**DEUTSCHLANDFUNK**

Redaktion Hintergrund Kultur / Hörspiel

Redaktion: Ulrike Bajohr

***Dossier***

# Computerforensiker. Ermittler im Cybercrime-Milieu

**Von Michael Reitz**

**Sprecherin: Claudia Mischke**

**Sprecher: Philipp Scheppmann**

Ton und Technik: Hanns Martin Renz und Jutta Stein

Regie: Ulrike Bajohr

Musik:



- unkorrigiertes Exemplar -

Sendung: Freitag, d. 16. März 2010, 19.15 - 20.00 Uhr

*Musik: James –Bond Thema , unter O-Ton bis Ansage (CD James Boin, 30th anniversary limited edition, CD 2/Track 1, Theme, Arch.nr.: 6011402)*

**O-Ton (1) Merkel (mit Atmo von laufenden Computern)** ... haben die Chinesen den Ghostnet- Trojaner, das Kommandozentrum erzeugt. Diese Trojaner sind dann auf diesen Server irgendwo in Russland auf dem PC eines Users abgelegt worden. Das war der erste Schritt. Ich zeige euch beides: wie ihr einfach durchs Klicken auf eine Website infiziert werdet und die Ghostratte übernehmt. Und wie wir ein PDF unterjubeln. Und wenn ihr dann mal seht, was diese Ghostratte kann, dann seht ihr auch die Gefahr dahinter.

**Sprecher: Eine Polizeischule im norddeutschen Eutin, Sitz der Spezialdienststelle „Informationsmanagement“ der schleswig-holsteinischen Polizei. Die besten Ermittler Deutschlands in Sachen Computerkriminalität sitzen zwei Wochen lang jeden Tag zehn bis zwölf Stunden in einer Fortbildung. Geleitet wird sie vom ehemaligen Kampfjetpiloten Hans-Peter Merkel, renommierter Spezialist für Straftaten im EDV- und Informationstechnologiebereich. Nur auf sein Zeichen hin dürfen wir den Recorder einschalten. Denn simuliert werden Konstruktion, Verfahrensweise und Abwehr eines der gefährlichsten Virenprogramme, Ghostnet oder auch Ghostratte genannt. Hans-Peter Merkel ist Computerforensiker**

**Sprecherin: – ein relativ junger Berufszweig mit bisher wenigen Experten. Doch das muss sich ändern.**

*Musik weg.*

**ANSAGE:**

**Computerforensiker. Ermittler im Cybercrime-Milieu. Ein Feature von Michael Reitz**

**Sprecher: In rasantem Tempo haben sich die Informationstechnologien in unserem Alltagsleben etabliert, keine technische Revolution hat die Kommunikationsprozesse so stark verändert wie die digitale.**

*Sprecherin tippt auf Tastatur*

**Sprecherin: Onlinebanking, Einkaufen übers Internet, Speichern großer Datenmengen in Firmennetzwerken oder Chatrooms**

**Sprecher: – fast täglich geben wir mehr von uns preis, als uns lieb sein kann. Denn mit dem Cyberspace ist eine neue Art von Kriminalität entstanden, die als Werkzeug das handhabt, was sie attackiert:**

**Sprecherin:**

**einen internetfähigen Computer. Längst nutzen auch Unternehmen und Regierungen diese Möglichkeit der Spionage.**

*Sprecherin Tippen weg*

**Sprecher:**

**Cybercrime, das Verbrechen im schier unendlichen Raum der internationalen Datenwelt, hat in den letzten Jahren auf allen Ebenen rapide zugenommen.**

*Musik Kraftwerk, CD Computerwelt, Track 3(Nummern), Arch.nr.: 6102002/5*
*ab Anfang bis 1`20, unter folg. Text*

**Sprecherin: Frühsommer 2007. Das Computernetz der estnischen Regierung ist vierzehn Tage vollkommen außer Gefecht, Ursache und Urheber bis heute unbekannt.**

**Sprecher: Sommer 2007: Rechner einiger bundesdeutscher Behörden und Ministerien sind mit einem neuartigen Virus infiziert. Zugang hat er sich wahrscheinlich über eine verseuchte Mail der Weltgesundheitsorganisation verschafft. Die Spur führt zu einem Stützpunkt der chinesischen Volksbefreiungsarmee**

**Sprecherin: – was jedoch nicht heißt, dass die Pekinger Regierung davon weiß.**

**Herbst 2009. In Spanien sind ohne Wissen der Besitzer massenhaft kleinere Beträge von Kreditkarten abgebucht worden. Der Schaden beträgt mehrere Millionen Euro.**

*(Musik unter folg. Sprecher mit O-Ton 2 verblenden)*

**Sprecher: Februar 2010: Aus Protest gegen die zunehmende Internet-Zensur der australischen Regierung legt die internationale Hacker-Organisation „Anonymouse“ für einen Tag zahlreiche Computersysteme australischer Ministerien lahm, indem sie deren Websites mit bis zu sieben Millionen Aufrufen pro Sekunde bombardiert.**

**O-Ton (2) Anonymouse-Botschaft:** Hello, this is Anonymouse (...) we do not forget, expect us.

**Sprecher: Das Bundeskriminalamt schätzt, dass jeder fünfte Fall von Wirtschaftsverbrechen mittlerweile über das Web begangen wird – im Vergleich zum Jahr 2007 eine Steigerung von siebzig Prozent. Computer sind anfällig gegen ungebetene Besucher: die herkömmlichen, den meisten Nutzern bekannten Programme weisen zwischen fünfzehn und fünfzigtausend Schwachstellen auf,**

**über die Eindringlinge – sogenannte Hacker – Zugang zu einem fremden Rechner erlangen können.**

**Sprecherin: Eine Unterscheidung ist dabei sehr wichtig: neben kriminellen Hackern, die das Netz für Straftaten missbrauchen,**

**Sprecher: existieren auch die ethischen Hacker,**

*(evt. wdh. Anonymouse, O-Ton 2)*

**die sich schon mal in Behördencomputer einklinken, um zu demonstrieren, wie ungesichert unsere persönlichen Daten sind.**

**Sprecherin: Auch Konzerne und Regierungen könnten sich grundsätzlich der Hilfe krimineller Hacker bedienen – ein Umstand, dem das Bundesverfassungsgericht 2008 mit einem Urteil Rechnung trug: es erweitert das Grundrecht auf die Unverletzlichkeit der Wohnung um den Bereich des Schutzes der informationellen Systeme – also auch von PCs.**

