Cyber Security:

die aktuelle Bedrohungslage und ihre Entwicklung

Autor
Dr. Stefan Frei, Security Architect, Swisscom

August 2015

Inhaltsverzeichnis

1 Einleitung

In den vergangenen zwei Jahrzehnten wurden durch die Entwicklung von neuen Technologien und insbesondere durch das Internet unglaubliche Möglichkeiten geschaffen, die unser privates wie auch geschäftliches Leben nachhaltig verändert haben und weiter verändern werden.
Die Umwälzungen, die durch das Internet ausgelöst wurden, dürfen als disruptiv gewertet werden. Sie haben globale Auswirkungen, vergleichbar mit den Folgen, welche die industrielle Revolution und Innovationen, wie die Exploration von Erdöl, die Erfindung des Automobils oder die Einführung von Antibiotika hatten.
Heute haben über drei Milliarden Menschen Zugang zum Internet, was 42% der Weltbevölkerung von 2014 entspricht[1]. Der Anteil der mobilen Nutzung steigt dabei stetig (94% der Weltbevölkerung besitzen ein Mobiltelefon), ebenso die durchschnittliche Zeit, die wir täglich mit dem Internet verbunden sind („always on"). Internet-Sicherheit ist zu einem kritischen Faktor geworden und wird an Wichtigkeit auch in dem Masse weiter zunehmen, in dem Menschen und Geräte zunehmend miteinander verbunden werden.
Wir sind sowohl als Gesellschaft als auch in der Wirtschaft immer noch in der frühen Phase der Adaption dieser Möglichkeiten. Selbstverständlich bringen diese Entwicklungen auch neue Bedrohungen und Gefahren mit. Das Umfeld der Internet-Sicherheit ist geprägt durch eine rasante Entwicklung und Veränderung an der Schnittstelle von Technologie, Wirtschaft und Gesellschaft.

In diesem Bericht beleuchten wir aus Sicht von Swisscom und der Schweiz die aktuelle Lage im Hinblick auf die Cyber-Bedrohungen und geben als führendes Schweizer ICT-Unternehmen eine Einschätzung der Entwicklungen für die kommenden 12 bis 24 Monate ab.

2 Entwicklung der Cyber-Bedrohungslage

In noch nie da gewesener Intensität verbindet das Internet heute Menschen, Maschinen, Technologie und Wirtschaft. Die Möglichkeiten, aber auch die daraus entstehenden Bedrohungen sind das Resultat unzähliger technischer Innovationen und darauf aufbauender neuer Applikationen und Dienste. Die aktuelle Bedrohungslage ist komplex und verändert sich fortwährend. Wir wollen uns in dieser Arbeit nicht auf die Extrapolation von historisch bekannten Bedrohungen oder auf einzelne Technologien limitieren. Unser Ziel ist es, aufgrund der beobachteten Dynamik und Entwicklung die

[1] Internet World Statistics - http://www.internetworldstats.com/stats.htm

derzeitigen Bedrohungen zu beurteilen und die aus unserer Sicht zu erwartende Entwicklung der nächsten 12 bis 24 Monate darzustellen.

2.1 Lagebild – Bedrohungsradar

Der Ursprung von Bedrohungen findet sich in der stetigen Entwicklung von neuen Technologien und deren Anwendung und Verbreitung in der Gesellschaft. Potenzielle Bedrohungen gilt es frühzeitig zu erkennen und systematisch zu erfassen. Um die Bedrohungslage und deren Evolution abzubilden, verwenden wir einen Radar, dargestellt in Abbildung 1. Themen und Bedrohungen sind als Punkte auf dem Radar eingetragen. Die Punkte in Abbildung 1 geben die aktuelle Lage wieder. Die jeweils eingezeichnete Spur zeigt für jede Bedrohung die Entwicklung, welche wir in den nächsten 12 bis 24 Monaten erwarten.

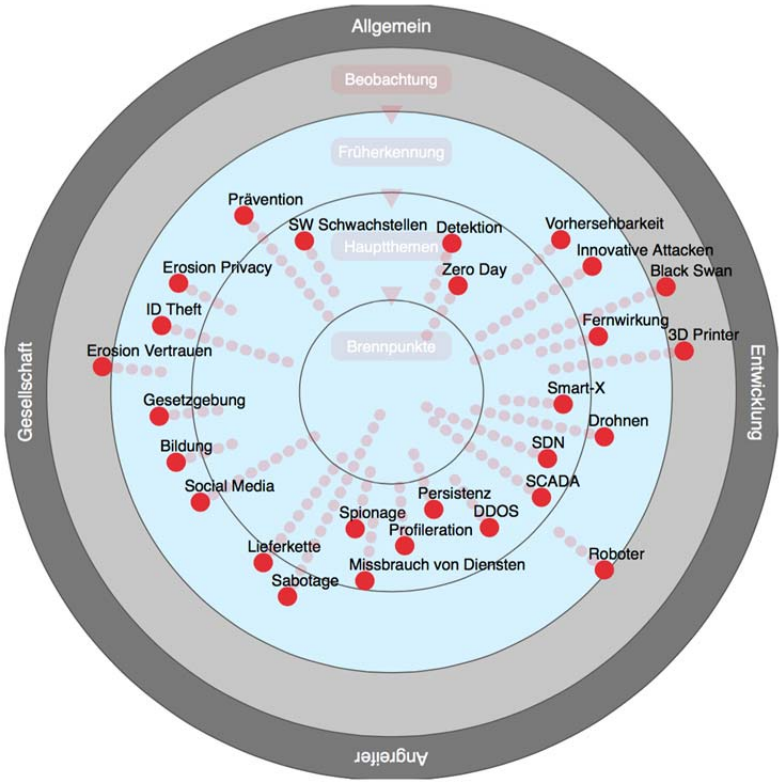

Abbildung 1 – Bedrohungsradar

In Abbildung 1 unterscheiden wir vier Arten von Themen und Bedrohungen, welche den Radar in die Segmente *Allgemein*, *Entwicklung*, *Angreifer* und *Gesellschaft* unterteilen:

