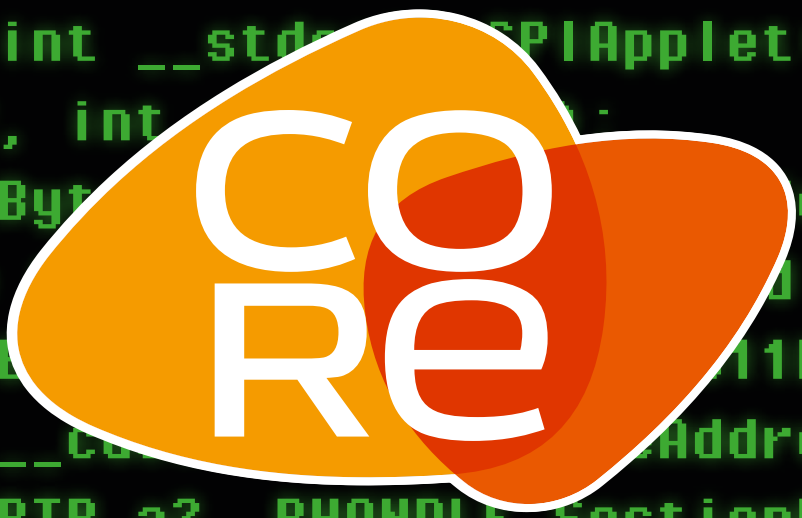
Das Kundenmagazin der Coop Rechtsschutz AG
Ausgabe 4



CYBERCRIME

_Cyberwar: Der lautlose Krieg

_Hacker: Lust auf «Datenreisen»

_Darknet: Surfen am Abgrund

Das Cybercrime-ABC

Darknet

Loser Verbund von Netzwerken, zu denen man in der Regel eingeladen werden muss. Die Daten werden verschlüsselt übertragen, die Nutzer sind anonym, eine Überwachung ist kaum möglich.

Distributed Denial of Service (DDoS)

Angriff auf ein Informationssystem mit einer Vielzahl von Anfragen, um es zu überlasten und lahmzulegen.

Hacker

Personen, die unautorisiert in Computersysteme eindringen. Man unterscheidet zwischen gesetzestreuen White-Hat-Hackern, kriminellen Black-Hat-Hackern und Grey-Hat-Hackern, die sich im Graubereich dazwischen tummeln.

Deep Web

Teil des Internets, der nicht über konventionelle Suchmaschinen auffindbar ist. Man schätzt, dass er rund 500-mal grösser ist als der «sichtbare» Teil des Internets.

Exploit

Systematische Möglichkeit, Schwachstellen einer Programmierung auszunutzen. Unter kriminellen Händlern der Hit im Darknet!

Intrusion Detection System

System, das Angriffe erkennt, die gegen ein Rechnernetz gerichtet sind. Meist eine Ergänzung zu einer Firewall.

Keylogger

Hard- oder Software, um die Eingaben an der Tastatur eines Computers zu protokollieren und damit zu überwachen oder zu rekonstruieren.

Malware

Schädliches Programm, das vom Hacker auf fremden Computern installiert wird, um Informationen abzuzapfen oder Spam-Mails zu verschicken.

Spyware

Schnüffelsoftware, die Daten eines Nutzers ohne dessen Wissen liest, um zu ihm passende Werbung einzublenden.

Virus

Sich selbst verbreitendes Computerprogramm, das sich, angeheftet an Dateien, in andere Computerprogramme einschleust.

Zombie

Computer, der durch Würmer, Viren oder Trojaner von Hackern kontrolliert und ferngesteuert wird. Meist, ohne dass der Benutzer es merkt.

Phishing

Versuch, über gefälschte E-Mails oder Kurznachrichten an persönliche Daten eines Internet-Benutzers zu gelangen («password fishing»).

Trojaner

Als nützliche Anwendung getarntes Computerprogramm, das im Hintergrund ohne Wissen des Anwenders eine andere Funktion erfüllt.

Wurm

Schadprogramm, das sich ohne Datei in Netzwerken oder über USB-Sticks verbreitet.

Editorial

Liebe Leserin, lieber Leser

Wir kaufen online ein und bezahlen per Kreditkarte übers Web. Unsere Geräte sind vernetzt, die Daten liegen irgendwo in einer Cloud: Das Internet ist ein Schlaraffenland für Kriminelle.

Sie schicken uns Spam-Nachrichten per E-Mail und versuchen, Trojaner in unsere Computer einzuschleusen. Hacker sind unsere (un)heimlichen Gäste. Einen 100-prozentigen Schutz vor ihren Angriffen gibt es längst nicht mehr.

<page=2>

Die wachsende Cyber-Kriminalität steigert auch das Bedürfnis nach Sicherheit. Hier sind wir als Rechtsschutzversicherung besonders gefordert. Doch reagieren reicht nicht. Wir müssen handeln, bevor es zum Schaden kommt – indem wir Möglichkeiten aufzeigen, wie Sie sich schützen können beispielsweise.

Wir haben uns für Sie in der Cyberwelt umgesehen und sind dabei auch in Sphären eingetaucht, die weit unter der Spitze des Eisbergs liegen: in die Tiefen des Deep- und Darknets. Das Ergebnis unserer Recherchen finden Sie in diesem Core: eine geballte Ladung Information, verpackt in spannende Reportagen, Hintergrundstorys und berührende Schicksale.

Daniel Siegrist
CEO Coop Rechtsschutz AG

Impressum
Herausgeber: Coop Rechtsschutz AG, Projektleitung: Petra Huser, Sibylle Lanz, Ioannis Martinis, Coop Rechtsschutz AG, Redaktion: Matthias Mächler, www.diemagaziner.ch, Optik/Realisation: Baldinger & Baldinger AG, Aarau, Produktion: Christoph Zurfluh, www.diemagaziner.ch, Druck und Versand: Schwabe Druck, Basel, Auflage: 5000 Exemplare, Erscheint: einmal jährlich, Bestellungen: Coop Rechtsschutz AG, Entfelderstrasse 2, Postfach 2502, CH-5001 Aarau, petra.huser@cooprecht.ch, In dieser Publikation vermittelte Informationen über Dienstleistungen und Produkte stellen kein Angebot im rechtlichen Sinne dar.

Inhalt

<page=3>

<page=4>

CYBERSCHMUTZ

text: Michèle Roten

<page=5>

Foto: Revolvermänner GmbH

Schiesst im Netz schon mal zurück: «Revolvermann» Christian Scherg entwickelt Strategien gegen Cybermobbing.

<page=6>

Sie haben bestimmt schon mal einen schlechten Witz gemacht. Da das aber mit grosser Wahrscheinlichkeit in Gegenwart von Menschen passiert ist, die Sie kennen und Ihnen wohlgesinnt sind, wurde darüber hinweggesehen. Die Tatsache, dass Sie etwas Dummes gesagt haben, lösten sich einfach in Luft auf.

Sie haben bestimmt schon mal etwas Peinliches gemacht und sich daneben benommen. Vielleicht gibt es sogar Beweismaterial: ein Video, wie sie sturzbetrunken Schwanensee tanzen, nur mit einer Unterhose bekleidet, und die war auf ihrem Kopf, aber das liegt sicher in der Kiste im Keller.

> Die digitale Welt kennt kein Pardon. Etwas rückgängig machen, geht nicht.

Sie haben vielleicht auch schon etwas richtig Schlimmes gemacht, aber das ist lange her, und seither führen Sie ein vorbildliches Leben. Und vielleicht findet jemand Sie enorm blöd und hat das an eine Hauswand gesprayt, aber das Graffiti wurde fix wieder übermalt. Die reale Welt ist nachsichtig.

Was raus ist, ist raus

In der digitalen Welt gibt es kein Aber, und der «Löschen»-Button ist eigentlich blanker Hohn. «Wenn etwas raus ist und Aufmerksamkeit gefunden hat, haben Sie keine Chance mehr, etwas rückgängig zu machen», sagt Christian Scherg, der Geschäftsführer der deutschen «Revolvermänner», einer Agentur für Online-Reputationsmanagement. In den meisten Fällen sind deren Auftraggeber grosse Firmen, Parteien und Organisationen, die die digitale Diskussion und Informationsverbreitung über ihre Inhalte oder Produkte im Griff oder zumindest korrekt halten wollen.

Aber auch Privatpersonen gehören zur Klientel, und um dort den Schaden zu begrenzen, sobald sich der Shitstorm zusammenbraut, müssen sich die «Revolvermänner» kreative Lösungen ausdenken. «Vielfach kann man nur moderieren und gegenkommentieren, um die Deutungshoheit über den eigenen Ruf zu behalten», erklärt Scherg. Diesen Aufwand können sich in der Regel nur grosse Konzerne leisten. Auch brauche man starke Kanäle oder Kontakte zu reichweitenstarken Medien – darüber verfügen die meisten Privatpersonen nicht. Scherg: «Für sie gibt es in besonders heiklen Fällen noch die Möglichkeit der persönlichen Veränderung: Ich kann meinen Namen ändern, mein Aussehen, meinen Wohnort und möglichst dafür sorgen, dass ich nicht mehr mit diesem Beitrag assoziiert werde.» Oder aber man verdrängt diese ungewünschte Information mit einer gezielten Flut massgeschneiderter Informationen.

> Am Ende bleibt nichts anderes, als seine Identität zu wechseln.

Nacktbilder gegen Nacktbilder

Ob die Gegenattacke der dänischen Journalistin Emma Holten auch mit einer Agentur wie der von Scherg zustande kam, ist nicht bekannt, aber funktioniert hat sie: Nachdem jemand Nacktfotos von ihr im Internet verbreitet hatte, machte sie, nachdem die Belästigungen nicht abnehmen wollten, einfach weiter damit – allerdings waren die von ihr autorisierten Aufnahmen dezidiert unerotisch und zeigten sie einfach nackt in ganz alltäglichen Situationen wie etwa beim Zähne-

5 Mal gut zu wissen: So tappen Sie nicht in die Mobbing-Falle

1) Weniger ist mehr

Persönliche Daten, Bilder und Videos in den sozialen Netzwerken wie Facebook nicht jedem zugänglich machen. Privatsphäre-Einstellungen regelmässig überprüfen und anpassen.

2) Wählerisch sein

Personen, die man nicht kennt, nicht einfach zu seinen Freunden hinzufügen. Lieber Unbekannte und Störer ignorieren oder sogar blockieren.

3) Nicht provozieren

Sich nicht auf beleidigende Diskussionen auf anderen Seiten oder Profilen einlassen oder zurückbeleidigen.

4) Darüber reden

Mit Eltern, Verwandten, Lehrern sprechen, hilft. Wichtig ist, dass man sich nicht den Mobbern ausliefert, während man allein vor dem Rechner sitzt.

5) Beweise sichern

Wenn doch etwas passiert ist: Ruhe bewahren und Screenshots von den Beleidigungen und Mobbing-Attacken machen. Auch wenn es kein spezifisches Gesetz gegen Cybermobbing gibt, ist es strafbar.

<page=7>

putzen. Es war eine Aktion, mit der sie die Herrschaft über den eigenen Körper und ihre Nacktheit zurückeroberte – und auch ein Lehrstück über Slut Shaming, das «Schlampen-Beschämen», im Internet.

> Manchmal hilft es, so viel offensichtlichen Müll zu posten, bis jedem die Lust vergeht, sich irgendetwas anzusehen.

«Das ist ein ganz probates Mittel, um Informationen zu verwässern», sagt Scherg. «Wenn kompromittierendes Material im Umlauf ist, macht es oft am meisten Sinn, einfach noch mehr vermeintlich spektakuläres Material gezielt zu streuen.» Noch eine Fotomontage mit einem Arm um Putins Schultern, noch ein Ritt auf einem weissen Elefanten, und irgendwann kursiert so viel offensichtlicher Müll, dass jedem die Lust vergeht, sich irgendetwas anzusehen.

<page=8>

Web und Wahrheit

Das sei ja überhaupt das Problem mit Google, erklärt Scherg, dass immer noch viele das Gefühl hätten, was da stehe, sei die Wahrheit, was gelistet werde, hätte etwas mit der Relevanz der Information zu tun. Deshalb ist es für die «Revolvermänner» wichtig, gute Kontakte zu kritischen und investigativen Journalisten zu pflegen – nicht zuletzt aus Selbstschutz – um nicht das Image einer tatsächlich schlechten Sache zu polieren. «Wir legen Mandate nieder, wenn wir merken, dass uns nicht die ganze Wahrheit gesagt wurde.» Also dass die Firma, der Abzockerei vorgeworfen wird, tatsächlich eine Abzockerfirma ist.

Was raus ist, ist raus

Die «Revolvermänner» kümmern sich auch darum, herauszufinden, wer dahintersteckt, wenn es um gezielte Rufschädigung geht. «Wir haben Psychologen und IT-Forensiker, die unter anderem über Sprach- und Textauswertungen Profile erstellen und andere aufwändige Recherchen in Foren und Blogs betreiben, von denen wir wissen, dass sie auch dazu genutzt werden, andere zu diffamieren.» Aber manchmal kann der Täter nicht eruiert werden, dann kommt man auch rechtlich nicht weiter.

Und manchmal sind die Menschen einfach selber schuld, wenn sich die Aufmerksamkeit, die sie so dringend suchen im Internet, plötzlich gegen sie richtet. Man erinnere sich an den Fall von Justine Sacco, die vor ihrem Abflug nach Südafrika twitterte: «Auf dem Weg nach Afrika. Hoffentlich kriege ich kein AIDS. Nur ein Witz, ich bin ja weiss!» Ein schlechter Witz: Als sie elf Stunden später landete, war sie weltweites Twitter-Thema Nummer 1 und hatte keinen Job mehr.

