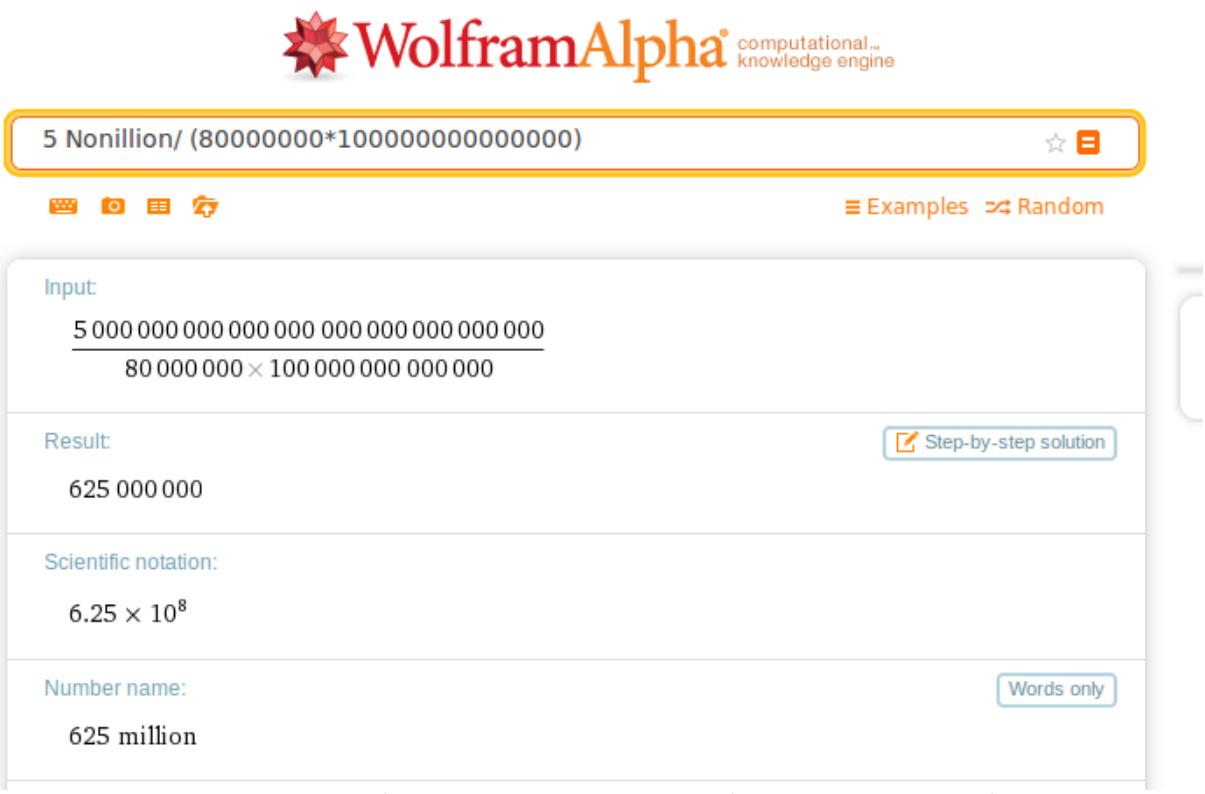
Vernetzte Bedrohungen verlangen nach vernetzten Verteidigungsstrategien!

Von Joachim Jakobs

Die Sicherheit der Sicherheitsbehörden ist bedroht: Insbesondere beim BND stehlen die US-Dienste wie die Raben. Jetzt werden wieder Schreibmaschinen angeschafft.

Die amtliche Hilflosigkeit ist kein Einzelfall – tatsächlich sind die Kombinationsmöglichkeiten aus Angreifern, Angriffsmitteln/ -wegen und Angegriffenen endlos: Geheimdienste, Mafiosi, Industriespione, Terroristen – oder auch Cyber-Söldner – klauen analoge Daten auf Papier und digitale Informationen auf elektronischen Speichern, physikalisch (per Einbruchdiebstahl) oder übers Internet. Mal mit, mal ohne die Unterstützung von „Innentätern“ – bei Behörden und Unternehmen. Und zwar seit Jahren – nur wollten wirs nicht sehen. Die Scherben unserer Ignoranz fallen uns jetzt vor die Füße.