Entwicklung	Bedrohungen, welche durch technologische Entwicklung hervorgerufen werden, ohne dass diese durch einen bestimmten Angreifer oder Akteur spezifisch getrieben werden.
Angreifer	Bedrohungen, welche gezielt von Angreifern ausgehen.

Gesellschaft	Bedrohungen, welche durch die zunehmende Vernetzung der Gesellschaft entstehen.
Allgemein	Bedrohungen, welche allgemeiner Natur sind und entweder keiner oder mehreren der obigen Kategorien zugeteilt werden können.

Die Unterscheidung in diese vier Kategorien kann nicht immer trennscharf vollzogen werden.

Neue Bedrohungen sowie deren Erkennung, Beurteilung und Gegenmassnahmen folgen jeweils einer typischen Evolution, welche durch die konzentrischen Ringe *Beobachtung*, *Frühwarnung*, *Hauptthemen* und *Brennpunkte* im Radar erfasst werden.

Im äussersten Ring *Beobachtung* des Radars werden Themen und Entwicklungen erfasst, die potenziell zu Bedrohungen werden können. Themen im Ring *Beobachtung* werden systematisch verfolgt, jedoch mit reduzierten Ressourcen. Im Ring *Früherkennung* werden erkannte Bedrohungen erfasst, welche in den kommenden Jahren relevant werden können. Diese werden aktiv und vertieft untersucht zum besseren Verständnis des Risikos und zur Ausarbeitung und Vorbereitung von Gegenmassnahmen. Bedrohungen im Ring *Hauptthemen* sind aktuell und Gegenmassnahmen sind eingeleitet und werden in regulären Projekten und Prozessen umgesetzt.

Verläuft die Entwicklung und Handhabung von Bedrohungen innerhalb der oben beschriebenen drei Phasen (*Beobachtung*, *Früherkennung*, *Hauptthemen)* so arbeiten wir proaktiv, von systematischer und frühzeitiger Erkennung bis zum operativen Einsatz von Gegenmassnahmen.

Überraschend auftretende Bedrohungen oder solche, welche sich schneller als angenommen entwickeln, werden reaktiv adressiert. Diese sind im Radar im innersten Ring *Brennpunktthemen* erfasst.

Der Radar dient der Übersicht und dem systematischen Erfassen des Lagebildes und der zu erwartenden Entwicklung. Im Folgenden gehen wir vertieft auf diese Entwicklungen und einzelne Bedrohungen ein.

3 Bedrohungen durch die Evolution

Innovationen in der Technik, neue Anwendungen, ein veränderter Umgang der Gesellschaft mit dem Internet sowie veränderte Rahmenbedingungen lassen neue Möglichkeiten wie auch neue Bedrohungen entstehen. Einige der Themen und

Bedrohungen im Radar leiten sich von übergeordneten Prozessen oder Entwicklungen ab:

3.1 Steigende Komplexität Gesellschaft & Internet

Unsere heutige Gesellschaft und die Internet-Nutzung haben nicht mehr viel gemeinsam mit der Zeit um 2000, als die „dot.com Blase“ platzte. Die kommenden Jahre dürften ähnlich dynamisch verlaufen und eine Vielzahl von Innovationen hervorbringen. Das System Internet und Gesellschaft wird stetig und schnell komplexer, mit einer steigenden Zahl von neuen Interaktions- und Kombinationsmöglichkeiten zwischen Mensch, Maschine, Diensten und diversen Rückkoppelungsprozessen. Ein Teil dieser sich täglich und in grosser Anzahl neu ergebenden Kombinations- und Interaktionsmöglichkeiten zwischen Mensch und Maschine („Devices“) erlauben fundamental neue Angriffsszenarien, welche wir aus der historischen Betrachtung heraus nicht vorhersehen können. Das bedeutet, dass wir vorhersehbare und modellierbare Bedrohungen („more of the same”) von prinzipiell nicht vorhersehbaren Bedrohungen unterscheiden müssen.

