eben auch ein Windows-System was eben entsprechend auch relativ stark überwacht wird. Wir sehen dann eben alles, was auf dem System funktioniert, führen die Schadsoftware aus und sehen, was die am System verändert, zum Beispiel, welche neuen Dateien auf dem Dateisystem erstellt werden oder was eben auch interessant ist, welche Netzwerkkommunikation stattfindet, also Daten hingeschickt werden und so.

Autor:
Der normale Computernutzer würde von diesen Vorgängen nichts merken: Weder, dass sein Rechner mit Schadsoftware infiziert ist, noch dass diese Schadsoftware heimlich über das Internet kommuniziert. Mit einem kriminellen Unbekannten, irgendwo auf dem Globus. Der kann die Schadsoftware nun ausbauen: Neue Funktionen werden eingespielt, zum Beispiel sogenannte Keylogger-Programme. Sie schreiben die Tastaturbefehle mit und übersenden das, was der Nutzer seinem Rechner anvertraut, unbemerkt weiter. Während Geheimdienste solche Programme für Spionage und Terrorabwehr nutzen, sind Kriminelle meistens an Passwörtern und Geheimzahlen interessiert. Innerhalb weniger Monate hatten Thorsten Holz und seine Kollegen rund 2.000 verschiedene Keylogger gefunden und analysiert. Dann begannen sie mit ihrem eigentlichen Forschungsprojekt: Sie wollten sehen, wie die Hintermänner ihre Identität verschleiern. Sie untersuchten, was die Keylogger-Programme mit den ausgespähten Daten machen:

Cut 5 (Holz):
Wenn der Angreifer die Infos per E-Mail rausschickt, ist es relativ einfach, so einen E-Mail-Account zu deaktivieren. Was die Angreifer jetzt mehr und mehr machen ist einfach selbst so einen Server zu betreiben, der einfach irgendwo im Internet steht

und dort werden einfach die Daten hingeschickt und er kann die dort später abholen.

Autor:
Ein Server ist in diesem Fall ein leistungsstarker Computer mit großer Speicherkapazität, der von einer unbeteiligten Firma vermietet wird. Er kann irgendwo auf der Welt stehen, in den USA oder Brasilien oder auch in Deutschland. Der kriminelle Kunde mietet den Server für seine Zwecke und muss sich dafür oft nicht einmal ausweisen. Letztlich kann dieser Kunde den Inhalt des Servers noch verschlüsseln, sodass nicht einmal der Dienstleister oder die Polizei den illegalen Inhalt entdecken könnten. Weil der Server zum Ablegen der ausgespähten Daten dient, wird er von den Fachleuten Dropzone genannt.

Cut 6 (Holz):
Wir haben durch die Analyse dann 300 verschiedene solcher Dropzones gefunden, die weltweit verteilt stehen und auf 70 von denen hatten wir dann auch Zugriff drauf, sprich, wir konnten dann auch sehen, was die Angreifer gestohlen haben und auf diesen 70 haben wir dann Information von 170.000 Opfern gefunden.

Autor:
Auf 170.000 verschiedenen Rechnern weltweit waren Keylogger-Programme heimlich installiert, die ganz bestimmte Daten mitschnitten und an die Dropzones verschickten. Viele dieser Rechner werden von mehreren Familienmitgliedern benutzt oder stehen in Internetcafés. Die Zahl der betroffenen Personen ist vermutlich noch deutlich höher. Aber das Forschungsprojekt, das ist sich Thorsten Holz sicher, hat nur einen Bruchteil der Gesamtmenge an gestohlenen Daten gezeigt.

Cut 7 (Holz):
Was wir viel gesehen haben waren Opfer in den USA beziehungsweise in Russland. Ich denke, das ist eben dadurch, dass dort viel mehr Internetnutzer sind. Ich glaube innerhalb von Deutschland haben wir etwas mehr als zehntausend Opfer gesehen. Also es gibt auch deutsche Opfer, klar, aber die großen Opferländer sind eigentlich auch die Länder, wo es – absolut gesehen – mehr Internetnutzer gibt.

