MERTON
Onlinemagazin des *Stifterverbandes*

Sandro Gaycken (Foto: David Ausserhofer)

„Eine riesige Überwachungs- und Manipulationsmaschine“

VERÖFFENTLICHT AM 11.03.2016

Das Internet ist längst zum Kriegsschauplatz geworden: Mächtige Player investieren massiv in Überwachungssoftware, ganze Bevölkerungen werden ausspioniert und manipuliert, sagt der IT-Security-Fachmann Sandro Gaycken. Wenige Spezialisten reichen aus, um komplexe Industriesysteme anzugreifen. Neue Betriebssysteme und Hardwarelösungen wären eine Antwort, sind aber noch nicht in Sicht.

LESEZEIT: 13 MINUTEN

TEXT:
ERNST TIMUR DIEHN

FOTOS: DAVID AUSSERHOFER

Ernst Timur Diehn: Noch hält man in den demokratischen Ländern eine optimistische Sicht auf das Internet aufrecht. Man hofft auf Gewinne für die Wirtschaft durch mehr Digitalisierung, auf neue Möglichkeiten für gesellschaftliche Transparenz und auf mehr Netzdemokratie.
Sandro Gaycken: Durch die wenig reglementierte und gleichzeitig kreative erste Wachstumsphase im Internet kam es natürlich zu einer gewissen gesellschaftlichen Befreiung durch mehr Information und Informationsvielfalt. Diese Phase ist vorbei. Es geht jetzt vor allem um Macht, geostrategische Interessen, um Sicherheit und um Kontrolle. Das Internet wird durch reiche und mächtige Global Player neu geformt und umgebaut. Alle Länder, die es sich leisten können, investieren verstärkt in neue Überwachungstechniken. Dabei sind wir technisch heute schon so weit, dass eine vollständige Kontrolle der Kommunikation und bald auch der Bewegungsmuster einer ganzen Bevölkerung möglich sein wird.

Wann immer sich eine neue Opposition über das Internet formiert, wird das der Staat in der Regel früher wissen als die Oppositionellen selbst. Soziale Unruhen oder eine politische Opposition können durch elektronische Überwachung im Keim erstickt werden. Neue Tracking-Software und der Einsatz von Big Data ermöglichen schon bald eine flächendeckende Überwachung der Bevölkerung. Das heißt: Ihr Verhalten wird automatisch erfasst, ausgewertet und dabei sogar antizipiert werden. Und es gibt keine technische Möglichkeit, das zu verhindern. Es wird ein großes Erwachen geben, wenn die Menschen weltweit verstehen, dass das Internet zu einer riesigen Überwachungs- und Manipulationsmaschine umgebaut werden kann. In China erlebt über eine Milliarde Menschen das Internet bereits komplett aus dieser Perspektive.

Gleichzeitig boomt weltweit die Überwachungs- und Ausspähsoftware.
Vor allem Firmen aus den USA, aus Russland, China und auch Deutschland entwickeln Überwachungs- und Ausspähsoftware und liefern diese nach Afrika, Lateinamerika, nach Saudi-Arabien und in andere arabische Länder. Gegen die Bemühungen, diese Aktivitäten wenigstens zu regulieren, gibt es bis heute Widerstand – übrigens auch in Deutschland. Gleichzeitig führen westliche Geheimdienste wie die NSA „Information Operations“, also digitale Propaganda und Sabotage, gezielt über das Internet durch. Die Russen sind in der Ukraine und in Osteuropa in diesem Feld aktiv, unterwandern zum Beispiel systematisch die sozialen Medien, greifen Wahlcomputer an, um Wahlen unglaubwürdig zu machen, und so weiter.

SANDRO GAYCKEN


Sandro Gaycken (Foto: David Ausserhofer)

Sandro Gaycken ist Direktor am Digital Society Institute (DSI) der ESMT European School of Management and Technology in Berlin. Als früherer „Hacktivist“ ist er spezialisiert auf die Gebiete Cyberkriegführung und -spionage und berät neben der Bundesregierung und der NATO auch mittlere und größere Unternehmen in den Bereichen der IT-Sicherheit. In seinem jüngsten Buch „Cyberwar“ beschreibt Gaycken das Internet als Kriegsschauplatz, in dem Hacker immer öfter eingesetzt werden, um Geheimnisse zu stehlen, Wirtschaften zu schädigen, Militäroperationen zu stören oder politische Meinungen zu manipulieren.

