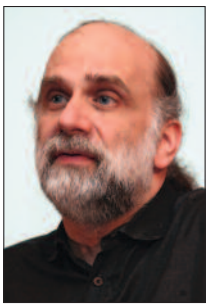
Wertvolles Gut: Für biometrische Daten könnte sich ein Schwarzmarkt entwickeln.

Neue Gefahren erkennen

IT-Experten berichteten auf der IT-Defense 2015, welche neuen Gefahren für die Sicherheit der Informationstechnologie bestehen und wie man mit ihnen umgehen kann.

Der unter dem Pseudonym „Starbug“ bekannte Spezialist für biometrische Systeme berichtete auf der IT-Defense 2015, die am 4. und 5. Februar in Leipzig stattgefunden hat, über Versuche, Smartphones, in die man sich per Fingerabdruck einloggen kann, mit Nachbildungen des Fingerabdrucks des Berechtigten zu täuschen. Da der verwendete Sensor auf Kapazitätsunterschieden zwischen den Papillarlinien aufbaut, ist das Verfahren gegenüber einem optischen Sensor insofern aufwendiger, als durch Ätzverfahren ein 3D-Modell des Fingerabdrucks erstellt werden muss.

Dennoch hat der hergestellte Dummy ausgereicht, die Zugangsberechtigung zu erhalten, weil biometrische Erkennungssysteme zwangsläufig größere Toleranzen zulassen müssen. Nicht nur wegen der besseren Lesbarkeit sollte also die Glasplatte von Handys sauber gehalten werden. Die technischen Möglichkeiten des Diebstahls der biologischen Identität reichen aber bereits weiter. Fingerkuppen können bei entsprechender Handhaltung und geeigneter Optik samt hoher Auflösung fotografiert und letztlich kopiert werden.



Bruce Schneier: „Verträge sollten regeln, dass kein Staat als erster einen Cyberwar beginnt.“

Die meist in Hochsicherheitsbereichen eingesetzten Iris-Erkennungssysteme arbeiten im Infrarot-Bereich, was bedeutet, dass ein Schwarz-Weiß-Abbild der Iris ausgewertet wird und die Farbe der Iris („Augenfarbe“) nicht von Bedeutung ist. Das Schwarz-Weiß-Bild macht es einfacher, mit einem handelsüblichen Drucker Fakes herzustellen, die vom System akzeptiert werden. Personen, deren Iris als Erkennungsmerkmal herangezogen wird, sollten vermeiden, dass ihre Gesichtspartie mit hochauflösenden Kameras fotografiert wird. Es könnte sogar möglich werden, Kontaktlinsen mit einem entsprechenden Irismuster herzustellen.

Auch Gesichtserkennungssysteme konnten durch Vorhalten entsprechender Abbilder getäuscht werden. Die Lebenderkennung, die auf Bewegungen etwa der Augenlider beruht, wurde durch kurzes Abdecken des Bildes simuliert. Auf der Hornhaut des Auges, besser aber beispielsweise auf Sonnenbrillen, spiegelt sich bei entsprechen-

Fotos: JohanSwanepoel/Fotolia, Kurt Hickisch

den Lichtverhältnissen das wider, worauf der Betreffende schaut, beispielsweise auf sein Smartphone oder sein Tablet. Etwa die Eingabe von Passwörtern aus dem Spiegelbild am Auge mitzulesen, befindet sich noch im Experimentierstadium und beruht vor allem auf einer hohen Bildauflösung, doch haben Fotos mit Handys mit einer Auflösung von 13 Megapixel schon brauchbare Ergebnisse geliefert.

Biometrische Daten sind insofern wertvoll, als sie nicht verändert werden können. Es könnte sich ein Schwarzmarkt für solche Daten entwickeln.

Biohacking. Neue Organismen im Do-it-yourself-Verfahren zu entwickeln, scheint laut Dipl. Biol. Rüdiger Trojok nicht mehr abwegig zu sein. Über die Netzwerkplattform *hackteria.org* kann die entsprechende Laborausrüstung bezogen werden. Die 2009 eingerichtete Plattform versteht sich als Sammelbecken für Wissenschaftler und Hacker auf dem Gebiet der Biotechnologie. Dem Open Source-Prinzip folgend, sollen Informationen und Tools allgemein zugänglich sein und allgemein genutzt werden können. 2011 wurden bei einem von *DIYbio.org,* einer weiteren Organisation dieser Art, veranstalteten Kongress ethische Grundsätze der informellen Biotechnologie erarbeitet.

Möglicherweise ist diese Öffnung gegenüber der Forschung ein Weg, die Krise zu überwinden, die derzeit durch die steigende Resistenz von Bakterien gegenüber Antibiotika gegeben ist. Die Entwicklung neuer Wirkstoffe hinkt demgegenüber nach. Während 1990 noch zehn neue Antibiotika auf den Markt gekommen sind und 18 Unternehmen auf diesem tätig waren, wurden 2011 nur mehr zwei neue Antibiotika entwickelt, und es gab nur mehr vier einschlägige Unternehmen. Globale Zusammenarbeit könnte helfen, Gesundheits- und ökologische Probleme zu lösen. Neues Wissen schafft allerdings neue Verantwortung. Gesetzliche Bestimmungen werden anzupassen sein.

