

Ich grüße Euch ganz herzlich!



*

Terminus kooperiert mit Anarchyrissen: <http://www.anarchyrissen.de/tl/Home.htm>

*

“Was wir brauchen, sind ein paar verrückte Leute; seht euch an, wohin uns die Normalen gebracht haben.” (George Bernard Shaw)

*

Konstantin Wecker über Stuttgart 21

<http://www.youtube.com/watch?v=sU0cEA1ssYo&feature=related>

Stuttgart 21 - Warum die Polizei wirklich so hart zuschlug

<http://www.wdr.de/tv/monitor/sendungen/2010/1021/stuttgart.php5>

Kritische Polizisten üben aktuelle Kritik

<http://www.kritische-polizisten.de/>

Juristen zu Stuttgart 21

<http://www.juristen-zu-stuttgart21.de/Home.html>

Agent Provocateurs Polizei

<http://www.radio-utopie.de/2010/10/12/30-september-polizei-prugeleinheit-attackierte-zuvor-in-zivil-schuler/>

Die Bereitschaftspolizeien werden mit neuen Wasserwerfern ausgerüstet.

<http://www.heise.de/tp/r4/artikel/33/33486/1.html>

INFORMATIONEN FÜR POLIZEIBEAMTE

<http://castoreinsatz.110mb.com/>

Nach Ansicht der "Kritischen Polizisten" erreichte Ende September 2010 das rechtswidrige Handeln der staatlichen Organe seinen Höhepunkt. Die "Kritischen", wie sie sich selbst nennen, sprechen davon, dass der Polizeieinsatz im Schlossgarten derzeit noch einmalig sei. Etwas Vergleichbares sei weder bei Auseinandersetzungen bei der Startbahn West, Gorleben, Brokdorf oder dem „Hamburger Kessel“ passiert. Es war rechtswidrig, Wasserwerfer einzusetzen, obwohl man sehr genau wusste, dass sich zahlreiche Schüler im Schlossgarten befinden.

Rechtswidrig war am 30. September auch, dass mehrere Polizeibeamte in Zivilbekleidung ihr Pfefferspray gegen Demonstranten zum Einsatz brachten.

Es war an diesem Tag ebenso illegal, dass Polizeikommissar (POK) Rene Marek mehrfach ohne erkennbaren Grund Pfefferspray gegen Versammlungsteilnehmer eingesetzt hat. Auch wirkt sehr verstörend und unverständlich, warum ihn keiner seiner Kollegen von seiner unerlaubten Tätigkeit abgehalten hat.

Ebenso rechtswidrig war es, dass ein Polizeibeamter einer elfjährigen Schülerin mit der Faust ins Gesicht schlug. Der Mann trug dabei einen Handschuh und trat Mädchen hinterher ins Kreuz. Die Mutter des Opfers war anwesend und kann dies bezeugen. Die Elfjährige befand sich fünf Tage in stationärer ärztlicher Behandlung.

Und auch, dass diverse Beamte bei ihrem Einsatz die Schutzplanen der Schüler hochgehoben haben, um ihnen gezielt Pfefferspray ins Gesicht zu sprühen.

Doch wir sind noch nicht am Ende des Katalogs angelangt. Nicht minder rechtswidrig erscheint der Einsatz eines Wasserstrahls, der gezielt auf einen Rollstuhlfahrer gerichtet wurde. Beim getroffenen Behinderten war auf den ersten Blick erkennbar, dass dieser für die Polizisten absolut keine Gefahr darstellen konnte.

Dass Beamte versuchten mit Hilfe von Wasserwerfern, Personen die in den Bäumen saßen herunter zu schießen, ist natürlich auch durch kein Gesetz gedeckt.

Das Bild des 66-jährigen Rentners Dietrich W., der durch den missbräuchlichen Einsatz des Wasserstrahles ein Auge verlor und auf dem anderen nahezu erblindete, ging durch die Medien und sorgte in der Bevölkerung für Unverständnis und Entsetzen. Es gibt mindestens drei weitere Schwerverletzte, unter anderem einen jungen Mann, dem ebenfalls der Verlust eines Augenlichtes droht.

*

Taste the Waste

<http://www.ardmediathek.de/ard/servlet/content/3517136?documentId=5652488>

Der Film „Taste the Waste“ („Koste den Abfall“ oder „Iss mal Müll“) zeigt in einer wunderbaren Klarheit, wie wir mit unserer Gier nach immer mehr, mit unserem maßlosen und beliebigen Konsum diesen Planeten zugrunde richten.

Plastic Planet

<http://www.youtube.com/watch?feature=related&hl=de&v=-OrQbPAqISY> (6 x 14 min)

Wir sind Kinder des Plastikzeitalters: vom Babyschnuller bis zur Trockenhaube, von der Quietscheente bis hin zum Auto.

Plastik ist überall: In den Weltmeeren findet man inzwischen sechsmal mehr Plastik als Plankton und selbst in unserem Blut ist Plastik nachweisbar!

Plastic Planet und **Taste The Waste**, waren für mich im letzten Monat die eindrucklichsten Dokus zu unserem Umgang mit dem Planeten. Erschütternd! Globales Umdenken ist vorstellbar. Unvorstellbar ist aber, dass eine gewinnorientierte Wirtschaft und Industrie damit im benötigten Umfang beginnt. Also kann das nur vom Regulator, den Regierungen kommen. Diese aber sind mit ihren Politikern hoffnungslos den Lobbyisten ausgeliefert. Diese setzen somit doch ihre Interessen durch und bremsen die nötigen Veränderungen ab. Die Atomkraft ist ein aktuelles Beispiel. Da haben wir als Gesellschaft bisher nicht den nötigen Druck erzeugt und eigentlich schon versagt. Denn der in den letzten 40 Jahren entstandene strahlende Müll, strahlt teilweise noch zehntausende Jahre lang. Und das Problem mit dem Plastik ist vergleichbar komplex. Keiner kann bei beiden Problemen heute sagen, ob es noch kontrollierbar ist. Ich empfinde das als eine "Schuld", die wir uns auflasten. Ich empfinde es als verantwortungslos an dem Planeten und allen seinen Lebewesen und auch an den nachfolgenden Generationen von allen Lebewesen. Von mir aus können wir SOFORT die Produktion von nicht biologisch abbaubaren Plastik und die Produktion von Atomstrom einstellen. Mit allen Konsequenzen die es hat. Denn wir haben nicht die Wahl, wir MÜSSEN damit aufhören!!! Ich habe keine andere Idee, als so wie z. B. in Stuttgart, Druck zu machen und zu protestieren. Und darüber hinaus im eigenen Leben mein Verhalten zu verändern.