Nach der Berechnung der Suchmaschine Wolfram Alpha wären im „Internet der Dinge“ ausreichend IP-Adressen vorhanden, um alle Körperzellen aller Bundesbürger 625 Millionen Mal durchzunummerieren.

Auch die Leistungsfähigkeit gehört dazu: Immer mehr Informationen können auf immer kleinerem Raum gespeichert und immer schneller übertragen werden. Die Angreifer nutzen künstliche Intelligenz, um damit verbundene menschliche und technische Schwächen automatisiert aus zu nutzen, die Angegriffenen meinen, sie hätten nix zu verbergen. Dieser digitale Graben droht explosionsartig zu

wachsen – die Dinge sollen „intelligent“ werden: Im kommenden Internet „der Dinge“ (IPv6) verfügt rein rechnerisch jeder der 80 Millionen Bundesbürger über 62,5 Trillionen IP-Adressen. Damit ließe sich jede der 100 Billionen Körperzellen eines jeden Bundesbürgers 625.000.000 Mal - weltweit einmalig – durchnummerieren. Diese Leistungsfähigkeit ermöglicht es, Politik, Wirtschaft und Gesellschaft in beliebiger Detailtiefe zu vernetzen. „Smart“ soll sie sein, die Zukunft.

Möglichkeiten und Wünsche sollten im Einklang stehen mit den Fähigkeiten derer, die Entscheidungen zur Informationsgesellschaft fällen, oder auf Basis dieser Entscheidungen Software entwickeln, implementieren oder nutzen, um diese „intelligenten“ Anlagen zu steuern oder personenbezogene Daten zu verarbeiten.

Ansonsten könnten uns Dritte das Fell über die Ohren ziehen: „Bonesaw“ kennt jedes Endgerät am Internet – samt seiner Löcher. „Turbine“ kann diese Geräte infizieren. Die Inhalte von Texten, gesprochener Sprache, Bildern, Handschriften und Videos

Der Tetraeder der Informationsgesellschaft: Möglichkeiten, Wünsche und Fähigkeiten sollten eine stabile Basis bilden – sonst droht das Risiko des Zerfalls. Bild: Martina Schettina

lassen sich maschinell erkennen und die beteiligten Personen können anhand ihrer biometrischen Merkmale identifiziert werden. Die Beute aus dem einen Raubzug läßt sich kombinieren mit der aus beliebig vielen Anderen. Der Verschlüsselungsexperte Bruce Schneier ist der Ansicht: „Bald wird Alles was wir tun, on- und offline, aufgenommen und für immer gespeichert. Die einzig verbleibende Frage ist, wer Zugang zu all den Informationen hat.“ Solche Informationen werden heute vielfach mit Hilfe von SAP

verarbeitet: Kaum ein DAX-Konzern kommt ohne die Software der Walldorfer – für Funktionen wie dem Controlling oder dem Personalwesen – aus. Zwei Dutzend Branchenanwendungen treiben die Produktivität in Wirtschaft und Verwaltung. Künftig werden aber auch Gebäude, Heizungen oder Fahrzeuge vernetzt. Wirbt SAP. Die „Dinge“ bieten sich Spionen und Saboteuren an. So debattieren Experten derzeit, ob sich ein ganzes Land mit Hilfe eines „Generalschlüssels“ zu SAP lahmlegen ließe – für Innentäter mit den Fähigkeiten von Edward Snowden sicher ein Kinderspiel. Wobei: 'SAP' ließe sich austauschen – etwa durch „Windows“.

Die US-Bundespolizei (FBI) meint, sie würde den Cyberkrieg „nicht gewinnen“. Die Angreifer scheinen schneller zu lernen als die Angegriffenen – und könnten ähnliche Schäden verursachen wie am „11. September“.