**Sprecher: Computerforensiker wie Hans-Peter Merkel haben es ausschließlich mit den Kriminellen zu tun.**

**O-Ton (3) Merkel:** Ich bin zweigleisig tätig, einmal im Bereich der Schulung und einmal im Bereich der Unterstützung bei Großeinsätzen . Im Rahmen der Ausbildung bin ich in ganz Deutschland tätig, zu den Ausbildungseinrichtungen, für die ich arbeite, gehören normale

Polizeischulen, Landeskriminalamt, Bundeskriminalamt, die Geheimdienste in Deutschland und NATO und andere Dienststellen, über die ich an der Stelle nicht sprechen möchte. Wenn wir hier Vorführungen machen wie die, die Sie grad eben gesehen haben, dann machen wir das mit Sicherheit nicht, um die Strafverfolger zu trainieren, solche Sachen in den Umlauf zu bringen, sondern wir müssen das als Eye-Opener zeigen, um den Strafverfolgungsbehörden einfach mal ne Idee zu geben, wie ein Hacker, Cracker arbeitet.

**Sprecher: Hans-Peter Merkel gehört zu den Top Ten der Computerforensiker in Deutschland. Eine Ausbildung mit anerkanntem Abschluss gibt es für diesen jungen Berufszweig noch nicht.**

**Sprecherin: – obwohl das notwendige Know-how enorm ist: genaue Kenntnis aller Betriebssysteme, Anwenderprogramme und Programmiersprachen; Computertechnik und EDV-Strafrecht zählen ebenso dazu wie das Schreiben von Hacker-Programmen.**

**Sprecher: Neben Freiberuflern wie Hans-Peter Merkel sind einige wenige Datenforensiker in der freien Wirtschaft angestellt. Polizei und Geheimdienste beschäftigen die meisten.**

*Sprecher tippt schnell*

**Sprecherin: Digitale Ermittler gegen kriminelle Aktionen im Web: Datenklau bei Online-Banking, Industriespionage per Computer, Kinderpornographie, Internet-Betrug jeglicher Art.**

**O-Ton (4) Merkel:** Jeden Tag kommen neue Ideen. Ganz übles Geschäftsmodell ist derzeit die Abo-Abzocke. Im Kleingedruckten steht dann oftmals, dass Sie einen Abo-Vertrag von 59 Euro irgendwas eingehen. Sie erhalten juristische Drohgebärden, wo drinsteht, dass Sie gefälligst zu bezahlen haben. Das ist Drohgebärde, es ist noch keine einzige Person zur Kasse gebeten worden.

**Sprecher: Computerforensiker sorgen dafür, dass gefundene Hinweise auch vor Gericht verwertbar sind. Denn anders als bei einem Autodiebstahl reicht es eben nicht, die Straftat aufzunehmen und dann nach dem Täter zu suchen. Digitale Ermittler müssen das Delikt genau genommen noch einmal begehen, damit sie den Weg der strafbaren Handlung dokumentieren können. Jeder Ermittlungsschritt wird auf gesonderten Speichermedien gesichert**

**Sprecherin: Eine Aufgabe, die hohen Einsatz erfordert. Zeugen können nicht befragt, Fingerabdrücke, Speichelspuren oder**

**Blutgruppen nicht festgehalten werden. Anders als bei herkömmlichen Straftaten gibt es für die Beamten keine Ermittlungsroutine, kein generalisiertes Schema, nach dem gehandelt werden kann.**

*Musik: James –Bond Thema , unter O-Ton bis Ansage (CD James Boin, 30th anniversary limited edition, CD 2/Track 1, Theme, Arch.nr.: 6011402) ab 40" als* ***Zäsur***

**Sprecher: Computerforensiker arbeiten rund um die Uhr. Ohne eine ausgeprägte Einzelkämpfer- und Tüftler-Mentalität ist dieser Beruf undenkbar.**

**Sprecherin: Der Bedarf an Fort- und Ausbildungsmaßnahmen für Computerforensik ist immens. Nur circa eintausend Datenermittler arbeiten bei den Strafverfolgungsbehörden, die Landeskriminalämter fordern mindestens weitere viertausend.**

**Sprecher: Sieht man sich das Arbeitsfeld der digitalen Ermittler genauer an, so springen drei Problemfelder ins Auge.**

*Musik Kraftwerk, CD Computerwelt, Track 3(Nummern), Arch.nr.: 6102002/5 ab 1`20*

**Sprecherin: Herkömmliche Kriminalität wie Diebstahl, Betrug, Unterschlagung, wobei private PCs und Internetverbindungen die Tatwaffen sind.**

**Sprecher: Zwischenstaatliche Spionage mit dem Ziel, die Wirtschafts- oder Militärmacht einer anderen Nation zu schwächen. Und schließlich:**

**Sprecherin: Wirtschafts- und Industriestraftaten.**

*Musik weg*

**O-Ton (5) Stoppelkamp:** Wir haben in der deutschen Wirtschaft die Situation, dass eigentlich nur in den größeren Unternehmen, insbesondere in den börsennotierten Unternehmen, Sicherheitsabteilungen bestehen, die sich um das Thema Informations- und Datenschutz kümmern.

**Sprecherin: Bertold Stoppelkamp ist Geschäftsführer der Arbeitsgemeinschaft für Sicherheit der Wirtschaft und versucht seit Jahren, die deutschen Unternehmen für das Thema Cyber-Kriminalität zu sensibilisieren. Ihren Schätzungen zufolge liegt das Gefährdungspotential, der jährlich durch Industriespionage zu erwartende Schaden, bei ungefähr zwanzig Milliarden Euro.**

**O-Ton (6) Stoppelkamp:** Erst mal sollte man natürlich klar definieren, welche Daten als Betriebsgeheimnisse, als sogenannte Kronjuwelen einzustufen sind, wo in einer zweiten Stufe dann genau geregelt werden muss, wer hat Zugang zu diesen Daten und wie darf mit diesen Daten umgegangen werden. Und drittens, und das ist der ganz

entscheidende Aspekt, ständige Sensibilisierung der Mitarbeiter durch Schulungen.