Autor:
[Die Daten der ausgespähten Opfer haben die Mannheimer IT-Forscher an spezialisierte Kollegen der australischen Regierung weitergegeben. Die haben die abgefischten Bankdaten, gestohlenen Passwörtern für E-Mail-Konten oder Internetgeschäfte sortiert und die Betroffenen gewarnt. Internationale Zusammenarbeit auf dem kleinen Dienstweg gewissermaßen.] Natürlich interessieren sich auch Ermittlungsbehörden für solche Forschungsergebnisse. Die Kontakte zu Bundes- und Landeskriminalämtern sind geknüpft, auf Fachtagungen der IT-Sicherheitsbranche sind oft auch Kriminalbeamte anzutreffen. Sie müssen sich ständig fortbilden um Schritt zu halten mit den mal mehr, mal weniger organisierten Kriminellen. Deren Zahl wird auf mehrere Tausend geschätzt. Es sind gut ausgebildete Programmierer, die in ihren Herkunftsländern keinen gut bezahlten legalen Job finden. Das trifft heute besonders für Russland, die Ukraine und andere osteuropäische Länder zu, aber

nicht nur. Erst vor wenigen Wochen hat das Landeskriminalamt Baden-Württemberg das Hackerforum „Codesoft“ vom Netz genommen. Die Ermittler hatten eine Dropzone auf einem deutschen Server gefunden und beobachtet, wer die zwischengelagerten Daten abholt:

Sprecher 1:
Die Internetfahnder des LKA werteten die Zugriffe auf diesen Server aus und konnten so zwei mutmaßliche Haupttäter, einen 25-Jährigen aus dem Ortenaukreis und einen 28-Jährigen aus Niedersachsen identifizieren. Sie stehen im Verdacht, seit September 2008 über 80.000 PCs weltweit mit der Schadsoftware „Codesoft PW Stealer“ infiziert zu haben.

Autor:
– so das Landeskriminalamt in einer Pressemitteilung

Sprecher 1:
[Die weiteren Ermittlungen zielen nun auf eine bisher noch nicht bestimmbare Anzahl von Tatverdächtigen, die mit den ausgespähten Daten betrügerische Warenkäufe im Internet begangen haben sollen.] Durch das schnelle Eingreifen der beteiligten Ermittlungsbehörden konnte jedoch größerer Schaden verhindert werden, sodass nur ein geringer Anteil der ausgespähten Daten in unbefugte Hände gelangte. Der tatsächliche Schadensumfang kann bisher noch nicht abgeschätzt werden.

Autor:
Gar nicht abschätzen lässt sich der mögliche gesellschaftliche Schaden, der daraus resultieren kann, dass Computerfreunde so leicht wie nie zuvor die Grenze zu strafbarem Handeln überschreiten. Oder sich radikalisieren, zumindest verbal. Beispielhaft der Eintrag des Users LALALALA in einem anderen Hacker-orientrierten Forum:

Sprecher 2:
Jedenfalls sind diese Lutscher jetzt der Meinung, das sie es voll drauf haben, weil sie **ein** Hackerforum von Tausenden vom Netz "genommen haben"... Dabei ist das nur ein kleiner Schritt, der nichts bewirkt. Es gibt noch genug Hackerforen in der Deutschen Szene.
Die sollen mal versuchen die ganz großen Russischen Hackerforen vom Netz zu nehmen, dann können sie sagen, sie haben was geleistet. Scheiß Kripo Lutscher! Ich hoffe ihr kommt irgendwann auch mal zu mir, aber bitte bewaffnet, denn ohne werdet ihr das nicht überleben!