Wir haben es offenbar mit einer vernetzten Bedrohung zu tun. Daher sind vernetzte Antworten gefordert – nicht unbedingt von denen, die über Geld, Macht und/oder Einfluß verfügen. Aber diese Spezies sollte dafür sorgen, dass das Gespräch in Gang kommt – etwa zur Frage, wie die 4482 Seiten „IT-Grundschutz“ vom „Bundesamt für die Sicherheit in der Informationstechnik“ (BSI) in Millionen Institutionen in unserem Land implementiert werden können.

Tatsächlich kommen die Maßnahmen nur schleppend in Gang: Ein Verband ist stolz auf 2000 Teilnehmer seines Projekts „(m)IT Sicherheit“. Bei 30 Millionen Arbeitnehmern ein Tropfen auf den heissen Stein.

Und ob von diesen 2000 Personen auch nur eine in der Lage wäre, den Europäischen Computerführerschein ECDL zu absolvieren oder bei ihrem Arbeitgeber ein Projekt für ein Sicherheits- oder ein Notfallkonzept angeschoben und erfolgreich abgeschlossen hat?

Eine der Ursachen dieses Erfolgsmangels liegt sicher darin, dass sich die Mittelstands-Maßnahmen gegenseitig kanibalisieren. Hinzu kommen Angebote für die Hoteliers und die Handwerker. Und natürlich die Ärzte. Die Kassenärztliche Vereinigung Rheinland-Pfalz bietet 2014 vier Termine an, bei denen den dortigen Ärzten Datenschutz-Informationshäppchen im Viertelstunden-Takt geboten werden. Bildung in einem einzelnen Bundesland in der 15-Minuten-Terrine!

Die zweite Mängelursache besteht in der künstlichen Trennung der natürlichen Vernetzung - und das auch noch nach Bundesländern separiert!

Der Höhepunkt des Aufklärungs-Aktionismus: Der 'Deutschland sicher im Netz e.V.' will Anwälte und Steuerberater dazu gewinnen, die Sensibilität ihrer Klienten zu erhöhen. Hoffentlich hat der Bock eine Umschulung genossen, bevor er seine Tätigkeit als Gärtner aufgenommen hat!

Das Klein-Klein führt dazu, dass die Medien nicht berichten – das Argument der Macher: „Wenn ich diese eine Veranstaltung vorstelle, wollen fünf andere auch genannt werden.“ Die Debatte über Fähigkeiten und Verantwortung der Handelnden bleibt aus. Der umworbene Mittelstand nimmt das Angebot nicht einmal zur Kenntnis. Und die Veranstaltungen bleiben leer: Die Resonanz ist so schlecht, dass Journalisten nicht einmal an den Veranstaltungen der Ärzte teilnehmen **dürfen**. Das Ergebnis des Gewurschtels dokumentiert eine Pressemeldung Ende Mai: „Nach einer aktuellen Umfrage von Deutschland sicher im Netz (DsiN) führen nur 28 Prozent der Unternehmen regelmäßige Schulungen für Mitarbeiter durch. Damit ist dieser Wert seit 2011 unverändert, obwohl die Digitalisierung des geschäftlichen Alltags im selben Zeitraum zugelegt hat.“ Andere formulieren ihre Erkenntnis knackiger: „Mittelständler sind stark bedroht und schlecht gerüstet.“

Wir müssen unkonventionelle Wege gehen, wenn wir nicht alle zur Schreibmaschine zurückkehren wollen: Ich versuche das mit SicherKMU und „Frei+Fit im Web 2.0“. Beim ersten Projekt handelt es sich um eine monatliche Kolumne, die Aspekte vom BSI-Grundschutz anschaulich aufgreifen, die Zusammenhänge erläutern und eine Lösung vorschlagen soll. Im Rahmen der zweiten Initiative will ich mit einem „Datenschutzmobil“ durchs Land fahren und die Teilnehmer der Informationsgesellschaft für ein Sicherheitsbewußtsein begeistern. Jeder ist aufgerufen, diese öffentliche Debatte mit eigenen Vorschlägen zu fördern – und wer immer mich dabei unterstützen möchte, kann mir gern schreiben an info@privatsphaere.org.

Das Datenschutzmobil – Blickfang und idealer Werbeträger 3DModell: Dosch Design Grafik: Hannes Fuß, CC-BYNCND