

„Jeder kann die intimste Vermarktung des gesamten Lebens gegen Geld zulassen“

Marc Elsberg, Bestsellerautor von „BLACKOUT – Morgen ist es zu spät“ und des Big-Data- und Datenschutz-Thrillers „ZERO – Sie wissen, was Du tust“, findet seine persönliche Science Fiction, die er vor 15 Jahren als Kurzgeschichte konzipierte, gegenwärtig bedrohlich nah in der Realität wieder. Deshalb spiegelt der gelernte Industriedesigner die digitale Big-Data-Wirklichkeit in seinem neuen, umfangreichen Roman. Dessen Basis: Menschen sammeln und verkaufen freiwillig ihre Daten als Teil eines Geschäftsmodells von immer mehr Anbietern. Bei einem Termin in München anlässlich der CeBIT, machte sich der Österreicher Gedanken darüber, wie die Digitalisierung der Wirtschaft unsere Gesellschaft verändert und wie die permanente Datenanalyse unsere Entscheidungsfreiheit limitiert. OBJEKTSpektrum lauschte seinen Ausführungen, dessen Motiv für seinen Stromausfall-Bestseller BLACKOUT vor drei Jahren ganz einfach war: „Ich wollte einen Thriller schreiben.“

Elsberg über die Ambivalenz seiner Bücher

„In BLACKOUT habe ich die Energie-Abhängigkeit unserer Gesellschaft als evident bedrohlich herausgestellt. In ZERO lernt die Hauptfigur, die neuen Technologien zu ihrem Vorteil zu nutzen. Man muss immer zwei Seiten sehen.“

Datenfreigaben

„Der schon länger bestehende Markt des Datenhandels hat sich für den ganz normalen Konsumenten geöffnet. Man erschließt sich hier einen Milliarden-Markt: Wenn Sie entsprechende Incentives haben, z. B. 100 Dollar bekommen dafür, dass man nur seine Daten abgibt, wird das für manchen Niedrigverdiener interessant. Die freiwillige Datenfreigabe sehe ich als eine Demokratisierung des Datenhandels: Jeder kann sein Intimstes preisgeben, die intimste Vermarktung des gesamten Lebens gegen Geld zulassen.“

Einschränkung des Endverbrauchers

„Wenn ich mir überlege, was Google und Co. alles über mich herausfinden! Was bekomme ich für meine Daten? Suchmaschinen, Landkarten, eine ganze Menge. Gesamtgesellschaftlich habe ich das Problem, dass ich das bekomme, was Google gut findet. Bis zu einem gewissen Grad muss ich diese Dienste nutzen, wenn diese Monopole entstehen. Sonst bin ich raus als Endverbraucher.“

Individualisierung und Diskriminierung

„Früher galt ein relativ gleicher Preis für ein bestimmtes Gut in einer Gesellschaft. Jetzt haben wir es mit einer Individualisierung der Preisgestaltung zu tun: Der Einzelne wird diskriminiert, weil er manches gar nicht gezeigt bekommt, wenn er in einer bestimmten Preisgruppe sucht. Bei Versicherungen müssen wir beispielsweise mehr zahlen, wenn unsere Daten ein schlechtes Fahrverhalten verraten.“

Überwachung

„Sie führt zur Konformität, Normierung, Gleichschaltung einer Gesellschaft. Das haben wir von Snowden gelernt. Überwachung stellt eine Bedrohung für eine offene, demokratische, rechtstaatliche Gesellschaft dar. Wie viel Innovation, Kreativität und marktwirtschaftliches Potenzial werden damit genommen?“

Selbstfahrende Autos

„Der Programmierer entscheidet, wer im Fall eines Unfalls dran glauben muss – wer weicht aus, wer crasht, das ist vorher festzulegen.“

Wahrscheinlichkeit

„Wenn ein Kommunikationsmuster auftaucht, das auf einen Terroristen hinweist, wird eine Drohne reingeballert. Mit zehn Prozent Unsicherheit erwischt es eine Hochzeitsgesellschaft oder einen Spritdieb.“

Globalisierung 2.0 und Google

„Was wir momentan erleben durch die Herrschaft der Information über uns alle, vor allem durch einzelne Player wie Google und Facebook, ist eine gewisse Bedrohung. Die können Wahlen entscheiden. Wir wissen nicht einmal, ob Google einen Diskurs beeinflusst, der davon handelt, ob man Google beschränken soll.“

