Der bürgerliche Traum von digitaler Souveränität

Technische Bemerkungen zur völligen Unsicherheit digitaler Kommunikation

Hartmut Pohl

In der digitalisierten Welt *interagieren Computer* zunehmend in allen Lebensbereichen über Handys, Smartphones, Tablets, Wearables … Sensoren wie Rauchmelder, Kameras bis hin zum Gesundheitsbereich (Insulinpumpe, Herzschrittmacher etc.), um private, behördliche und unternehmerische Prozesse (Akquise, Einkauf, Verkauf, …, Strom- und Wasserversorgung etc.) sowie Maschinen in der Produktion – vernetzt zu steuern. Soweit die politisch korrekte Formulierung.

Tatsächlich wird jegliche digitale (und auch die analoge) Kommunikation von Interessierten wie der Organisierten Kriminalität und den Sicherheitsbehörden *vollständig abgehört* („jedes Gerät, überall, jederzeit"). Gespeicherte Daten (Forschungsdaten, Personendaten, Meinungen, Dokumente, Bilder, Industriesteuerungen – auch von (Kern-)Kraftwerken, Wahlergebnisse, Gesundheitsdaten) werden vollständig ausgelesen oder werden per Tauschhandel von Anderen erworben. Alle abgehörten und ausgelesenen Daten werden für die – eventuell zukünftige – Auswertung gespeichert. Diese Daten werden auch bei Bedarf (fast) in Echtzeit *manipuliert*.

Einschlägige Spionage- und Sabotagesoftware sowie Auswertungssoftware (Tools) wird – weit überwiegend selbständig oder als Auftragsarbeit für Sicherheitsbehörden – von der *Organisierten Kriminalität* entwickelt, am Markt angeboten und auch selbst benutzt. Einige Sicherheitsbehörden erwerben diese Tools und geben sie ggf. an andere weiter. Nach zwei bis vier Jahren werden diese Methoden, Verfahren und Tools Allgemeingut. Letztlich entsteht dabei ein umfangreicher Markt weltweit von der OK vertriebener Produkte.

Technische Sicherheitsmaßnahmen wie Firewalls, Intrusion Detection und Protection Systems, Antivirenprogramme, digitale Signaturen, Verschlüsselungen – auch Ende–zu-Ende etc. – werden umgangen oder geknackt, Implementierungen werden mit Backdoors und Sicherheitslücken versehen. Technische Maßnahmen helfen daher weder gegen Abhören noch gegen Manipulationen. So ist z. B. die

M. Friedrichsen (Hrsg.), *Digitale Souveränität,* DOI 10.1007/978-3-658-07349-7_2

Ende-zu-Ende Verschlüsselung nur sicher, wenn sie selbst und die erforderliche umfangreiche Sicherheitsinfrastruktur tatsächlich sicher implementiert sind – also z. B. keine Backdoors und Sicherheitslücken enthalten. Kompromittierungen wurden in der Vergangenheit allerdings schon mehrfach bekannt. Das Sicherheitsniveau, der Widerstandswert gegen Angriffe lässt sich vielleicht etwas erhöhen – jedenfalls aber nicht signifikant.

Schengen-Routing und Euro-Routing nutzen genauso wenig wie deutsche Clouds, weil Server, Router, Gateways in den Netzen vollständig überwacht werden.

Die Mehrheit der *Bürger* argumentiert heute, sie habe nichts zu verbergen – nur 21 % der Bürger sind über die Risiken sehr beunruhigt. Dies ist verständlich angesichts der technisch heimlichen (stealth) im Hintergrund ablaufenden Aktivitäten im virtuellen Raum. Regierungen klären nur unvollständig auf – sei es auch nur technischer Art. Bisher haben die Bürger mehrheitlich noch gar nicht ihre eigene Abhängigkeit und die Abhängigkeit der gesamten Gesellschaft von der – dank Organisierter Kriminalität und Sicherheitsbehörden – unsicheren IT erkannt und auch nicht erkennen können. Je mehr Unternehmen und Bürger diese Unsicherheit erkennen, umso stärker könnte die unternehmerische und private Internetnutzung zurückgehen. Nur durch völlige Abstinenz vom Internet und der Digitalisierung (Verweigerung) können sich Unternehmen und Bürger gegen Überwachung überhaupt wehren.