Man kann darüber diskutieren, ob der Witz gut oder schlecht war, ob Ironie oder Zynismus, ob rassistisch oder eben gerade eine Veräppelung rassistischer Ignoranz, aber diese Sätze waren lange nicht das Schlimmste, was jemals auf einer Social Media Plattform gepostet wurde im Versuch, die Mitmenschen mit der eigenen Originalität zu erquicken. Justine Sacco hatte halt einfach Pech.

«Ihr Problem war, dass das ein Journalist gesehen und geteilt hat», sagt Martin Steiger, Zürcher Anwalt mit dem Schwerpunkt Recht im digitalen Raum. «Oft geht es erst richtig los, wenn die traditionellen Medien etwas aufgreifen. Meines Erachtens war dieser Fall ein Ausrutscher. Etwas in der Art könnte uns allen passieren.» Ab wann ein Beitrag rechtlich problematisch ist, liegt letztlich am Zusammenspiel von Kontext, Absicht und negativen Folgen. Erster Gatekeeper (nach dem gesunden Menschenverstand des Absenders) ist aber die Ethik eines Plattformbetreibers.

Möglichst wenig Zensur

«Der Betreiber einer Social-Media-Plattform ist natürlich in der Zwickmühle. Einerseits kann er durchaus sagen: Diesen Inhalt toleriere ich nicht. Aber er ist kein Richter. Und grundsätzlich möchte er so wenig wie möglich eingreifen und Zensur üben», sagt Steiger. Aber je mehr der Betreiber einfach mal zulässt, desto eher könne das kippen. Und plötzlich gehe es um Grund- und Menschenrechte, Privatsphäre, Meinungsfreiheit, informationelle Selbstbestimmung. Steiger: «Wenn er alles der Justiz überlässt, wird es schnell recht ungemütlich auf so einer Plattform, die dann alles andere als attraktiv wird für Werbekunden.»

> Betreiber von Social-Media-Plattformen sind keine Richter.

Darf man das eigentlich?

Und dann ist ja auch noch das Volk, das richtet. Die Beschimpfungen während eines Shitstorms sind meist heftig und sehr verletzend für die Betroffenen. Darf man das denn eigentlich, jemanden auf dem Netz beschimpfen und ihm oder ihr die Pest an den Hals wünschen? «Nein, das darf man nicht, da sind sehr oft Straftatbestände erfüllt, also Ehrverletzungen. Auch zivilrechtlich kennt man Persönlichkeitsverletzungen», sagt Steiger. Aber das Opfer müsste einen Strafantrag stellen oder klagen. Beides sind aufwändige und teure Prozedere mit unklarem Ausgang oder bei einem globalen Phänomen auch vom Ausmass her nicht zu bewältigen. «Kommt dazu, dass die Geschichte dann halt weitergeht, obwohl man die Angelegenheit einfach mal hinter sich lassen möchte», sagt Steiger. «Das ist für viele Opfer ein Grund, nichts zu unternehmen.» Sich zu wehren, hat seinen Preis.

Erst denken, dann posten

Ob es nun darum geht, auf dem Internet lustig zu sein, jemandem die Meinung zu geigen oder ihn auch nur zu veräppeln: Erst denken, dann posten, ist immer die günstigste Variante.

«Sich wehren, hat seinen Preis», sagt Rechtsanwalt Martin Steiger, der Spezialist für Recht im digitalen Raum.

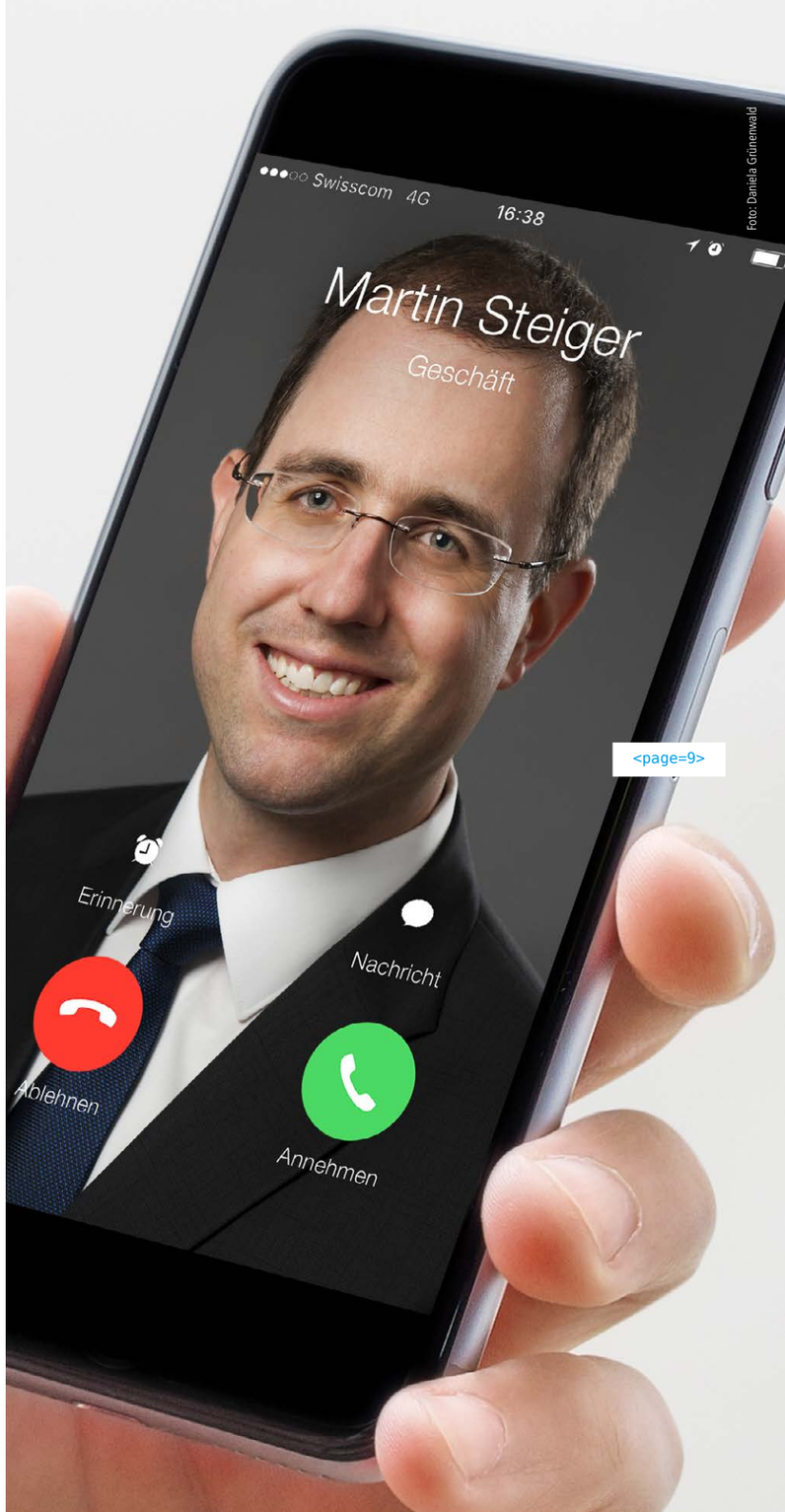


Foto: Daniela Grünenwald

<page=9>

Nichts fehlt – aber alles ist weg

Gefahr aus dem Internet drohe in der Schweiz vor allem den KMUs, sagt IT-Forensiker Lionel Bloch. Dabei wäre ein besserer Schutz einfach – und durchaus bezahlbar.

text: Matthias Mächler fotos: Roland Tännler

Es geschah in einer mittelgrossen Firma im Kanton Basel. Die Geschäfte liefen gut, die hochpräzisen CNC-Werkzeugmaschinen waren ausgelastet, und die Pläne, mit denen sie für die Herstellung von Auto- und Flugzeugteilchen gefüttert wurden, hatten einen derart guten Ruf, dass dem Geschäftsführer Peter Portmann* in jüngster Zeit auffallend oft Interesse an einer Lizenz signalisiert wurde.

Das Herzstück seines Unternehmens gab Portmann selbstverständlich nicht her: Würden die Pläne erst in die Hände von Billigproduzenten – zum Beispiel in China – gelangen, wäre er weg vom Markt. Unter Umständen ziemlich reich, aber ohne Aufgabe, und das wäre nicht sein Ding. Angst davor, dass die Pläne via Internet gestohlen werden, hatte Portmann trotzdem nicht. Die Geräte liefen losgelöst vom Netz, wie üblich in einem solchen Betrieb. Dann wurden die alten Maschinen durch eine neue Generation ersetzt, und als Portmann am nächsten Tag in die Firma kam, produzierten diese bereits auf Hochtouren. Sofort schrillten bei ihm die Alarmglocken: Wie war das möglich? Wer hatte die geheimen Pläne auf die neuen Geräte geladen? Und vor allem – wie? Die Originalpläne lagerten sicher in einem Safe, jene auf den alten Geräten waren mit einem Kopierschutz gesichert.

«Schweizer KMUs gehen unverhältnismässig hohe Risiken ein.»

Er knackt fast jeden Code

Der Zürcher IT-Forensiker Lionel Bloch, der an dieser Stelle ins Spiel kommt, ist trotz seiner jungen 28 Jahre ein alter Hase in seinem Fach. Bevor er die Firma ForenTec gründete, war er als IT-Forensiker bei führenden Wirtschaftsinstituten tätig. Bloch ist eines jener Genies, in dessen Händen ein Chip zu einem einfach lesbaren Plakat wird und eine elektronische Zahnbürste zum offenen Buch über die Pflegerituale seiner Verwender. Dank hochkomplexen Technologien kommt Bloch fast jedem Code auf die Schliche, und wenn er sie erst mal geknackt hat, setzen sich die Puzzleteile bald zu einer heissen Spur zusammen. Wie ein klassischer Forensiker an einem Tatort sammelt er systematisch Beweismittel, bis vor seinem geistigen Auge ein Film abläuft, wie sich die Dinge abgespielt haben müssen.

Als Bloch von Portmann um Hilfe gebeten wurde, wusste er: Entweder ist es längst zu spät oder nicht so schlimm, wie man befürchten könnte. «Wir leiteten sofort eine Untersuchung ein und stellten als Erstes fest, dass am Eingang der neuen Geräte ein USB-Stick Spuren hinterlassen hatte.» Der Verdacht fiel auf den Lieferanten der neuen Geräte.

Den Lieferanten im Visier

Man verzichtete auf die harte Tour – eine über die Staatsanwaltschaft angeordnete Hausdurchsuchung. Denn der Lieferant gewährte den Forensikern sofort uneingeschränkten Zugang zu den Firmencomputern. «Wir überprüften jeden Computer, jeden USB-Anschluss, jedes Betriebsprogramm, fanden aber nicht den geringsten Hinweis», sagt Bloch. «Das bedeutet: Entweder gab es keine Kopien der Pläne, oder wir hatten es mit professioneller Spionage zu tun.»

Das ist denn auch der Punkt, der Lionel Bloch am meisten beschäftigt: «Früher wurden Unternehmen noch zufällig attackiert, von Einzeltätern oder kleinen Banden, heute steckt hinter Hackerangriffen oder physischem Datendiebstahl fast immer ein organisierter Auftrag.» Oder anders gesagt: Die Zeiten, als Mathematiker aus purem Spieltrieb in Systeme eindrangen und sich danach mit ihrer Tat brüsteten, ist vorbei. Bloch: «Um an gute Programme zu kommen, investieren mafiöse Organisationen Millionen in Ausbildung und Programme.» Der Schwarzmarkt für solche Daten sei inzwischen grösser als der Drogenmarkt. Und gerade Schweizer Firmen mit ihrem Anspruch auf Perfektion müssten fast damit rechnen, früher oder später zum Ziel eines Angriffs zu werden.

«Nichts interessiert in Ländern, in denen billig produziert werden kann, so sehr wie hochqualitative Programme und Pläne», ist Bloch überzeugt

Während grosse, exponierte Firmen wie die UBS viel Geld und Know-how in die Sicherheit ihrer Daten investieren und gemäss Bloch sehr gut aufgestellt sind, gehen die meisten Schweizer KMUs unverhältnismässig grosse Risiken ein: «Wir haben mal eine Firma untersucht, die hatte seit sechs Jahren einen Trojaner im System, der monatlich Kundendaten abzweigte, und niemand hat's gemerkt.»

«Der Schwarzmarkt für solche Daten ist grösser als der Drogenmarkt.»

Etwas IT-Wissen genügt

Das ist das Perfide an der neuen Gefahr: Man hört nichts, spürt nichts, es fehlt nichts – und trotzdem ist alles weg. Selbst wer netzunabhängig produziere, sei nicht sicher, sagt Bloch. Man brauche ja nur einzubrechen: Mit etwas IT-Wissen knacke man jede Maschine.

Im Fall unserer Basler CNC-Firma stellte sich der Monteur als Urheber des Fiaskos heraus: Weil er über gerätespezifisches Insiderwissen

Liest Daten wie andere Bücher: Der IT-Forensiker Lionel Bloch.

verfügte, war es kein Problem, den Kopierschutz zu umgehen, die Pläne von den alten Geräten auf einen USB-Stick zu laden und auf den neuen Geräten zu installieren. Er tat dies ohne Auftrag, aus reinem Goodwill, damit möglichst schnell

> «Verschlüsselt wenigstens Eure Daten!»

weiterproduziert werden konnte. Der USB-Stick wurde sichergestellt, der private Computer des Monteurs gecheckt, und der Mann unterschrieb eine Erklärung, dass er den Stick sonst nirgends angeschlossen hatte. «Damit können wir einen Missbrauch zwar nicht vollends ausschliessen», sagt Bloch. Aber wenn irgendwo nur annähernd ähnliche Pläne auftauchen, wüsste man, wo ansetzen.