Netzwelt

Angriff aus dem Netz



Auf Seiten wie „Darkode“ wird Software für den Online-Betrug gehandelt. Für den BankingTrojaner „SpyEye“ werden 2000 Dollar verlangt.

Wie sicher ist mein Computer? Tagesspiegel-Reporter Harald Schumann machte den Test – und erlebte eine böse Überraschung. Von elektronischen Bankräubern und dem Milliardengeschäft mit der Sicherheitssoftware.

Die Email kam laut Absender vom Chef persönlich. „Interessanter Bericht, bitte lesen“ lautete die Aufforderung in der Betreffzeile, da war das Öffnen der angehängten Datei selbstverständlich. Der Artikel mit vermeintlichen Neuigkeiten über das Enthüllungsportal Wikileaks erwies sich als längst bekannt und war mit dem Drücken des Löschknopfes schon wieder vergessen. Auch dass sich kurz darauf der Rechner plötzlich abschaltete und gleich wieder neu startete, erschien allenfalls lästig – es war schließlich nicht das erste Mal, dass die Maschine abstürzte.

Was sollte schon passieren? Das Virusschutzprogramm der weltbekannten Firma Kaspersky war aktiv und auf dem neusten Stand. „Der Computer ist sicher!“ verhiess die Statusabfrage beruhigend.

Doch dann öffnet sich unvermutet ein Chat-Fenster auf dem Bildschirm. „Hallo, Ihr Computer gehört jetzt mir“, schreibt ein Anonymus da und liefert auch gleich den Beweis. Erst übermittelt er die Liste der Passworte, die im Internet-Browser gespeichert sind und anschließend eine Reihe von „Screenshots“, also Bilddateien, die dokumentieren, wofür der Computer seit dem ungeplanten Neustart genutzt wurde. Wie von Geisterhand bewegt sich sodann der Mausanzeiger, der Eindringling öffnet willkürlich neue Webseiten, und nun verschwindet auch noch der „Start“-Knopf des Windows-Systems. „Soll ich weitermachen?“, fragt er, aber das ist nicht nötig.

Das Experiment ist gelungen: Der Rechner, auf dem dieser Artikel geschrieben wurde, wurde per Internet überfallen – und hätte sich der Angreifer nicht gemeldet, wäre er unbemerkt geblieben.

Ein Angriff aus dem Internet trotz eingeschalteter „Firewall“ und aktueller Schutzsoftware? Ein elektronischer Räuber, der fremde Computer beliebig manipulieren kann? Das mutet an wie eine Szene aus den Thrillern des Schweden Stieg Larsson über die Hackerheldin Lisbeth Salander.

Tatsächlich jedoch geschieht genau das jeden Tag tausendfach irgendwo auf der Welt. In diesem Fall war der Angriff nur eine Demonstration. Dessen Urheber war Peter Kleissner, ein 19 Jahre junger Programmierer aus Österreich, der im Nebenzimmer saß. Schon vor zwei Jahren schrieb er ein Programm, das einen elektronischen Einbruch so gut tarnt, dass kein Schutzprogramm ihn erkennen kann. Als er sein „Bootkit“ bei einem Kongress für Internetsicherheit vorstellte, brachte ihm das den Vorwurf ein, er betreibe das Geschäft von Kriminellen. Doch Kleissner geht es nur um Anerkennung seiner Fähigkeiten. „Ich muss kein Banksystem knacken, um berühmt zu werden“, sagt er lachend. Darum zeigte er auf Einladung auch gern bei einem Besuch im Tagesspiegel, wie verwundbar selbst Geräte mit modernster Software sind. Böse Absichten verfolgte Kleissner nicht.

Im wahren Leben jedoch werden längst Millionen von Computernutzern weltweit Opfer von elektronischen Attacken, mit denen international organisierte Banden jedes Jahr viele hundert Millionen Euro oder Dollar per Online-Betrug erbeuten oder wertvolle Industriedaten stehlen. Von mehr als 50 000 Straftaten über das Netz berichtete das Bundeskriminalamt (BKA) allein in Deutschland schon für das Jahr 2009, 33 Prozent mehr als im Vorjahr. Ronald Noble, der Chef der Weltpolizeibehörde Interpol, warnte gar, „Cybercrime“ sei inzwischen „die größte kriminelle Bedrohung, der wir je gegenüberstanden“.

Dabei sind die Methoden der Netztäter so vielfältig wie das Internet selbst. Mal stehlen sie Kreditkartendaten, um damit auf Kosten der Opfer einzukaufen. Mal schließen sie Tausende gekapertter Rechner zu einem aus der Ferne gesteuerten Netzwerk zusammen, um mit Hilfe dieses „botnets“ ungebetene Werbebotschaften („Spam“) für illegale Pharmahändler zu verschicken. Dann wieder erschrecken sie arglose Nutzer mit plötzlich aufscheinenden Warnungen vor Virus-Infektionen, um sie zum Kauf angeblicher Schutzsoftware zu zwingen.