Sie beobachten eine Art Wettrüsten im Internet?
Das Wettrüsten um digitale Spionage-Informationstechnologien hat doch gerade erst begonnen. Es ist lange bekannt, dass Hacker kritische Infrastrukturen, die an offenen Netzwerken hängen, weltweit angreifen können. Auch hat man in vielen IT-Systemen sogenannte Backdoors, also Hintertüren, finden können, über die Angreifer auch in komplexe digitale Systeme hineinspionieren konnten. Die Hauptproduzenten von Hardware sind heute die USA und China. Und beide Länder haben sehr starke Interessen, dass solche Hintertüren im jeweiligen System integriert bleiben – für politische Spionage und für Industriespionage.

Sie behaupten ernsthaft, neue Software und Informationstechnologien machen uns nun alle für Cyberangriffe verwundbar? Das heißt: Mein Rechner kann in jedem Augenblick komplett ausgelesen und auch übernommen werden?
Der Skandal um den amerikanischen Geheimdienst NSA hat die relevanten Daten doch längst ans Licht gebracht: Man muss einfach davon ausgehen, dass in Firmen und auch auf Privatrechnern viele Daten und Prozesse mitgelesen und vielleicht auch beeinflusst werden. Dabei bleibt es weiterhin der effizienteste Weg, die Verschlüsselung eines IT-Systems zu brechen, indem man in dieses System durch eine „Hintertür“ einen Fehler einbaut. Wir haben Beweise, dass die NSA die größten und wichtigsten IT-Firmen in den USA dazu zwingt, extraschwache Crypto-Produkte oder sogenannte Default Modes einzubauen, also „IT-

Sicherheit“, die von der NSA einfach umgangen werden kann.

Fehlende IT-Security, das betrifft auch die deutsche Industrie.
In den letzten Jahrzehnten haben sich die Firmen IT-Sicherheit nur vorgaukeln lassen. Es gab keine wirklichen Lösungen, also war man zufrieden, wenn das eigene Ingenieurteam immerhin Standards vorweisen konnte, die zum gleichen Zeitpunkt alle anderen ja auch erreichen konnten. Klar, für die eigene Sicherheit ist letztlich jeder selbst zuständig. Aber hier geht es schon lange nicht mehr nur um klassische Industriespionage: Wer komplexe Maschinen für Kraftwerke und andere kritische Infrastrukturen, für smart factories und Industrie 4.0 verkaufen möchte und dabei chinesische und amerikanische Hardware und amerikanische Betriebssysteme mit verkauft, verkauft da eben auch die systemisch eingebaute Industriespionage gleich mit. Solange Ihre eigenen sicherheitssensiblen Systeme weiterhin gehackt werden können, bedroht das nun auch als Exportfirma das Vertrauen Ihrer internationalen Kunden in Ihre Produkte.

> Heute genügt ein Team von 20 Spezialisten – Hacker, IT-Entwickler und Fachingenieure –, um komplexe Wirtschafts- und Industriesysteme anzugreifen, ohne dass dies vom Gegner schnell genug bemerkt wird.
>
> **SANDRO GAYCKEN**

Sandro Gaycken (Foto: David Ausserhofer)

Dabei könnte die deutsche IT- und Softwareindustrie hier von den Fehlern der Amerikaner profitieren.
Die US-Firmen haben ihr Vertrauen weitgehend verschenkt und bereits extreme Probleme, weiter in kritische Strukturen eingebaut und dort verwendet zu werden. Wir könnten als Alternative neue und erstmals wirklich nützliche Hochsicherheits-IT entwickeln. So könnten wir doch auch unsere Vorstellungen von Datenschutz und Freiheit im Netz technisch umsetzbar anbieten und verkaufen. Denn wenn endlich die Computer sicher wären, gäbe es wesentlich weniger Überwachung, weil Überwachung dann einfach nichts mehr bringt!