Wieder ruhig schlafen …

«Ich sage das nicht, weil mein Businessmodell darauf aufbaut», mahnt Bloch. «Aber liebe Schweizer KMUs, verschlüsselt wenigstens Eure Daten! Und reagiert, wenn Ihr den geringsten Verdacht schöpft!» Es muss ja nicht erst etwas Dummes passieren, das möglicherweise das Ende eines Unternehmens bedeutet. Die CNC-Firma aus dem Baselbiet jedenfalls liess von Blochs Forensikern die gesamte Infrastruktur neu aufsetzen, Sicherheitssensoren einbauen und die Mitarbeitenden schulen. Inklusive Soforthilfe kostete das im Vergleich zum Nutzen wenig: Peter Portmann bezahlte rund 20 000 Franken dafür, dass er wieder ruhig schlafen kann.

* Name geändert

Blochs 10 Gebote zum IT-Schutz

1) Wachsam sein!
Wenn immer das Bauchgefühl sagt, dass etwas nicht stimmt, ziehen Sie besser einen IT-Forensiker bei und schaffen Sie Klarheit.

2) Daten verschlüsseln!
Spezielle Programme machen aus Ihren Daten einen Salat – und Sie damit unattraktiv für Dritte.

3) Ex-Angestellten misstrauen!
Ändern Sie nach Abgang von Mitarbeitenden immer die Zugriffsdaten auf das System.

4) Mobile Geräte schützen!
Wer sensible Daten auf mobilen Geräten speichert, muss dringend Vorkehrungen treffen: Tablets, Handys & Co. sind einfach zu hacken.

5) Mitarbeitende kontrollieren!
Erstellen Sie ein Pflichtenheft für IT-Verantwortliche und IT-Benutzerrichtlinien für alle.

6) Daten sichern!
Erstaunlich, dass man noch immer darauf hinweisen muss: Ohne regelmässige Backups gibt es keine Sicherheit!

7) Schützen Sie sich!
Neben einem aktuellen Antivirusprogramm empfiehlt sich die Installation von elektronischen Brandschutztüren (Firewalls).

8) Starke Passwörter verwenden!
Durch Passwortdiebstahl gelangen Unbefugte ohne grossen Aufwand an vertraulichste Geschäftsinformationen. Machen Sie Dieben die Arbeit so schwer wie möglich!

9) Zugang beschränken!
Die beste Firewall nützt nichts, wenn sich Fremde in die Büros einschleichen können: Gelebte, sichtbare Sicherheit ist heute ein Qualitätskriterium und schafft Vertrauen bei Kunden und Lieferanten.

10) Ordnung wahren!
Daten und Dokumente gehen auf einem ordentlichen Arbeitsplatz weniger verloren, als wenn er mit Papieren, Handzetteln und Mäppchen übersät ist. Dasselbe gilt für die Arbeitsfläche im Computer!

So schützen Sie Ihre Daten

Google weiss alles: was Sie suchen, welche Apps Sie nutzen, welche Musik Sie hören, wo Sie wohnen, arbeiten und einkaufen. Mit ein paar Klicks kann man das Datensammeln stoppen.

text: Andreas Hirstein © NZZ am Sonntag

Google ist die grösste Suchmaschine der Welt, kontrolliert das meistverbreitete Smartphone-Betriebssystem (Android) und dominiert den Markt der Internet-Browser (Chrome). Auf allen Kanälen sammelt der Konzern persönliche Daten: aus Suchanfragen und der Nutzung von Apps. Kürzlich änderte Google die Datenschutzrichtlinien für den Chrome-Browser. Seither darf die Suchmaschine den gesamten Verlauf und nicht nur Suchanfragen auswerten, um «interessenbezogene Werbung» anzuzeigen. Berücksichtigt wird dabei auch Geschlecht und Alter der Nutzer. Die Änderung wird jedoch nur wirksam, wenn der Nutzer mit einem Google-Konto angemeldet ist und wenn er der Nutzung des Verlaufs zugestimmt hat (Opt-in).

Kaum ein Kunde macht von der Möglichkeit Gebrauch, Googles Umgang mit Daten zu kontrollieren. Dabei wäre das eigentlich kein Problem. Fast alle Daten, die Google gespeichert hat, kann man aufrufen und löschen – einzeln oder über beliebige Zeiträume.

Und auch das zukünftige Datensammeln kann man personalisieren, sofern man – wie zwangsweise bei jedem Android-Nutzer der Fall – mit einem Google-Konto angemeldet ist. Die entsprechenden Google-Webseiten sind übersichtlich gestaltet. Trotzdem kann allein die Fülle von möglichen Anpassungen verwirrend sein. Auf einen Blick zeigen wir hier Schritt für Schritt die wichtigsten Einstellungen. Man kann sie auf einem Android-Handy über «Google Einstellungen» aufrufen oder, wie im Folgenden beschrieben, im Browser.

1 Individuelle Werbung

Melden Sie sich im Chrome-Browser bei Google an, und klicken Sie rechts oben auf Ihr Profilbild und «Mein Konto». Anschliessend wählen Sie «Einstellungen für Werbung» und dann «Einstellungen für Werbung verwalten». Jetzt können Sie bestimmen, ob Google den Browserverlauf für interessenbezogene Werbung nutzen darf oder nicht. Kehren Sie nun ins Menu zurück, und wählen Sie «Verbundene Apps und Websites». Die Aufzählung zeigt Smartphone-Apps und Webdienste, denen Sie Zugang zu Ihrem Google-Konto gewährt haben. Falls Sie die entsprechende Anwendung nicht mehr nutzen, klicken Sie auf «Entfernen».

2 Zugriff auf Ihr Konto

Öffnen Sie noch einmal das Hauptmenu «Mein Konto» und klicken Sie auf «Geräteaktivitäten und Benachrichtigungen». Hier können Sie kontrollieren, mit welchen Geräten wann und von welchem Ort aus auf Ihr Google-Konto zugegriffen wurde. Falls etwas verdächtig erscheint, ändern Sie Ihr Passwort. Verlorene oder gestohlene Smartphones kann man automatisch suchen – der Standort wird dann auf einer Google-Maps-Karte eingetragen. Bei Google angemeldete Android-Smartphones lassen sich zudem aus der Ferne sperren oder zurücksetzen.

3 Datensammlung prüfen

Googles Datensammlung ist weitaus umfangreicher, als man es sich vorzustellen vermag. Nicht nur der Besuch einer Google-Seite wird registriert, sondern jede einzelne Eingabe mit Orts- und Zeitangabe. Falls man ein Android-Handy nutzt, speichert Google auch, welche Apps wann geöffnet wurden. Bei Suchen mit Spracherkennung werden Tondatei und transkribierter Text archiviert. Auch nach Jahren kann man sich somit noch anhören, was man einmal ins Mikrofon des Smartphones gestottert hat. Das alles dient dazu, die Google-Dienste zu personalisieren, und natürlich auch dazu, die Zielgenauigkeit der Werbung zu verbessern. Aufrufen lässt sich die Datensammlung, indem man im Hauptmenu auf «Google-Aktivitäten verwalten» und anschliessend auf «Meine Aktivitäten aufrufen» klickt. Man gelangt dann zu einer Liste, in der sich alle Aktivitäten minutengenau zurückverfolgen lassen – über Jahre hinweg, wenn man bereits so lange Google-Kunde ist. Man kann die Liste auch filtern und so auf bestimmte Zeiträume und Google-Dienste einschränken (z.B., welche Musik ich mir auf Google Play angehört habe). Jedes Ereignis kann man markieren, weitere Details dazu anzeigen und es per Klick löschen. Alternativ lassen sich beliebige Zeiträume definieren, deren Einträge gelöscht werden sollen.

4 Regeln bestimmen

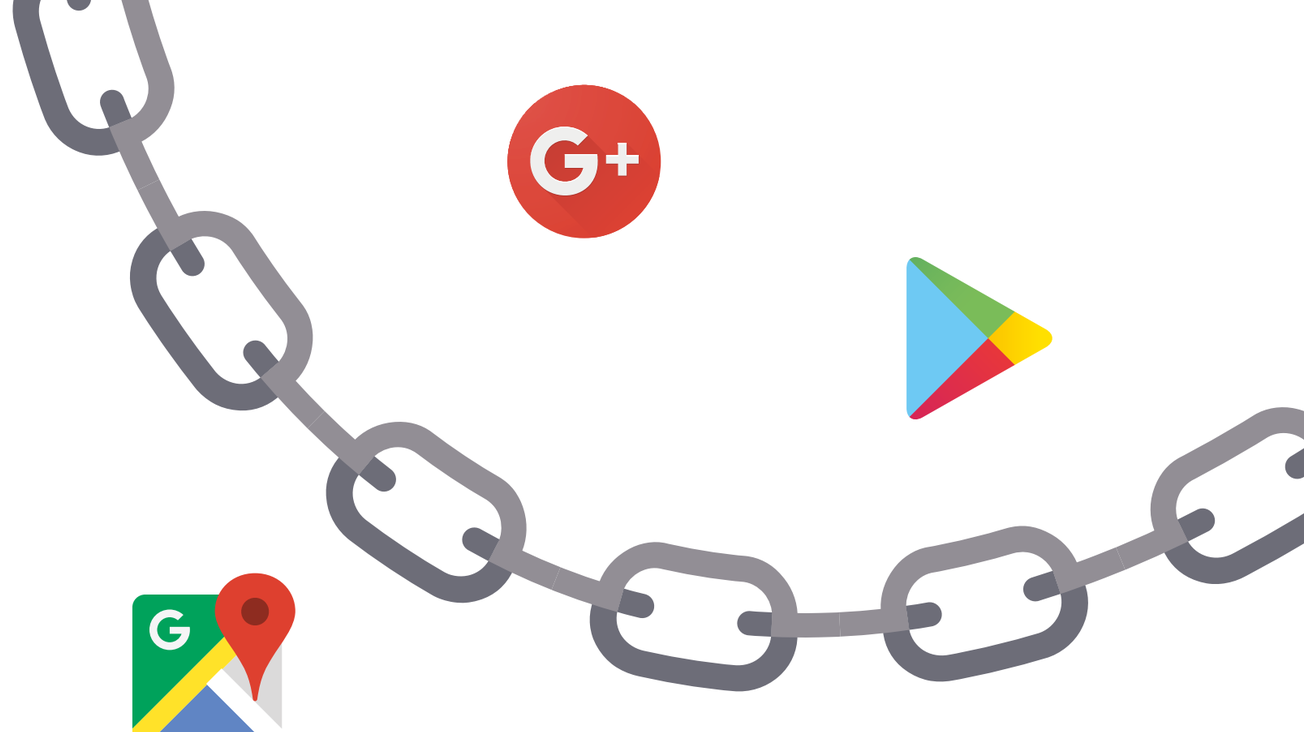
Nachdem Sie die Datensammlung auf den Google-Servern Ihren Wünschen oder Toleranzgrenzen angepasst haben, sollten Sie den zukünftigen Umgang mit neu generierten Daten festlegen. Google unterscheidet hier eine Reihe unterschiedlicher Datentypen (Websuchen, Standorte, Audiodaten von Spracheingaben, Youtube-Daten usw.), für die sich jeweils eigene Regeln bestimmen lassen. In den folgenden Punkten werden wir sie separat besprechen. Zunächst klicken Sie dazu erneut auf «Google-Aktivitäten verwalten» und anschliessend auf «Aktivitätseinstellungen aufrufen».

5 Web- und App-Aktivitäten

Der erste Datentyp heisst «Web- und App-Aktivitäten». Darunter fallen die Google-Suche und der Google-Now-Dienst, der personalisierte Informationen auf dem Smartphone bereitstellt: Verkehrshinweise für die Fahrt ins Büro, Flugverspätungen für bevorstehende Reisen und vieles mehr. Damit Google relevante Informationen bestimmen kann, müssen Sie die Speicherung «Web- und App-Aktivitäten» einschalten. In diesem Fall archiviert Google sämtliche Suchbegriffe, die verwendeten IP-Adressen, ob man einen Browser oder eine App benutzt hat und vieles mehr. Zusätzlich können Sie die Auswertung des gesamten Browser-Verlaufs autorisieren. Falls Sie das nicht möchten, können Sie die Speicherung der Daten «pausieren». Damit verzichten Sie allerdings auf Google Now. Die Qualität der Suchergebnisse dürfte zurückgehen, und bei der Eingabe werden Sie weniger Hilfe durch vorgeschlagene Suchbegriffe erhalten.

6 Standortdaten verwalten

Der zweite Datentyp sind die Standortdaten. Wenn Sie diesen Dienst ausschalten, werden die mit angemeldeten Geräten besuchten Orte nicht mehr auf den Google-Servern gespeichert. Der Standortverlauf ist daher auch auf Google Maps auf dem Smartphone nicht mehr verfügbar, und Sie müssen mehrmals aufgesuchte Orte immer wieder neu eingeben, statt sie bequem aus einer Liste auszuwählen. Achtung: Selbst wenn Sie den Standortverlauf deaktivieren, werden einige Ortsinformationen im Rahmen der vorgenannten «Web- und App-Aktivitäten» weiterhin erfasst und gespeichert, zum Beispiel, wenn Sie Google Maps nutzen oder die Google-Suche. Um das Speichern von Ortsdaten vollständig zu unterbinden, müssen also beide Datenkategorien (Punkt 5 und 6) deaktiviert sein. Wichtig: Auf die Funktion der Standortdienste, die man auf dem Smartphone ein- und ausschalten kann, haben die hier geschilderten Einstellungen keinen Einfluss. Wenn man den Standortverlauf pausiert, wird lediglich die Speicherung der Daten gestoppt. Navigations-Apps und Google Maps funktionieren weiterhin.
Der bereits gespeicherte Standortverlauf lässt sich auch bearbeiten und vollständig löschen. Dazu klicken Sie auf «Verlauf verwalten». Sie gelangen dann zu einer Weltkarte, die alle von Ihnen besuchten Orte durch rote Punkte markiert – vorausgesetzt, Sie hatten ein bei Google angemeldetes Handy oder Tablet bei sich. Durch einen Klick auf den Kehrichteimer unten rechts können Sie nun den vollständigen Verlauf löschen. Wenn Sie oben links ein bestimmtes Datum auswählen, können Sie einzelne Tage löschen.