Den größten Gewinn bringt der elektronische Bankraub. In Deutschland erledigen bereits rund 26 Millionen Bankkunden ihren Geldverkehr vom heimischen Computer aus. Aber immer häufiger gelingt es Online-Tätern, ein Programm einzuschleusen, das Überweisungen auf andere Konten umleitet. Diese illegale Nutzung von Konto- und Kreditkartendaten seien so „einfach geworden wie nie“, warnte vergangenen Monat BKA-Chef Jörg Ziercke. Die „Carding-Straftaten“ würden zum „Ladendiebstahl des 21. Jahrhunderts“. Den Schaden nur im deutschen Online-Banking kalkuliert das Amt in diesem Jahr schon auf 17 Millionen Euro.

Wer wissen will, wie die Täter solche elektronischen Raubzüge betreiben, der stößt auf eine bizarre Untergrundwelt im Netz. Ihr Werkzeug sind die „Trojaner“ – Programme, die über E-Mails und Webseiten auf fremde Rechner geladen werden, ohne dass die Benutzer dies bemerken. Füllen die Opfer dann online eine Banküberweisung aus, wähnen sie sich in Sicherheit. Schließlich müssen sie den Vorgang mit einer geheimen Transaktionsnummer (TAN) autorisieren, die ihnen die Bank vorab zugesandt hat. Doch während der Bankkunde den Adressaten, Kontonummer und Betrag einträgt, wird der eingeschleuste Trojaner aktiv.

Er stellt eine Verbindung mit einem anderen Rechner her und holt sich von dort die Anweisung über das Zielkonto des Angreifers. Diese falschen Angaben sowie den gewünschten Betrag schreibt das Raubprogramm sodann im Hintergrund in das elektronische Formular. Gibt das Opfer schließlich nichtsahnend seine TAN ein und klickt auf den Sendeknopf, wird nur diese andere Überweisung an den Bankrechner übermittelt – samt der eingegebenen TAN. Darum interpretiert die dortige Software die Transaktion als legitim und schreibt den Betrag über meist mehrere tausend Euro einem Empfänger gut, den der Absender gar nicht kennt.

Derlei Raubsoftware ist keineswegs einfach zu schreiben, und doch ist kaum ein Onlinebetrüger selbst ein genialer Programmierer. Denn die digitalen Einbruchswerkzeuge gibt es auf virtuellen Marktplätzen zu kaufen. Einer davon firmiert unter dem Namen „Darkode“. Dort brachte es in diesem Jahr ein Programmierer unter dem Netznamen „gribodemon“ zu Weltruhm. Mit dem Werbespruch „Hack the Planet, take your Money“ wirbt er für den Kauf seines Banking-Trojaners, dem er sogar einen Markennamen verpasst hat. „SpyEye“ heißt das Betrugswerkzeug und war bis vor kurzem für „2k WMZ“ zu haben, das Kürzel für 2000 Dollar in „Webmoney“, das einen Geldtransfer ohne Namen und Adresse ermöglicht (siehe Abbildung).

Wie ein normales Softwareunternehmen bietet „gribdemon“ auch technischen Support und regelmäßige Updates, gegen Aufpreis natürlich. Seine Kunden lobten denn auch „den großartigen Job“ des Herstellers.

Dabei brauchen sich „gribdemon“ und seine Kunden vor Entdeckung kaum zu fürchten. Den Standort ihrer eigenen Rechner können sie verbergen, indem sie den Datenverkehr über Verbindungsserver leiten, deren Eigentümer die Netzadressen oder „IP-Nummern“ ihrer Kunden nicht speichern. Darum können Ermittler selbst beim Abfangen der kriminellen Datenströme nicht erkennen, wo der eigentliche Adressat sitzt. Und darum ist es sogar möglich, mit Mitgliedern der kriminellen Online-Szene ins Gespräch zu kommen.

Folgt man seinen Einträgen auf „Darkode“, dann kennt sich da zum Beispiel ein „Sutekh“ im Onlinebetrug gut aus. Auf Nachfrage berichtet er im verschlüsselt übertragenen und darum abhörsicheren Chat freimütig, dass in Deutschland derzeit vor allem Sparkassen im Visier der NetZRäuber stehen, einfach weil diese „viel mehr Kunden“ hätten als andere Banken. Für ihre Raubzüge bedienen sich er und seinesgleichen „unschuldiger Leute“, die über Stellenanzeigen im Netz angeheuert werden, um „als Vertreter einer Firma XYZ ein Konto einzurichten“. Dessen Daten tragen die Betrüger in die Steuerung des Trojaners für die gefälschten Überweisungen ein. „Dann müssen die Helfer nur noch das Geld empfangen und für eine kleine Provision ins Ausland schicken“, erzählt „Sutekh“. Dort könne man sich mit gefälschten Pässen auszahlen lassen.

Fast immer endet die Strafverfolgung darum bei den oft ahnungslosen Helfern. Nur wenn es den Ermittlern gelingt, V-Leute einzuschleusen und international zu kooperieren, landen auch die eigentlichen Täter im Knast. Im großen Stil gelang dies erstmals Ende September. Da setzte das FBI in der „Operation Trident Beach“ gemeinsam mit britischen und ukrainischen Behörden eine global agierende Gang fest. Ihr Werkzeug war ein Banking-Trojaner namens „Zeus“, mit dem die Bande allein in den USA gut 70 Millionen Dollar erbeutet haben soll und dafür an die 3500 Helfer als Geldwäscher beschäftigte.

Gegen mehr als 100 Täter wurde Anklage erhoben. Der Autor der Zeus-Software, der unter dem Netznamen „sladik“ auftrat, gab daraufhin seinen Rückzug bekannt.

Aber das tut dem Geschäft seiner Kunden keinen Abbruch. „Gribodemon“ kündigte an, er werde sie weiter betreuen und „Zeus“ mit „SpyEye“ zu einem „noch mächtigeren Trojaner“ kombinieren.

Doch so groß die Gewinne der Netzkriminellen sind, so umstritten sind die Methoden, die Behörden und Softwareindustrie zu ihrer Bekämpfung propagieren. Polizei- und Industrievertreter betonen stets, die größte Gefahr sei die mangelnde Vorsicht der Nutzer. Noch immer sei ein Fünftel der Surfer im Internet „ohne Virusschutz“ unterwegs, klagt etwa Dieter Kempf, Vorstand des Branchenverbandes Bitkom. Darum gelte es die „Nutzer zu überzeugen, sich aktiv zu schützen“. Im Klartext: Die Opfer sind selbst schuld und sollten erst einmal die Antivirus-Produkte der Branche kaufen.