**Sprecherin: Denn in der Wirtschafts- und Industriespionage, so Bertold Stoppelkamp, verlassen sich Spitzel und Späher nicht allein auf die technischen Möglichkeiten des Hackens, um an wichtige Passwörter oder Zugangscodes zu kommen.**

*Musik Kraftwerk, CD Computerwelt, Track 6, Arch.nr.: 6102002/5*
***ab Anfang 5 Sekunden als Zäsur**, evt. wdh.*

**Oft werden gezielt Personen beobachtet und begleitet, zum Beispiel auf Dienstreisen.**

**O-Ton (7) Stoppelkamp:** Also Sie können eine Kommunikation über ein verschlüsseltes Handy führen, dann haben Sie eine technische Sicherheit, aber wenn Sie das Telefongespräch führen und fünf Leute stehen um sie herum, oder Sie sitzen im Intercity und diese Leute hören Ihr Gespräch, dann können Sie zehnmal mit einer verschlüsselten Kommunikationstechnik kommunizieren. Denn das wird nichts bringen. Gar nicht mal, dass die Mitarbeiter das mit der Absicht gemacht haben, den Arbeitgeber, das Unternehmen zu schädigen. Aber es ist vielfach eine Unbedarftheit, ein laxer Umgang mit diesen Dingen und deshalb ist es sehr, sehr wichtig die Mitarbeiter zu sensibilisieren.

*Musik: James –Bond Thema , unter O-Ton bis Ansage (CD James Boin, 30th anniversary limited edition, CD 2/Track 1, Theme, Arch.nr.: 6011402) ab 40" als* ***Zäsur***

**Sprecher: Der Grund für Wirtschaftsspionage zwischen einheimischen Firmen ist in den seltensten Fällen Produktpiraterie**

**Sprecherin: - also der Versuch, dem Konkurrenten Ideen für ein Auto, eine Maschine oder ein neues Stoffmuster zu stehlen. Viel eher geht darum, Verkaufs-, Werbe- und Personalstrategien des ausspionierten Unternehmens zu unterwandern,**

**Sprecher: beispielsweise herauszubekommen, wie die Gehaltsstruktur in der Entwicklungsabteilung des Wettbewerbers beschaffen ist, um dort gezielt Personal abziehen zu können.**

**Sprecherin: Dies zu verhindern bedarf es solcher Fachleute wie Alexander Geschonneck. Er leitet bei der KPMG, einem der größten internationalen Wirtschaftsprüfungs- und Beratungsunternehmen, ein Team von Computerforensikern.**

**O-Ton (8) Geschonneck:** Wenn jemand über ihre Webpräsenz in ihr Unternehmen eindringt oder über andere Kanäle und dort versucht, Daten zu stehlen oder zu manipulieren, dann sind unsere Kollegen gefragt, das zu erkennen, zu bestätigen und wenn möglich

aufzuklären. Anderer Fall wär beispielsweise, wenn ein Mitarbeiter aus der Entwicklungsabteilung Daten unberechtigt an den Wettbewerber verschickt oder ins Ausland, dann kommen wir auch in das Unternehmen und schauen uns an, was ist dort passiert, können wir das nachweisen und können wir eine Empfehlung aussprechen, das zu verhindern. Oder ein anderer Fall wäre, wenn jemand Bilanzzahlen manipuliert.

**Sprecher: Bei herkömmlichen Einbrüchen, zum Beispiel in eine Wohnung oder ein Haus, erkennt selbst der Laie sofort, dass etwas nicht stimmt und alarmiert die Polizei. Computerstraftäter sind jedoch nicht nur in der Ausführung, sondern auch im Verschleiern ihrer Taten sehr geschickt.**

**Sprecherin: Oft fällt erst nach Tagen oder Wochen auf, dass ein Rechner gehackt und seine Festplatte kopiert wurde.**

**O-Ton (9) Geschonneck:** Und da komme ich (...) zu dem Punkt der Anomalieerkennung. Wir wissen wie ein Computer oder ein IT-System im Normalfall aussieht, wir müssen versuchen zu identifizieren, was könnte dort an dem Rechner passiert sein, welche Lücke wurde ausgenutzt. Und das zu bewerten bedarf einer gewissen Kenntnis auch der Möglichkeiten, die ein Angreifer zur Verfügung hat.

**O-Ton (10) Anonymouse (verzerrte Computeranimation):** We have been watching you ....

**Sprecherin: Alexander Geschonneck wird meist dann angefordert, wenn ein Angriff von außerhalb des Unternehmens stattgefunden hat – so beispielsweise, wenn Schadcodes eingeschleust wurden, die eine sogenannte Denial of Service-Attacke starten:**

**O-Ton (10) Anonymouse (verzerrte Computeranimation):** We have been watching you ....

**Sprecher: bei einer aufgerufenen Website erscheint die Meldung, dass diese Seite nicht besucht werden kann. Oft dauert eine solche Blockade tagelang.**

**Sprecherin: Doch auch innerhalb einer Firma geschehen Straftaten am Computer: Arbeitszeitbetrug oder Weitergabe von Betriebsgeheimnissen,**

**Sprecher: zum Beispiel bei einem Arbeitsplatzwechsel.**

**Sprecherin: Computerforensiker gehen dabei ausgesprochen vorsichtig ans Werk. Sie überwachen nicht die Beschäftigten**

**eines Betriebes, oder dringen in ihre Privatsphäre ein, sondern sie verfolgen lediglich Auffälligkeiten in den Netzwerken eines Unternehmens.**

*Musik: James –Bond Thema , unter O-Ton bis Ansage (CD James Boin, 30th anniversary limited edition, CD 2/Track 1, Theme, Arch.nr.: 6011402) ab 40" als* ***Zäsur***

**Atmo:** *Bei Kroll Ontrack; Schritte, Stimmen im Hintergrund, Geräusche aus Reinraum, in dem Computer untersucht werden (unter folg. Sprecherin weg)*

**Sprecherin: Spezialist in der Bekämpfung dieser Art von Cybercrime ist das US-Datenrettungslabor Kroll Ontrack, mit der deutschen Niederlassung in Böblingen. Reinhold Kern ist dort Leiter der computerforensischen Abteilung. Er beschreibt, was zu tun ist, wenn im Betrieb ein Anfangsverdacht besteht.**

**O-Ton (11) Kern:** Das erste wäre, möglichst nicht mehr weiterzuarbeiten am Computer, sondern den intern beschlagnahmen. Nicht an den Originaldaten arbeiten, mit dem Einschalten oder Ausschalten des Computers werden schon Daten verändert. Und das will man vermeiden, indem man zuerst eine forensische Kopie erstellt. Wir bauen dann die Festplatte wirklich aus, dass man möglichst früh nach dem Erkennen eines solchen Vorfalls rangeht, so dass nicht die Daten, die Hinweise geben könnten, gelöscht werden oder vielleicht sogar so gelöscht werden, dass sie nicht wiederherstellbar sind.