7 Geräteinformationen

Ein weiterer Datentyp sind die «Geräteinformationen». Hier speichert Google Kontakte, Termine, installierte Apps, Musik und technische Informationen des Handys. Auch dies soll Websuchen verbessern. Klicken Sie auf den Schieberegler, wenn Sie die Speicherung der Daten auf den Servern pausieren wollen. Bereits gespeicherte Daten können Sie löschen, indem Sie auf «Verlauf verwalten» klicken und anschliessend im Menu rechts oben «Löschoptionen» auswählen.

8 Audiodaten

Google speichert auch die Tondateien von Sprachsuchen. Durch einen Klick auf den entsprechenden Schalter kann man die Archivierung stoppen. Damit verschlechtert sich die Qualität der Spracherkennung, weil die Algorithmen weniger Beispiele haben, um ihre Funktion zu trainieren. Bereits gespeicherte Daten kann man löschen: Klicken Sie auf «Verlauf verwalten» und anschliessend rechts oben auf «Aktivitäten löschen nach». Nun können Sie beliebige Zeiträume definieren, in denen die Audiodaten gelöscht werden sollen.

9 Änderungen mit Folgen

Alle Einstellungen unter «Mein Konto» wirken sich auf die Google-Dienste auf allen Geräten aus, egal ob in einem Browser auf einem PC, einem Android-Handy oder (etwas weniger) auf einem iPhone, sofern diese bei Google angemeldet sind. Wenn Sie sich abmelden, findet die Speicherung auf den Google-Servern nicht statt, sondern nur lokal in den Apps. Dann funktionieren einige Dienste allerdings nicht mehr oder weniger komfortabel und weniger genau.

Das grosse Säbelrasseln

Der Krieg ist lautlos geworden: Spionage, Datenhandel und Terror finden im Cyberspace statt. Doch was ist Show, was echte Gefahr? Ein Gespräch mit Myriam Dunn Cavelty, Dozentin für Sicherheitspolitik an der ETH Zürich.

interview: Matthias Mächler fotos: Samuel Wimmer

NORSE: Alle Arten von Cyber-Attacken in Echtzeit
http://map.norsecorp.com

Sie studierten Internationale Beziehungen, Geschichte und Internationales Recht. Warum sind Sie nicht Spionin geworden?

«Daten sind das Geschäft von morgen, die Gier danach ist grenzenlos.»

(Lacht) Ich habe nie ein Angebot bekommen! Nein, im Ernst, was mich an diesen Themen immer gereizt hat: In der sonst extrem engen Forschungslandschaft gibt es kaum Leute, die Cyber-Themen, also etwas Technisches, mit Politik verbinden. Entsprechend frei bin ich bei meinen Arbeiten.

Statt selber zu spionieren, untersuchen Sie Spionagefälle?
Nicht nur. Im Moment schreibe ich über die Auswirkungen von TV-Serien auf Cyber-Gefahren. Das ist faszinierend, weil die Cyber-Terrorszenarien zum Beispiel in «Die Hard», «24» oder «Homeland» visuell beschreiben, was es in der Realität noch gar nie gab. Sie beeinflussen damit die Gesellschaft und vor allem die Politik, die dann zu Angstreaktionen neigt und das Geld falsch ausgibt.

Der Cyber-Krieg kennt keine Landesgrenzen. Inwiefern betrifft er die Schweiz?
Es ist wichtig, zu definieren, über welches Gewaltphänomen wir sprechen. Die Schweiz ist selbstverständlich betroffen von Cyber-Kriminalität, vor allem auch von Cyber-Spionage. Daten sind das Geschäft von morgen, die Gier danach ist grenzenlos.

Kommt das gut? Müssen wir uns um unsere Daten sorgen?
Dass es Vorfälle und Schäden gibt, ist leider nicht zu vermeiden. Man tut, was man kann. Die «Awareness», also das Gefahrenbewusstsein, ist hierzulande aber recht hoch. Vor allem der Finanzsektor gibt viel Geld aus für den Schutz ihrer, also unserer Daten. Ein Problem haben wir aber vor allem bei den KMUs. Sie sind punkto Innovation und Entwicklung sehr wichtig für unser Land, aber meistens ungenügend geschützt. Es fehlt ihnen an Personal und Mitteln.

Und was ist mit Cyber-Terrorismus?
Ein Angriff aus dem Nichts auf kritische Infrastrukturen wie ein Atomkraftwerk ist ausserordentlich unwahrscheinlich. Um eine Schadsoftware zu schreiben, die so etwas kann, braucht es einen richtig guten Geheimdienst und viel Geld. Und auch dann müssen Sie das Ziel in allen Details kennen, brauchen Insider, müssen die Software testen. Kosten-Nutzen-mässig lohnt sich das für Terroristen kaum. Zumal der gewünschte Effekt nicht garantiert ist. Als Terrorist sind sie mit einer Autobombe auf einem belebten Platz viel besser aufgestellt.

Es gibt gar keinen Terrorismus im Cyberspace?
Den gibt es wohl. Der Cyberspace dient Terroristen zur Rekrutierung, für Propaganda und als Geldmaschine. Es gibt immer mehr Verknüpfungen zwischen organisiertem Verbrechen und Terrorismus. Das ist ein grosses Thema: Terroristen beschaffen sich zum Beispiel mit Medikamentenhandel Geld für ihre Aktionen.

Wie steht es denn nun um die Cyber-Welt? Von wem droht am meisten Gefahr?
So genau weiss man das nicht, wie immer, wenn Geheimdienste tätig sind. Aber das Verhalten der Staaten spricht für sich: In den letzten fünf, sechs Jahren beobachten wir sehr viel mehr Anstrengungen in der Diplomatie, Cyber-Gefahren durch internationale Zusammenarbeit zu stabilisieren. Leider scheint auch sehr viel Geld in die Cyber-Offensive zu fliessen. Und die Nervosität, die herrscht, ist eine schlechte Voraussetzung für eine stabile Weltsituation. Wenn dann mal was schiefgeht, braucht es wenig. Die Eskalationsgefahr ist relativ hoch.

Ist es angesichts des Riesenhypes nicht erstaunlich, wie wenig bislang geschah?
Bis vor sechs, sieben Jahren dachte man, der anonyme Cyberspace spiele auch schwächeren Staaten Trümpfe in die Hand und gebe Ländern wie Nordkorea eine gewisse Macht. Dann drehte die Meinung: Heute sagt man, dass nur noch Grossmächte fähig sind, wirklich gute Cyber-Angriffe zu führen. Aber die haben wenig Interesse an einer Eskalation.

«Nur Grossmächte sind in der Lage, gute Cyber-Angriffe zu führen.»

Dann ist die Entwicklung einigermassen überschaubar – und sogar beruhigend?
Wenn Sie daran glauben, dass Staaten untereinander verbindliche Abkommen schliessen können, die etwas bringen, dann ist es eher etwas Gutes.

Und wenn nicht?
Weil mehr und mehr Staaten einsteigen in diesen unsichtbaren Raum, gibt es auch den Faktor der Destabilisierung. Erst müssen die internationalen Beziehungen greifen.

Es wird also vor allem mit den Säbeln gerasselt, handfeste Beweise für Cyber-Offensiven gibt es nicht. Ist der Cyberwar bloss eine Verschwörungstheorie?
Es hat viele verschwörungstheoretische Elemente drin. Aber eben nicht nur. Verbindliche Daten über Kapazitäten von Staaten zu bekommen, ist schwierig. Wir wissen nicht, was die Amerikaner wirklich können – und wollen. Wir wissen es auch nicht von den Chinesen, von den Russen oder von den Israelis. Die Enthüllungen von Edward Snowden sind wohl nur die Spitze des Eisbergs. Das meiste, was da passiert, liegt im Dunkeln.

Der Cyberwar ist ein Giga-Business. Viele Menschen und Firmen machen eine Menge Geld mit der Angst vor Krieg im Netz …
So ist es. Das ist ein grosses Problem auch für die Forschung. Wir möchten mit möglichst unabhängigen Daten unsere eigene Meinung bilden. Aber es gibt keine unabhängigen Daten. Nur Daten von Anti-Viren-Firmen und halbstaatlichen Organisationen, bei denen überall ein Interesse dahintersteckt, dass das Thema am Köcheln bleibt. Das ist sicher nicht optimal.

> «Wir wissen nicht, was die Amerikaner, Russen oder Israelis können und wollen. Das meiste, was da passiert, liegt im Dunkeln.»

Vor welcher Entwicklung haben Sie persönlich am meisten Angst?
Angst habe ich vor allem dort, wo es um die Dummheit einzelner Akteure geht. Dass gewisse Aktionen schlummernde Kräfte wecken, gerade heute mit dem ganzen Nationalismus. Und dass so etwas schon mal ganz blöd laufen kann. Das Instabile ist die Gefahr.

Wie wird die Cyber-Welt in ein paar Jahren aussehen?
Ich glaube, wir gehen eher einer Stabilisierung entgegen. Einfach deshalb, weil die Grossmächte kein Interesse an Instabilität haben. Der Cyberspace – in Zukunft vielleicht auch verschiedene Netze mit unterschiedlichen Sicherheitsstandards und Zugangsmöglichkeiten – ist eine Realität, er wird gebraucht und missbraucht werden, aber alles wird normaler, alltäglicher, und die Hysterie nimmt ab. Das ist wie mit dem Terrorismus: Je mehr Terrorismus, desto normaler wird er. Und desto weniger nützt er den Akteuren als Strategie.

Zurück zu Ihnen als verhinderte Spionin …
Oh, nein, ich würde mich zu Tode langweilen. Wissen Sie, worin Geheimdienstarbeit vor allem besteht? Sie sitzen an einem Tisch, bekommen Daten, müssen diese analysieren und haben häufig keine Ahnung, was das soll. Dann schreiben sie so kleine Berichte, von denen sie annehmen können, dass sie bald für immer in der Versenkung verschwinden. Ausserdem: Spione haben wir nicht wahnsinnig viele hier in der Schweiz. Ich kenne jedenfalls keinen einzigen.

Hat vor allem Angst vor der Dummheit: Cyberspace-Expertin Myriam Dunn Cavelty an ihrem Arbeitsort, der ETH Zürich.

Cyberwoman

Dr. Myriam Dunn Cavelty (geboren 1976) ist seit 2006 Dozentin für Sicherheitspolitik an der ETH Zürich und seit 2014 Vizedirektorin für Forschung und Lehre am Center for Security Studies (CSS) an der ETH Zürich. Im Fokus ihrer Arbeiten stehen Cyber-Sicherheit, Cyberwar und der Schutz kritischer Infrastrukturen. Privat bloggt Myriam Dunn Cavelty erfolgreich über koreanische und chinesische Fernsehserien (der Blog habe gegenwärtig 6,5 Millionen Aufrufe, sagt sie), hört am liebsten Heavy Metal, hat eine Tochter und zwei Katzen und ist verheiratet mit dem Autor Gion Mathias Cavelty.

_

Link encap: Ethernet HWaddr 08:00:27:40:04

Ein düsteres Kapitel

Es gibt viele Missverständnisse in Bezug auf Hacker, glaubt Marc Rubin, der selber auf «Datenreisen» geht. Eine Begegnung im Graubereich.

text: Florian Leu fotos: Roberto Ceccarelli

Für Marc Rubin, Mitglied des Chaos Computer Clubs und Gründungsmitglied der Zürcher Piratenpartei, spielte es keine Rolle, was er auf seinen Datenreisen auftrieb. Er war ein Einbrecher, dem es nicht darum ging, den Safe auszuräumen, nur darum, ihn zu knacken. Rubin, heute 25 Jahre alt, nennt sich einen Grey Hat Hacker: Einer, der sich meist im legalen Bereich bewegt.

> Der Hacker, dein Freund und Helfer.

Hacken aus Sicherheitsgründen
Aber nicht immer. Eine Aktion, an der er sich zum Beispiel beteiligen würde: Wie seine Kollegen des Chaos Computer Clubs Deutschland eine Reihe von Wahlcomputern hacken. Nicht aber, um Stimmen für sich selbst zu holen, sondern um auf die Gefahr hinzuweisen, die die digitale Demokratie birgt. Rubin und der Club versuchten in der Schweiz ebenfalls, in Wahlcomputer einzudringen, allerdings auf Einladung der Fachhochschule Bern. Dabei spürten sie Sicherheitslecks auf, wenn auch nur kleine: Der Hacker, dein Freund und Helfer.

Nachts hinter dem Bildschirm
Rubin hat eine Lehre als Informatiker gemacht, Schwerpunkt Systeminformatik, dann Wirtschaftsinformatik studiert, aber noch nicht abgeschlossen – eine Diplomarbeit lässt sich nicht hacken. In den letzten drei Jahren arbeitete er als Sicherheitsingenieur, betreute Banken und Kommunikationsanbieter, war stolz darauf, dass die Seite von Cablecom nur dank eines seiner Scripts lief. Oft sass er auch nachts hinter dem Bildschirm. Die Arbeit glich dem bestimmenden Gefühl seiner Kindheit: Games mochte er damals vor allem, wenn er Rätsel lösen musste und mit Tricks und Cheats schneller ans Ziel kam. Dank seiner Programmierkünste griff er wie ein zehnjähriger Gott in die künstlichen Welten ein: Den Himmel eines Ballerspiels färbte er lila, in Abenteuerspielen programmierte er seinem Avatar einen unerschöpflichen Goldbeutel. Sich als Teenager in einen fremden Server einzuklinken, das war die Fortsetzung davon: Immer noch ein Game, doch diesmal draussen in der Wirklichkeit. Seine Arbeit hatte für Rubin ebenfalls die Textur eines Spiels, mit einem angenehmen Unterschied: Es gab nun Geld fürs Rätsellösen.