Das ist nicht einmal die halbe Wahrheit, und die angepriesenen Schutzprogramme lösen keineswegs das Problem. Denn die Grundlage für den Boom der Internetkriminalität hat zunächst die Industrie für Informationstechnik (IT) selbst gelegt.

Gleich ob Windows oder Apple, ob Adobe mit dem verbreiteten „Reader“ für „pdf“-Dokumente oder die Firma Sun, deren Java-Software auf zahlreichen Webseiten Anwendung findet: Alle großen Hersteller haben über Jahre Programme verkauft, die kaum darauf geprüft wurden, ob sie Angreifer die Türen zu fremden Rechnern öffnen. Erst diese Praxis aber hat die Einfallstore für Online-Betrüger überhaupt geschaffen. Um die Nachfrage auf dem boomenden Internetmarkt zu bedienen, werden die Programme oft viel zu hastig geschrieben. Auf je eine Million Zeilen „Code“ sei daher mit etwa 50 000 Fehlern zu rechnen, kalkulieren unabhängige Fachleute. Betriebssysteme wie Windows bestehen jedoch aus rund 50 Millionen solcher Codezeilen. Nur wenige Fehler führen auch zu Sicherheitslücken. Aber wegen der schiereren Fülle werden die Angreifer bisher immer fündig.

Keineswegs zufällig hat sich deshalb die Produktion von „Sicherheit“ zum lukrativsten Zweig der gesamten IT-Branche entwickelt. Auf mehr als 16 Milliarden Dollar jährlich kalkuliert das Marktforschungsunternehmen Gartner die weltweiten Ausgaben für Sicherheitstechnik und -Software. Binnen drei Jahren werde der Umsatz der Securitybranche sogar noch einmal um 25 Prozent zulegen, erwarten die Marktforscher. Darum bietet derzeit der US-Chip-Konzern Intel für den Kauf von McAfee, den kalifornischen Marktführer für Sicherheitssoftware, mit 7,7 Milliarden Dollar fast das Vierfache des Jahresumsatzes der Firma.

Ob die Rechnung auch für die Kunden aufgeht, ist jedoch zweifelhaft. Denn vielfach versprechen die Verkäufer von „Total Protection“ (McAfee) oder „Internet Security“ (Kaspersky) mehr als sie halten können. Die auf das Testen der Anti-Virus-Software spezialisierte Magdeburger Firma AV-Test berichtet, dass die kommerziellen Schutzprogramme im Schnitt gerade mal drei Viertel der bereits genutzten „Malware“, also schädliche Software, tatsächlich erkennen. Und Tests des US-Prüfers NSS Labs ergaben sogar, dass die von Microsoft kostenlos zum Download angebotenen „Windows Security Essentials“ mehr Schutz boten als die Programme vieler kommerzieller Anbieter, die ihren Kunden bis zu 60 Euro berechnen – und das jedes Jahr aufs Neue. Denn fortwährend kommen neue Schadprogramme in Umlauf. Insofern seien „Virusschutzprogramme“ wahre „Gelddruckmaschinen“, kritisiert Felix von Leitner, ein weltweit gefragter deutscher Experte für IT-Sicherheit.

Eindringlich warnt er vor überzogenen Sicherheitsversprechen: „Die Antiviren führen in der Praxis eher zu mehr Unsicherheit, weil sich die Anwender geschützt fühlen und daher vor gefährlichen Aktionen weniger zögern“. Zudem haben alle Schutzkonzepte ein grundsätzliches Problem: Sie können nur Malware blockieren, die bereits bekannt ist. Die

Technik der Datendiebe ist jedoch so ausgefeilt, dass sie mit wenig Aufwand immer neue Varianten ihres Schadcodes produzieren können.

Entscheidend für den Erfolg der Datenräuber sind jedoch nicht nur diese Fernlenkinstrumente, sondern die Methode, mit der sie zu den Opfern gebracht werden. Der Schlüssel sind „Exploits“, kleine Programme, die gezielt eine Lücke im Internetbrowser, der Bürosoftware oder dem Betriebssystem nutzen, um unentdeckt einen Befehl auszuführen. Ziel ist zumeist, dass im Hintergrund ein fremder Webserver angesteuert wird, von dem dann das eigentliche Schadprogramm geladen wird. Dafür sind E-Mail-Nachrichten mit gefälschtem Absender eher die altmodische Methode. Weit häufiger sind Webseiten, die als Pornoangebot oder Musiktauschbörse getarnt Internetsurfer anlocken und deren Rechner im „Drive-by-Verfahren“ infizieren. Verbreitet ist auch die Zwangsumleitung von einer sicheren Webseite auf solche, die Schadcodes übertragen. Wie leicht das geht, erfuhr vorletzter Woche ausgerechnet die russische Sicherheitsfirma Kaspersky. Stundenlang wurden Kunden auf eine Seite umgeleitet, die ihnen weismachte, ihr Rechner sei befallen und sie müssten ein neues Abwehrprogramm kaufen.

Der Aufwand, den die Angreifer betreiben müssen, steigt allerdings fortwährend an. Aus Sorge um ihren Ruf können die Softwarehersteller das Sicherheitsproblem nicht mehr ignorieren. Microsoft investierte mehr als eine Milliarde Dollar in die Sicherheit des Windows-Systems und bietet regelmäßige Updates gegen neu entdeckte Lücken.

Netzbetrüger setzen daher zusehends auf Schwächen in populären Anwenderprogrammen wie den pdf-Reader oder den „Flashplayer“ von Adobe und die Javaprogramme von Sun Microsystems, die nun auch vermehrt die im Branchenjargon „patches“ genannten Sicherheitsupdates verschicken.