Cyber-Abwehr. Wie soll auf Cyber-Angriffe größeren Stils geantwortet werden? Bruce Schneier hat die Attacken auf ein südkoreanisches Unternehmen Ende 2014 zum Anlass für die Frage genommen, mit welcher Sicherheit gesagt werden kann, ob ein Staat

Ross Anderson: „Die Technik muss dem Menschen so weit entgegenkommen, dass er intuitiv das Richtige macht."

Leo Martin: „Bei Vernehmungen so weit Stress aufbauen, dass dem Gegenüber keine Zeit mehr zum Überlegen bleibt."

oder etwa doch nur eine autonome Gruppe hinter solchen Angriffen steckt. Im Gegensatz zu konventioneller Kriegsführung gibt es keine Unterschiede in der Art der verwendeten Waffen; niemand deklariert sich, die Gefahr von Missdeutung und unberechtigter Schuldzuweisung ist groß. Durch internationale Verträge sollte geregelt werden, dass kein Staat als Erster mit Cyberwar beginnt, keine zivilen Ziele angegriffen werden und dass sich die eingesetzten „Waffen" nach einer bestimmten Zeit selbst zerstören.

Bill Cheswick verglich die Entwicklung von Sicherheitseinrichtungen im Automobilbau seit dem *Ford-T*-Modell 1913 mit den Autos der heutigen Zeit. Beispielsweise wurden Sicherheitsgurte erst in der Mitte der 1960er-Jahre eingeführt. Etwa zehn Jahre später wurden die ersten Personal-Computer entwickelt. Die Sicherheitseinrichtungen auf diesem Gebiet hinken noch nach. Dennoch müsste es mit den heute zur Verfügung stehenden Erkenntnissen und Mitteln gelingen, sichere Programme zu schreiben, die weder vom User noch von Angreifern von außen verändert werden können.

Security Engineering. Dass Sicherheit viel mit Psychologie zu tun hat, war Kernthema des Referats von Prof. Ross Anderson, Cambridge. Sicherheit muss gelebt werden. Die Technik muss dem Menschen so weit entgegenkommen, dass er intuitiv das Richtige macht: „Schauen, wohin die Leute gehen, und dann den Weg anlegen." Macht man es umgekehrt und an den Gewohnheiten der Menschen vorbei, werden sie sich einen anderen Weg suchen. Es genügt nicht, Regeln aufzustellen und Vorschriften zu erlassen. Immerhin ist es geradezu eine Drohung, „Dienst nach Vorschrift" zu machen. „Blame and train" ist nicht der optimale Ansatz.

In der Automobil- und der Flugzeugtechnik ist es evident, dass schwere Folgen eintreten, wenn am Menschen vorbei konstruiert wird. In der Informationstechnologie ist man noch nicht so weit. Entstehen im Geldverkehr über Internet Schäden, wird schnell eine Regelung gefunden werden, die der User nicht beachtet hat, sodass der Schaden an ihm hängen bleibt. Hätte man nicht umgekehrt das System mehr dem User und seinen Gewohnheiten anpassen können?

Nach einer Studie von Harold Thimbleby 2008 kommen in Großbritannien jährlich etwa 2.000 Menschen in Spitälern durch Fehler in der Anwendung medizinischer Geräte ums Leben – etwa so viele wie bei Verkehrsunfällen. Folgt man der Studie, ist schon die Verwendung von Taschenrechnern wegen der Vielfalt der Funktionen problematisch: Sie können we-

FOTOS: KURT HICKISCH

IT-DEFENSE

Infos für IT-Spezialisten

Seit 2003 veranstaltet die cirosec GmbH jährlich an jeweils wechselnden Orten in Deutschland die IT-Defense. Der Teilnehmerkreis setzt sich aus IT-Spezialisten sowie Sicherheitsbeauftragten von Behörden, Polizei und Militär zusammen. Die Anzahl der Teilnehmer ist mit 200 begrenzt. Die Vorträge an zwei Tagen bilden den Kern der Veranstaltung. Am Tag davor wird ein Hacking-Seminar angeboten, um Angriffstechniken und deren Abwehr kennenzulernen. Am vierten Tag werden Themen in Gesprächsrunden (Round Tables) vertieft, wobei sich diese Themen erst im Lauf der Vortragsveranstaltung auf Grund der Nachfrage ergeben können.

Die cirosec GmbH, Heilbronn, ist ein IT-Beratungsunternehmen mit dem Schwerpunkt Informations- und IT-Sicherheit. Die nächste IT-Defense wird vom 27. bis 29. Jänner 2016 in Mainz stattfinden.

www.it-defense.de

sentlich mehr, als ein Arzt oder eine Krankenschwester beruflich jemals braucht – was etwa bei der Berechnung der Dosis von Medikamenten zu Fehlern führen kann. Infusionspumpen sollten Programme eingebaut haben, die Eingabefehler erkennen, um Fehldosierungen zu vermeiden.