**Sprecher: Viele Unternehmen scheuen aus Imagegründen den Gang zum Staatsanwalt.**

**Sprecherin: Wer will schon gerne zugeben, dass in den eigenen Betriebsräumen Datendiebstahl möglich ist und damit potentielle Kunden verschrecken.**

**Sprecher: Sollte eine Firma jedoch an einer weiteren Strafverfolgung interessiert sein, ist es Ziel der Computerforensiker, die gefundenen Beweise zu sichern und gerichtsfest aufzuarbeiten. Um den Verdacht zu vermeiden, an den sichergestellten Spuren nachträglich manipuliert zu haben, wird ein digitaler Fingerabdruck erstellt,**

**Sprecherin: der sogenannte Hash-Code. Er wird gebildet durch ein kompliziertes mathematisches Verfahren, das man sich als Quersumme der vorhandenen Datenmengen vorstellen kann.**

**O-Ton (12) Kern:** Diese Quersumme ist ein 24-stellige Zahl mit Buchstaben und Zahlen. Selbst wenn an diesen Daten im Nachhinein nur ein einzelnes Bit verändert würde, also ein Punkt auf einer Seite würde diese Quersumme nicht mehr übereinstimmen mit der originalen . Wir erstellen diese Kopie, nehmen diese Kopie mit in

einem versiegelten Umschlag, so spezielle Tüten, Beweistüten, wie sie auch bei den Strafverfolgungsbehörden verwendet werden, inklusive des Protokolls und erstellen eine zweite Kopie bei uns im Labor. Die erste Kopie wird wieder in den Safe gelegt mit dem Protokoll , die heben wird für zwei Jahre auf, kostenfrei für unsere Auftraggeber.

*ev. Musik Kraftwerk, CD Computerwelt, Track 6 Arch.nr.: 6102002/5*

**Sprecher: Der Nachweis für betriebsinternen Datenklau ist oft schwer zu führen. Der Computerforensiker kann zwar mittels seiner Spezialsoftware sehen, dass bestimmte Dateien angefasst wurden. Doch ob sie kopiert worden sind, lässt sich durch die bloße Festplattenbetrachtung nicht definitiv sagen. Dieser Beweis ist nur möglich mit dem Speichermedium, auf das die Datei kopiert wurde**

**Sprecherin: – einem USB-Stick etwa. Dieser hinterlässt über seine Treibersoftware Spuren der digitalen Identifizierung, die der Fahnder erkennen kann.**

**O-Ton (13) Kern:** Ich hab gerade heute früh einen Fall neu hereinbekommen, da hat auch ein Mitarbeiter das Unternehmen verlassen und hat auf seinem Rechner Daten gelöscht. Und zwar sind das (...) Kontaktinformationen zu Kunden, die sonst im ganzen Unternehmen nirgends gespeichert sind. Das Unternehmen weiß jetzt

nicht mehr, welche Kontakte vorhanden waren mit welchen Unternehmen, welche Vertragsregelungen getroffen wurden vorher (..) Das ist ein enormer Schaden für das Unternehmen.

**Sprecherin: Vergleichsweise harmlos ist dagegen der Arbeitszeitbetrug**

**Sprecher: – wenn auch mitunter nicht weniger peinlich für das betroffene Unternehmen.**

**O-Ton (14) Kern:** Das sind Fälle, dass Mitarbeiter einfach zu stark im Internet surfen oder privaten Emailverkehr sehr stark ausdehnen, so dass einfach Stunden pro Tag für private Zwecke drauf gehen. Bevor man eine Kündigung ausspricht oder Abmahnung ausspricht, würde man da sicher versuchen nachzuweisen, wie oft ist es vorgekommen, wie viel Zeit hat er möglicherweise damit verbracht. Einen krassen Fall, den wir hatten, dass ein Mitarbeiter ca. 40.000 pornographische Bilder und Videos auf seinem Computer hatte. Das können Sie nicht bei einer oder zwei Sitzungen im Internet runterladen.

*Sprecherin **und** Sprecher tippen, ad libitum )*

**Sprecher: Knapp 170.000 Computerstraftaten wurden im Jahr 2008 aktenkundig, Folge: das Misstrauen unter den Beteiligten steigt.**

**Sprecherin: Kann man beispielsweise noch auf eine Bank zählen, der es nicht auffällt, dass ein Mitarbeiter über Jahre hinweg kleine Beträge von Kundenkonten auf sein eigenes Konto transferiert hat?**

**Sprecher: Den Computerforensikern wird auch in Zukunft die Arbeit nicht zu knapp werden.**

*Tastaturgeklapper weg*

**O-Ton (15) Kern:** Die meisten sind natürlich bei den Strafverfolgungsbehörden (...) ich würde mal schätzen, dass wir in Deutschland ca. 1000 haben. In der privaten Wirtschaft sind es weniger. Das kostet wirklich viel Geld, sich die Hardware anzuschaffen, sich die Software anzuschaffen. So eine Lizenz für einen Teil der Software liegt bei 3000 Dollar, eine Lizenz, die nur auf einem Computer läuft. Und wenn Sie dann mehrere brauchen, dann müssen Sie neue Lizenzen kaufen, Sie müssen Schulungen besuchen. So eine Schulung kostet pro Woche runde 4000 Euro. Das kann sich ein kleineres Unternehmen einfach nicht leisten.

*Musik: James –Bond Thema , unter O-Ton bis Ansage (CD James Boin, 30th anniversary limited edition, CD 2/Track 1, Theme, Arch.nr.: 6011402) ab 40" als* ***Zäsur***

**Sprecherin: Während in Großbritannien und den USA große Summen in die Computerforensik investiert werden,**

**Sprecher: beginnt in Deutschland erstmals im Wintersemester 2010 an der Fachhochschule Albstadt-Sigmaringen ein Studiengang „Forensik in der Informationstechnologie“. Einer der Initiatoren dieses Projekts ist der Mannheimer Informatikprofessor Felix Freiling. Denn die Polizeibehörden suchen dringend Kriminalisten, die sich mit dem Bereich Cybercrime wissenschaftlich befasst haben.**

**O-Ton (16) Freiling:** Das sieht man auch allein daran, dass die immer noch rekrutieren in dem Bereich, und dass es erfahrungsgemäß auch schwierig ist, entsprechende Leute zu rekrutieren, die entsprechenden Sachverstand haben und auch zu den Polizeigehältern dann auch arbeiten wollen (...) Aber generell ist mein Eindruck, dass sowohl das BKA als auch die LKAs, mit denen ich Kontakt habe, auf oberstem Niveau arbeiten in diesem Bereich (...) dass sie sich auch bewusst sind, trotz ihres hohen Niveaus, dass sie sich weiterentwickeln müssen.