> Der Abschluss als Wirtschaftsinformatiker muss warten – eine Diplomarbeit lässt sich nun mal nicht hacken.

Wenn er sich mit Leuten unterhält, die wenig über Hacker wissen, muss Rubin ausholen. Denn Hacker sind nichts Neues. Die ersten waren Studenten und Mitarbeiter des Massachusetts Institute of Technology in Cambridge. Doch ihre Hacks hatten wenig mit Computern zu tun. Sie unterhielten auf dem Gelände der Hochschule eine Modelleisenbahn und bezeichneten es als Hack, wenn es ihnen gelang, die Anlage auf geschmeidige Weise zu verbessern – das ist sechzig Jahre her. Dann gab es die Phreaks: Angestellte von Telegrafen-, später auch von Telefongesellschaften, die im 19. Jahrhundert ihr Wissen dazu nutzten, sich kostenlos austauschen zu können. Sie hatten kriminelle Energie, setzten sie aber für etwas relativ Harmloses ein: Sie wollten nicht zahlen, um mit anderen zu reden.

Ein wenig Grips
«Ein Hack ist wertneutral: Es geht darum, Abkürzungen zu finden, Bestehendes mit ein wenig Grips besser zu machen, andere daran

> Vor 60 Jahren waren Hacker Modelleisenbähnler: Gelang ihnen eine Verbesserung, nannten sie es einen «Hack».

Mehr Heizung als Computer: Marc Rubin vor einem alten Server der ETH im Chaos Computer Club.

Für Nicht-Hacker das perfekte Bild zum Ort: Chaos Computer Club …

teilhaben zu lassen», sagt Rubin, tief in eine abgewetzte Couch versunken. Im Hintergrund hängen wie in einem Museum die alten Server der ETH Zürich – der Chaos Computer Club, Treffpunkt von Hackern und Netzaktivisten, nutzt sie aber nur noch selten, sie fressen zu viel Strom, sind mehr Heizung als Rechner. Zwischendurch nippt Rubin an seinem Mate, dem Zaubertrank des Clubs, grosszügig mit Koffein versetzt für allfällige Nachtschichten vor dem Computer.

Das Bild, das vielen einfällt, wenn sie von Hackern hören, wirkt wie aus dem Film «Matrix» heruntergeladen: Lichtscheue, schwarz gekleidete Wesen, die nachts vor matt schimmernden Bildschirmen sitzen und versuchen, sich in Netzwerke zu stehlen. Oberflächlich gesehen, entspricht Rubin diesem Klischee: Auch er ist bleich, hager, schwarz gekleidet, wirkt etwas verloren. Nur dem Bild, das viele von der Arbeit eines Hackers haben, will er nicht entsprechen: Dass sie Bankdaten klauen, Bauernfängerei betreiben, die Konten von Leuten am anderen Ende der Welt plündern. Er sagt: «Wer so handelt, ist einfach nur ein Finanzkrimineller.»

> Wer bloss die Konten fremder Menschen am anderen Ende der Welt plündert, ist einfach nur ein Finanz-Krimineller.

Die Gefahr, dass einem im Internet die Kreditkartendaten geklaut werden, schätzt Rubin als verschwindend gering ein. Wer sich halbwegs vernünftig verhält, etwa bei grossen Anbietern einkauft, braucht sich kaum Sorgen zu machen: «Da liegt die Wahrscheinlichkeit, dass etwas geschieht, bei eins zu hundert, wenn nicht noch tiefer.»

Immer auf die Kleinen

Heikler wird es für jene, die oft bei kleinen Anbietern bestellen. Deren Sicherheitsvorkehrungen sind weniger ausgereift, deswegen werden ihre Datenbanken eher leergefischt. Jeden Tag werden weltweit die Daten von etwa 2000 Kreditkarten entwendet – ziemlich wenig, gemessen an ihrer Gesamtzahl. Cyber-Kriminelle holen sie oft von solch kleinen, schlecht geschützten Onlinehändlern. Aber: «Es ist wahrscheinlicher, dass einem in

> Der Kopf ist die einzig sichere Festplatte.

der realen Welt das Portemonnaie geklaut wird», sagt Rubin, «dass jemand sich mit einem Gerät, das Magnetstreifen lesen kann, im Café oder im Flughafen neben einen setzt, oder dass Diebe Geldautomaten mit einem Magnetstreifenleser und einer Kamera bestücken.»

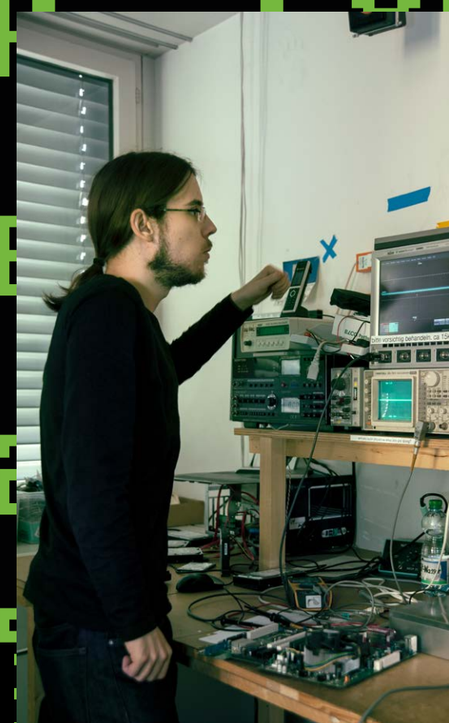
Sorgen macht sich Rubin eher um private Daten. Geschäftsideen etwa würde er nie auf einem Computer speichern: «Der Kopf ist die einzig sichere Festplatte.» Ausserdem sei das Filterprogramm ausgereift: «Die schlechten Ideen vergisst man wieder.» Die Angst vor Hackern hält Rubin indes für übertrieben, fast schon für ein Ablenkungsmanöver. Wenn Regierungen Staatstrojaner kaufen, um die Bevölkerung auszuhorchen, ist das für ihn ein Hack von oben: Die Polizei kann so virtuelle Hausdurchsuchungen durchführen, ohne dafür eine Genehmigung einzuholen. Mit Staatstrojanern lassen sich Kameras und Mikrophone von Computern in nahezu jedem Privathaushalt nutzen, als wäre das ganze Land verwanzt. Rubin: «Wir erleben gerade eine Zeit, in der Regierungen versuchen, unsere Privatsphäre aufzuheben. Ein düsteres Kapitel.»

Web wie im Wilden Westen

Da erstaunt es nicht, dass er geradezu wehmütig an seine Kindheit denkt. Wie er sich damals im Internet bewegte, das sei der Wilde Westen gewesen. «Mittlerweile befinden wir uns im Industriezeitalter, die Sorglosigkeit ist weg.»

> Anonymous ist so diffus, wie die Hippies es waren.

Rubin unterstützt nicht von ungefähr Whistleblower wie Edward Snowden und hegt Sympathien für «Anonymous», selbst wenn das für ihn nichts Konkretes ist: «Die Bewegung ist so diffus, wie die Hippies es waren. Aber ich mag die Werte, die dahinterstehen: Freiheit, Privatsphäre, unzensierter Spass». Längst kein Kind mehr, das zum Spass bei anderen einbricht, fürchtet Rubin nun aber, dass die anderen bei ihm einbrechen, dass Polizisten seinen Computer durchstöbern, auf seiner Festplatte auf Datenreise gehen und alles auf Vorrat speichern. Nicht dass sie einen Anlass dazu hätten. Das Problem ist für Rubin, dass die Unschuldsvermutung nicht mehr gilt, sondern dass man seine Unschuld dauernd unter Beweis stellen muss. Schon möglich, dass die Beamten bei ihm etwas finden würden. Nur wären die Daten etwa so abenteuerlich wie der Businessplan eines Herstellers von Zementmischern.



Fürchtet sich mittlerweile vor seinesgleichen: Hacker Marc Rubin.

Höchste Zeit, einzuschreiten: Carole Aubert bekämpft den Handel mit gefälschten Uhren im Internet.

Alles echt falsch hier

Weltweit werden heute mehr gefälschte Schweizer Uhren hergestellt als echte, und die Fälscherbanden lauern ihren Kunden vor allem im Internet auf. Dagegen kämpft ein kleines Team in Biel – die Netzdetektive des Schweizerischen Uhrenverbands.

text: Barbara Meier fotos: Roberto Ceccarelli

«Voilà», sagt Carole Aubert, und für einen Moment glimmt in ihren Augen Jagdlust auf: «Damit kriegen wir sie!» Die elegante Rechtsanwältin sitzt in ihrem Büro in einem Art-Deco-Gebäude in Biel, dem Sitz des Schweizerischen Uhrenverbandes. Aubert gehört zum zwölfköpfigen Team für Fälschungsbekämpfung. Sie leitet die «Internet Unit», die 2004 gegründet wurde. Denn der Handel mit gefälschten Uhren findet längst nicht mehr nur auf exotischen Märkten in Grossstädten oder bei fliegenden Händlern am Strand statt. Heute lauern die Fälscher ihren Kunden im Netz auf.

Auf dem Bildschirm von Carole Aubert hat sich eine Seite von AliExpress aufgebaut, einem Ableger des chinesischen Onlinehändlers Alibaba. Uhren leuchten auf, die aussehen wie Klassiker von Omega, Cartier oder Hublot, ohne dass Omega, Cartier oder Hublot draufstehen würde. «Achten Sie auf die Zeiger», sagt Aubert. Tatsächlich ist es auf allen Uhren fünf vor zwölf – oder fünf nach. Jedenfalls stehen die Zeiger stets so eng beieinander, dass sie den grössten Teil des Markennamens verdecken, die

restlichen Buchstaben wurden mit Photoshop wegretouchiert.

Der Anbieter dieser Uhren arbeite mit zwei Tricks, erklärt Carole Aubert: Einerseits verwendet er nirgends verräterische Worte wie Replika, Imitat oder Duplikat, nach denen die Uhrendetektive mit einer speziellen Software das Netz absuchen. Andererseits verzichtet er darauf, die Uhren unter dem

> Neuerdings schleichen sich die Fälscher in soziale Netzwerke wie Facebook und Instagram.

geschützten Markennamen anzubieten. Es ist zwar bereits verboten, das Design zu kopieren, doch die Verantwortlichen von Plattformen wie AliExpress zeigen sich erst bei gefälschtem Logo bereit, einen Anbieter zu sperren.

«Korrektes Logo» – falsche Uhr
Da kein Kunde eine Uhr kauft, die aussieht wie eine Omega, ohne dass Omega draufsteht, muss der Anbieter beschwichtigen. «Genau hier verrät er sich», sagt Carole Aubert und zeigt auf einen Satz in der Beschreibung: «All watches come with correct known logo», wird in wackligem Englisch versprochen: Alle Uhren werden mit dem bekannten Logo geliefert.

Aubert schickt eine Meldung an AliExpress und verlangt, dass man diesen Handel stoppt. Kurze Zeit später wird das Angebot von der Plattform verschwunden sein.

Ein vielköpfiges Monster
In Zahlen sind die Erfolge von Carole Auberts Interneteinheit beeindruckend: Dank ihrer Intervention sind 2015 mehr als 600 000 Inserate für gefälschte Uhren zurückgezogen worden. Doch die Netzdetektive kämpfen gegen ein vielköpfiges Monster: Schlagen sie hier einen Kopf ab, wachsen dort zwei neue nach. Neuerdings schleichen sich die Fälscher in soziale Netzwerke wie Facebook und Instagram. Dort entscheiden Algorithmen, welcher Nutzer welche Werbung sieht; Suchprogramme finden diese Inserate nicht. Aubert versucht, die Fälscher mit ihren eigenen Waffen zu bekämpfen: Sie bespielt eine ganze Reihe von falschen Facebook- und Instagram-Profilen. «Doch obwohl ich allen Uhrenmarken folge und alles like, was es nur zu liken gibt: Bisher ist auf meinen Profilen noch kein einziges Uhreninserat aufgetaucht, was sehr seltsam ist.»

Zum Glück hat Aubert Informanten. Auf ihrem Smartphone öffnet sie ein Bild, das ihr ein Freund geschickt hat: Der Screenshot einer Werbung für eine Rolex mit «Superrabatt» für 119 statt 1117 Franken. Auch dieser Link führt auf eine Website, die so programmiert ist, dass sie Suchmaschinen verborgen bleibt. Trotzdem sind die Netzdetektive den Fälschern auf den Fersen. Denn Aubert hat festgestellt, dass sich die Pakete, in denen diese Uhren in die Schweiz geliefert werden, extrem ähneln und meistens aus Rotterdam kommen. Darauf schulte ihr Team die Zöllner in den grossen Postverteilstellen – und allein in den letzten Wochen hat der Schweizer Zoll bereits Hunderte dieser «sensationellen Schnäppchen» beschlagnahmt.