Wer seine Programme stets auf dem neuesten Stand halte, sei deshalb halbwegs geschützt, bestätigt sogar Online-Betrüger „Sutekh“. Der Rat nutzt nur all den Millionen Anwendern wenig, deren Computer Teil eines Firmen- oder Behördennetzwerks ist, auf dessen Ausstattung sie keinen Einfluss haben. Die Mitarbeiter der dortigen IT-Abteilungen wiederum sind mit der Fülle der versandten Lückenschließer aber meist überfordert, weil sie stets erst prüfen müssen, ob die Updates nicht das ganze System durcheinanderbringen. Das „Patch-Management“ sei „ein Riesenproblem“, gesteht ein amtlicher Sicherheitsbeauftragter, der aber lieber nicht genannt werden möchte.

Das gilt sogar für den Bundestag, dessen Verwaltung ein strenges Sicherheitsregime führt. Zehn Abgeordnete und Mitarbeiter aus mehreren Fraktionen nutzten auf Bitte des Tagesspiegels ein Service-Angebot des Technik-Verlages Heise. Dies erlaubt per Internet eine schnelle Überprüfung der jeweils installierten Versionen aller gängigen Programme. Das Ergebnis war ernüchternd. Auf allen geprüften Rechnern lief mindestens ein veraltetes Programm mit bekannten Sicherheitslücken. „Aus Gründen der Sicherheit“ könne man zum Thema aber keine Auskunft geben, erklärte ein Bundestags-Sprecher in unfreiwilliger Ironie.

Doch selbst wenn es irgendwann gelingen sollte, die ganze Online-Welt auf den neuesten Stand zu bringen, wird es wirkliche Sicherheit wohl niemals geben. Über mobile Endgeräte vom Smartphone bis zu den Kartenlesern in Supermärkten wird die Vernetzung immer dichter. Unaufhaltsam wächst so die Zahl potenzieller Sicherheitslücken.

Das Zauberwort für Angreifer wie Verteidiger in der digitalen Welt ist deshalb der „Zero-Day-Exploit“, ein Angriffsprogramm auf Basis bisher unbekannter Lücken, so dass dem jeweiligen Hersteller „Null Tage“ bleiben, eine passende Nachbesserung zu verschicken. „Zero-Days“ können dem Erfinder 50 000 Dollar und mehr einbringen, entsprechend hoch ist der Anreiz für talentierte Programmierer. Die Nachfrage sichert aber keineswegs

nur die Untergrundökonomie. Neues Angriffswerkzeug wird auch ganz legal erforscht und gehandelt. Denn gehackt wird ebenso im Staatsauftrag. Auch Geheimdienste und Polizeibehörden spähen fremde Daten aus, genauso private Sicherheitsdienste.

In dieser Grauzone florieren darum Unternehmen wie die US-Firma Immunity oder deren französischer Wettbewerber Vupen. Beide bieten komplette Bausätze für Hackerangriffe, inklusive eines Abonnements für neue Zero-Day-Exploits. Beide Unternehmen versprechen, ihre gefährlichen Werkzeuge seien nur für ausgewählte Kunden zu haben, die damit ihre eigenen Netzwerke testen.

Doch Fachleute wie Felix von Leitner halten das für unglaublich. Am Ende sei es „nicht verhinderbar, dass auch Kriminelle Zugriff kriegen“, etwa indem sie eine etablierte Sicherheitsfirma kaufen und so als seriöser Kunde auftreten. Aber einen Fortschritt gebe es schon im Kampf gegen den Datenraub, meint Leitner: „Die Sicherheitslücken werden immer teurer.“

31.10.2010, Quelle: <http://www.tagesspiegel.de/medien/digitale-welt/angriff-aus-dem-netz/1969710.html>

"Schwarzsurfen" in ungesichertem WLAN-Netzwerk ist legal

Das "Schwarzsurfen" in unverschlüsselten WLAN-Funknetzwerken ist nicht strafbar. Wer sich in ein offenes Drahtlosnetzwerk einwählt, verstößt weder gegen Telekommunikations- und Datenschutzvorschriften noch gegen das Strafgesetzbuch, entschied das Landgericht Wuppertal. Die Strafkammer verwies unter anderem darauf, dass weder bei der Einwahl noch beim "Schwarzsurfen" personenbezogene Daten im Sinne des Bundesdatenschutzgesetzes abgerufen würden. Auch der Tatbestand des versuchten Computerbetrugs oder des Erschleichens von Leistungen sei nicht erfüllt.

Das Landgericht wies damit die Beschwerde der Staatsanwaltschaft gegen eine Entscheidung des Wuppertaler Amtsgerichts zurück, das den Antrag der Strafverfolger auf Eröffnung der Hauptverhandlung gegen einen "Schwarzsurfer" ablehnt hatte. Die Staatsanwaltschaft hatte dem Internet-Nutzer vorgeworfen, sich mit seinem Laptop in das unverschlüsselte Funknetzwerk eingewählt zu haben, um unrechtmäßig die Kosten für die Internetverbindung zu sparen.

Mit einem WLAN-Netzwerk können Nutzer eine drahtlose Verbindung mit dem Internet herstellen. Oft strahlen solche Netzwerke so weit, dass sie etwa auch für Nachbarn empfangbar sind. Ist das Netzwerk nicht mit einem Passwort geschützt, kann sich der Nachbar auch darin einwählen. Da die meisten Internet-Nutzer heutzutage mit einer sogenannten Flatrate surfen, mit der durch eine Einmalzahlung das monatliche Internet-Surfen komplett abgegolten ist, fällt die Einwahl durch fremde Nutzer in ein Netz auf der Rechnung nicht auf.

20.10.2010, Quelle: http://www.berlinonline.de/aktuelles/nachrichten/detail_afp_CNG.76bffc40879a1f114db98794814242a.631.php



Real Live

Die deutsche Status-quo-Diktatur

Befindet sich Deutschland noch in einer Demokratie? Was können Wahlen in einem Land raffiniert verwobener Interessen überhaupt bewirken? Gedanken eines so verzweifelten wie selbstbewussten Bürgers zur deutschen Status-quo-Diktatur, inklusive einer kleinen Litanei der politischen Tatenlosigkeit.