Die Vielzahl elektronischer Geräte, die im Krankenhausbetrieb eingesetzt werden und kein einheitliches Design in den Bedienungsfunktionen aufweisen, macht laut Anderson ein User-Interface-Engineering im Sinne des Gestaltens einheitlicher Benutzeroberflächen erforderlich, um Eingabefehler oder Fehlbedienungen wegen ungewohnter Bedienfelder hintanzuhalten.

Psychologie spielt auch dabei mit, dass sich Delikte mehr ins Internet verlagern. Nach dem British Crime Survey werden jedes Jahr eine Million Menschen Opfer von Beschaffungsdelikten wie Einbruch oder Fahrzeugdiebstahl – Täter und Opfer stehen einander mehr oder weniger gegenüber („Face-to-Face"). Die modernen Varianten wie Phishing, Auktions- oder Lotteriebetrug fordern doppelt so viele Opfer, doch wird nur ein Zehntel dieser Straftaten geahndet. „Die Kriminalität wird nicht weniger, sie verlagert sich bloß ins Internet".

Die Evolution der menschlichen Intelligenz wird nach der gängigen Auffassung darauf zurückgeführt, dass der Mensch gezwungen war, immer bessere Werkzeuge herzustellen. Anderson stellte die Macchiavellistische Theorie vor: Die Entwicklung ist erfolgt, um andere besser ausnützen und als Werkzeug benützen zu können. Dann wären Betrug und Täuschung, und das Erkennen dieses Verhaltens, der Schlüssel für die Entwicklung der menschlichen Intelligenz.

Technische Mittel, Täuschung und Lügen zu erkennen, waren der 1935 zum ersten Mal getestete Polygraph („Lügendetektor"), bei dem durch Messung verschiedener physiologischer Parameter wie Blutdruck, Puls, Atmung, Hautleitwiderstand und den Vergleich dieser Werte mit einem Normalzustand herauszufinden versucht wird, ob eine Person lügt. Ein erhöhtes Aktivitätsniveau deute auf Nervosität und damit auf Lügen hin.

Anderson berichtete über Versuche, mit Hilfe von „Motion Capture" die Bewegung des ganzen Körpers, insbesondere der Extremitäten, zu erfassen.

Personen, deren Iris als Erkennungsmerkmal herangezogen wird, sollten vermeiden, dass ihre Gesichtspartie mit hochauflösenden Kameras fotografiert wird.

Bei dem Verfahren, das aus der Herstellung von Animationsfilmen bekannt ist, werden am Körper, speziell an Händen, Armen, Beinen und Füßen Sensoren angebracht. Bewegungen werden in der Folge erfasst, in ein strukturiertes Bild umgerechnet und ausgewertet. Ergebnis war, dass zu 82 Prozent zutreffend erkannt wurde, ob eine Person lügt oder die Wahrheit sagt. Wahrheit wurde zu 89 Prozent erkannt, Lügen zu 76 Prozent. Dass Wahrheit besser erkannt wird als Lügen, wertet Anderson als Schutz für Unschuldige.

Lügen erkennen. Ohne technische Hilfsmittel, mit bloßem Beobachten der Reaktion des Gegenübers, kommt Leo Martin aus, der unter diesem Pseudonym auch Bücher („Ich krieg dich!" „Ich durchschau dich!") veröffentlicht hat. Martin war beruflich für einen Nachrichtendienst als Ermittler im Bereich der organisierten Kriminalität tätig, musste aus Menschen Informationen herausholen und Vertrauensleute anwerben. „Lügen ist eine hochkomplexe Angelegenheit. Man muss bei Vernehmungen so weit Stress aufbauen, dass dem Gegenüber keine Zeit mehr zum Überlegen bleibt." Im Stress wird nicht mehr rational abgewogen, sondern die Entscheidung auf Angriff oder Flucht eingeengt. Entweder sagt der Einzuvernehmende gar nichts mehr (ein Indiz, in die Enge getrieben worden zu sein) oder er verrät sich selbst.

Den Aufbau von Stress bezeichnet Martin als „Stresstreppe". Je näher sie dem Schockzustand als oberer Grenze kommt, umso kleiner wird der Handlungsspielraum. Mit Probanden wurde auf der Bühne durchgespielt, wie diese Vorgänge ablaufen. Das Saalpublikum wurde eingebunden, mit verblüffenden Ergebnissen, die gezeigt haben, wie bei Spannungsaufbau Nachdenken und Überlegen gegenüber kurzen Befehlen ausgeschaltet werden.

Will man einen Menschen, auch im Alltagsleben, für sich gewinnen, geht es darum, dessen Grundbedürfnis auf Wertschätzung und Anerkennung zu befriedigen. Person und Verhalten müssen voneinander getrennt werden. Bewusst soll auf das Positive im anderen geachtet werden, man muss ihn sein Gesicht wahren lassen. Und man soll ihm das Gefühl der Sicherheit geben, auf den Gesprächspartner vertrauen zu können. *Kurt Hickisch*

FOTO: LASSEDESIGNEN/FOTOLIA.COM