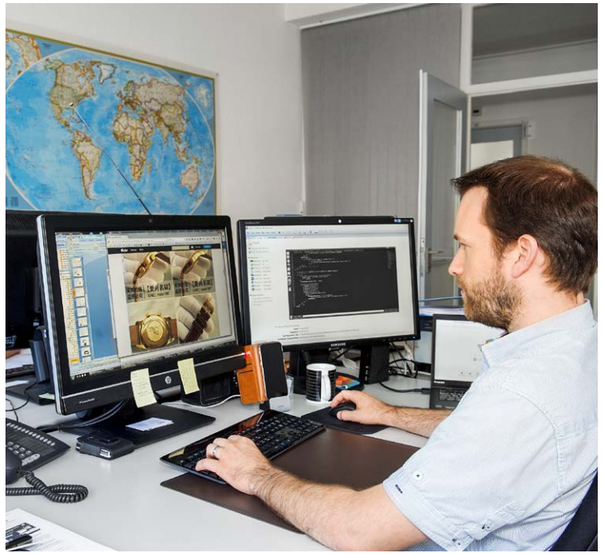
Eine neue Art von Kunden
Die Kriminellen fänden in den sozialen Netzwerken nicht nur den idealen Schatten für ihre Geschäfte, sagt Carole Aubert: «Sie kommen dort auch an eine neue Art von Kunden heran.» Denn die Käufer, die bisher im Internet eine «Hublot Replica» oder ein Modell bestellten, das aussieht wie eine Omega ohne Markenschriftzug, die wussten, dass sie eine Fälschung kauften. Die neuen Kunden hingegen glauben, sie bekämen tatsächlich eine

> Gegen 40 Millionen gefälschte Schweizer Uhren kommen jedes Jahr auf den Markt – und nur 29 Millionen echte.

echte Rolex zu einem sensationellen Preis. Stattdessen bekommen sie einen Brief vom Uhrenverband. Darin steht, warum ihre Uhr vom

Und weg damit: Gefälschte Uhren werden am Zoll beschlagnahmt – und zerstört.

Schwer zu täuschen: Die «Internet Unit» des Uhrenverbandes mit Michel Arnoux, Carole Aubert und Yves Brouze.



Surfen durch den Online-Dschungel.

Zoll beschlagnahmt wurde, dass sie zerstört werde und sie dafür auch noch bezahlen müssten. Erstaunlicherweise sind die Käufer darüber nur selten wütend, sondern meist beschämt. «Manche schicken Entschuldigungsschreiben», sagt

> Getäuschte Käufer sind wertvolle Informanten.

Carole Aubert. Der gute Kontakt zu enttäuschten Käufern ist für die Netzdetektive enorm nützlich, denn von ihnen bekommen sie wertvolle Informationen: Über verborgene Internetseiten, Kontaktadressen, Zahlungsbedingungen, Kontodaten. Alles Fäden im riesigen Netzwerk der kriminellen Fälscherbanden. Im Gegenzug bietet Aubert Hilfe an, wenn die Käufer ihr Geld von der Kreditkartenfirma zurückfordern wollen. Solange jemand ein «Replikat» bestellte, war das nicht möglich. Doch wenn jemand glaubt, er bezahle für eine echte Uhr, wird der Verkauf zum Betrug. Und wenn das oft genug vorkomme, hofft Aubert, wachse der Druck auf die chinesischen Banken, von denen einige vermutlich direkt in das Milliardengeschäft verwickelt sind.

2000 Razzien allein in China

Gegen 40 Millionen gefälschte Schweizer Uhren kommen jedes Jahr auf den Markt – und nur etwa 29 Millionen echte. Um das vielköpfige Monster in Schach zu halten, kämpfen die Detektive mit allen Waffen, mit virtuellen, juristischen, aber auch mit handfesten: Rund 2000 Razzien liess der Schweizer Uhrenverband letztes Jahr alleine in China durchführen; Weltweit hat man in Werkstätten, Fabriken, Lagerhallen und Märkten etwa eine Million falsche Uhren beschlagnahmt.

Der kleine Unterschied

Es existierten Fälschungen für jedes Kundensegment, sagt Michel Arnoux, der Chef des Bieler Antifälschungsdiensts. «Von Billigstuhren für die Dritte Welt bis hin zu qualitativ sehr hochstehenden Fälschungen, etwa für die Schweiz.» Bei manchen können nur gute Uhrmacher den Unterschied erkennen. Arnoux holt aus der Vitrine eine falsche Hublot Big Bang, die ein Tourbillonwerk hat wie das Original – «nur wurde das Werk eben nicht in der Schweiz, sondern in China gebaut», sagt er. Die Uhren nutzt Arnoux zu Schulungszwecken, etwa um die Zöllner am Flughafen zu instruieren: Die falsche Rolex GMT-Master erkennt man am Band, das aus Plastik statt aus Kautschuk ist, bei der Tissot ist das Etikett verräterisch, auf dem steht, die Uhr sei bis zu 200 Meter wasserdicht: «Bei Schweizer Uhren wird der Wert nicht in Metern angegeben, sondern in bar, der Einheit für Druck.»

Gier macht erfinderisch

Doch manche Fälscher sind besonders erfinderisch: So kaufte ein Mann im Internet für sehr viel Geld eine Rolex aus der Uhrensammlung von Eric Clapton inklusive Bestätigung des Musikers. Dennoch hatte er Zweifel und meldete sich beim Uhrenverband. Michel Arnoux liess die Rolex von seinen Uhrmachern untersuchen, forschte ein bisschen nach, und siehe da: Sie war echt - gefälscht war allerdings die Bestätigung mit der Unterschrift von Eric Clapton, der nie ein solches Modell besessen hatte.

Mache ich mich strafbar?

Seit 2008 ist es verboten, gefälschte Markenartikel in die Schweiz einzuführen – auch für den privaten Gebrauch. Das Verbot gilt unabhängig davon, ob man nun eine gefälschte Gucci-Tasche aus den Ferien mitbringt oder sich eine falsche Omega übers Internet bestellt. Eine Strafe ist bei Privatpersonen nicht vorgesehen, der Zoll darf Fälschungen aber einziehen und vernichten. Ausserdem erhebt der Schweizerische Uhrenverband eine Umtriebsentschädigung in der Höhe von 250 Franken, wenn ein solches Paket beschlagnahmt wird.

Der Antifälschungsdienst weist aber darauf hin, dass man mit dem Kauf von Fälschungen im Internet weitere Risiken eingeht: Einerseits kann das Material, aus dem die Uhren hergestellt werden, mit Schadstoffen belastet sein und so die Gesundheit gefährden. Andererseits: Wer seine Bestellung mit Kreditkarte bezahlt, müsse davon ausgehen, dass die kriminellen Netzwerke die Karteninformationen weiterverkaufen. Im Moment liege der Wert bei rund 100 Dollar pro Karte und damit oft um ein Vielfaches höher als der Kaufpreis für die gefälschte Uhr.

Informationen: www.fhs.ch

WAS IST DAS DARKNET, HERR RUEF?

Um seine Kunden vor Cyber-Angriffen zu warnen, bewegt er sich im tiefsten Untergrund des Internets und am Rande der Legalität: Marc Ruef gibt Einblicke in die dunklen Seiten des Netzes.

interview: Christine Brand fotos: Roland Tännler

Fällt der Begriff Darknet, denkt man an einen düsteren virtuellen Ort, wo man Auftragsmörder anheuern und Sprengstoffgürtel kaufen kann. Ein falsches Bild?
Das Darknet ist vielschichtiger. Auf der einen Seite gibt es durchaus legitime Angebote wie Anonymisierungsdienste, die nicht nur von Kriminellen genutzt werden. So haben während des arabischen Frühlings Aufständische darauf zurückgegriffen, um unbeobachtet vom Regime miteinander zu kommunizieren. Auf der anderen Seite gibt es aber tatsächlich viele dubiose Bereiche.

Das heisst?
Man sieht immer wieder Dinge, auf die man nicht vorbereitet ist. Kürzlich haben wir Material von Terroristen ausgewertet, um deren technische Ausrüstung zu identifizieren. Dabei stiessen wir auf Bilder mit geköpften Menschen. Es ist schwierig, sich das anzusehen. Es gibt auch Foren, in denen man auf noch kaputtere Sachen stösst, die ich gar nicht beschreiben mag.

Versuchen Sie es trotzdem.
Ich sage es mal so: Ich habe mich als Jugendlicher für Horrorfilme interessiert und fand deshalb, ich sei eher eine spezielle Person. Jetzt weiss ich: Meine Fantasien waren harmlos.

Es ist also auch Tatsache, dass man sich im Darknet unbeschränkt Waffen, Drogen oder eben sogar Auftragsmörder kaufen kann?
Es gibt Seiten, die einem nur vorgaukeln, einen Mörder buchen zu können. Aber es existieren durchaus echte Angebote. Die grössten Märkte im Darknet sind jedoch Drogenhandel, Waffenhandel, Handel mit Daten wie Kreditkartennummern und E-Mail-Adressen, Handel mit Medikamenten und mit Pornografie.

Diese Geschäfte florieren, weil sich die Nutzer anonym bewegen können. Wie funktioniert das Darknet?
Das Darknet ist nicht ganz einfach zu definieren. Wir haben einerseits das öffentliche Internet, das wir alle kennen und nutzen. Daneben gibt es das Deepnet, in das man nur schwierig hineinkommt. Das Darknet ist Teil dieses Deepnets.

Sie haben das Internet und das Deepnet in einer Illustration als Eisberg dargestellt. Die kleine Spitze, die aus dem Wasser ragt, ist das Internet. Und darunter …
… liegen unsichtbar das Deepnet und das Darknet. Zugang erhalten Sie nur über spezielle Software wie den Tor-Browser. Er verschlüsselt den Datenverkehr und stellt sicher, dass es nicht mehr nachvollziehbar ist, wer der Absender und wer der Empfänger war. Oft werden die Endpunkte eingeschränkt, damit die Ermittlungsbehörde nicht eindringen kann. Es gibt Foren, in die man nur hineinkommt, wenn man jemanden kennt, der schon drin ist und einen dazu einlädt.

Es genügt also nicht, allein den Tor-Browser zu installieren, um

> «Man sieht immer wieder Dinge, auf die man nicht vorbereitet ist.»

mir Zugang in die Unterwelt des Netzes zu verschaffen?

Zugang erhalten Sie schon. Und nach einigem Suchen werden Sie vielleicht auch die richtigen Seiten finden, um, sagen wir mal, bis zu fünf Kilogramm Heroin oder Kokain zu kaufen. Wollen Sie aber 15 Kilo kaufen, wird es schwieriger.

Warum?

Man muss Beziehungen haben, um das Darknet im grossen Stil nutzen zu können. Man kann nicht einfach www.drogenhandel.ch eingeben. Die Adressen der Webseiten sind sehr kryptisch und lang, und sie wechseln oft. Wenn ein Betreiber merkt, dass die Behörden hinter ihm her sind, baut er seinen Markt an einem anderen Ort unter einer anderen URL-Adresse wieder auf. Wenn man niemanden kennt, der die neue Adresse weiss, verpasst man den Anschluss.

Wie stellen Sie es an, dass Sie solche Einladungen erhalten?

Man muss mit den Leuten kommunizieren, man muss ihre Terminologie kennen, und man muss einen Wert haben für diese Szene. Natürlich benütze ich eine Scheinidentität, doch die muss glaubwürdig sein. Denn Lügen kostet Energie und generiert Fehler. Das ist nicht immer einfach. Im Waffenhandel beispielsweise kann ich nicht als Schweizer Händler auftreten, das ergäbe keinen Sinn. Gebe ich mich aber als Russe aus, muss ich Russisch können. Dann fragt mich vielleicht jemand: Wo bist Du zur Schule gegangen? Darauf muss ich eine schlaue Antwort wissen. Worstcase ist, dass er sagt: Da bin ich auch zur Schule gegangen, warst Du auch bei Lehrer XY? Das könnte wiederum eine Fangfrage sein … Es ist extrem schwierig, sich in solchen Märkten zu bewegen.

Sie arbeiten als privater verdeckter Ermittler im Darknet. Dürfen Sie das überhaupt?

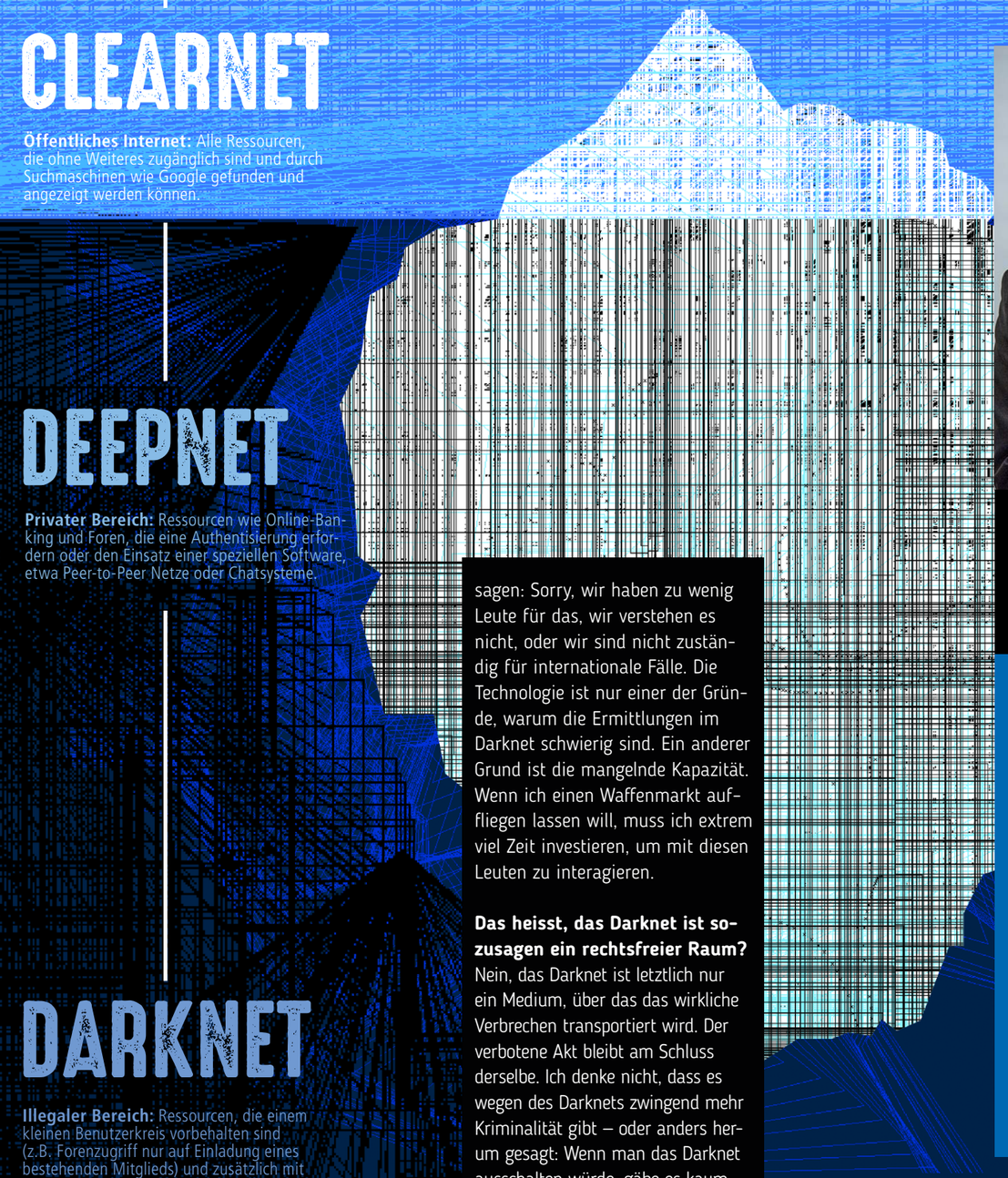
Wir ermitteln zwar für Behörden und Versicherungen. Aber es ist richtig: Wir bewegen uns manchmal juristisch in einer Grauzone. Wir diskutieren darum regelmässig, welche Risiken wir einzugehen bereit sind. Und es kommt vor, dass wir sagen: bis hierhin und nicht weiter. Wir respektieren die Schweizer Gesetze.