**Sprecher: Noch sind die ermittelnden Behörden sehr stark auf Beamte angewiesen, die sich aus eigenem Antrieb, in ihrer**

**Freizeit, umfangreiches Hackerwissen aneignen, es in polizeiinternen Fortbildungen weitergeben und für die der Achtstundentag nicht existiert.**
**Die zeitaufwendigen Verfolgung von Straftätern, die die mittels Rechner agieren, wird mehr und mehr zur notwendigen Routine.**

**Sprecherin: Dabei sind die Tatmotive so alt wie die Menschheit –**

**Sprecher: aber die Ermittler treffen nicht nur auf altbekannte Delikte, sondern auch auf solche, die das Netz erst hervorgebracht hat.**

*Musik Kraftwerk, CD Computerwelt, Track 3(Nummern), Arch.nr.: 6102002/5*
*ab 2`20 bis max. 2`50, notfalls doppeln (Unter Sprecher)*

**Sprecherin: Phishing. Abfangen vertraulicher Kontendaten aus dem Internet-Banking.**

**Sprecher: Phonefreaking. Einhacken in die Internet-Telefonie, um so auf fremde Rechnung telefonieren zu können.**

**Sprecherin: Spammailing. Massenhaftes Versenden von Werbe-Emails um so den Server des jeweiligen Providers lahmzulegen.**

**Sprecher: Trojaner-Angriff. Einschleusen eines Spähprogramms oder Virus, um so den attackierten Rechner ohne Wissen des tatsächlichen Besitzers zu benutzen.**

**Sprecherin: Keylogging. Das ist Hard- oder Software, die die Eingaben eines fremden Computers mitprotokolliert. Zweck: Ausspähen von Passwörtern oder PIN-Nummern.**

*Musik weg*

**O-Ton (17) Merkel:**

Es ist im Bereich Hacken nicht mehr so, dass ein Spaßfaktor verbunden ist wie das früher war, beim Opfer das CD-Rom Laufwerk zu öffnen, oder den Bildschirm zu drehen, solche albernen Dinge. Sondern 60 Prozent der forensischen Auswertearbeit hat mit Auswertung von kinderpornographischem Material zu tun.

Also Bildersuche auf Computern, Dateisuche auf Computern gehört zum täglichen Brot, ist auch keine allzu schwierige Aufgabe in der Regel für den Forensiker, nur hat sich das Szenario durch die Bedrohung Internet in den letzten Jahren natürlich massiv geändert.

**Sprecherin: Mit der Kriminalität im Netz lässt sich viel Geld verdienen. Zumal ein großer Teil der Computernutzer nach wie vor sehr leichtsinnig mit persönlichen Daten umgeht und auch nicht weiß, dass etwa die Weitergabe der eigenen Handynummer an unbekannte Dritte zu kriminellen Handlungen führen kann.**

**Sprecher: Hans-Peter Merkel nennt einen Fall aus dem Jahr 2009, an dem er als beratender Ermittler beteiligt war.**

**O-Ton (18) Merkel:** Vor Gericht stehen vier Geschäftsführer von Unternehmen, die SMS-Betrug durchführen, das heißt, die haben Premium-Nummern angemietet von Telefonprovidern und bieten SMS-Chats an, jede SMS gaukelt vor, dass man den Traumpartner seines Lebens findet und jede SMS wird mit 1, 99 Euro abgerechnet. Die Beschuldigung läuft derzeit auf einen Streitwert von 46 Millionen Euro und 700.000 Geschädigten. Es wird angeboten, den Traumpartner des Lebens zu finden, es werden immer wieder Angebote zu einem Meeting gemacht (...) wenn der Geschädigte oder die Geschädigte dann sagen, schick mir deine Telefonnummer, dann behauptet der Animateur, bei mir

sind nur Sternchen und Fragezeichen angekommen, der Computer hat die Nummer verfälscht und verschliffen, so dass man sie nicht lesen kann. Wenn wir in diese Chat-Datenbanken gehen, in die Protokolle, sehen wir, dass das alles nicht stimmt, weil wir über 90 Millionen Chats reproduziert haben, den Verlauf dann ordentlich dargestellt, mit dem Beweis, dass diese Aussage gar nicht zutrifft.

*Musik: James –Bond Thema , unter O-Ton bis Ansage (CD James Boin, 30th anniversary limited edition, CD 2/Track 1, Theme, Arch.nr.: 6011402) ab 40" als* ***Zäsur***

**Sprecher: In Vor-Computerzeiten war es aufwendig und gefährlich, sich kriminelles Wissen anzueignen. Es gab keine Lehrbücher darüber, wie man in ein Haus einbricht, ein Auto knackt oder einen cleveren Betrug einfädelt. Heute sind diese Kenntnisse im Netz zu haben. Besonders zu schaffen macht den Ermittlern eine Entwicklung, die seit Beginn des 21sten Jahrhunderts unter dem Namen „Botnet" bekannt ist.**

**Sprecherin: Was das ist, erklärt Informatikprofessor Felix Freiling.**

**O-Ton (19) Freiling:** Bot kommt von Robot und bezeichnet einfach ein Programm, was automatisiert irgendetwas macht. Und früher war das so, dass diese Bots in den sogenannten Chatrooms oder in den Chatkanälen benutzt wurden, um zum Beispiel Anrufbeantwortung zu machen, das waren einfach Roboter oder Programme, die im Chatkanal mitgehört haben und die gesagt haben, wenn jemand angesprochen

wurde, der ist grad nicht da. (..) Ein Bot bezeichnet man heute als ein Programm, was automatisiert irgendwelche Aktivitäten macht und von Externen ferngesteuert oder programmiert werden kann.

**Sprecherin: Also: ein sogenannter Kommandoserver, der zentrale Computer eines Botnetzes mit Standort, sagen wir, Wanne-Eickel, aktiviert per Mausklick den digitalen Supergau und**

**O-Ton (2) Anonymouse-Botschaft:** (...) we do not forget, expect us.

**Sprecher: fünfzig- bis hunderttausend gekaperte Rechner überall auf der Welt greifen entweder ein einziges Computernetzwerk an – wie im Fall der australischen Parlamentsrechner – oder führen gezielt breit gestreute Aktionen durch. Welche Dimensionen das mittlerweile angenommen hat, beschreibt Alexander Geschonneck.**

**O-Ton (20) Geschonneck:** Man kann so ein Botnetz für wenige 100 Dollar die Stunde mieten. Sie können Know-how anmieten, das Ihnen jemand so ein Angriffstool so bastelt (...) und weil es so zugeschnitten ist, wird es von einem klassischen Virenscanner nicht erkannt, bis hin zu der Tatsache, dass es Websites gibt und Kontaktmöglichkeiten, wo sie Zugriffsmöglichkeiten haben auf Botnetze und dort einfach Rechenleistung mieten, und dem Betreiber oder dem Eigentümer des Botnetzes mitteilen, was diese hunderttausend Rechner alles machen

sollen und dann wird der Befehl in Auftrag gegeben und dann führen diese Rechner diesen Auftrag aus: eine Stunde lang Spammails verschicken oder eine Stunde lang eine gewisse Website mit Verbindungsanfragen überlasten oder eine Stunde lang nach Seriennummern von kommerzieller Software suchen oder nach Kreditkartendaten.