Allein das *Eindringen in Computer* kann durch Identifizierung der Sicherheitslücken und deren Behebung verhindert werden.

Tatsächlich wird also

- jegliche digitale (und auch die analoge) technische Kommunikation vollständig abgehört,
- werden gespeicherte Daten (Texte, Kontodaten, Steuerdaten, Gesundheitsdaten) vollständig ausgelesen und
- alle Daten werden für die – eventuell zukünftige – Auswertung gespeichert.
- Kommunikation und gespeicherte Daten werden bei Bedarf manipuliert.

Der *bürgerliche Traum* von technischer Vertraulichkeit, Integrität, Authentizität, Anonymität, Freiheit, Gleichheit, Netzneutralität, Privatheit, Verfügbarkeit etc. im Internet bleibt daher ein unerfüllbarer Traum. Dies wissen die Regierungen aller Industriestaaten und der Dritten Welt; und sie wissen auch, dass es so etwas wie private und unternehmerische – und auch staatliche – digitale Souveränität nie gegeben hat. Regierungen wollen auch gar keine private und unternehmerische digitale Souveränität.

Im Folgenden werden die aktuell-praktizierten Techniken zur Überwachung und Manipulation von Daten dargestellt und es wird auf das in der IT erreichbare Sicherheitsniveau eingegangen. Ziel ist der Versuch einer Bewertung, inwieweit zukünftig selbständiges und unabhängiges Handeln (digitale Souveränität) von Privaten, Unternehmen, Behörden und Regierungen überhaupt möglich ist und welche grundsätzlichen Auswirkungen dies auf eine Staatsform wie die Demokratie und (grundsätzlicher) Rechtsstaatlichkeit hat.

1 Abhören elektronischer Kommunikation

Die erste elektronische Überwachung der (geschichtlich anfangs ausschließlich analogen) Kommunikation datiert aus der Zeit vor dem Ersten Weltkrieg (1914 – 1918) durch das damalige deutsche Kaiserreich.

Heutzutage wird die über alle Medien wie Kabel (Telefon, Überseekabel), Satellit oder Radiowellen übertragene digitalisierte (verbale und nonverbale) Kommunikation aufgefangen, ausgeleitet, kopiert und ausgewertet.

Die folgenden Gerätearten z. B. werden abgehört: Festnetz-Telefon, Satelliten-Telefon, Mobiltelefon (Smartphone), Telefonanlagen (auch und insbesondere virtuelle Telefonanlagen in der Cloud).

Dienste werden in Echtzeit abgehört: Twitter, WhatsApp, Snapchat etc. Short Message Service (SMS), Fax, Video-Konferenz, E-Mail, File Exchange, Social Media (Facebook …), Cloud- und Storage und Streaming Services (YouTube, Netflix …) etc.

Folgende Daten sind von besonderem Interesse: Kreditkartendaten, Passagierdaten, Passwörter … sowie Standortdaten von Handys, Smartphones und Tablet PCs, Notebooks, Bankkonten und Kontobewegungen (SWIFT).

Soweit nützlich wird die Hardware von Geräten (Handys, Notebooks, Router …) manipuliert und auch die Firmware (BIOS) sowie das Betriebssystem und Anwendungsprogramme.

2 Eindringen in Computer und Netze

Die NSA hat weltweit 100.000 Server (‚Strategic Server') nachhaltig mit Software-Hintertüren (Backdoors) versehen. Dies geschieht nicht „von Hand"; vielmehr werden programmgesteuerte Prozesse eingesetzt – von der automatisierten Identifizierung von Sicherheitslücken über deren Ausnutzung, ggf. Infizierung mit eigenem Code

… bis hin zur automatisierten Erfolgskontrolle: Wiederholte programmgesteuerte Überprüfung auf tatsächliche und nachhaltige Ausnutzbarkeit der installierten Backdoors.