Autor:
Vor dem Bildschirm setzt das Gewissen offenbar noch leichter aus als im echten Leben. Dann ist es oft nur noch eine Frage des Geldes, ob man für Wissenschaft, Wirtschaft, Polizei auf der einen Seite oder eine kriminelle Struktur auf der anderen Seite arbeitet. Deshalb will Thorsten Holz auch noch ein wenig mehr über den kriminellen Untergrund herausfinden:

Cut 8 (Holz):
Wo wir jetzt noch gerne weitermachen würden wäre eben zu verstehen: Wie groß ist jetzt wirklich diese Underground Economy. Also wie viel Geld kann man

verdienen, in dem man so was macht. Wie viel verdient so ein typischer Angreifer oder was ist die Größe dieses Markts. Ist das im Bereich von ein paar Tausend Euro? Vermutlich nicht! Ist das im Bereich von 100 Millionen Euro? Vermutlich auch nicht! Wahrscheinlich irgendwo dazwischen.

Autor:
Geld als Motivationsfaktor steckt auch hinter einem anderen Übel, mit dem sich eine jungen Forschergruppe an der Fachhochschule Gelsenkirchen beschäftigt: Botnetze. Die Angreifer infizieren zigtausenden Computer in Privathaushalten mit Schadsoftware – die Computer werden zu Robotern, zu Bots, die teure Schäden anrichten, erklärt der Projektleiter Christian Dietrich:

Cut 9 (Dietrich):
Die Auswirkung von Botnetzen kriegt wirklich fast jeder mit. Fast jeder hat schon mal eine Spam-Mail bekommen, also eine unerwünschte – in der Regel: Werbe-E-Mail, in der halt für irgendwelche komischen Produkte geworben wird. Und die werden halt hauptsächlich über Botnetze verteilt. Eine andere Auswirkung, die wir sehen, sind sogenannte Denial-of-Service-Attacken. Das heißt, das sind Angriffe, bei denen ein Dienst oder ein Zielsystem quasi unwirksam gemacht wird, weil es einfach mit Anfragen überschüttet wird.

Autor:
Mit ähnlichen Methoden wie in Mannheim, sammelt Christian Dietrich am Institut für Internet-Sicherheit der Fachhochschule Gelsenkirchen Erkenntnisse über die Schadprogramme, die harmlose Heimcomputer zu willenlosen Botrechnern werden lassen:

Cut 10 (Dietrich):
Man unterscheidet zwei Arten von Botnetzen: Zum einen die zentral ausgerichteten Botnetze. Die haben also irgendwo eine Zentrale und wenn man diese Zentrale vom Internet nimmt, dann wissen die Bots auch nicht mehr, was sie tun sollen, bis auf vielleicht irgendwelche Back-up-Mechanismen, die dann nach einiger Zeit irgendwie aktiviert werden. Im Fall von Peer-to-Peer-Botnetzen ist das ganze ein bisschen schwieriger, denn dort kann rein theoretisch jeder Bot Botmaster werden, also quasi das ganze Netz kontrollieren und das macht das Ganze natürlich relativ schwierig vom Netz zu nehmen, denn sobald ich einen Botmaster oder einen temporären Botmaster vom Netz nehme, springt wahrscheinlich direkt der nächste ein und kontrolliert den Rest des Netzes.

Autor:
Das englische Wort „Peer“ bedeutet Gleichgestellter, Ebenbürtiger. Ein peer-to-peer-Netzwerk von Computern stellt also eine hierarchiefreie Kommunikation zwischen gleichgestellten Computern über das Internet her. So ein Botnetz ist sehr schwer zu stören, aber es gibt erste Forschungsansätze:

Cut 11 (Dietrich):
Wir haben jetzt kürzlich Methoden gesehen: Wiederum Angriffe gegen dieses Botnetz, die man machen kann, wenn man einmal in diesem Botnetz drin ist. Und damit kann man sozusagen das Netz mehr oder weniger stören und es quasi ineffektiv machen. Aber es ist deutlich schwieriger so ein Netz vom Internet zu

trennen oder die Bots zu eliminieren als das mit den zentral ausgerichteten Botnetzen ist.