**Sprecher: Bei dieser Spielart von Netzkriminalität herrscht eine klare Arbeitsteilung. Der Vertrieb der Dienstleistung „feindliche Übernahme fremder Computer“ wird ebenso professionell organisiert wie das Anwerben neuer Kunden und die ausreichende Verfügbarkeit gehackter Rechner.**

**Sprecherin: Zum Service gehören auch Kundenzufriedenheitserhebungen und korrekte Abrechnung.**

**O-Ton (21) Geschonneck:** Es ist nicht so, dass diese Kontaktmöglichkeiten überall offen rumliegen. Sie müssen schon gewisse Kanäle nutzen, aber mit etwas Know-how sind Sie relativ schnell an den Kontaktpersonen dran, die können Sie über die einschlägigen Chatchannel, Foren oder Webseiten natürlich kontaktieren. Die Schwierigkeit, die im Rahmen einer Ermittlung zu fangen oder einer Strafe zuzuführen oder das Botnetz abzuschalten, liegt in der Regel darin, dass die Betreiber irgendwo im Ausland sitzen,

ihre Identität über mehrere Schritte verschleiern und die Bezahlung erfolgt in der Regel auch über anonyme Bezahldienste und das macht es nicht einfach, diese Personen zu identifizieren, die dahinter stecken.

*Musik: James –Bond Thema , unter O-Ton bis Ansage (CD James Boin, 30th anniversary limited edition, CD 2/Track 1, Theme, Arch.nr.: 6011402) ab 40" als* ***Zäsur***

**Sprecherin: Doch nicht nur die individuelle Netzkriminalität gedeiht. Der Verdacht liegt nahe, dass auch Regierungen Botnetze und Hackerwissen nutzen, um Websites von Oppositionellen und Nichtregierungsorganisationen außer Kraft zu setzen oder zwischenstaatlich Spionage zu betreiben.**

**Sprecher: Die Herrschaft über Daten ist mittlerweile fast genauso wichtig wie die Kontrolle von Erdölreserven. Cyberkriminelle bilden dabei eine Art fünfter Kolonne staatlicher Behörden, die mit psychologischer Kriegsführung oder Wirtschaftsspionage natürlich nicht offiziell in Verbindung gebracht werden wollen.**

*Musik Kraftwerk, CD Computerwelt, Track 3(Nummern), Arch.nr.: 6102002/5*
***ab 2`52 bis Ende, evtl. Anfang Track 4***

**Sprecher: Sommer 2008. Russland und Georgien befinden sich im Krieg. Wie sich Monate später herausstellt, hat ein riesiges Botnetz unbekannter Herkunft die georgischen Regierungs- und**

**Militärcomputer bereits zwei Wochen vor dem Überfall dauerhaft funktionsunfähig gemacht.**

**Sprecherin: Mit einem Schadprogramm, dem amerikanische Sicherheitsexperten den Namen „Titan Rain“ geben, dringen kriminelle Hacker in die Rechnersysteme von US-Rüstungskonzernen ein,**

**Sprecher: Anfang 2009 werden so die Baupläne des neuen Kampfjets „Lightning II“ gestohlen.**
**Im selben Jahr wird der Internet-Konzern Google von einem Virus heimgesucht, der den Namen „Trojan Point Hydraq“ erhält. Ziel: das Abfischen von Verteileradressen und Mailverkehr politischer Aktivisten in China.**

**Sprecherin: Und schließlich das Ghostnet, das Ende 2008 enttarnt wird. Unbekannten Hackern war es gelungen, über zwölfhundert Rechner auf der ganzen Welt zu verbinden und damit nicht nur den Computer des Dalai Lama zu attackieren, sondern auch die Kommunikationssysteme von Ministerien fast aller westlicher Staaten.**
*Musik weg*

**Sprecher: Man weiß zwar immer noch nicht, wer oder was die Angreifer waren. Aber wo das Ghostnet geknüpft wurde, scheint mittlerweile geklärt: auf der chinesischen Insel Hainan.**

**O-Ton (22) Stoppelkamp:** China, das sich hohe Ziele gesetzt hat die führende Wirtschaftsnation in der Welt zu werden und dort entsprechende Pläne umsetzt, die eben beinhalten, dass man sich praktisch Informationen in sogenannten Schlüsselbranchen beschafft, dass man eben dann dort entsprechend versucht, alle Informationen zu sammeln.

**Sprecherin: Bertold Stoppelkamp, Geschäftsführer der Arbeitsgemeinschaft für Sicherheit der Wirtschaft.**

**O-Ton (23) Stoppelkamp:** Das kann durchaus sein, dass zu 80% die Sammlung der Information über öffentlich zugängliche Quellen erfolgt, und dann geht's eben darum, inwieweit man dann praktisch die Schwelle zur illegalen Informationsbeschaffung überschreitet seitens der ausländischen Nachrichtendienste.

**Sprecher: Auch wenn die Spurensuche der Computerforensiker direkt zu einem Server oder einem Rechnernetz in einem bestimmten Land führt, fällt es schwer, diesem Staat eine direkte Beteiligung an cyberkriminellen Aktionen nachzuweisen. Spezialmethoden der Geheimdienste**

**Sprecherin: – Abhörpraktiken, ein nicht bemerkter Einbruch in eine Rüstungsfirma, das Fotografieren von Konstruktionsplänen mit der Minikamera –**

**Sprecher: sind heute nicht mehr nötig. Jeder Laie mit ausreichend hoher krimineller Energie und computertechnischem Wissen kann im Informationszeitalter Späh- und Blockadeaktionen gegen beliebige Ziele durchführen. Buchstäblich alles ist im World Wide Web erhältlich, inklusive Online-Fortbildungen zum Bombenbasteln und Computerlahmlegen.**

**Sprecherin: Hinzu kommt: es existiert international längst kein Einvernehmen darüber, was eigentlich strafbar ist.**

*Musik: James –Bond Thema , unter O-Ton bis Ansage (CD James Boin, 30th anniversary limited edition, CD 2/Track 1, Theme, Arch.nr.: 6011402) ab 40" als* ***Zäsur***

**O-Ton (24) Gehrke:** In rechtlicher Hinsicht ist die Rückverfolgung von entsprechender Spionage nicht ganz einfach, weil es Zugriff auf Daten erfordert, die mitunter in anderen Ländern gespeichert sind.