Da dieses Vorgehen nicht weltweit flächendeckend nützlich ist, kann davon ausgegangen werden, dass nur die wichtigsten Server in den wichtigsten Staaten mit Backdoors versehen sind. Geht man davon aus, dass die wichtigsten Staaten die G8 sind, dann sind in Deutschland durchschnittlich mehr als 10.000 Server mit Backdoors versehen. Das sind weit mehr Unternehmen als an der Börse in Deutschland gelistet sind; vielmehr dürften alle größeren Unternehmen und auch kleine Unternehmen infiltriert sein sowie wichtige Behörden.

Das Wissen über Backdoors in bestimmten Systemen und die Zugriffsweise und ggf. auch Identifizierungsinformation wie Passwörter etc. fließt an Dritte ab, so dass davon ausgegangen werden muss, dass diese Backdoors auch von Dritten wie Kleinkriminellen genutzt werden (Lerneffekt).

Allerdings lassen sich Backdoors und die für erfolgreiche Angriffe unverzichtbaren Sicherheitslücken mit heuristischen Methoden identifizieren. Software lässt sich so angriffssicher machen (Security Testing Process nach ISO 27034): Sicherheitslücken – insbesondere die Zero-Day-Vulnerabilities – beheben.

3 Speicherung und Auswertung abgehörter und ausgelesener Daten

Alle abgehörten und durch Eindringen in Computer erhaltenen Daten werden im Original (z. B. verschlüsselt) gespeichert.

Ausschließlich bei Bedarf werden gespeicherte Daten themenbezogen (ggf. entschlüsselt) ausgewertet und als Ergebnis wird ein Dossier erstellt.

Kommunikationsdaten und durch Eindringen in Computer erhaltene Daten werden nach bestimmten Suchbegriffen, Namen und Adressen etc. ausgewertet. So sind z.B, die Strafverfolgungsbehörden in einer Reihe von Staaten in der Lage, binnen 40 Minuten bestimmte benutzte Geräte zu identifizieren, sie zu lokalisieren und damit den Aufenthaltsort von Personen zu bestimmen und diese festzunehmen.

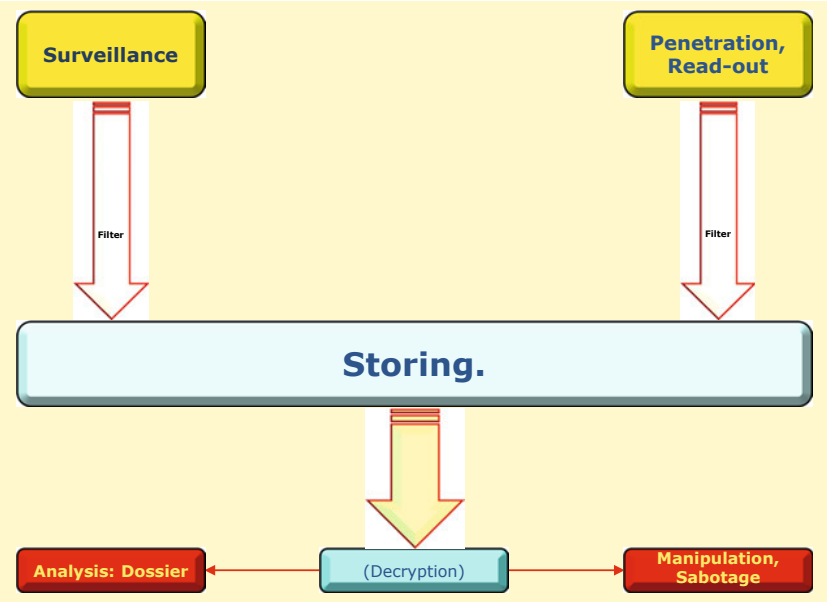

Abb. 1 Datenspeicherung und Auswertung

4 Manipulation von Daten

Alle abgehörten und ausgelesenen Daten können manipuliert werden und – auch in Echtzeit – wieder eingespielt werden (Desinformation). Beispiele sind Krankenakten, Dokumente zur Veröffentlichung für Medien, Prozesssteuerungen, digitale Stimmzettel und Wahlergebnisse. Weitere Szenarien sind realistisch.

5 Sicherheitslücken

Alle IT-Angriffe basieren auf der Ausnutzung sicherheitsrelevanter Fehler (Sicherheitslücken – Vulnerabilities) in Software und Firmware: Ohne Sicherheitslücke kein erfolgreicher Angriff.