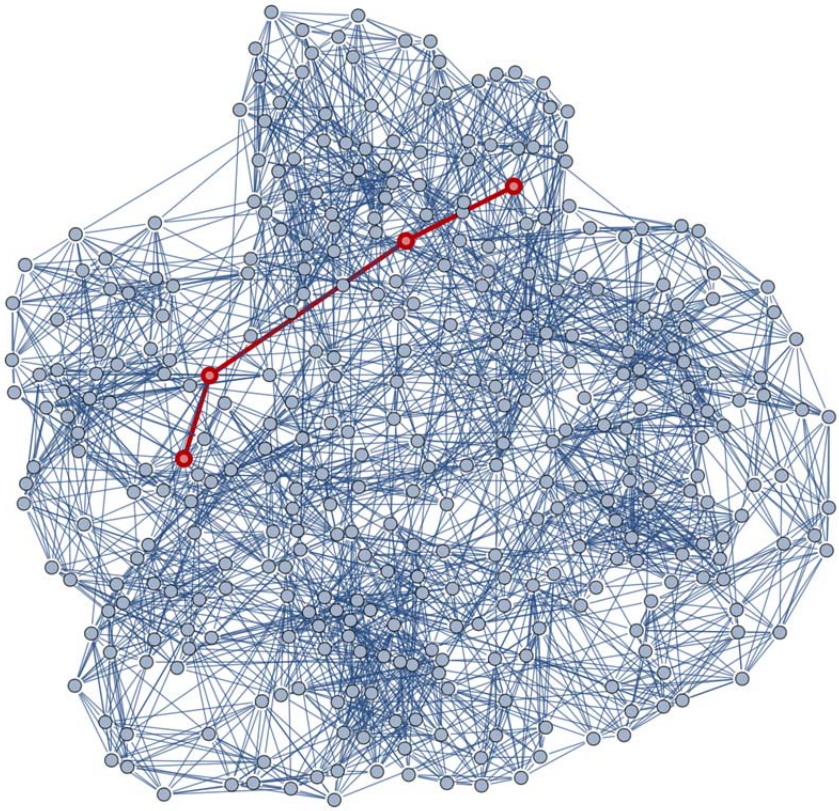

Abbildung 2 – Vereinfachte Darstellung des komplexen Systems Internet & Gesellschaft. Knoten stellen Menschen, Maschinen, Applikationen und Dienste dar, welche vielfältig miteinander interagieren können. Mit jedem neuen Knoten steigt die Anzahl möglicher neuer Interaktionswege (dargestellt als Linien) zwischen den Knoten überproportional an.

Mit der fortschreitenden Vernetzung werden stetig neue Knoten in das System Internet & Gesellschaft eingebunden. Aus der dadurch täglich entstehenden grossen Zahl neuer

und teils überraschender Interaktionswege leiten wir folgende Erkenntnisse für die Bedrohungslage ab:

Neue innovative Attacken	Qualitativ neue Attacken, basierend auf neuen Interaktionswegen, werden zunehmen. Solche fundamental neue Attacken müssen nicht zwingend technisch anspruchsvoll sein. Ungenügender Basisschutz neu eingeführter Systeme und deren Vernetzung sowie mangelndes Verständnis der neu geschaffenen Interaktionen lassen fortwährend überraschend neue Angriffspfade zu.
Vorhersehbarkeit	Die Vorhersehbarkeit von Bedrohungen wird abnehmen. Trends und Entwicklungen wie *Internet of Things*, *Smart Home*, *Smart Grid* etc. stehen derzeit im Vordergrund dieser Entwicklung und der daraus resultierenden Bedrohungen.
Prävention	Mit zunehmender Vielfalt der Angriffsmöglichkeiten wird eine Prävention schwieriger. Zudem lassen sich qualitativ neue Attacken prinzipiell nicht vorhersehen. Bestehende Sicherheitssysteme und Dienste können nur Schutz gegen Szenarien bieten, welche diese Sicherheitssysteme bereits modellieren.
Fernwirkung, Kaskaden	In einem komplexen System, wie in Abbildung 2 dargestellt, sind auch entfernt geglaubte Komponenten miteinander verbunden und können zum Teil vielfältig wechselwirken. Das bedeutet, dass Angriffe auf entfernte Komponenten des Systems (oder vorher isolierte Komponenten) plötzlich einen direkten Einfluss auf eigene Komponenten ausüben können. Weiter können kleine (oder gut gemeinte) Eingriffe an einem Ort des Systems zu schweren und unvorhergesehenen Auswirkungen an einem gänzlich anderen Ort des Systems führen („Kaskaden"). Wir erwarten deshalb vermehrt Angriffe auf Subsysteme oder Lieferanten mit der Absicht, ein Primärziel zu kompromittieren. Weiter erwarten wir vermehrt, dass kleine Fehler oder Attacken durch eine Kaskadierung überraschende Schäden anrichten.

Ein Beispiel zur Illustration dieser Mechanismen:
GPS-Geräte sind jedermann bekannt und werden zur Ortsbestimmung vielfältig eingesetzt. Weniger bekannt ist, dass unzählige kritische Dienste und Geräte von GPS-Signalen abhängen, um die *genaue Uhrzeit* zu erhalten und um Prozesse zu synchronisieren. Ein unbeabsichtigter oder gezielt herbeigeführter Ausfall des GPS-Systems (z.B. durch extreme Sonnenaktivität, Konfigurationsfehler oder Jamming) wird daher nicht nur navigationsnahe Systeme beeinträchtigen.