Jubel vor dem Reichstag am 3. Oktober 1990 zur Wiedervereinigung: Jetzt fehlt nur noch eine Verfassung

Eine seltsame Stimmung herrscht in Deutschland, ein Art rasender Stillstand. Es fällt schwer zu beschreiben, was nicht in Ordnung ist. Die Unzufriedenheit und Unsicherheit der Bürger, die in der Luft liegen, finden keinen Punkt, an dem sie sich kristallisieren, von wo aus sie sich artikulieren und zur Wehr setzen könnten. Denn: zur Wehr wogegen? Es scheint eine neue Situation zu sein, die vielleicht mit der Globalisierung, den Medien oder einfach mit uns selbst als verwöhnten und zugleich überforderten Menschen des 21. Jahrhunderts zu tun hat. Niemand kann sich daran erinnern, so etwas schon einmal erlebt zu haben.

Doch all das gab es schon einmal. Vor sehr langer Zeit. Der Althistoriker Christian Meier hat dieses seltsame Phänomen als eine Krise ohne Alternative bezeichnet und erstmals in den Jahren des Niedergangs der römischen Republik verortet: „Je mehr vonseiten des Senats – oder auch von anderer Seite – im Gemeinwesen reformiert wurde, umso schlimmer wurde es. Denn dann wurden alle möglichen Kräfte wach, weil sie sich plötzlich darin, wie sie sich in dem Gemeinwesen eingerichtet hatten, gestört sahen. ... Das heißt, es fehlte an der gesellschaftlichen Kraft, die die Disposition gehabt hätte, ausgehend von handfesten Interessen und Meinungen die Dinge in eine neue Richtung zu treiben, um in einem Bewusstseinsbildungsprozess schließlich als politische Kraft alternativen Gedanken Resonanz, Materie, Intensität und Richtung zu geben.“

Es kam nicht zur notwendigen Zuspitzung der Krise, die es dem politischen System ermöglicht hätte, sich im Zuge der Problemverarbeitung kontinuierlich weiterzuentwickeln. „Kurz: Man kam nicht auf die Idee, an der überkommenen Ordnung etwas zu verändern.“ Diesen Knoten durchschlug Julius Cäsar im Jahr 46v.Chr. mit der Errichtung der Diktatur.

Die auffälligen Ähnlichkeiten machen es verständlich, dass Christian Meier mit dem Szenario der Krise ohne Alternative schon 1997 die vage gefühlte Malaise der Bundesrepublik erklären wollte. Doch seine Idee von der Krise ohne Alternative errang nur unter Intellektuellen einige Prominenz. Sie konnte aber weder handfeste Interessen in eine Richtung treiben noch den Konflikt zuspitzen und schon gar nicht eine neue politische Kraft bilden.

Eine Erklärung wäre, dass die Krise einfach noch nicht reif genug war. Heute befänden wir uns demnach in ihrem fortgeschrittenen Stadium, und die Symptome wären an Zahl und Intensität gewachsen. Dazu könnte man neben der unaufhaltsamen Wucherung der Kosten in den Sozialversicherungen, der Explosion der öffentlichen Schulden und der Innovations- und Reproduktionsverweigerung inzwischen auch die Verschlimmerungserwartung zählen, die vom Begriff „Reform“ ausgeht.

Die moderne Expertendemokratie wird schon länger von einer an sich harmlosen Inkompetenz-Kompensations-Kompetenz am Laufen gehalten, wie der Philosoph Odo Marquard das einst so schön nannte. Doch allmählich haben die viel gefährlicheren Reform-Folgeschäden-Begrenzungsreformen dieser Scheinexperten das Vertrauen der Bürger erodiert, das für jede demokratische Kultur lebenswichtig ist.

Es gibt inzwischen beunruhigend viele Stimmen, die aus unterschiedlichen Richtungen eine Verschlechterung der Lebens-, Arbeits- und Wirtschaftsbedingungen beklagen, ein ungehemmtes Wuchern der Verwaltungen und darunter das Verschwinden von Initiative, Mut und Zuversicht.

Doch es gibt noch eine andere Möglichkeit, den Verlauf der Krise ohne Alternative zu beschreiben. Vielleicht ist die Krise ohne Alternative schon vorbei – und wir sind bereits

mitten in einer Diktatur! Allerdings wäre das tatsächlich eine historisch neue Form. Kann eine Demokratie überhaupt eine Diktatur sein? Herkömmliche Diktaturen, vor allem die verfassungswidrigen, sind wie auch immer unangemessene Versuche zur Lösung sozialer, wirtschaftlicher oder politischer Probleme durch eine radikale Veränderung des institutionellen Rahmens.

Sie haben meistens sogar einen revolutionären Charakter. Könnte es eine dezidiert antirevolutionäre Diktatur in einer Demokratie geben? Sie würde ausschließlich die Erhaltung der bestehenden öffentlichen Ordnung trotz aller ungelösten und in ihr unlösbaren Probleme betreiben. Das Postdemokratisch-Diktatorische an ihr wäre nicht nur das Fehlen jeglicher politischer Kräfte, die sich einen solchen Systemwandel ernsthaft zum Ziel setzen, sondern vielmehr noch die Komplizenschaft aller etablierten Parteien, die solche Bestrebungen bewusst vermeiden oder sogar unterdrücken.

Das alles ist der Fall in der Bundesrepublik, und den Pakt gegen den Wandel, gar eine Erneuerung des politischen Systems haben ausnahmslos alle im Bundestag vertretenen politischen Parteien mit dem öffentlichen Dienst geschlossen. Dass die politischen Institutionen, der Länderföderalismus, das Verfassungsgericht, das Parlament, die Parteien, das Beamtentum und die Politiker selbst ein wesentlicher Bestandteil des Problems sind, das wird von den etablierten politischen Kräften mit aller Gewalt verdrängt.