Zwar korrigieren (patchen) alle Software-Hersteller mehr oder weniger regelmäßig Sicherheitslücken – allerdings nicht alle. Die Menge der Sicherheitslücken kann in die folgenden fünf Klassen gruppiert werden:

1. Gepatchte (veröffentlichte und unveröffentlichte) Sicherheitslücken – im Einzelfall haben Anwender aber die Patches (noch) nicht eingefahren.
2. Veröffentlichte Sicherheitslücken – ungepatcht.
3. Dem Hersteller bekannte Sicherheitslücken – unveröffentlicht, ungepatcht.
4. Identifizierte Sicherheitslücken – dem Hersteller (noch?) nicht bekannt – aber womöglich Dritte
5. (Noch?) nicht identifizierte Sicherheitslücken – unbekannte Sicherheitslücken

Der Lebenslauf einer Sicherheitslücke kann wie folgt in drei Phasen klassifiziert werden:

Phase des größten Risikos (‚Black Risk')

Nach Auslieferung eines Produkts oder einer neuen Version sind erst einmal keinerlei Sicherheitslücken bekannt. Nach Identifizierung einer Sicherheitslücke ist diese nur dem Spezialisten bekannt. Manchmal informiert der Spezialist den Softwarehersteller über die Sicherheitslücke oder veröffentlicht sie sogar. Häufig werden unveröffentlichte Sicherheitslücken gegen Entgelt damit handelnden Unternehmen angeboten oder auch eigenständig direkt an Nachrichtendienste, Sicherheitsbehörden oder Wirtschaftsspionage und/oder –sabotage treibende Unternehmen verkauft. Meist liefert dieser Spezialist ‚zum Beweis', dass seine Entdeckung tatsächlich eine Sicherheitslücke darstellt, einen diese Sicherheitslücke ausnutzenden Angriff (Exploit) gleich mit; die Exploits werden (unberechtigt, missbräuchlich) genutzt. Grundsätzlich sind Angriffe, die unveröffentlichte Sicherheitslücken ausnutzen, nicht erkennbar (stealth).

Phase mittleren Risikos (‚Grey Risk')

Der Hersteller kennt nun die Sicherheitslücke; sie bleibt aber unveröffentlicht. Im Unterschied zur Phase des Black Risk ist der Kreis derjenigen, die die Details der Sicherheitslücke kennen, sehr viel größer. Die Sicherheitslücke kann in dieser Phase von den Mitwissern gegen Entgelt auf dem ‚Markt' angeboten werden.

Phase hohen Risikos (‚White Risk')

Der Hersteller, ein Unternehmen oder der Spezialist veröffentlichen die Sicherheitslücke. Dieser Zeitpunkt wird Zero-Day genannt. Wenn nicht zeitnah ein Exploit veröffentlicht wird, wird ein solcher meist von Dritten für Angriffszwecke entwickelt.

Aus Wirtschaftlichkeitsgründen werden von den Herstellern nicht alle Sicherheitslücken (zeitnah) gepatcht; so sind einige veröffentlichte Sicherheitslücken seit mehreren Jahren ungepatcht.

Nach Veröffentlichung des Patches muss es zeitnah eingefahren werden, da die zugrundeliegende Sicherheitslücke nunmehr einem sehr großen Kreis bekannt ist und breit – auch von Skriptkiddies – ausgenutzt werden kann. Ebenfalls aus Wirtschaftlichkeitsgründen oder Kompatibilitätsgründen aktualisieren Endverbraucher nicht alle betroffenen Systeme – trotz vorhandenem Sicherheitspatch.