**Sprecherin: Der Kölner Jurist Marco Gehrcke.**

**O-Ton (25) Gehrcke:** Und diese Zugriffe unterliegen internationalem Recht, das heißt, deutsche Strafverfolgungsbehörden können selbstverständlich nicht in ein anderes Land fahren und dort Ermittlungstätigkeiten durchführen, sondern sie sind dort auf die Zusammenarbeit mit den lokalen Behörden angewiesen, und das

gestaltet sich insbesondere bei Spionagefällen mitunter etwas kompliziert. Es ist erforderlich, dass Rechtshilfeersuchen gestellt werden, die Cybercrime-Konvention des Europarates hat eine gewisse Entspannung herbeigeführt, weil dort Vorschriften enthalten sind, die die Zusammenarbeit verbessern sollen, das betrifft insbesondere die Geschwindigkeit, mit der solche Ersuchen bearbeitet werden, aber nichtsdestotrotz ist es ein sehr formaler und komplizierter Vorgang, der darüber hinaus voraussetzt, dass das Delikt in beiden Ländern strafbar ist, was halt bei vielen Delikten in Internet nicht der Fall ist.

**Sprecherin: Marco Gehrcke ist Direktor des Cybercrime Research Institute in Köln, einer unabhängigen Forschungseinrichtung, deren Fokus auf die rechtliche Problematik der Internetkriminalität gerichtet ist. Der Jurist berät Regierungen darüber, wie sie zwischenstaatliche Vereinbarungen am besten umsetzen.**

**Sprecher: Denn um möglichst viele Staaten auf verbindliche Normen festzulegen, existieren mehrere internationale Initiativen, unter anderem von den Vereinten Nationen.**

*Musik Kraftwerk, CD Computerwelt, Track 7(More fun to compute), Arch.nr.: 6102002/5*
*ab 1`01*

**Und 2001 wurde die Cybercrime Konvention des Europarates ins Leben gerufen, die auch nicht-europäische Staaten unterschreiben können.**

*Musik weg*

**Sprecherin: Mit diesem Instrument wird eine Harmonisierung der Strafrechtsnormen angestrebt. Ähnlich dem Atomwaffensperrvertrag oder der Genfer Konvention stellt dieses Abkommen eine Richtlinie dar, wie mit Cybercrime international verfahren soll. Ergänzend stellte der Europarat 2007 eine Liste von Straftatbeständen zur Kinderpornographie zusammen, zu deren strafrechtlicher Verfolgung sich die Unterzeichner verpflichten.**

*(Musik unter 16 weg)*

**O-Ton (26) Gehrcke:** Die Cybercrime Konvention beinhaltet unter anderem materiell-rechtliche Vorgaben, das heißt die Staaten verpflichten sich mit der Unterzeichnung der Konvention, entsprechende Strafvorschriften in ihrem Gesetz zu schaffen, beispielsweise gegen Kinderpornographie im Internet oder gegen Computerbetrug oder das Eindringen in Computersysteme. Darüber hinaus verpflichten sie sich aber auch, entsprechende strafprozessuale Maßnahmen zu schaffen, die es den Ermittlungsbehörden dann auch ermöglichen, in solchen Fällen dann auch wirklich ermitteln zu können. Und darüber hinaus verpflichten sie sich, Möglichkeiten der internationalen Zusammenarbeit zu schaffen, also was beispielsweise die Einrichtung eines speziellen Kontaktpunktes beinhaltet, der 24 Stunden am Tag und sieben Tage die Woche verfügbar ist.

*Musik Kraftwerk, CD Computerwelt, Track 7(More fun to compute), Arch.nr.: 6102002/5*
***ab Anfang***

**Sprecherin: Bei aller Gefahr, die im Internet durch internationale Spionage oder Wirtschaftskriminalität lauert, ist die Frage angebracht, wieweit der Staat gehen darf, um solche Straftaten von vornherein auszuschließen.**

**Sprecher: Soll er sich des Computerwissens Krimineller bedienen, um sich in die Rechner einer Drogenrings einzuhacken?**

**Sprecherin: Darf er sich selbst strafbar machen, um Schlimmeres zu verhindern? Letztendlich schleust die Polizei ja auch verdeckte Ermittler in Banden ein, die unter Umständen an Delikten beteiligt sein könnten.**

*Musik weg*

**Sprecher: Einer der schärfsten Kritiker solcher Praktiken ist der ehemalige Bundesinnenminister Gerhard Baum. Als Rechtsanwalt setzt er sich heute für die Wahrung der Grund- und Bürgerrechte in Deutschland ein.**

**O-Ton (27) Baum:** Die Verführung ist sehr groß, sich da fachkundigen Rat zu holen von Leuten, die das können und möglicherweise auch illegal machen, die also Schwachstellen kennen, die es ermöglichen, ohne dass man etwas an den Computer physisch anbringt, in den Computer einzudringen. Also, es liegt dann nahe, dass der Staat sagt, jetzt holen wir uns mal einen Menschen, der da einbrechen kann. Also

mal übertragen auf eine frühere, normale kriminelle Situation: wir holen uns einen Einbrecher, der macht uns die Bank auf. Wir nutzen dessen Knowhow, das normalerweise für kriminelle Zwecke eingesetzt wird, für unsere Zwecke. Das ist natürlich auch eine Ermutigung des Täters, nicht wahr. Irgendwo muss die Polizei ja auch den Täter dann belohnen. Man wird nicht diesen Täter einer Strafverfolgung aussetzen wegen anderer Delikte. Das ist eine ganz schwierige Gratwanderung, und sobald es aber in den kriminellen Bereich hineingeht, wird es sehr anrüchig.