Sie stehen mit Verbrechern in Kontakt und warnen ihre Kunden vor Angriffen. Doch sie melden dies nicht der Polizei – ein zweischneidiges Schwert?

Wir müssten der Polizei jeden Tag zig E-Mails schicken. Und sie würde sagen: Sorry, wir haben zu wenig Leute für das, wir verstehen es nicht, oder wir sind nicht zuständig für internationale Fälle. Die Technologie ist nur einer der Gründe, warum die Ermittlungen im Darknet schwierig sind. Ein anderer Grund ist die mangelnde Kapazität. Wenn ich einen Waffenmarkt auffliegen lassen will, muss ich extrem viel Zeit investieren, um mit diesen Leuten zu interagieren.

Das heisst, das Darknet ist sozusagen ein rechtsfreier Raum?

Nein, das Darknet ist letztlich nur ein Medium, über das das wirkliche Verbrechen transportiert wird. Der verbotene Akt bleibt am Schluss derselbe. Ich denke nicht, dass es wegen des Darknets zwingend mehr Kriminalität gibt – oder anders herum gesagt: Wenn man das Darknet ausschalten würde, gäbe es kaum weniger Kriminalität.



Bubentraum: Verbrecher

Als Marc Ruef ein Kind war, sagte er zu seiner Mutter, er wolle einmal der beste Verbrecher der Welt werden. Jetzt ist er auf der anderen Seite gelandet: Er schützt Kunden vor Angriffen im Bereich der Cyber-Kriminalität und warnt sie vor Lecks im Sicherheitssystem. Marc Ruef ist Mitinhaber der SCIP AG in Zürich und publiziert seine Erkenntnisse regelmässig in Fachzeitschriften und Büchern. «Die Kunst des Penetration Testing – Handbuch für professionelles Hacking» gilt als Klassiker.

Wegschauen verboten!

text: Christine Brand

Es ist das traurigste Kapitel der Cyber-Kriminalität und darf deshalb niemals tabuisiert werden: Kinderpornografie macht einen grossen Teil des Darknets aus. Die Arbeit der Fahnder ist oft ein Kampf gegen Windmühlen.

Beige Hose, blauer Pulli, Kurzhaarschnitt über einem erwachsen gewordenen Lausbubengesicht: Auffällig an Michael Meier* ist nichts, ausser den wachen Augen, die gesehen haben, was niemand wirklich sehen will. An einer Wand in seinem Büro hängen Bilder, Artikel, Protokolle zu den Fällen, an denen er und sein Team beteiligt waren. Erfolgsgeschichten, die zum Weiterkämpfen motivieren. «Jeder gelöste Fall, jedes Kind, das nicht mehr leidet, ist die Mühsal dieser Arbeit wert», sagt Meier.

Fahnden im virtuellen Raum

Der Fahnder, der anonym bleiben will, ermittelt in schrecklichen Verbrechen an den wehrlosesten Opfern. Er gehört zu einem Team des Bundesamts für Polizei (fedpol), das sich mit Kinderpornografie im Internet befasst. Die Büros, in denen in einer virtuellen Welt nach realen Sexualverbrechern gesucht wird, bestehen aus ein paar Tischen, ein paar Computern, von draussen ist das Rauschen der Strasse zu hören. Hier durchforsten die Ermittler mit speziellen Programmen das Netz und begeben sich in Bereiche, in denen sie Pädokriminelle vermuten. Für erfolgreiche Ermittlungen in dieser relativ jungen virtuellen Welt sind durchaus alte Qualitäten gefragt: klassische Polizeiarbeit. «Die Täter können selten allein mit technischen Mitteln identifiziert werden», erklärt Michael Meier. «Wenn wir mit Pädosexuellen kommunizieren, müssen wir darum psychologisch geschickt vorgehen. Nur wenn man sich viel Vertrauen erarbeitet hat, gelangt man an eine Mailadresse oder einen anderen Hinweis zur Identität der Kriminellen.»

Meiers Arbeit ist kein Job für jedermann. Wer sich für eine Stelle in seinem Team interessiert, wird schon beim Bewerbungsgespräch mit schrecklichen Bildern konfrontiert. «Wir sehen in unserem Alltag abscheuliche Fotos und Filme, die man sich kaum vorstellen kann», erzählt Michael Meier. Das sei belastend, selbst nach vielen Jahren im Beruf. «An eine solche Straftat gewöhnt man sich nie. Aber man gewöhnt sich ans Betrachten der Bilder und entwickelt eine Art professionellen Scanner-Blick.» Dieser ermögliche es, die wichtigen Elemente sofort zu erkennen und den Rest auszublenden: «Wir können in wenigen Sekunden beurteilen, ob es sich um ein Bild mit strafbarem Inhalt handelt – aber wir registrieren kaum, welche Haarfarbe das Kind auf der Aufnahme hat.»

Keiner arbeitet allein im Büro

In Meiers Team ist niemand länger als vier Stunden am Tag mit Ermittlungen im pädosexuellen Bereich beschäftigt. Kein Fahnder arbeitet alleine in einem Büro. Isolation darf es nicht geben. «Wir reden miteinander über das, was wir sehen, darüber, wie es uns geht.» Die Fahnder werden zudem von Fachpsychologen begleitet, zwei Sitzungen pro Jahr sind obligatorisch. Jeder habe seinen eigenen Weg, mit der schwierigen Arbeit umzugehen, sagt Meier. Für ihn sind seine Familie, seine Kinder wichtig, um Distanz zur Arbeit aufzubauen. «Ich gehe auch oft hinaus in die Natur, das tut mir gut.»

Laut Schätzungen werden weltweit jährlich 20 Milliarden Dollar für Kinderpornografie ausgegeben. Das Internet macht es den Tätern leicht, sich zu vernetzen, an Aufnahmen heranzukommen oder sie zu vertreiben. Kriminelle Organisationen mischen im Milliardengeschäft mit. Wie eh und je findet der Missbrauch von Kindern auch heute vor allem im familiären Umfeld statt. Oft in Ländern, in denen grosse Armut herrscht. An Orten, an denen der Sextourismus boomt. Dort haben sich neue Missbrauchsformen entwickelt: Ein Täter bestellt einen Kindsmissbrauch im Livestream, er wird in Echtzeit via Skype übertragen. So bleibt kein strafbares Material auf seinem Server zurück.

Kampf gegen Windmühlen

Der Einsatz gegen Kinderpornografie im Internet gleicht einem Kampf gegen Windmühlen. «Würden wir uns dauernd das Gesamtproblem vergegenwärtigen, würden wir daran wohl zerbrechen», sagt Michael Meier. «Darum beschäftigen wir uns immer mit dem individuellen Schicksal eines Kindes und versuchen, dieses eine Kind zu retten. Und dann das nächste.» Um zu verdeutlichen, wie er das meint und warum es so wichtig ist, dass das Thema Kindsmissbrauch enttabuisiert und öffentlich diskutiert wird, erzählt Meier eine Geschichte: Ein alter Mann spaziert dem Strand entlang und trifft auf ein Kind, das eifrig Seesterne sammelt und zurück ins Meer wirft – ungeachtet dessen, dass die Wellen immer wieder neue Seesterne ans Ufer spülen. Warum es die Seesterne ins Meer werfe, fragt der Mann das Kind, es spüle doch immer wieder neue an. Es mache keinen Unterschied, wenn es sie einfach liegen lasse. Da schüttelt das Kind den Kopf, hebt einen Seestern auf und sagt: «Für diesen einen Seestern hier macht es sehr wohl einen Unterschied, ob er überlebt.»

Höchstmass an Idealismus

Michael Meier und seine Kollegen müssen für ihre Arbeit ein Höchstmass an Idealismus mobilisieren. Es gibt Niederlagen, die sie müde machen, zweifeln lassen am Sinn ihrer Tätigkeit, an der sie zuweilen fast verzweifeln. Zum Beispiel wenn von einem Kind über Jahre Aufnahmen auftauchen und die Internetfahnder immer wieder von neuem Zeugen seines Missbrauchs werden, ohne etwas gegen sein Schicksal tun zu können. «Es gab einen Fall, an dem wir drei Jahre gearbeitet haben», erzählt Meier. Das Kind wurde zu einem Teil ihrer Welt, sie hatten das Gefühl, es zu kennen – und trotzdem kamen sie nicht an die Täter heran.

Aber es gibt eben auch die Erfolgsgeschichten, von denen die Bilder und Dokumente an Michael Meiers Bürowand erzählen. Gelöste Fälle, bei denen der Missbrauch eines Kindes gestoppt werden konnte, und die zum Weiterkämpfen motivieren, weil sich jeder einzelne gelöste Fall lohnt. «Als Fahnder habe ich schon in vielen Bereichen gearbeitet», sagt Meier. «Aber in keinem anderen hatte ich so sehr das Gefühl, einen Beitrag zum Besseren leisten zu können.»

* Name geändert

Mindestens 3 Meldungen pro Tag

Beim Bundesamt für Polizei (fedpol) befasst sich ein Team von Netztechnikern, Psychologen, Juristen und Kriminalanalytikern mit Meldungen von Personen, die auf verdächtige Internetinhalte gestossen sind, und fahnden nach Webseiten mit strafrechtlich relevanten Inhalten. 2015 gingen bei fedpol 1193 Meldungen zu Internetseiten mit pädosexuellem Inhalt ein, das sind mehr als drei pro Tag. Die Zahl der Meldungen ist zwar rückläufig. Das heisst aber nicht, dass weniger Delikte begangen werden: Die pädosexuelle Szene verlegt ihre Aktivitäten zunehmend ins Darknet, wo sie im Schutz der Anonymität in kleinen Netzwerken funktioniert.

GAMEN, CHATTEN, NAVIGIEREN

Mitarbeitende der Coop Rechtsschutz AG verraten, was sie am Cyberspace fasziniert und auf welche Apps sie setzen.

fotos: Valentina Verdesca

Gian Hess
Kaufmann
in Ausbildung

In meiner Freizeit verbringe ich viel Zeit mit Online-Games, vor allem mit «Counter-Strike». Dann tauche ich von der realen in eine künstliche Welt ab und lerne immer wieder spannende Menschen kennen. Daraus entstehen durchaus reale Freundschaften: Letzten Frühling besuchte ich einen langjährigen Internet-Kollegen in Hamburg und verbrachte mit ihm ein unvergessliches Wochenende.

Auf meinem iPhone habe ich heute nur noch wenige Apps, dafür solche, die ich auch tatsächlich benütze: SBB Mobile, SRF Verkehr, Coop Supercard, Bank Coop, Facebook, WhatsApp und TomTom Europe. Vor allem die TomTom-Navigation ist mir wichtig. In einer fremden Stadt gibt es mir die Sicherheit, immer wieder zum Parkhaus, in dem mein Auto steht, zurückzufinden. Beim Verlassen des Parkhauses schnell ein Foto schiessen, und wenn ich den Weg zurück nicht mehr wissen sollte: TomTom einschalten, «TomTom bitte zurück zu Foto», und schon werde ich zuverlässig zurückgelotst – perfekt!

Paolo Schincariol
Leiter Rechnungswesen

Tobias Mani
Leiter Juristenteam
Rechtsdienst

Ich finde es super, dass ich dank den neuen Technologien auch unterwegs im Zug arbeiten kann. Dies nutze ich fürs Geschäft, aber auch für meine nebenberuflichen Engagements. Sobald ich zu Hause bei meiner Familie bin, versuche ich den Medienkonsum auf ein Minimum zu beschränken. Apps habe ich eine ganze Menge, so zum Beispiel den Guitar Tuner – damit ich die Saiten an meiner Gitarre jederzeit stimmen kann. Und das ohne zusätzliche Kabel oder dergleichen. Das App funktioniert ganz einfach und lässt sich intuitiv bedienen.