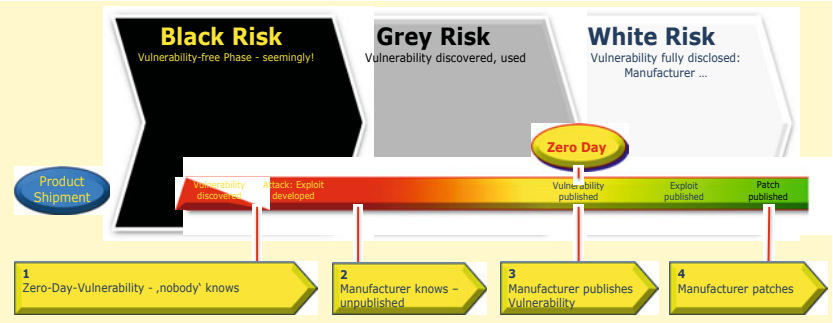

Abb. 2 Lebenslauf von Sicherheitslücken

Durch die Bekanntheit der Sicherheitslücke sind Anwender allerdings in der Lage, betreffende Komponenten zu deinstallieren oder einen Fix bzw. Workaround zu entwickeln, so dass sie nicht mehr erfolgreich angegriffen werden können.

6 Security Testing Process

Software und programmgesteuerte Computer können also nach dem Stand der Technik nicht (beweisbar) sicher entwickelt werden. Menschliche Fehler und daraus folgend auch technische Fehler sind bei der Entwicklung unvermeidbar. Allerdings

können erfahrungsgemäß sicherheitsrelevante Fehler (Sicherheitslücken – Vulnerabilities) methodisch identifiziert werden.

Angesichts der beiden Fakten:

- Software kann nicht fehlerfrei entwickelt werden,
- kein (erfolgreicher) Angriff ohne Sicherheitslücke.

Daher ist über das bekannte funktionale Testen hinaus Security Testing als vollständiger Prozess unverzichtbar, um das Sicherheitsniveau von Produkten sowie von IT-Infrastrukturen zu steigern. Zur Identifizierung insbesondere bisher nicht-erkannter Sicherheitslücken werden erfolgreich die folgenden fünf Methoden – massiv Tool-gestützt – eingesetzt:

1. *Security Requirements Analysis*: Ziel dieser Methode ist es exakte Sicherheitsanforderungen für die darauf folgende Designphase bereitzustellen. Dabei werden alle die Sicherheit betreffende Anforderungen identifiziert, definiert und Bestehende validiert.
2. Security By Design: *Threat Modeling* ist eine Methode, um systematisch eine Architektur auf Sicherheit hin zu prüfen. Diese Methode wird sowohl bei der Software- und Hardwareentwicklung verwendet, als auch zur Prüfung von sicherheitskritischen IT-Infrastrukturen und Netzwerken.
3. Code Review: *Static Source Code Analysis* – Semi-automatisiertes Scannen des Quellcodes auf Sicherheitslücken zum Auffinden von Race Conditions, Deadlocks, Zeiger- und Speicherverletzungen.
4. Simulated Attacks: *Penetration Testing* ist eine dynamische Sicherheitsprüfung, bei der bekannte Angriffe auf ein System simuliert werden, um in dieses einzudringen. Damit werden bekannte Sicherheitslücken identifiziert und damit das Sicherheitsniveau ermittelt.
5. Dynamic Analysis: *Fuzzing* ist eine Methode zur dynamischen Sicherheitsprüfung, bei der manipulierte und bisher nicht bekannte Angriffe auf ein System simuliert werden, um Anomalien herbeizuführen. Herbeigeführte Anomalien werden reproduziert und untersucht, mit dem Ziel unbekannte oder nicht-veröffentlichte Sicherheitslücken (Zero-Day-Vulnerabilities) zu identifizieren.

Der Einsatz dieser fünf Methoden wird umso wirkungsvoller und kostengünstiger je früher in der Software-Entwicklung Sicherheitslücken identifiziert werden, möglichst also beginnend in der Requirementsphase. Am teuersten wird es, wenn die Software schon ausgeliefert ist (Release Phase) und erst dann korrigiert wird.

Zudem lassen sich diese fünf Verfahren für alle Anwendungsbereiche einsetzen: Anwendungssoftware (Web Applications, ERM, CRM, SCM, ERP, E-Business, CIM etc.) und Netzwerk-Protokolle, Embedded Systems (auch die Hardware) und Industrial Control Systems (ICS) (auch proprietärer Systeme), Manufacturing Execution Systems (MES), Produktionsleitsysteme, SCADA (Leittechnik und -systeme), SPS bis zur Feldebene, Cyber Physical Systems (CPS), Industrie 4.0, Apps und Applets für smart and mobile Devices, Cloud Computing und auch Hardware. Im Bereich Smart Grid / M2M wurden erfolgreich Energy Management Systeme – EMS und Machine-to-Machine Communication und Smart Meter Gateways (SMGW) abgesichert.