Autor:
Ein weiterer Schlag gegen die Spam-Versender gelang im Herbst 2008. Am 11.11. wurde in den USA der Internetdienstleister McColo vom Netz genommen, von dessen Servern aus Botnetze gesteuert wurden. Das weltweite Spam-Aufkommen brach auf ein Viertel zusammen. IT-Experten jubelten, die Szene spricht vom McColo-Day.

Cut 12 (Dietrich):
Leider hat sich das in der jüngeren Vergangenheit wieder etwas relativiert. Wir sehen wieder deutlich mehr Spam als im Vergleich zu dem 11.11.2008. Aber es ist immer noch etwas weniger als wir kurz vor dem Vom-Netz-Nehmen gesehen haben.

Autor:
Noch ist keine wirksame Waffe gegen Spam und die dahinter stehenden Botnetze erfunden. Aber im Köln-Bonner-Raum hat ein Internetdienstleister Konsequenzen gezogen: Die Firma NetCologne bietet schnellen Internetzugang, macht die Verbindung aber notfalls auch schnell dicht. Der Diplom-Informatiker Dietmar Braun erklärt das automatisierte Vorgehen, mit dem NetCologne seine Kunden schützt:

Cut 13 (Braun):
Also wir betreiben derzeit bei NetCologne zwei Systeme hauptsächlich. Zum einen sind das reaktive Maßnahmen, die passieren. Das sind Maßnahmen, die aufgrund von Beschwerden, die wir bekommen, durch Kunden, die irgendwie Spam versenden oder sich nicht konform verhalten. Und das zweite System ist eben das Honeypot-System mit dem wir proaktiv quasi Kunden erfassen können, die sich gerade frisch infiziert haben oder versuchen andere Rechner zu infizieren.

Autor:
Das Honeypot-System erfasst, wenn der Rechner eines Kunden große Menge E-Mails in kurzer Zeit versendet, und sich damit anders verhält als ein normaler Nutzer. Das deutet darauf hin, dass der Computer des Kunden mit Schadsoftware infiziert wurde und nun Teil eines Botnetzes ist, wovon der Kunde im Normalfall nichts weiß. Aber nur der Kunde kann effektiv etwas gegen den Befall tun, nämlich eine Anti-Virensoftware installieren und aktuell halten. Also ist es konsequent, wenn der Internetdienstleister seine Kunden dazu motiviert – auch wenn die Maßnahmen drastisch klingen:

Cut 14 (Braun):
Der Kunde wird ermittelt, der Kunde wird gesperrt im System, der Kunde wird anschließend aus der Leitung rausgeschmissen, sodass er nicht mehr online versenden kann, kein Spam mehr versenden kann und er landet auf einem Zwangssystem, das wir Forced Portal nennen, was dazu führt, dass sämtliche Internet-Konnektivität des Kunden gesperrt ist, also kein weiterer Spam-Versand geschehen kann.

Autor:

Einmal auf dem Zwangssystem isoliert, wird der betroffene Kunde darüber aufgeklärt, was passiert ist und wie er den Internet-Zugang wieder herstellen kann. Das Management habe anfangs befürchtet, mit diesem drastischen Vorgehen Kunden zu verärgern und zu verlieren, erinnert sich Dietmar Braun. Und so argumentieren auch viele andere in der Branche. Natürlich gebe es auch mal verärgerte und uneinsichtige Kunden, die meisten aber würden positiv reagieren – und manche wünschen sich noch mehr Schutz durch ihren Internetdienstleister:

Cut 15 (Braun):
Ein Geschäftskunde, der Spam versendet hat, der von unserem Geschäftskundensupport darauf hingewiesen worden ist, der dann wie meistens unsere Geschäftskunden so sind, sehr kooperativ war und das Problem beseitigt hat, hat uns anschließend gefragt, so nach dem Motto „Ich hab jetzt das Problem beseitigt, könnt ihr bitte mal auf meine Leitung schauen ob ich denn jetzt sauber bin?“ Und da mussten wir ganz klar sagen: Nein, das können wir nicht, das dürfen wir nicht und insbesondere: Das wollen wir auch nicht.