Eine Welt ohne Internet? Ich kann sie mir nicht mehr vorstellen. Rasch das Wetter checken, den Weg ausrechnen mit GoogleMaps, eine Behauptung überprüfen mit Google. Auch meine Ferienvorbereitungen laufen weitgehend über das Smartphone, dank TripAdvisor & Co. kann man sich stundenlang mit Hotelbewertungen, Restaurants und Ausflugstipps beschäftigen. Flüge, Hotels oder airbnb-Apartments zu buchen, gehört inzwischen zum Standard. Ich kann mir gar nicht mehr vorstellen, wie das ohne Internet überhaupt funktionieren könnte.

Andrea Mathys
Leiterin Frontoffice
Privatkunden

Joël Fischer
Jurist Rechtsdienst

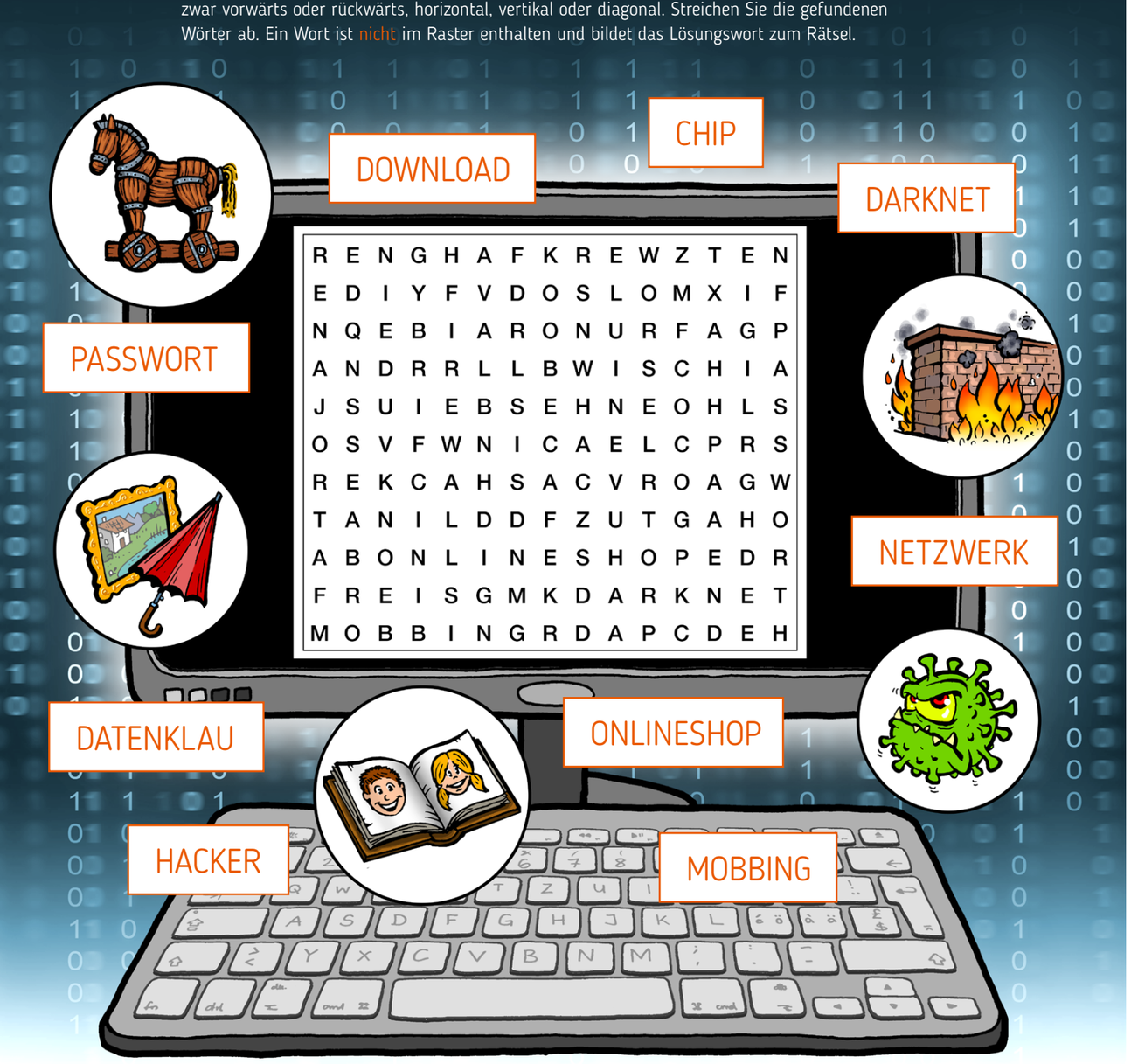
Für die Organisation des Lacrosse-Teams, das ich leite, benutze ich das Angebot von teamplanbuch.ch. Es ist damit ein Einfaches, Termine wie Trainings oder Spieltage zu organisieren, Ämtli zu verteilen und die Mitgliederliste zu verwalten. Der wohl grösste Vorteil ist, dass es eine einfache und übersichtliche Mobile-App gibt, mit der in Sekundenschnelle jedes Mitglied mitteilen kann, ob es an den Events teilnimmt oder verhindert ist. Ferner gibt es Funktionen, um sich auszutauschen, etwa einen Blog, wo jeder Spieler Mitteilungen platzieren kann. Alles in allem ein super Tool, um einen Verein zu organisieren und zu koordinieren.

Ich benutze Apps wie WhatsApp, Facebook, Snapchat und Online-Zeitschriften. In Sekundenschnelle kann ich Freunden Nachrichten schicken oder Erlebnisse in Form von Fotos teilen. Vor allem WhatsApp ist für mich nicht mehr aus dem Alltag wegzudenken. Als ich das erste Mal von dieser App hörte, weigerte ich mich, sie zu installieren. Ich wollte kein weiteres Symbol auf meinem Handy, und per SMS konnte ich bis dahin auch sehr gut kommunizieren. Also lud ich das App erst zwei Jahre später herunter. Plötzlich war auch ich im berühmten Klassenchat, konnte lustige Smileys verschicken, und meine damalige Prepaid-Karte wurde erst noch geschont, da WhatsApp über WLAN läuft und somit kostenlos ist.

Martina Frey
Kauffrau
in Ausbildung

CYBERCRIME-RÄTSEL
Finden Sie das Codewort?

Die geschriebenen und gezeichneten Begriffe sind im Buchstabenraster in der Mitte versteckt und zwar vorwärts oder rückwärts, horizontal, vertikal oder diagonal. Streichen Sie die gefundenen Wörter ab. Ein Wort ist nicht im Raster enthalten und bildet das Lösungswort zum Rätsel.



R	E	N	G	H	A	F	K	R	E	W	Z	T	E	N
E	D	I	Y	F	V	D	O	S	L	O	M	X	I	F
N	Q	E	B	I	A	R	O	N	U	R	F	A	G	P
A	N	D	R	R	L	L	B	W	I	S	C	H	I	A
J	S	U	I	E	B	S	E	H	N	E	O	H	L	S
O	S	V	F	W	N	I	C	A	E	L	C	P	R	S
R	E	K	C	A	H	S	A	C	V	R	O	A	G	W
T	A	N	I	L	D	D	F	Z	U	T	G	A	H	O
A	B	O	N	L	I	N	E	S	H	O	P	E	D	R
F	R	E	I	S	G	M	K	D	A	R	K	N	E	T
M	O	B	B	I	N	G	R	D	A	P	C	D	E	H

Gewinnen Sie ein MacBook!

Beweisen Sie Ihre Qualitäten als «Cybercop»! Wenn Sie die Lösung gefunden haben, schicken Sie uns Ihre Antwort auf dem Datenhighway über www.core-magazin.ch – und gewinnen Sie einen unserer drei tollen Preise!

1. PREIS

Damit sind Sie ganz schön mobil: Das leichte und kompakte MacBook ist der perfekte Begleiter für unterwegs und ein zuverlässiger Partner zu Hause.

2. PREIS

Wo Sie wollen, wann Sie wollen, wie Sie wollen: Das iPad ist Ihr Zugang zur digitalen Welt – handlich, stylisch und leistungsstark.

<page=47>

3. PREIS

Sie werden hören – und staunen: Der Beats On-Ear-Kopfhörer verspricht nicht nur Hörgenuss vom Feinsten. Er bietet ihn.

Das Codewort lautet:

Teilnahmeschluss: 30. November 2016

Senden Sie uns das Lösungswort einfach über www.core-magazin.ch.

Die Gewinner werden schriftlich benachrichtigt. Keine Barauszahlung. Der Rechtsweg ist ausgeschlossen. Über die Verlosung wird keine Korrespondenz geführt. Mitarbeitende der Coop Rechtsschutz AG und deren Angehörige sind von der Teilnahme ausgeschlossen.

TOTAL ABGESPACED

Vor wenigen Tagen erschien das neue Yello-Album «Toy». Es entstand virtuell ohne echte Instrumente. Dafür mit Zutaten, die aus aller Welt stammen. Boris Blank über die befreiende Wirkung des Cyberspace.

interview: Matthias Mächler fotos: Ben Wolf

Inwiefern empfinden Sie den Cyberspace als befreiend?
Ohne die Möglichkeiten des Cyberspace wäre eine Zusammenarbeit wie jene mit Fifi Rong nicht möglich: Sie ist eine der Gastsängerinnen auf dem neuen Album und hat ihren Gesang in Peking aufgenommen und hochgeladen.

Macht Ihnen der Cyberspace auch Angst?
Nein, einzig, dass die Logistik unserer Konsumgesellschaft auf dem Spiel steht. Es könnte ja sein, dass eines Tages das ganze Netz zusammenbricht.

Halblegale Downloads setzen der Musikindustrie zu, die Bands verdienen mit Alben kaum mehr Geld. Wie gehen Yello damit um?
Wir haben das Glück, dass 60 Prozent unserer Fans nicht auf den Kauf eines physischen Tonträgers verzichten. Trotzdem gehen die Gewohnheiten der Musikliebhaber in Richtung Streaming, wo leider viel weniger Geld für den Künstler übrig bleibt.

Sie stellen der Welt Ihre Sounds sozusagen gratis zur Verfügung – mit der Yellofier-App. Warum?
Auf dem Yellofier-App gibt es 6 Banken mit je 8 Sounds, das sind also 48 Klänge. Ich denke, dass ich nach 38 Jahren Yello-Geschichte schon mal was an Sounds springen lassen kann als Dank an unsere Fans.

Ihre Musik entsteht am Computer, ohne physische Instrumente. Vereinsamen Sie nicht bei dieser Arbeit? Oder sind Sie froh, allein arbeiten zu dürfen, weil eh niemand Ihrem Perfektionismus gerecht würde?
Ich arbeitete schon vor Yello meistens alleine. Ich kann mir nicht vorstellen, das zu ändern. Ich brauche diese Ruhe, um meine Klangwerke zu kreieren.

Tragen Sie stets ein Aufnahmegerät bei sich, falls Ihnen ein guter Sound begegnet? Zum Beispiel das Jammern von nassem Tau in Ihren Ferien auf Sardinien?
Immer! Für mich gibt es fast täglich neue Geräusche zu entdecken. Sie werden alle archiviert, um vielleicht irgendwann mal in einen Song eingeflochten zu werden.

Was ist einträglicher: ein neues Yello-Album oder die Musikproduktion für eine Werbekampagne?
Ich glaube, dass gerade heute ein finanzieller Ertrag aus Musik für Werbung wichtig ist, um den Zirkus Yello am Leben zu erhalten. Nur mit den Einkünften aus Spotify-Streamings würde es höchstens für ein Variété reichen.

«FÜR MICH GIBT ES FAST TÄGLICH NEUE GERÄUSCHE ZU ENTDECKEN.»

Sie erhalten jedes Jahr einen anderen wichtigen Preis für Ihr Lebenswerk, zuletzt den IMS Pioneer Legend Award. Man will Sie doch nicht etwa in den Ruhestand ehren?
Wie ich schon beim «Echo»-Preis in Berlin erwähnte: Es ist ein grosses Glück, dass wir all diese Lifetime Achievement-Awards erhalten, solange wir noch jung und voller Tatendrang sind.

Es steht noch ein kleines Wunder an: Ende Oktober treten Yello viermal live in Berlin auf. Dabei hiess es immer, Sie mögen keine Auftritte.
Ich wurde von Ian Tregoning, einem langjährigen Freund aus London, dazu motiviert. Er meinte, dieses Album sei das Beste seit Beginn der Yello-Ära und dass es eine Sensation wäre, diese Musik auf einer Bühne zusammen mit den Fans zu erleben. Er hat mich überzeugt.

Zurück zum Cyberspace: Wenn Sie eine Institution oder eine Person hacken dürften, wer wäre das – und wieso?
Ich wüsste nicht wen. Mir fehlen neben dem Bedürfnis, jemanden zu hacken, auch die technischen Kenntnisse dazu.

Danke!

Liebe Leserin, lieber Leser

Die Coop Rechtsschutz hat seit Jahren starke Partner an ihrer Seite. Nicht zuletzt sie haben uns zu dem gemacht, was wir heute sind.

Dafür bedanken wir uns ganz herzlich bei: Angestellte Schweiz, Atupri, Beobachter, Collecta, Coop, Europäische Reiseversicherung, Gewerkschaft des Zoll- und Grenzwachtpersonals garaNto, Helsana, Helvetia, KPT, Mieterinnen- und Mieterverband des Kantons Bern MVB, ÖKK, Personalverband des Bundes PVB, Personalverband der Suva, Schweizerischer Bankpersonalverband, Gewerkschaft des Verkehrspersonals SEV, Schweizerischer Bühnenkünstlerverband, smile.direct, Patientenschutz SPO, SWICA, Sympany, Syna, Syndicom, Unia, VCS Verkehrs-Club der Schweiz, Verband des Personals öffentlicher Dienste VPOD.