Ein Beispiel: In San Diego/USA sind 2007 nach einem Ausfall von GPS-Signalen durch unabsichtliches Jamming stadtweit *Notfallpager*, *Mobiltelefone*, *Verkehrsmanagement-Systeme* und *Bankomaten* für zwei Stunden ausgefallen.[2]
Die Abhängigkeiten von GPS zur Zeitgebung und Synchronisation vieler Prozesse sind seit diesem Ereignis noch gewachsen. Unzählige Dienste, welche äusserlich keinen Zusammenhang mit Navigation oder Ortsbestimmung aufweisen, können betroffen sein:[3]

- Kommunikationssysteme, Telefon, Mobil und Datennetze
- Energieverteilsysteme („Power Grid“)
- Finanztransaktionssysteme
- Globale Synchronisation von Transaktionen
- Verteilte Systeme und Sensoren

Die Vorhersehbarkeit der möglichen Schäden bei einem Ausfall des GPS-Signals ist gering und Ausfälle werden kaskadieren. Prävention ist äusserst schwierig, da in fest verbauten Systemen die GPS-Empfänger nicht einfach erweitert werden können.
Im *Nachhinein* ist es einfach, diese geschilderten Ausfälle zu erklären, da die Abhängigkeiten im beschriebenen Fall aufgedeckt wurden. Die aktuellen Abhängigkeiten der GPS-Zeitgebung vollständig aufzulisten, dürfte jedoch wiederum ziemlich schwierig sein.

3.2 Innovationsdynamik

Durch die stetige Innovation sowie die anhaltende Verbesserung bestehender Technologien bei gleichzeitigem Preiszerfall sinkt die Eintrittsschwelle für viele Angriffstypen. Sicherheitsannahmen, welche

- auf der beschränkten Verfügbarkeit von Angriffstechnologien,
- deren hohen Preisen
- oder deren eingeschränkter Leistungsfähigkeit

[2] http://www.newscientist.com/article/dn20202-gps-chaos-how-a-30-box-can-jam-your-life.html
[3] http://www.gps.gov/applications/timing/

basieren, werden in den nächsten Jahren vermehrt in ihrer Wirkung geschwächt werden. So sind zum Beispiel neue und überraschende Anwendungen und Attacken durch die allgemeine Verfügbarkeit von 3D-Druckern, Flugdrohnen, Robotern etc. zu erwarten und absehbar.

3D-Drucker	Sicherheitsannahmen, welche auf der Komplexität oder Einzigartigkeit mechanischer Elemente basieren, werden untauglich. Mechanische Schlüssel oder spezifische Werkzeuge lassen sich vermehrt einfach kopieren oder neu erstellen. Der Austausch der betroffenen Sicherheitselemente ist oft sehr komplex und teuer und kann nicht zeitnah oder durch ein Software-Update mitigiert werden.
Flugdrohnen, Roboter	Sowohl Flugdrohnen wie auch Miniaturroboter können ferngesteuert operieren und dadurch Zugangsbarrieren einfach überwinden. Bestehende Annahmen über den physischen Zugangsschutz müssen überdacht werden. Das Ausspionieren physisch unzugänglicher Bereiche zur Vorbereitung von Attacken wird zunehmen. Zutrittssysteme, die den Eintritt in den geschützten Bereich verwehren, den Austritt von innen nach aussen jedoch unbeschränkt zulassen (z.B. Notfalltüren, Brandschutz, Garagenausfahrten) können durch infiltrierte Roboter einfach umgangen werden.
Software Defined Radio (SDR)	Mit der Verbreitung von Software Defined Radios (SDR) werden alle Arten von Funknetzwerken und Kontrollsystemen für Attacker vermehrt und einfacher zugänglich. Die vermeintliche Sicherheit durch Verwendung undokumentierter Protokolle erodiert. Sicherheitsannahmen, welche auf dem privilegierten Zugang zu Funkequipment und Frequenzbändern basieren, werden somit untauglich. Neue Attacken auf alle Arten von Funkfernsteuerungen und Kommunikation (Fahrzeug, Gebäude, Verkehr, Zugangssteuerung, WiFi, GSM, GPS, ...) werden zunehmen. Beispielsweise werden GPS-Jammer heute für weniger als USD 100. – angeboten.

3.3 Internet & Maschinen

Getrieben durch die jederzeit und überall verfügbare Vernetzung und die andauernde Miniaturisierung von Komponenten werden immer mehr Maschinen, Gerätschaften („Devices“) und Sensoren aller Art an Netzwerke angebunden. Diese Entwicklung schreitet in unterschiedlichen Gebieten rasch voran. Neben Kontrollsystemen, die Industrieprozesse und Energieflüsse steuern, verbreiten sich immer mehr Geräte und Sensoren, die unseren Alltag bestimmen. Prominente Beispiele sind die angestrebte Energiewende mit „smart grid“, die Heimautomatisierung „smart home“, intelligente Verkehrssteuerung und „smart cars“ sowie „wearable devices“ und „robotics“. Mit der steigenden Verbreitung dieser Technologien steigt auch deren Potenzial aus Sicht des Angreifers.
Fehlfunktionen sowie Angriffe im Internet werden vermehrt nicht-virtuelle Schäden verursachen, mit potenziell fatalen Folgen für Mensch, Umwelt, Gesellschaft und Material. Aufgrund fortschreitender absichtlicher oder unabsichtlicher Vernetzung von Geräten erwarten wir in den kommenden Jahren vermehrte Angriffe in diesem Bereich.