Autor:
Denn der Internetdienstleister ist nur zum Durchreichen des Datenverkehrs befugt, nicht zu seiner inhaltlichen Kontrolle – eine Situation, die die meisten Anbieter auch gerne so belassen möchten, weil es Geld und Ärger erspart. Der Kampf gegen Computerkriminalität ist auch in diesem Bereich eng an die Frage geknüpft, wie im Internet Geld verdient wird, ob nun legal oder illegal. So fanden Forscher an der Universität Berkeley kürzlich heraus, dass Spam-Mails einen äußerst geringen Wirkungsgrad haben: Nur eine von zwölfeinhalb Millionen dieser Werbemails bringt einen Empfänger dazu, etwas zu bestellen.
Die Logik der Spam-Versender wird also von großen Zahlen beherrscht. Die Logik ihrer Gegner ebenfalls. Um den riesigen Datenmengen, die bei solchen Studien anfallen, überhaupt Herr zu werden, müssen die Forscher ihre Rechner in die Lage versetzen, möglichst viel Arbeit selbstständig zu erledigen.
Auch bei der Bekämpfung der Kinderpornografie im Internet werden Ermittler längst von automatisierten Prozessen unterstützt. Finden sie bei einem Tatverdächtigen große Bildersammlungen, kommt PERKEO zum Einsatz. Die Software vergleicht die neue Sammlung mit einer Datenbank bereits bekannter Bilder, hilft also bei der Beweissicherung wenn es um den Besitz von Kinderpornografie geht. Das Programm EXCALIBUR kann sogar die Bildhintergründe erkennen – ist dort eine Landschaft zu sehen, die auch in anderen Bilderserien auftaucht, oder etwa eine Mineralwasserflasche, die nur in einer bestimmten Region verkauft wird, kann so ein Hinweis schon mal zu einem Täter führen und einen sexuellen Missbrauch beenden. Um den meist sehr großen Bildersammlungen beizukommen, wird in Bochum noch an einer ganz anderen Idee geforscht – Hans-Martin Bröker vom Sicherheitsunternehmen L-1 Identity Solutions formuliert das Ziel:

Cut 16 (Bröker):
Es ist möglich, eine große Menge von Gesichtsbildern, die kindliche Gesichter und Erwachsenengesichter enthalten, gemäß des Alters zu sortieren. Und das ist auch ein Schwerpunkt dieses Projektes, eben die Idee, dass eine große Datenmenge, die händisch nicht mehr bewältigt werden kann, dass man die in automatisierter Form sortiert, sodass man gezielter nach kindlichen Gesichtern suchen kann und diejenigen Bilder, die nur Erwachsenengesichter enthalten und somit per Definition

keine Kinderpornografie in den Hintergrund schiebt und man sich auf das verdächtigste Material konzentrieren kann bei der Suche.

Autor:
Die Entwickler haben mehrere mathematische Verfahren kombiniert, die aus der biometrischen Gesichtserkennung bekannt sind. Dabei werden – sehr vereinfacht gesagt – Augen, Nasen oder Münder als Kanten beschrieben. Der Computer vergleicht deren Lage zueinander nach bestimmten Denkroutinen, sogenannten Algorithmen. *Eine* Herausforderung sei es gewesen, den schon vorhandenen Programmen abzugewöhnen, *individuelle* Gesichtsmerkmale zu erfassen – schließlich soll es hier nur ums Alter gehen. Wenn das Programm erst einmal zuverlässig für den Polizeieinsatz funktioniert, wird es ganz andere Wege gehen, als Menschen, wenn sie Gesichter betrachten und das Alter schätzen, meint Hans-Martin Bröker:

Cut 17 (Bröker):
Ich bin auch der Meinung, dass der Mensch sicherlich Gesichter ganz anders sieht. Der Mensch misst keine Kanten aus, beim Betrachten eines Gesichtes. Und algorithmisch ist das Verfahren natürlich wesentlich einfacher und elementar, aber es ist im Resultat, in der Güte der Erkennung durchaus mit menschlichen Fähigkeiten vergleichbar. In manchen Bereichen sogar überlegen. Von der Geschwindigkeit mal ganz abgesehen.