Wie reagierte die deutsche Wirtschaft bis jetzt auf die Entwicklungen?
Mittlerweile boomt „IT-Sicherheit“, das heißt, die Lobbyisten technischer Beratungsfirmen stehen bei den Regierungen regelrecht Schlange, um Druck zu machen, möglichst viele kurzfristige Maßnahmen umzusetzen. So kann man seine eigenen „aktuellen“ Produktreihen möglichst gut verkaufen. Dafür werden Konferenzen zur IT-Sicherheit von der IT-Industrie regelrecht gekapert: Man erkauft sich den Platz auf dem Podium und beteiligt sich an der Erzeugung kurzfristiger Hypes. Dabei ergeben sich in der Regel die alten und falschen Lösungen, die schon früher nichts gebracht haben. Viele aktuelle Lösungen, auch bekannter Softwareschmieden in Deutschland, bleiben somit noch unzureichend. Den deutschen Maschinenbauern zum Beispiel ist klar, dass sie hier eine offene Flanke haben. Für eine wirkliche Sicherung von kritischen Strukturen fehlt es in Deutschland immer noch an einer nationalen Implementierungsstrategie. Und es fehlt an Geld.

Und dabei ist nun die digitale Souveränität des Landes, auch die der EU, infrage gestellt?
Der Schutz unserer privaten Daten zum Beispiel bei Facebook ist noch das geringste Problem, mit dem sich Staaten und Gesellschaften in Europa zurzeit beschäftigen sollten. Die aktuellen Sicherheitslücken in sicherheitsrelevanten Systemen, wie sie sich heute auch durch offengelegte NSA-Papiere offenbaren, sind

weit gravierender. Heute genügt ein Team von 20 Spezialisten – Hacker, IT-Entwickler und Fachingenieure –, um komplexe Wirtschafts- und Industriesysteme anzugreifen, ohne dass dies vom Gegner schnell genug bemerkt wird. Ich spreche hier von IT-gesteuerten Kraftwerken, von Wasser- und Stromnetzen, von Banken- und Regierungsdiensten, von sensibler militärischer Infrastruktur. Russland, China, die USA, Frankreich und Israel bauen offiziell ihre Teams von militärischen Hackern weiter aus, die dabei natürlich ihre Kapazitäten für Sabotage und für Cyberspionage so schnell es geht ausdehnen. Rein technisch gesehen besteht schon längst die Möglichkeit, dass zum Beispiel die Stromversorgungssysteme einer Nation so gestört werden, dass man diese über Wochen nicht mehr anschalten kann.

FORSCHUNGSGIPFEL 2016

(Foto: Stifterverband)

Das zentrale Thema auf dem Forschungsgipfel 2016 ist „Digitalisierung“. Dabei spielen auch Aspekte wie IT-Sicherheit eine Rolle. Der Forschungsgipfel bringt Führungspersönlichkeiten und Fachexperten aus Wirtschaft, Wissenschaft, Politik und Zivilgesellschaft zusammen, um gemeinsam Lösungen dafür zu entwickeln, wie die Digitalisierung für den Innovationsstandort Deutschland genutzt werden soll.
Der Forschungsgipfel 2016 findet am 12. April 2016 in Berlin statt. Der Stifterverband wird die Veranstaltung per Livestream ins Web übertragen.

ALLES ZUM FORSCHUNGSGIPFEL 2016

LAHMGELEGTE KRAFTWERKE

In der Ukraine wurde bereits ein Kraftwerk lahmgelegt …
Das war der Fall „Black Energy 3“. Das Ergebnis: 60.000 Menschen ohne Strom. Ein weiteres Beispiel, das die Brisanz der aktuellen Entwicklungen hier aufzeigt: China unterhält eine Anti-GPS-Einheit, die zurzeit so erfolgreich arbeitet, dass es die US-Flotte immer wieder vermeidet, im Pazifik bestimmte Gewässer nahe der chinesischen Küste anzusteuern. Denn dann müssten sie riskieren, dass Chinas Militär die Kontrolle über ihre Raketenlenkungssysteme übernimmt. Auf solche Szenarien sind unsere Bundeswehr, unsere Geheimdienste, aber auch staatliche wie private Anbieter von Energie, Verkehrsüberwachung und so weiter immer noch nicht richtig vorbereitet. Auch das Beispiel Stuxnet …