Industriekontrollsysteme ICS/SCADA	Schwachstellen und Angriffswerkzeuge gegen ICS/SCADA-Systeme verbreiten sich schneller, als diese Systeme geschützt werden können. Gezielte und erfolgreiche Angriffe gegen solche Kontrollsysteme werden zunehmen. Fest verbaute und unzugängliche Kontrollsysteme, welche über keinen eingebauten Mechanismus zur sicheren Softwareaktualisierung verfügen, lassen sich nicht oder nur sehr teuer schützen. Ferner sind solche Kontrollsysteme erheblich länger im Einsatz als typische Endbenutzersysteme wie PCs, Tablets und Mobiltelefone. Viele der heute im kritischen Einsatz stehenden Kontrollsysteme sind veraltet und wurden zu einer Zeit gebaut, in der das Bedrohungsumfeld noch vergleichsweise unbedeutend war. Entsprechend sind diese Systeme heute extrem verwundbar und zum Teil durch triviale Attacken kompromittierbar.
Smart Home, Smart Grid, Smart Car, Smart Was-auch-immer	Starker Wettbewerb, Preiszerfall und Miniaturisierung führen zu einer schnellen Verbreitung jeder Art von „Smart“-Systemen und Gerätschaften. Oft spielt die Sicherheit beim Design eine untergeordnete Rolle: • Mangelnde Awareness für komplexe-innovative Attacken

	• Time to Market ist wichtiger als Sicherheit • Die Sicherheit der Einzelkomponenten sowie des Zusammenspiels vieler Komponenten wird weiterhin schlecht verstanden • Mangelde Ressourcen für effektive Sicherheit auf stark miniaturisierten Geräten Weiter werden solche Systeme durch die Benutzer vermehrt für innovative, ursprünglich im Design nicht vorgesehene Zwecke eingesetzt. Dies führt zu ungenügendem Schutz von solchen Kontrollsystemen oder deren Kommunikation. Wir erwarten vermehrte Angriffe und neue spektakuläre Ausfälle mit Schäden nicht-virtueller Natur.

3.4 Automatisierte Sicherheits-Updates

In einem stetig steigenden Bedrohungsumfeld ist die Möglichkeit, ein System einfach mit Sicherheits-Updates zu aktualisieren von herausragender Wichtigkeit. Hersteller von Betriebssystemen und verbreiteter Softwareprodukte (Windows, Web Browser, App-Stores etc.) haben dies erkannt und die Bedienbarkeit und Automatisierung des Einspielens von Sicherheits-Updates weit vorangetrieben. In Abbildung 3 ist skizzenhaft die Entwicklung der Bedrohung zusammen mit der Entwicklung des Schutzes durch Sicherheits-Updates für typische Computer dargestellt. Durch Sicherheits-Updates wird der Schutz laufend der neuen Bedrohung angepasst.
Kontrollsysteme jeder Art (ICS/SCADA, Smart-X etc.), welche über keinen Mechanismus verfügen, um Sicherheits-Updates schnell und einfach einzubringen, werden immer verwundbarer. Die Bedrohung steigt, der inhärente Schutz erodiert, wie in Abbildung 3 dargestellt. Dies wird noch verschärft durch die Tatsache, dass solche Systeme typischerweise viel länger im Einsatz sind als PCs.

Effektive Update-Mechanismen für jede Art von vernetzten Systemen sind eine zwingende Voraussetzung für den sicheren Betrieb über eine lange Einsatzdauer.

Das Fehlen eines Sicherheits-Update-Mechanismus in einem Produkt oder vernetzten Gerät ist als sicherer Indikator für künftige Attacken und Ausfälle zu werten.

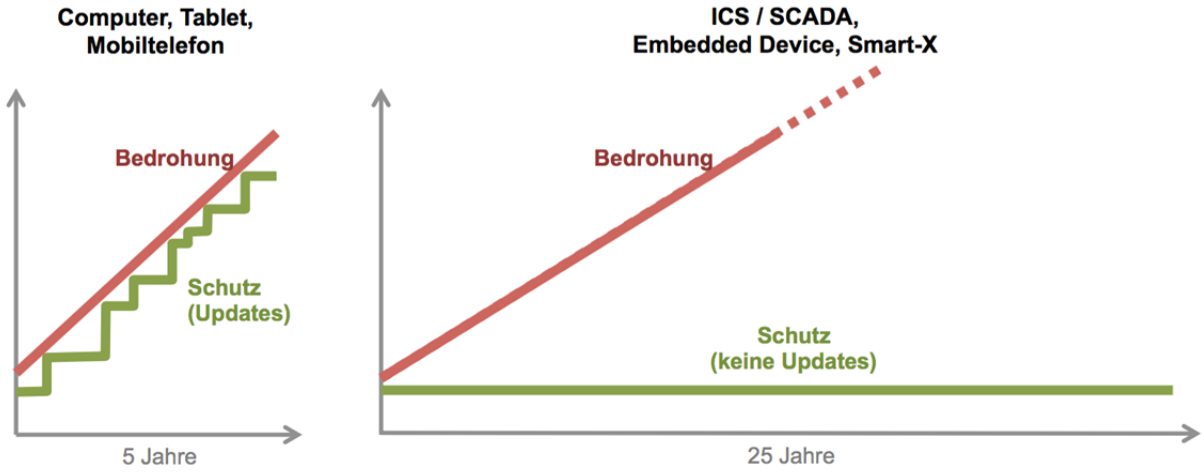

Abbildung 3 – Lange Betriebszeit ohne die Möglichkeit von Sicherheits-Updates bei ICS/SCADA Systemen führt zu stetiger Vergrösserung der Verwundbarkeit.