Autor:
Seit gut drei Jahren läuft das EU-geförderte Projekt und die Fortschritte sind greifbar. Man ist nun in einer dritten Phase, die nach einer Gesetzesänderung im vergangenen Herbst nötig wurde: Die Bundesregierung hat eine EU-Richtlinie umgesetzt, die auch Pornographie mit Jugendlichen unter 18 Jahren erfasst, also muss die Vergleichsdatenbank so ausgeweitet werden, dass die Altersschwelle zur Volljährigkeit erkennbar wird. Sollte das einmal zuverlässig funktionieren, kann sich Brökers Kollege Michael Dose theroretisch auch noch ganz andere Anwendungen des Programms vorstellen:

Cut 18 (Dose):
Auch das wäre eine Möglichkeit, dass man Automaten, die alkoholische Getränke ausgeben, eben auch mit so einem System verknüpft, das eine Altersschätzung durchführt.

Autor:
Man führe aber nur Grundlagenforschung durch, betont Michael Dose. Aus verständlichen Gründen, denn das Thema birgt nicht nur ein riesiges Geschäftspotenzial, sondern auch gesellschaftspolitischen Zündstoff: Was gäbe es nicht alles zu kontrollieren, wenn eine Maschine einstmals zuverlässig das Alter ihres Gegenübers bestimmen könnte! Martin Werner, der Chef der beiden Entwickler und Vorstand der L-1 Identity Solutions AG in Bochum scheut die Diskussion nicht, die in der Gesellschaft um solche Technologiefortschritte geführt wird, wie etwa dem elektronischen Ausweis und der biometrischen Gesichtserkennung:

Cut 19 (Werner):

Gesichtserkennung ist noch was, wo ich sagen würde, das ist noch am ehesten unproblematisch, weil das Bild etwas ist, was ich sowieso einigermaßen öffentlich hab. Das heißt: Man ist gewohnt, Bilder auszutauschen. Ich meine, dass es natürlich Missbrauch gibt, das ist bei Technologie glaube ich fast überall so. Insofern ist ein regulierter Umgang mit den Daten sicherlich wichtig und eine Diskussion und die Einbeziehung der Datenschutzmaßnahmen ist auch wichtig. Wenn das geklärt ist, finde ich, dann macht es keinen Sinn, die Technologie zu verteufeln.

Autor:
Doch wird die Debatte um solche Technologien, ihren möglichen Segen und ihren möglichen Missbrauch wirklich fundiert und breit in der Gesellschaft geführt? Wer ist eigentlich noch in der Lage, all die technischen Details zu verstehen und ihre gesellschaftlichen Folgen abzuschätzen? Reicht es, zu sagen: Die Technik ist neutral, es kommt nur darauf an, was der Menschen mit ihr macht? Der Wiener Kriminalsoziologe Reinhard Kreissl hat Zweifel, die er im Rahmen einer Fachtagung des Bundesforschungsministeriums im vergangenen November in die Diskussion einbrachte. Die Tagung trug den Titel: „Mit Sicherheit: für Freiheit – die gesellschaftlichen Dimensionen der Sicherheitsforschung“:

Cut 20:
Es gibt diese wunderschönen Volten der Geschichte – oder diese Paradoxien – denken Sie an die berühmte Sache mit dem Internet. War eigentlich eine militärische Erfindung, hat sich jetzt zum World Wide Web entwickelt. Nehmen Sie den Telekommunikationsbereich: Okay, wir sind alle telekommunikativ erreichbar, gleichzeitig hab ich aber damit auch die Möglichkeit jeden jederzeit und überall zu orten. Denken Sie an die Debatte über die Vorratsspeicherung von Verbindungsdaten. Technologie hat sozusagen eingebaut immer diesen Kontrolle und diesen Sicherheitsaspekt. Ich kann jedes großtechnologische System, was massenhaft verbreitet ist, unter Sicherheits- und Kontrollaspekten verwerten.