Die selbstregulierende Kraft der Wirtschaft

„Die Unternehmen betonen die Vorteile und kehren die Risiken gerne ein wenig unter den Teppich. Die selbstregulierende Kraft der Wirtschaft funktioniert nicht immer oder sie funktioniert in ziemlich brutaler Art und Weise. Wenn ich zu wenige Regeln mache – das haben wir in den Finanzindustrien in den vergangenen zwei Jahrzehnten gesehen – haben wir lauter Runs and Busts, weil diese Wirtschaften keinerlei Verantwortungsbewusstsein zeigen und irgendwelche seltsamen Dinge konstruieren, die die gesamte Weltwirtschaft an den Rand des Abgrunds bringen. Das reguliert, aber auf eine Art und Weise, die Milliarden Menschen in die Trägerschaft zieht. Das ist ein schwieriger Grad: Wie viele Regeln setze ich, bevor etwas völlig erstarrt? Wie viele Regeln lasse ich weg, bevor solche Wellen entstehen können?“

Chancen durch die Digitalisierung der Wirtschaft

„Ich bin relativ optimistisch, dass sie uns auf lange Sicht nach vorne bringen wird. Technologie und komplexitätsschürende Gesellschaft haben im letzten Jahrhundert zu einer gesamtgesellschaftlichen Wohlstandssteigerung geführt, mit Auf und Abs. Natürlich hat es auch Verlierer gegeben. Im Gesamtbild lebt jeder von uns heute besser als jeder Kaiser vor über 100 Jahren. Wir sollten versuchen, die Digitalisierung in einer für möglichst viele Menschen möglichst verträglichen Weise zu gestalten. Immer mehr Menschen werden beides gleichzeitig sein: Kunde und Produzent. Ob das in der Energiegewinnung ist, mit Solaranlage auf dem Dach, in der Produktion, wo ich mir mit dem 3D-Drucker etwas ausdrucken kann, oder im Crowd-Sourcing. Ich bin sehr gespannt, ob das neue Geschäftsmodelle herausbringt. Ebenso, wie sich in den nächsten fünf Jahren das Machtverhältnis gestalten wird, das dem einzelnen sehr viele Möglichkeiten der Mitbestimmung und Gestaltung gibt.“

Maschinen statt Menschen

„Seit dem Aufkommen der Künstlichen Intelligenz setzen wir den Prozess fort, menschliches Handeln an Maschinen auszulagern. In der Automobilindustrie arbeiten Menschen plus Roboter. Jetzt übernehmen die Maschinen intelligente Aufgaben: Im Controlling, bei Versicherungen, im Investment-Banking. Hoch qualifizierte Leute werden von Maschinen abgelöst und es gibt sogar



Foto: Annegret HandekKempf

Marc Elsberg (47) wollte nur einen Thriller schreiben. Doch jetzt brennt er für das Thema Digitalisierung im Spannungsfeld der Gesamtgesellschaft.

Überlegungen, einen Roboter, ein Programm zu einer eigenen Persönlichkeit zu machen, die rechtsversicherbar ist. Das klingt nur kurios, aber schon lange sind Unternehmen Rechtspersönlichkeiten. Ausreichend Arbeitsplätze zu erhalten, die die Menschen ernähren, wird zum Problem.“

Die digitale Zukunft

„Was machen die Menschen? Junge Männer in der Blüte ihrer Jahre kommen auf dumme Ideen und fangen Kriege an, siehe arabische Staaten. Lagert das denkende Tier Mensch immer mehr an Maschinen aus, die schlauer sind als wir? Was bleibt von diesem denkenden Tier? Werden wir unser Menschenbild umgestalten müssen?“

„Die Angriffe beginnen mit gezieltem Social-Engineering“

Thomas Uhlemann, Security-Experte bei ESET, sprach vor Journalisten in München über die Security Trends 2015.



Foto: PREVIEW.

Security-Experte Thomas Uhlemann beklagt den Mangel an Sicherheitsbewusstsein

Gesundheitsattacken

„Laut US-amerikanischem Identity Theft Resource Center (ITRC) wurden 2014 bei insgesamt 720 Vorfällen, von denen 304 den Gesundheitssektor betrafen, 81.597.485 Datensätze gestohlen.“

Advanced Persistent Threats (ATP)

„Zielgerichtete Angriffe mit maßgeschneiderten Methoden auf Unternehmen nehmen zu, bleiben aber

oft lange Zeit unentdeckt. Die Angriffe beginnen mit gezieltem Social-Engineering¹⁾ der Mitarbeiter.“

Höhere Wahrscheinlichkeit von 0-Day-Bedrohungen²⁾

„Bekannteste Beispiele unserer Analysen sind die ‚BlackEnergy-Kampagne‘ und die ‚Windigo-Operation‘.“