3.5 Altsysteme (Legacy)

Viele IT-Systeme und die darauf laufenden Applikationen sind deutlich über das vom Hersteller vorgesehene Lebensende in Betrieb. Solche Systeme werden vom Hersteller nicht mehr unterstützt und verwenden veraltete Betriebs- und Entwicklungsumgebungen sowie Kommunikationsprotokolle. Zudem sind die eingebauten Schutzmechanismen, wie wir sie von Personalcomputern kennen (z.B. Antimalware, Exploit Mitigation), meist nicht vorhanden. Typischerweise sind diese Systeme komplex und erfüllen kritische und spezielle Funktionen – beides Gründe dafür, weshalb sie nicht ersetzt werden.
Gleichzeitig sind solche Legacy-Systeme demselben Druck auf vermehrte, direkte und indirekte Vernetzung, sowohl intern als auch extern, ausgesetzt. Die Widerstandsfähigkeit solcher Systeme gegen Attacken bleibt konstant, während sich die Gefährdung stetig weiter entwickelt, wie in Abbildung 3 dargestellt.

Legacy Systeme & Protokolle	Wir erwarten vermehrt Angriffe auf kritische & veraltete Systeme und Protokolle. Mit der Verbreitung von Spezialwissen zu diesen Systemen steigt die Gefährdung.
Vernetzung & API	Legacy-Systeme ohne direkten Aussenkontakt werden vermehrt durch sogenannte API Schnittstellen mit einem modernen Überbau verbunden. Dadurch werden diese Systeme, ihre Daten und einst isolierte Funktionen gegen aussen exponiert. Wir erwarten eine weitere Zunahme in der Verbreitung von APIs und Maschine-zu-Maschine-Protokollen und Kommunikation, welche bisherige Schutzbereiche durchbrechen. Daraus

	resultieren u.a. innovative neue Angriffsvektoren. Weiter erwarten wir vermehrt Data-Breaches, welche die Daten einst isoliert betriebener Systeme exponieren.

3.6 Software-Komplexität

Trotz grosser Fortschritte und Investitionen in die Entwicklung sicherer Software, schafft es die Industrie bislang nicht, von Haus aus sichere Software zu erstellen und auf den Markt zu bringen. Nur vier von zehn grossen Softwareherstellern konnten die Anzahl Schwachstellen in ihren Produkten über die letzten zwölf Monate gegenüber dem Durchschnitt der vorhergehenden fünf Jahre reduzieren. Abbildung 4 zeigt die Entwicklung von Schwachstellen in Software über die letzten 20 Jahre hinweg.

Software-Schwachstellen	Wir erwarten weiterhin eine grosse Anzahl von Schwachstellen, welche vor allem Produkte mit grossem Marktanteil betreffen. Davon sind Systeme, welche nicht direkt als „Computer“ wahrgenommen werden, nicht ausgenommen (z.B. Kontrollsysteme, SmartX, Sensoren).

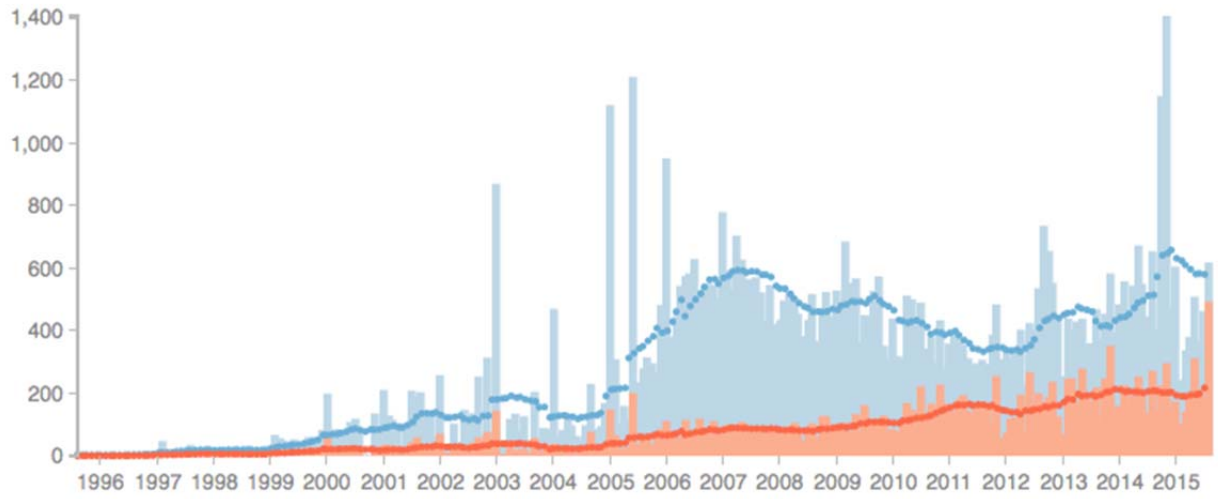

Abbildung 4 - Publizierte Schwachstellen pro Monat, 1995 bis 2015. In Rot: Schwachstellen der Top-10-Hersteller. Die Linien zeigen den Durchschnitt über die jeweils vorangehenden 12 Monate.[4]

[4] http://techzoom.net/BugBounty/SecureSoftware

Die Bedeutung effektiver Software-Update-Mechanismen, die eine grosse Zahl von betroffenen Systemen zeitnah aktualisieren können, wird zunehmen. Das Fehlen eines solchen Mechanismus in einem Produkt oder vernetzten Gerät ist als sicherer Indikator für künftige Attacken und Ausfälle zu werten.