… der Computerwurm, der in der iranischen Atomanlage Natans die Zentrifugen für die Urananreicherung ausschaltete …
… zeigt, wie weit hier die Entwicklungen gediehen sind. Stuxnet ist so komplex und lief als Programm so reibungslos, dass man sich hier nur sehr finanzstarke und sehr gut organisierte Player als Operateure vorstellen kann, in diesem Fall die USA und wahrscheinlich auch Israel. Und was bedeutet das? Dass alle anderen das inoffiziell auch machen. Oder es gerade erlernen.

Wie könnte man digitale Souveränität überhaupt wiederherstellen? Was sollte national und auf EU-Ebene getan werden?
Wir brauchen dringend mehr nationale IT-Kompetenz auf Bundes- und auf Länderebene. Auch auf der technischen Ebene müsste man mehr Personal ausbilden, das in der Lage ist, wirklich passende Lösungen zu entwickeln und umzusetzen. Für den Aufbau komplett neuer Hardware, also letztlich neuer Computer, die international wirklich konkurrenzfähig wären, müsste man nach Schätzungen circa 1,5 Milliarden Euro Risikokapital bereitstellen. Das wird von der Bundesregierung – jedenfalls im Moment – noch als zu hoch angesehen. Dabei benötigen wir vor allem dringend neue Betriebssysteme und Hardwarelösungen, die in Deutschland selbst entwickelt werden, gerne auch in Kooperation mit kompetenten europäischen Partnern. Einige große deutsche Unternehmen gehen das nun in Eigenregie an. Sie bauen sogenannte Mikrokerne, das sind kleine Betriebssysteme, die sie in ihre eigenen Maschinen und technischen Exportprodukte integrieren. Mittlerweile entwickeln Firmen auch eigene Hardware für Router und ihre eigenen digitalen Netzwerke, um sich zum Teil von den großen Netzen zu entkoppeln. Auch private Nutzer könnten sich ihre eigenen Intranets schaffen. Das ist natürlich aufwendig und natürlich will kein Unternehmer das Sicherheitsthema an die große Glocke hängen und unnötig Aufmerksamkeit auf etwaige

eigene Sicherheitslücken ziehen. Trotzdem halte ich mehr Koordination der großen industriellen Player in Deutschland hier langfristig für die größte Chance.

Wie ist die Lage in der EU?
In Sachen IT-Sicherheit und Datenschutz suchen viele europäische Länder noch ihre eigene Position. Länder, die gezielt ins digitale Zeitalter aufbrechen wollen, möchten nicht durch zu komplizierte Datenschutzrichtlinien aus Brüssel ausgebremst werden. Dazu gehören auch die wirtschaftlich gebeutelten Staaten im europäischen Süden – also Spanien, Portugal oder Italien. Die osteuropäischen Länder machen sich vor allem große Sorgen, was die Russen in ihren Netzen anstellen. Sie brauchen dringend mehr IT-Sicherheit, sind aber gleichzeitig selber stark daran interessiert, ihre eigenen Netze und sozialen Medien im Land auszuspionieren. Die Briten arbeiten in Spionagedingen offensiv mit den USA zusammen. Und die Franzosen wollen vor allem ihre eigenen Lösungen anbieten – wenn sie denn alsbald Lösungen haben sollten. Also misstraut in der europäischen IT-Security zurzeit eher jeder jedem.

Was ist mit dem Vorschlag geschehen, EU-weit das Schengen-Routing einzuführen?
Im Schengen-Routing ging es darum, Daten nur im europäischen Raum zu halten und den amerikanischen und chinesischen Datenhändlern somit nicht mehr zur Verfügung zu stellen. Dagegen wurde mit Erfolg sehr viel Lobby-Widerstand eingesetzt. Auch sind die großen europäischen Telekommunikationsfirmen, die in diesem Fall zum Teil neue Infrastrukturen hätten aufbauen müssen, in den Vorgesprächen nicht immer allzu flexibel aufgetreten. Eine verpasste Chance.