Erpressung

„Verschlüsselungstrojaner verlangen Geld für einen Entschlüsselungscode. Manche Erpresste zahlen, um den Code für die Entschlüsselung zu bekommen. Aber der Code kann die Daten nicht zurückholen. Nur mit sehr viel Geld und über viele Jahre Arbeit kann eine einzige Datei wieder entschlüsselt werden.“

Bequemlichkeit

„Beim Sony-Vorfall an Weihnachten war nichts gesichert. Wir sind eine Plug&Play-Gesellschaft. Wir packen die Fritz Box aus und nutzen sie, ohne Drumherum. Das voll vernetzte Haus kann dann locker von außen genutzt werden, vor allem bei einem Passwort wie 1,2,3.“

Internet der Dinge

„Das wird ein Riesentrendthema sein. Es erleichtert den Alltag und Verkauf ungeheuer. Man muss jedoch beizeiten daran den-

¹⁾ Anm. der Redaktion: Zwischenmenschliche Beeinflussung, um an vertrauliche Informationen zu kommen.

²⁾ Anm. der Redaktion: Ausnutzen einer Sicherheitslücke, bevor ein Patch als Gegenmaßnahme entwickelt wurde.

ken, das Thema sicher zu halten. Besonders das Smart Home. Wenn wir die Heizung übers Internet einschalten, läuft das über Heimrouter. Viele Bot-Netze bestehen nur aus Heimroutern.“

Smart TVs

„Wenn ich dort Kreditkartendaten drin habe – für Maxdome, Amazon-Einkäufe etc. – sind Internet-Fernseher, die nicht speziell geschützt sind, gefährlich. Wenn dort Bewegungssensoren und Kameras eingebaut sind, bin ich voll zu sehen. Diese Frage sollte ich mir stellen: „Was passiert mit den Daten, die mein Fernseher aufzeichnet, wo gehen die hin?“ Jeder sollte fünf Minuten pro Tag investieren, um sich über neue Methoden und Technologien für Sicherheit zu informieren.“

Vernetztes Geld

„Schadcodes werden verstärkt für Bezahlssysteme und Internet-Währungen entwickelt. Bitcoins erleben weiter eine große Verbreitung. Sie sind viel wert und dadurch interessant für Angreifer. Ein Hacker stahl mithilfe eines Netzwerks von kompromittierten Maschinen digitale Währungen im Wert von 600.000 Dollar. Durch infizierte NAS-Geräte hat der Angreifer einen Ordner namens ‚PWNED‘ erstellt, der ein Programm mit dem Namen ‚CPU Miner‘ enthielt, mit dem Bitcoins und Dogecoins generiert werden konnten. Bei dieser Art von Angriff werden die Nutzer nicht direkt bestohlen. Mithilfe der Rechenleistung der infizierten Computer wird neues Geld erzeugt: Eine neue Art des Stehlens.“

Mehr Sicherheit für Cyber-Geld

Der Online-Handel boomt – auch dank Bitcoin. Derzeit entspricht ein Bitcoin (BTC) rund 290 Euro. Die erhoffte Anonymität dieser virtuellen Währung hängt von den so genannten Bitcoin-Adressen ab. „Sie sind Decknamen, unter denen die Anwender öffentlich einsehbar ihre Transaktionen durchführen und dokumentieren. Lassen sich diese Decknamen auf die realen Personen dahinter zurückführen, ist die Anonymität von Bitcoin gebrochen“, erläutert Aniket Kate von der Universität des Saarlandes.



Foto: Universität des Saarlandes, Manuela Meyer

Forscher Aniket Kate will mit einem neuen Verfahren Internet-Währungen sicherer machen

Ähnlich wie bei dem Netzwerk „Tor“, das anonymes Surfen im Internet ermöglicht, bilden bei einem neuen Verfahren aus Kates Excellencecluster mehrere Bitcoin-Nutzer ad hoc eine Art verschworene Gemeinschaft. Um die Herkunft ihrer Überweisungen zu vertuschen, hält sich jeder von ihnen an eine vorab festgelegte Abfolge, dem von Kate und seinem Team entworfenen CoinShuffle-Protokoll. Jeder Teilnehmer entschlüsselt die ihm zugesandte Liste mit Empfänger-Adressen, fügt seine eigene ein und schickt die Liste verschlüsselt an den nächsten weiter.

„Das Ergebnis ist eine Liste von Adressen, die keine Hinweise auf die Auftraggeber dahinter gibt. Um Missbrauch auszuschließen, überprüft jeder die nun veröffentlichte Liste“, sagt Kate. Doktorand Tim Ruffing hat die Kunde davon bereits in die Bitcoin-Gemeinde getragen. „Momentan programmieren mehrere Entwickler unseren Ansatz nach, um diesen in ihre Bitcoin-Clients zu integrieren“, so Ruffing.