Herzlichen Glückwunsch :-(

Wer glaubt, dass Schweizer Steuer-CDs zu richtigem Unwohlsein in Teilen der Bevölkerung führen, dem möchte ich sagen: vielleicht heute noch. Denn schon morgen sind es möglicherweise ganz andere Inhalte auf billigen Datenträgern, die deutlich machen, wovor Datenschützer bereits vor vielen Jahren gewarnt haben. Jetzt malen wir mal bewusst den Teufel an die Wand und glauben die Schlagzeile: USA – Angst vor gehackten Herzschrittmachern. Geht der Trend zur Tele-Technik unaufhaltsam weiter, erhält vielleicht bald jedes noch so kleine Gerät eine eigene IP-Adresse.

Ich ahne, worauf Sie hinaus wollen, Kollege Mühlberger: Dann werden Datenträger mit IP-Adressen und Zugangscodes ebenso wertvoll – zwar nicht für unseren Staat, dafür aber für dunkle Kräfte in unserer Gesellschaft. Während bisher meist nur von personenbezogenen Daten gesprochen wird, betritt ein solches Szenario das nächste Level im Kampf um die Sicherheit digitaler Daten.

Exakt, Dr. Zimmermann. Meist ist im Zusammenhang mit dem Verlust von Patientendaten von Imageschaden, Bußgeldern oder Strafvorschriften die Rede. Wenn die ‚Black Hat' allerdings Ernst machen, wird vielleicht so manchem braven Bürger nicht nur die Luft wegbleiben, sondern auch das Herz stehen bleiben. Wie leicht Daten im falschen ‚Endlager' landen können, haben wir ja erst in Hamburg gesehen. Dort lagen Akten, die zur Vernichtung vorgesehen waren, nicht im Sicherheitscontainer, sondern im Behälter daneben.

Ich gebe zu – ein ungutes Gefühl, Mr. Mühlberger. Wie wichtig das Thema Datenschutz und Datensicherheit im Gesundheitswesen ist, hat der BVMed Mitte März auf seiner MedInform-Konferenz mit Nachdruck betont. Dort kamen Berater, Anwälte und IT-Spezialisten zu Wort, die viele Facetten digitaler Daten beleuchtet haben. Mir ging das allerdings immer noch nicht weit genug.

Ich teile Ihre Meinung, Monsieur Zimmermann. Wir Medienvertreter haben Zugang zu zahlreichen Informationsquellen, die wir dazu nutzen sollten, Zusammenhänge zu bilden. Damit können wir heute auf die Chancen und Risiken der Zukunft aufmerksam machen. Und selbst wenn medizinische Geräte bisher nur unter Laborbedingungen gehackt wurden, bietet allein die Vorstellung genügend Anlass zur Besorgnis.

Jeder Computerfreak kennt vermutlich die Suchmaschine www.shodanhq.com, wo weltweit ‚offene' Systeme mit einem Mausklick gefunden werden können. Haben die Black Hat erst einmal die Pain Points lokalisiert, bleibt der Zero Day Exploit nicht aus.

Ok – für die Praktiker unter uns: Die von den bösen Buben gefundenen Schwachstellen in Systemen oder Softwareprogrammen werden sehr schnell per Hackerangriff mit schlimmen Absichten ausgenutzt.

Ganz recht, Kollege. Stuxnet und Duqu haben uns gezeigt, dass Viren, Würmer und Trojaner nicht in der Office-Welt bleiben. Die Schädlinge dringen nun auch tief in unsere Technikwelt ein, wo sie viel schlimmeren Schaden anrichten können als das Löschen einer Festplatte. Ein Beispiel: Wie die Redaktion pressetext berichtet, hat im August 2011 ein US-Sicherheitsexperte während einer Konferenz seine eigene Insulinpumpe gehackt. Dabei war das Gerät lediglich durch einen sechsstelligen Code geschützt – für Hacker und ihre Brute-Force-Attacken eine Aufwärmübung vor dem Frühstück.

Genau, lieber Dr. Zimmermann. Und selbst wenn von Geräteherstellern mit Nachdruck darauf hingewiesen wird, dass nur wenige Geräte Kommunikation über größere Distanzen zulassen, werfe ich ein: heute noch. Hat ein solches Gerät eine IP-Adresse, was dann? Ich meine, so weit sollten wir es nicht kommen lassen. Vielleicht ist es besser darüber nachzudenken, ob die Fernwirktechnik tatsächlich vollkommen ausgereizt werden muss. Am Regler für die Insulinpumpe, am Taktgeber für den Herzschrittmacher und an vielen weiteren wichtigen Gerätschaften sollte eine Grenze gezogen werden.

Tja, Mühlberger. Und da beruhigt es mich nicht zwangsläufig, wenn ich höre, dass Gerätehersteller die Handhabung personenbezogener Daten von einer 128- auf eine 256-bit-Verschlüsselung umstellen wollen. Das genügt vielleicht beim Versand von Arztbrief-Diktaten, bei lebenswichtigen medizinischen Geräten allerdings ist ein komplettes Sicherheitsmanagement mit Virenscanner, VPN, Firewall und einer Statefull Inspection unerlässlich – also der zustandsorientierten Paketprüfung.

So schön jeder von uns Handys und dauernde Erreichbarkeit, permanente Online-Informationen auf dem Smartphone sowie Apps und eBooks schätzt, so gefährlich ist Fernwirktechnik, wenn es um lebenswichtige Angelegenheiten geht. Es wäre schön, wenn das von den Medizintechnikern rechtzeitig erkannt würde. Im anderen Fall kann ich mich nur sarkastisch äußern: Herzlichen Glückwunsch zum ultimativen Fortschrittsdenken.

Und das aus Ihrem Munde,
Herr Ingenieur! :-(

Eugen Mühlberger
Dr. Wolf Zimmermann