4 Bedrohungen durch Angreifer

Die im vorhergehenden Teil dargelegten Bedrohungen sind das Resultat der Entwicklung des Internets, der Technologie und der Gesellschaft, ohne dass ein bestimmter Akteur eine Bedrohung plant, steuert, oder initiiert.

In Teil 4 betrachten wir jedoch Bedrohungen, welche von Akteuren ausgehen.

Dabei unterscheiden wir fünf Gruppen von Akteuren mit unterschiedlichen Zielen, verfügbaren Mitteln und Vorgehensweisen. Diese Gruppen sind in Abbildung 5 aufgelistet.

	Angreifer	Ziele	Mittel	Vorgehen
Gezielt	Staatliche Akteure, Geheimdienste	• Information • Spionage • Bekämpfung Terrorismus / Kriminalität • Schaden	• Grosse finanzielle Möglichkeiten • Fokus auf Nutzen weniger auf Kosten	• Kaufen Know-how ein und bilden aus • Unauffällige, nachhaltige Angriffe
	Terroristen	• Schaden • Aufmerksamkeit • Manipulation, Beeinflussung der Politik	• Mittlere finanzielle Mittel, die für physische und logische Angriffe eingesetzt werden	• Kaufen Know-how auf dem Schwarzmarkt ein • Angriffe physisch und logisch
Opportunistisch	(Organisierte) Kriminalität	• Geld	• Business • Langfristig Geld verdienen • Kosten-Nutzen muss stimmen	• Bestehende Banden • Spontan organisierte Banden von Spezialisten • Bestechung
	Hacktivists, Gruppen	• Aufmerksamkeit • Schaden • Anprangern der Verletzlichkeit von Systemen	• Minimale Mittel • Grosse Reichweite	• Hoch motivierte Amateure & Spezialisten • Entwickeln unvorhersehbare Eigendynamik
	Vandalen, Skript Kiddies	• Ruhm und Ansehen	• Minimale Mittel und Wissen	• Einsatz verfügbarer Tools

Abbildung 5 – Klassifikation von Angreifern

Weiter unterscheiden wir Akteure, die *opportunistisch* vorgehen, von *gezielt vorgehenden* Akteuren, wobei der Übergang mitunter fliessend ist.

Opportunistisch	Akteure nutzen die Möglichkeiten des Internets, entweder weil sich die Gelegenheit zufällig ergibt, oder weil das Ziel schlecht geschützt ist.
Gezielt	Akteure haben ein klar definiertes Ziel, das sie konsequent und typischerweise mit beträchtlichem Ressourceneinsatz (Finanzen, Expertise, Personal, Material) verfolgen. Solche Angreifer sind oft persistent, d.h., die Zielverfolgung erfolgt auch über einen längeren Zeitraum und auf verschiedenen parallelen Kanälen.

4.1 Staatliche Akteure & Geheimdienste

Seit jeher betätigen sich Staaten und Geheimdienste in der Spionage und Sabotage. Cyber-Spionage und -Sabotage wird zunehmend in militärische Verteidigungs- und Angriffsstrategien eingeplant. Etliche Staaten bauen derzeit ihre offensiven und defensiven Cyber-Fähigkeiten massiv aus.
Im Unterschied zu Cyber-Kriminellen und anderen Angreifern können sich Staaten direkten Zugriff auf kritische Teile der Infrastruktur des Internets verschaffen („Internet Backbone“) und Dienstanbieter oder Hersteller per Gesetz zur Überwachung oder Mitarbeit zwingen. Staatliche Tätigkeiten reichen vom systematischen und umfangreichen Überwachen des Internetverkehrs bis zum versteckten Einbringen von Malware in Hardware und Software der Zielsysteme anderer Länder (oder Konkurrenten). Ziel ist einerseits die Informationsgewinnung, andererseits wird aber auch durch versteckte Implantate („Backdoors“, „Kill-Switches“) die Möglichkeit der Sabotage für den Bedarfsfall vorbereitet. Insbesondere im Namen der Terrorbekämpfung und zur Kontrolle der Opposition werden Daten im Internet systematisch und umfangreich abgefangen. Staatliche Angreifer verfügen über enorme Ressourcen und den langen Atem, um ein Ziel persistent über mehrere Angriffskanäle und lange Zeiträume zu erreichen.