Autor:
Neue Technologien schaffen nicht nur neue Möglichkeiten der Kontrolle, also neue Sicherheit, sondern auch neue Unsicherheiten. Und neue kriminelle Möglichkeiten. Früher wurden Geldscheine gefälscht, heute Kreditkarten. Und wenn die Bankenbranche dies auch zu Recht beklagt, hat sie doch durch Online-Banking und sonstige Automatisierungen ein Vielfaches verdient. Die Computerkriminalität und besonders das emotional hoch aufgeladene Thema Kinderpornografie verschaffen der IT-Sicherheitsbranche, aber auch Polizeiermittlern und Politikern starke Argumente für mehr Regulierung und den Einsatz von mehr Überwachungstechniken. Aber die gesellschaftlichen Debatte um Sinn oder Unsinn der Technologien und entsprechende Gesetzgebungen, müsse offen geführt werden, meint Reinhard Kreissl. Denn es gelte, sowohl die möglichen Folgen als auch die Akteure und deren Interessen zu betrachten:

Cut 21 (Kreissl):
Die Umwelt wird maschinenlesbar. Man erhofft sich dadurch eine Erhöhung der Sicherheit, vergisst dabei, dass das ganze natürlich auch gleichzeitig Unsicherheiten produziert – Punkt eins. Und zum anderen, was immer sehr elegant ausgespart wird, ist die Frage: Wer verdient an dem Ganzen eigentlich?

[Was Eisenhower 1961 schon den militärisch-industriellen Komplex genannt hat, haben wir das heute nicht wieder, sozusagen den Sicherheitsindustriell-Politischen Komplex?]

Autor:
Der US-Präsident Dwight D. Eisenhower hatte bei seiner Abschiedsrede Anfang 1961 vor einem zu großen Einfluss des Militärs auf die Politik gewarnt.

Cut 22 O-Ton Eisenhower

Übersetzer:
„Es besteht die Gefahr, dass unkontrollierte Macht desaströse Folgen haben könnte. Wir dürfen nicht zulassen, dass dieser Komplex unsere Freiheit und Demokratie bedroht."

Autor:
Die drastische Warnung von damals hallt bis heute nach, noch verstärkt durch den 11. September, nach dem die Sicherheitsapparate weltweit entfesselt wurden.

Cut 22 (Kreissl):
Sie haben sozusagen zwei grundlegende Perspektiven: Die eine Perspektive ist: Oh, es gibt ziemlich große Bedrohungen, wir haben den Terrorismus, wir haben das organisierte Verbrechen, wir haben eine ganze Reihe von Gefahren, die über uns hereinbrechen, oder Gott sei dank noch nicht, aber die uns drohen und auf diese Gefahren müssen wir reagieren. Und ich sage dann immer: Das typische Szenario ist: Technik ist die Antwort, aber was war die Frage?

Autor:
Beispiel für eine solche Frage: Wie soll die Gesellschaft mit der Verbreitung von Kinderpornografie im Internet umgehen? Das pädosexuelle Interesse am Kind und an derartigen Abbildungen gibt es zwar seit Menschengedenken, aber erst das Internet hat das Phänomen in den Blickpunkt der Öffentlichkeit gerückt. Zwar wird die Masse der entsprechenden Bilder oder Filme offenbar nur in abgeschirmten Kreisen getauscht und gehandelt. Aber manche kommerzielle Anbieter haben sich auch schon dreist in das World Wide Web vorgewagt, also dem leicht erreichbaren Teil des Internets. Dagegen soll nun Technik helfen, fordert die Bundesfamilienministerin Ursula von der Leyen:

Cut 23 (Leyen):
Das Bundeskriminalamt identifiziert die einzelnen Seiten. Die volle Haftung dafür, dass die „richtigen" Seiten, nämlich die Seiten, die die kinderpornografischen Inhalte zeigen, auch nur geblockt werden, liegt bei uns, bei der Bundesregierung. Aber die technische Umsetzung, die liegt bei den Internetzugangsanbietern.