*Sprecherin tippt*

**Sprecher: Anrüchig wurde es beispielsweise, als den bundesdeutschen Finanzbehörden Anfang des Jahres 2010 eine CD der besonderen Art angeboten wurde. Sie enthielt Daten von Bürgern, die ihr Geld zum Zweck der Steuerhinterziehung in die Schweiz verfrachtet hatten. Die Sammlung dieser hochbrisanten Daten war ganz offensichtlich illegal zustande gekommen. Trotzdem wurde sie gekauft**

*Tippen weg*

**Sprecherin: - eine Privatperson hätte sich in diesem Falle der Hehlerei schuldig gemacht.**

**O-Ton (28) Baum:** Ich geh davon aus, dass die Kriminalität im Netz sich weiter ausbreiten wird. Das ist ein großes neues Kriminalitätsfeld. Und der Staat muss sich selber in die Lage versetzen, das zu bekämpfen . Er sollte sich hüten, der Verführung zu unterliegen, diesen Sachverstand

sich von außen zu holen, insbesondere zu holen von Leuten, die normalerweise das Recht brechen. Dann sind die Grenzen des Rechtsstaats überschritten. Das heißt, wir schicken ja auch nicht Kriminelle auf die Straße, um Straßenkriminalität zu bekämpfen. Wir brauchen auf den Staat verpflichtete Polizeikräfte, die jetzt auch im Netz das Recht durchsetzen. Das bedeutet also, dass diese Situation in der Ausbildung der Polizei eine große Rolle spielen muss in Zukunft.

*Musik: James –Bond Thema , unter O-Ton bis Ansage (CD James Boin, 30th anniversary limited edition, CD 2/Track 1, Theme, Arch.nr.: 6011402) ab 40" als* ***Zäsur***

**Sprecherin: Die Computerforensiker in Wirtschaft und Strafverfolgungsbehörden setzen bei der Bekämpfung der Cyberkriminalität in erster Linie auf ihre schöpferische Intelligenz. Ihr Ideenreichtum ist mindestens ebenso groß wie der der Gesetzesbrecher. Ein Beispiel hierfür ist die Erfindung des Informatikprofessors Felix Freiling und seiner Kollegen an der Universität Mannheim. Sie hat den Namen Honeypot – Honigtopf.**

**Sprecher: Eine Falle für kriminelle Hacker.**

**O-Ton (29) Freiling:** Ein Honigtopf ist ein Rechner, den man ans Internet ranklemmt, der also am Internet horcht und auch vom Internet erreichbar ist und der also nichts anderes tut als zu warten, bis er angegriffen wird. Das ist wie so eine Art Köder, den man auslegt, und man hofft halt, dass ein Hacker vorbeikommt und sich einhackt, oder das halt irgendwie ne Malware oder `n Wurm sich zufällig diese IP-Adresse

aussucht und versucht da ne Schwachstelle auszunutzen und sich dort einnistet. Und es gibt verschiedene Arten von Honeypots, und die, die wir so im großen Stil einsetzen, die warten einfach, bis da ein Bot anklopft oder ein Trojaner und tun dann so, als wären sie ein ganz verletzliches Opfer. Und der Bot will ja dann eigentlich auch auf diesen Rechner draufkommen, so hat man dann entsprechend die Möglichkeit den runterzuladen, und so machen wir dann die Klappe zu und können dann weiter analysieren.

**Sprecher: Ein Trick also, der den Spieß umdreht:**

**bei dem Versuch, einen harmlosen PC zu kapern,**

*Musik Kraftwerk, CD Computerwelt, Track 7(More fun to compute), Arch.nr.: 6102002/5*
*weiter*

**Sprecherin: lädt der Angreifer unwissentlich seine Daten im Honigtopf ab - und ist anhand dieser Spuren leichter zu identifizieren.**
**Doch gibt es eine wirksame Strategie, einen Angriff abzuwehren, bevor er überhaupt stattgefunden hat?**

**Sprecher: Eine Art Alarmanlage etwa, von außen sichtbar, die einen potentiellen Eindringling abschreckt?**

**(***Musik weg)*

**Alexander Geschonneck von der Wirtschaftsprüfungsgesellschaft KPMG.**

**O-Ton (30) Geschonneck:** Zum einen sollte man seinen Computer immer auf dem aktuellsten Softwarestand halten, dass man die Herstellermaßnahmen, die empfohlen werden zum Absichern des Betriebssystems und der Anwendung auch umsetzt, regelmäßig, täglich am besten. Dass man einen aktuellen Virenscanner hat, eine Firewall und vor allem sich überlegt, welche Software installiert man denn? Die, die man von Wildfremden übers Internet zugeschickt bekommt, die einfach installieren ohne nachzudenken, das ist schon mal ein großes Risiko. Oder auf jede Website klicken oder jede Email öffnen, die einem angeboten wird, auch das kann ein Risiko sein. Mit einer anderen Maßnahme kann man, wenn der Schaden eingetreten ist, die Auswirkungen beschränken, indem man seine wichtigen Daten auf einem Backup speichert, extern, und vor allem, dass man die privaten Daten mit leistungsfähiger Verschlüsslungssoftware gegen unberechtigte Einsicht schützt.

**Sprecher: Computerforensiker empfehlen privaten und kommerziellen Nutzern von PCs und Netzwerken dringend,**

*Sprecher tippt*

**sich auch die Website des Bundesamtes für Sicherheit in der Informationstechnik anzusehen.**

**Hier sind per Mausklick die wesentlichsten Maßnahmen zum Schutz vor Cybercrime abzurufen.**

*Sprecher und Sprecherin tippen*

**Sprecherin: Computerforensiker – vor Jahren noch ein Häuflein einsamer Freaks, das gegen die Übermacht krimineller Hacker ankämpfte und dafür auch noch schlecht bezahlt wurde. Heute verdienen Freiberufler in dieser Sparte nicht selten vierstellige Tagessätze. Informationstechnologie- und Computerforensiker gewinnen zusehends an Boden, Popularität und gesellschaftlichem Ansehen, zumal die Öffentlichkeit immer stärker für Gefahren aus dem Netz sensibilisiert ist.**

**Sprecher: Aber leider auch, weil der Erfindungsreichtum der Cyberkriminellen offenbar niemals endet – und damit auch nicht die Arbeit der digitalen Detektive.**

*Musik: James –Bond Thema , unter O-Ton bis Ansage (CD James Boin, 30th anniversary limited edition, CD 2/Track 1, Theme, Arch.nr.: 6011402)*

**darauf :**

**Absage**

**Computerforensiker. Ermittler im Cybercrime-Milieu.**

**Sie hörten ein Feature von Michael Reitz**

**Es sprachen: Claudia Mischke und Philipp Scheppmann**

**Ton und Technik: Hanns Martin Renz und Jutta Stein**

**Redaktion und Regie: Ulrike Bajohr**

Eine Produktion des Deutschlandfunks 2010