DEUTSCHLANDS DIPLOMATISCHE CHANCE


Sandro Gaycken (Foto: David Ausserhofer)

Gaycken: „Wirtschaftsspionage und Sabotage wird sprunghaft zunehmen“

Wie ist die aktuelle Lage für die Schwellenländer und für die Weltwirtschaft?
Viele Länder, die gerade Schwellenländer der Informationsgesellschaft werden, haben wesentlich weniger kritische Dienste am Internet hängen und sind gegenüber solchen Angriffen wesentlich resilienter als die Hightechindustrie-nationen. Dafür werden diese Länder in fünf bis zehn Jahren selber in der Lage sein, Industriestaaten – inklusive deren Wirtschaftsunternehmen – zu attackieren. Auch solche schweren Cyberangriffe sind ja weiterhin nur sehr schwer zu identifizieren. Aus all diesen Gründen wird digitale Wirtschaftsspionage und Sabotage international sprunghaft weiter zunehmen: Weil sie mit dem heutigen technischen Stand kaum aufzudecken ist, also relativ risikolos und dabei natürlich sagenhaft kostengünstig ist.

Wie geht es nun mit den Themen Zensur und fortlaufende „Information Operations“ weiter?
Hier könnte Deutschland in der Diplomatie eine besondere Position einnehmen, weil wir das alles noch nicht in der Form machen und auch auf keinen Fall damit anfangen sollten. Wird unser Land stattdessen in das Bündnis der sogenannten „Five Eyes“ aufgenommen – also in den Club der Geheimdienste, die direkt mit der NSA zusammenarbeiten –, würde früher oder später jeder glauben, die „Five Eyes“ steckten jetzt auch in jeder deutschen IT-Maschine. Dann stünde auch Hightech aus Deutschland im Verdacht, „Helfer angloamerikanischer Spionage“ zu sein.

Sie malen die Dinge immer so schwarz. Es gibt mittlerweile auch Widerstand aus der kalifornischen IT-Industrie. Zum Beispiel hat sich Apple geweigert, die Sicherheitssoftware für das iPhone zu manipulieren,

und sich darüber mit dem FBI medienwirksam eine Art Schlagabtausch geliefert.
Wir haben im Westen weiterhin ein starkes Interesse daran, hohe Verschlüsselungstechnologien auch in autoritäre Staaten und Diktaturen zu importieren, damit sich dort demokratische zivile Bewegungen überhaupt entwickeln und lebensfähig halten können. Gleichzeitig beschweren sich auch bei uns die Strafverfolgungsbehörden, wenn gute Verschlüsselungstechnik auf den Massenmarkt kommt. Denn dann werden einige Dinge de facto relativ „straffrei“, wo sie nicht mehr über Datenüberwachung aufgeklärt werden. Natürlich könnte man hier wieder mit mehr Personal und Budget, etwa mit eingeschleusten Insidern, mehr klassische polizeiliche Aufklärung betreiben. Aber dafür fehlt, so sagt man, zu oft das Geld. In der Aufklärung des San-Bernardino-Attentats geht es um das iPhone eines Attentäters, das nun entschlüsselt werden soll. Natürlich ist dieser Wunsch gerechtfertigt, aber hier hätten wir einen Präzedenzfall, nämlich, dass Apple seine eigene Software hacken und damit die Hintertür für den Staat eigenständig in das eigene IT-System einbauen soll. Software ist endlos kopierbar. Eine solche Software könnten andere Akteure weiterentwickeln, um damit alle iPhones bestimmter Baureihen zu knacken. Ich bin sicher: Es wird noch zu weiteren Konfrontationen zwischen Apple und staatlichen US-Behörden kommen – zum Beispiel mit der CIA. Ob das hinter verschlossenen Türen weiterhin glimpflich für Apple ausgehen kann, ist unklar.

QUELLE: HTTPS://MERTON-MAGAZIN.DE/„EINE-RIESIGE-ÜBERWACHUNGS-UND-MANIPULATIONSMASCHINE“