Die Bürger spüren das jedoch, und es lässt sie immer mehr zweifeln, ob Wahlen überhaupt noch das richtige Mittel sind, um in dieser Situation am politischen Prozess noch teilzunehmen. Dieser Zustand verdient den Namen einer Status-quo-Diktatur.

Das postdemokratische Prinzip der Status-quo-Diktatur besteht darin, dass es egal ist, wen man wählt, denn es wird sich nach der Wahl nichts ändern. Links und Rechts sind nur noch die schillernden Farben ein und derselben politischen Fata Morgana. Doch an den Rändern, da franst die Bindungskraft der Status-quo-Ideologie langsam aus. Martin Sonneborns Partei Die Partei, Initiativen wie Willi Weise, die 299 Direktkandidaten gegen die etablierten Parteien antreten lassen wollen, die Piraten-Partei und natürlich Horst Schlämmer, all das ist viel mehr als politisches Kabarett, sondern akute Symptome eines schleichenden Legitimationsverlusts, einer Erosion der demokratischen Substanz in den wichtigsten Repräsentativorganen des Staates.

Wie kommen wir aus dieser hoffnungslosen Situation heraus? Es ist eine legale, demokratische Revolution nach Artikel 148 des Grundgesetzes, deren Ziel eine neue Verfassung für Deutschland ist, und das bedeutet nicht weniger als das Abreißen der alten und die gleichzeitige Gründung einer neuen Republik. Die Römer konnten sich einen Verfassungswechsel noch nicht vorstellen – Meier schreibt: „Man hatte nicht eine Verfassung, sondern man war eine Verfassung“ –, wir aber schon, wenn wir es nur wollen.

Carlo Schmid, einer der Väter des Grundgesetzes, machte es am 6. Mai 1949 im Parlamentarischen Rat so deutlich wie nur möglich zu unserer Aufgabe, ganz unabhängig von der Wiedervereinigung eine neue Verfassung und die nächste Republik in Deutschland vorzubereiten. „Auch der Beitritt aller deutschen Gebiete kann dieses Grundgesetz nicht zu einer gesamtdeutschen Verfassung machen.“

Die neue, die echte Verfassung unseres Volkes wird also nicht im Wege der Abänderung dieses Grundgesetzes geschaffen werden, sie wird ‚originär‘ entstehen, und nichts in diesem Grundgesetz wird die Freiheit des Gestaltungswillens unseres Volkes beschränken, wenn es sich an diese Verfassung machen wird.“ Die Beraubung genau dieser Freiheit ist das Wesen und das Ziel unserer Status-quo-Diktatur.

18.09.09, Quelle: <http://www.welt.de/politik/bundestagswahl/article4565626/Die-deutsche-Status-quo-Diktatur.html>

Die Demokratie-Diktatur und der Wandel



Einmal in vier Jahren dürfen wir zwei Kreuze machen. Das war's. Mehr Demokratie ist nicht drin. Trotzdem heißt es im Grundgesetz: "Alle Macht geht vom Volke aus" - nur wo? Oder ist Herr Volke vielleicht heimlicher Bundestags-Chefdiktator? Dann könnte alle Macht tatsächlich von ihm ausgehen - wir sind jedoch ganz sicher nicht gemeint.

Und was wir wählen, ist mittlerweile auch fast egal. Wir wählen eine Friedens-Partei und die beschließen den ersten deutschen Angriffs-Krieg, wir wählen Sozialdemokraten, sie geben uns Hartz 4, wir wählen Politiker, die schwören, die Steuern nicht zu erhöhen, und sie tun hinterher genau das. Sie lügen, betrügen, brechen Wahlversprechen und wir können sie weder dafür zur Rechenschaft ziehen noch vorzeitig abwählen. Ist das Demokratie?

Und für wen? Die Lebens-, Arbeits- und Wirtschaftsbedingungen verschlechtern sich zunehmend, der Einfluss von Lobbys auf die Politiker wird immer größer, die wirtschaftlichen Verbindungen der Abgeordneten undurchschaubar. Ist das wirklich der "Wille des Volkes"?

Die Status-quo-Diktatur

In seinem hervorragenden Aufsatz "Die deutsche Status-quo-Diktatur" in der Zeitung "Die Welt" analysiert Reginald Grünenberg die deutsche Politik und kommt zu dem Ergebnis: Wir leben in einer Diktatur - und zwar in einer historisch recht neuen. Im Gegensatz zu den Diktaturen der Vergangenheit will sie keine revolutionäre Veränderung zugunsten einer neuen Ideologie - im Gegenteil. Sie will das Alte mit aller Macht gegen das Neue verteidigen: eine Status-quo-Diktatur.

Was würde eine solche Diktatur ausmachen?

"Sie würde ausschließlich die Erhaltung der bestehenden öffentlichen Ordnung trotz aller ungelösten und in ihr unlösbaren Probleme betreiben. Das Postdemokratisch-Diktatorische an ihr wäre nicht nur das Fehlen jeglicher politischer Kräfte, die sich einen solchen Systemwandel ernsthaft zum Ziel setzen, sondern vielmehr noch die Komplizenschaft aller etablierten Parteien, die solche Bestrebungen bewusst vermeiden oder sogar unterdrücken.

Das alles ist der Fall in der Bundesrepublik, und den Pakt gegen den Wandel, gar eine Erneuerung des politischen Systems haben ausnahmslos alle im Bundestag vertretenen politischen Parteien mit dem öffentlichen Dienst geschlossen.

[...] Das postdemokratische Prinzip der Status-quo-Diktatur besteht darin, dass es egal ist, wen man wählt, denn es wird sich nach der Wahl nichts ändern. Links und Rechts sind nur noch die schillernden Farben ein und derselben politischen Fata Morgana."