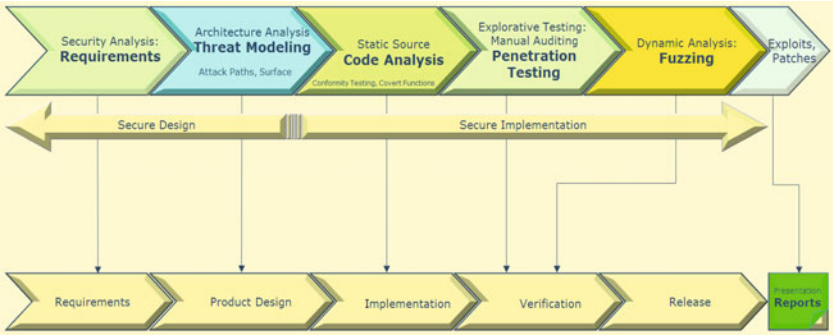

Abb. 3 Security Testing Process

Mit der Identifizierung und Behebung bisher nicht-erkannter Sicherheitslücken kann sporadischen Betriebsausfällen und unbeabsichtigten Datenabflüssen – den häufigsten Folgen sicherheitsrelevanter Softwarefehler – entgegengewirkt werden und so können proaktiv hohe Umsatzausfälle und Reputationsschäden gemindert werden.

7 Stand des Wissens, der Forschung und Entwicklung

Derzeit hängt Deutschland bei allen digitalisierten Anwendungen völlig von ausländischen (US-amerikanischen und asiatischen) Komponenten und Produkten ab! Um unabhängiger (souveräner) zu werden, erscheint eine eigenständige nationale Forschungspolitik also alternativlos.

Allerdings muss sorgfältig geprüft werden, in welchen Bereichen nationale Sicherheitsforschung nützlich sein könnte. Im Bereich der Verschlüsselung erscheint sie fraglich. Jedenfalls mag die Sicherheitsqualität der eingesetzten Algorithmen noch so hoch sein – Verschlüsselung wird derzeit erfolgreich auf den folgenden Wegen gebrochen:

- *Berechnen* der benutzten Schlüssel;
- *Auslesen* der benutzten Schlüssel;
- Strategische *Schwächung* internationaler Standards;
- Ausnutzen von *Backdoors* in Verschlüsselungsprogrammen – auch in Open Source;
- Ausnutzen von *Sicherheitslücken* in Verschlüsselungsprogrammen – auch in Open Source;
- Angriff auf die *Trust Center*: Backdoors, Sicherheitslücken zum Auslesen benutztet Schlüssel;
- Selbst wenn sie aktuell nicht gebrochen werden kann, werden die Daten gespeichert und können in *naher Zukunft* dechiffriert werden, wenn geeignete Verfahren entwickelt wurden.

Abhören von Kommunikation und Eindringen in Computer wird weltweit von nationalen Sicherheitsbehörden und Nachrichtendiensten der Industriestaaten vollständig betrieben – (partiell) auch von deutschen.

Software-Angriffe auf die IT werden seit langem durch programmgesteuerte Gegenangriffe beantwortet (Cyberwar).

8 Politik, Behörden, Regierungen, organisierte Kriminalität, Kulturen

Nachrichtendienste und Strafverfolgungsbehörden arbeiten auf der Grundlage nationaler Gesetze mit einem gewissen Freiraum. Internationale Vereinbarungen dürften daher schwer durchsetzbar sein. ‚Die Politik' scheut eine Diskussion der

http://www.springer.com/978-3-658-07348-0

Digitale Souveränität
Vertrauen in der Netzwerkgesellschaft
Friedrichsen, M.; Bisa, P.-J. (Hrsg.)
2016, XII, 421 S. 1 Abb. in Farbe., Softcover
ISBN: 978-3-658-07348-0