Autor:
... die sich lange gegen diese Regelung gewehrt haben – nicht nur, weil sie Kosten auf sich zukommen sehen, sondern weil sie sich rechtlich absichern wollten. Dafür wird nun das Fernmeldegeheimnis aufgeweicht. Dabei werden die Maßnahmen zum Teil ins Leere laufen: Schon kursieren im Internet Beschreibungen, wie die Sperren zu umgehen sind. Die meisten Kritiker der Regelung haben weder mit Pädophilie noch mit Kinderpornografie irgendetwas zu tun. Sie fürchten aber, dass

die technische Antwort auf das gesellschaftliche Problem eine neue Ära im Umgang mit dem Internet einläuten könnte. So etwa der IT-Sicherheitsberater und Internetaktivist Florian Walther aus Berlin.

Cut 24 (Walther):
Die Maßnahmen, die diskutiert werden, bergen natürlich erhebliches Risiko, dass in Zukunft eben nicht nur Kinderpornografie zensiert wird, sondern dass in Zukunft eben auch andere Lobbyvereinigungen und Gruppen diese Infrastruktur und technischen Maßnahmen die man jetzt diskutiert und einführen möchte, nutzen, um eben ganz andere Interessen durchzusetzen und ganz andere Sachen zu sperren.

Autor:
Zwar vertreten bisher nur wenige Politiker solche weitergehenden Absichten öffentlich. Aber die Zensur in undemokratischen Staaten wie China zeigt, was technisch machbar ist. Und es gibt durchaus auch in Europa Bestrebungen, den Schattenseiten des Internets mit weiteren Maßnahmen entgegenzutreten. Die öffentliche Zustimmung ist leicht zu gewinnen, wenn man die Debatte am Beispiel Kinderpornografie aufzieht. Vor diesem schillernden Hintergrund verblassen die möglichen negativen Folgen für Meinungsfreiheit und Menschenrechte allzu leicht. Ausgerechnet vor einem Fachgremium im Europarat, der ja für die Menschenrechte in Europa streiten soll, formulierte jüngst der eingangs zitierte Sicherheitsexperte Jewgeni Kaspersky seine Maximalforderungen zum Thema Internetsicherheit:

Cut 25 (Kaspersky):
Introduce Internetregulation!

Übersetzer:
Führt eine Regulierung des Internets ein! Das heißt: Internet-Ausweise, Internet-Identitäten für jeden Nutzer. Akkreditierungen für Organisationen, Firmen und Regierungen, die ins Internet wollen.

Autor:
Seine Position leitet der russische Sicherheitsexperte wohl vor allem aus seinem täglichen Umgang mit Schadsoftware und ihren kriminellen Autoren ab. Die Grundprobleme aber sind in der Natur des Internets angelegt: Anonymität und leichte Verfügbarkeit von Daten hebeln die alten nationalen Gesetzgebungen aus, sei es beim Urheberrecht, beim Jugendschutz oder bei der Strafverfolgung. Und sie senken die Hemmschwelle zu kriminellem Verhalten, dass es mit anderen technischen Mitteln immer schon gegeben hat. Technik ist die Antwort, aber was war die Frage? Die Gesellschaft wird aushandeln müssen, ob der Computer als Ermittler eingesetzt wird, ob Überwachung, Sperrung und Regulierung die Antwort sein sollen, auf die gesellschaftlichen Fragen, die dahinter stehen.

* * * * *