Von innen ist dieses System kaum zu ändern, von außen abzuwählen schon gar nicht - auch wenn sich immer wieder frische Geister auf den "Weg durch die Instanzen" machen. Zu fest ist das alte System etabliert, zu eng die Verbindungen und Machtbündnisse.

Das erkennen auch die Wähler: Sie gehen einfach nicht mehr hin. Die Politiker haben das Vertrauen und die Legitimation durch die Bevölkerung verloren, das System ist als großangelegtes Kasperle-Theater entlarvt. Quatsch- Parteien wie "Die PARTEI" oder Horst "Hape Kerkeling" Schlämmer versuchen mit Humor auf diesen Umstand aufmerksam zu machen. Aber es ist ernst.

Abreißen und Neubauen

Was also tun? Grünenberg sieht die einzige Chance in einer Revolution:

"Wie kommen wir aus dieser hoffnungslosen Situation heraus? Es ist eine legale, demokratische Revolution nach Artikel 146 des Grundgesetzes, deren Ziel eine neue Verfassung für Deutschland ist, und das bedeutet nicht weniger als das Abreißen der alten und die gleichzeitige Gründung einer neuen Republik."

Das ist keine realitätsferne Utopie, sondern sogar vom Grundgesetz so vorgesehen. Unsere derzeitige "Verfassung" ist nämlich gar keine, sondern nur ein Provisorium bis zur Gründung eines neuen gesamtdeutschen Staates: Besonders deutlich hat dies Carlo Schmidt, einer der Väter des Grundgesetzes, am 6. Mai 1949 in seiner Rede zum Parlamentarischen Rat gemacht:

„Auch der Beitritt aller deutschen Gebiete kann dieses Grundgesetz nicht zu einer gesamtdeutschen Verfassung machen. Die neue, die echte Verfassung unseres Volkes wird also nicht im Wege der Abänderung dieses Grundgesetzes geschaffen werden, sie wird ‚originär‘ entstehen, und nichts in diesem Grundgesetz wird die Freiheit des Gestaltungswillens unseres Volkes beschränken, wenn es sich an diese Verfassung machen wird."

Genau das zu verhindern ist nach Ansicht Grünenbergs *"das Wesen und das Ziel unserer Status-quo-Diktatur"*.

Weltweites Symptom

Nun ist aber weder die Wahlverdrossenheit noch die Verfilzung der Politik ein rein deutsches Phänomen. Ähnliches sehen wir weltweit. Es geht also nicht um eine Verfassung oder eine deutsche Revolution. Es geht darum, dass sich die Politik weltweit vom Willen der Menschen abgekoppelt hat und nur mehr als Agent einer Wirtschaftselite arbeitet - oder selbst Teil von ihr ist. Es geht darum, dass ein neues Bewusstsein in den Menschen zu arbeiten beginnt. Und auch wenn sich in den USA die Hoffnung auf "Change" noch verzweifelt (und dank eines riesigen Medien-Aufwands) an einen Politiker hängt - grundsätzlich ist die Politik in ihrer heutigen Form in einer tiefen Krise.

Gleichzeitig breiten sich Ideen, die in den Reden der Politiker und der politischen Diskussion insgesamt kaum Platz finden immer weiter aus - und das unter Menschen, die

sich zum Teil eher als "politikfern" einschätzen würden: Bedingungsloses Grundeinkommen, eine neue Wirtschaftsordnung, Transition Towns, Fließendes Geld, Familienfarmen, Urbane Landwirtschaft, Gemeinschaften und Kooperationen - alles Ideen, die sich ohne Unterstützung durch die Politik, ohne große Diskussion in den Mainstream-Medien aus der Gesellschaft selbst verbreiten. Mit dem Ende des Vertrauens in "die da oben" scheint ein neues Zusammen von "uns hier unten" zu beginnen.

Kritische Masse

Es ist zunächst die Idee selbst, die den Samen zur Veränderung setzt: *"Nichts ist so stark, wie eine Idee, deren Zeit gekommen ist"*, sagte der französische Schriftsteller Victor Hugo. Die Status-Quo-Diktatur hält sich die Augen zu und versucht zu ignorieren, was längst offensichtlich ist: Das alte System ist gescheitert und am Ende. Es wird Zeit für einen umfassenden Wandel, für ein Zeitalter des gesunden Menschenverstandes, der Kooperation und Selbstverwaltung. Das Bewusstsein dazu ist schon hier, verbreitet sich immer weiter, unaufhaltsam.

Die neue Bewegung ist anders, als die Protestbewegungen der Vergangenheit. R. Buckminster Fuller schrieb:

"Du veränderst Dinge nicht, indem Du die bestehende Realität bekämpfst. Um etwas zu verändern, musst Du ein neues Modell erschaffen, welches das bestehende Modell überflüssig macht."

Dieses neue Modell entsteht gerade an Tausenden Orten und in Tausenden Köpfen und Herzen gleichzeitig - fern ab von politischen Diskussionen, außerhalb der Wahlkabinen. Teile davon existieren längst, schon lange. Vielleicht sind wir schon weiter, als wir zu denken wagen. Vielleicht akzeptieren wir selbst insgeheim nicht, dass wir alle noch in alten Kategorien denken, leben und handeln. Vielleicht haben wir alle unsere innere Status-Quo-Diktatur, die uns nicht erlaubt zu sehen, was offensichtlich ist: Dass die Art, wie wir lebten, nicht funktioniert hat. Dass unsere Angst kein Fundament für die Zukunft ist. Dass es Zeit wird, erwachsen zu werden.

"Der Wandel ist geschehen, was wir jetzt beobachten ist nur die Zeitverzögerung zwischen dem Wandel und seiner Realisation und Anwendung im täglichen Leben."

Alles hat sich geändert. Alles. Ergibt euch dem, wie die Natur es tut, oder kämpft, widersetzt euch, leugnet es. Die Welt liegt in unseren Händen."

Und ein afrikanisches Sprichwort sagt: *"Wer glaubt er wäre zu klein, um einen Unterschied zu machen, hat noch nie eine Nacht mit einem Mosquito verbracht."*