Lieferkette Supply Chain	Wir müssen davon ausgehen, dass Teile der kritischen Infrastruktur unseres Landes bereits kompromittiert sind. Die Integrität von Lieferobjekten wird in Zukunft vermehrt herausgefordert und in Frage gestellt werden müssen.
Industriespionage	Ein Grossteil der Wertschöpfung in unserem Land erfolgt aus der Verwertung gewerblicher Schutz - und Urheberrechte. Wir erwarten eine Zunahme an Attacken zum Zwecke der Industriespionage.
Sabotage/Vorbereitung	Geheimdienste werden vermehrt Kill Switches oder andere Vorbereitungsmassnahmen treffen, um eine Sabotage im Bedarfsfall vorzubereiten. Betroffen

	sind sowohl Hardware- als auch Software-Produkte. Solche Funktionalität kann sich z.B. in „Software Schwachstellen" oder fest eingebauten Zugriffs-Konten zu „Wartungszwecken" manifestieren. Eine eindeutige Zuordnung eines Defekts als absichtliche Massnahme eines Gegners ist mitunter schwierig. Hardware kann auch mit Sicherungen und Sollbruchstellen versehen ausgeliefert werden, damit eine entsprechende Funktion durch Softwareimpulse aus der Ferne an- bzw. ausgeschaltet werden kann.
Mobilfunk, WiFi	Mobilfunknetze und WiFi-Netze werden vermehrt aktiv oder passiv angegriffen (Sniffing, Jamming, Spoofing, SS7, ...).
APT/Zero Day	Technisch raffinierte Attacken werden zunehmen, unter gleichzeitiger Abnahme der Detektierbarkeit solcher Attacken.

4.2 Terrorismus

Genauso wie Kriminelle nutzen auch Terroristen die Möglichkeiten des Internets. Ihr Ziel ist jedoch nicht finanzieller Natur, sondern sie streben das Erlangen oder die Vermehrung der Aufmerksamkeit für ihre Sache sowie eine Manipulation und Beeinflussung von Politik und Gesellschaft an. D.h., grösstmögliche Schadensverursachung zum Zwecke einer grösstmöglichen Aufmerksamkeit sowie die Verbreitung von Angst und Schrecken sind durchaus reale Szenarien.

Missbrauch von Diensten	Der Missbrauch von etablierten Diensten zu Propaganda- und Rekrutierungszwecken (z.B. Hosting, Social Media, Kommunikation) wird zunehmen.
DDOS	Distributed Denial of Service Attacken zur Machtdemonstration oder einer grösstmöglichen Schadenserzeugung werden zunehmen.
Events	Grossanlässe oder Konferenzen zu heiklen Themen werden vermehrt Ziel von Cyber-Attacken werden. Dabei werden auch Lieferanten und Dienstanbieter solcher Anlässe vermehrt angegriffen.
Elektronische Medien	Wir erwarten vermehrt gezielte Angriffe auf jede Art von Medien (TV, Radio, Web, Social Media) mit grosser Gefolgschaft. Dies sind geeignete Ziele zur Verbreitung von Propaganda, Angst und zur Machtdemonstration.

Kritische Benutzerkonten	Wir erwarten vermehrt gezielte Angriffe gegen individuelle Benutzerkonten mit einer grossen Gefolgschaft (Facebook, Twitter, Blogs, ...).

Grossanlässe oder Dienste, welche ein grosses Publikum bedienen (z.B. TV-Stationen, die Übertragung von Grossanlässen wie eine Fussball-WM), sind geeignete Plattformen für Attacken von Terroristen. Neben solchen Diensten sind auch individuelle Konten (z.B. bei Twitter, Facebook etc.), über die eine grosse Audienz erreicht wird, häufiger gefährdet. Wir erwarten, dass solche Dienste und Konten vermehrt das Ziel gezielter Attacken werden.

4.3 Organisierte Kriminalität

Kriminalität und organisierte Kriminalität gehören zu den ältesten Phänomenen der Gesellschaft und die Geschichte lehrt uns, dass sich Kriminelle neue Technologien jeweils sehr schnell aneignen und zunutze machen.
Kriminelle gehen professionell zur Erreichung ihrer finanziellen Ziele vor, sowohl gezielt wie auch opportunistisch.
Diverse kriminelle Gruppen spezialisieren sich auf bestimmte Gebiete, wie z.B. das Suchen von Schwachstellen, die Erstellung von Malware, dem Verkaufen/der Vermietung von Tools, der Verwaltung von Botnets, dem Rekrutieren von Money Mules, der Erstellung von Phishing Mails etc. Traditionelle und Cyber-Kriminalität ergänzen und vermischen sich.
Durch diese Arbeitsteilung werden qualitativ hochwertige „Services“ und „Tools“ bereitgestellt, welche prinzipiell jedem Interessenten käuflich oder im Mietmodell verfügbar gemacht werden.

Verbreitung von Tools und Services (Proliferation)	Angriffstools wie auch Services zur Verwaltung kompromittierter Systeme werden raffinierter und weiter verbreitet.
Komplexe Attacken	Komplexe und mehrstufige Attacken (z.B. Ablenkung durch DDOS) werden zunehmen. Phishing-Attacken werden psychologisch raffinierter und in Darstellung, Inhalt, und Zeitpunkt genau auf das Opfer abgestimmt („Spearphishing“).
Tarnung, Verhinderung der Detektion	Malware und Angriffswerkzeuge werden raffinierter in ihrer Fähigkeit, der Detektion durch Sicherheitsprodukte zu entgehen.
Persistenz	Schwachstellen werden vermehrt systematisch gesucht und ausgenutzt und entsprechende Attacken werden kommerzialisiert und Kaufwilligen angeboten.

4.4 Hacktivisten

Hacktivisten haben eine Mission, typischerweise im Kontext eines emotionalen Themas. Um ein Vorgehen zu koordinieren, können sich durch Social Media (oft spontan) in kurzer Zeit grosse Gruppierungen Gleichgesinnter bilden bzw. finden. Das Ziel des Angriffes ist entweder durch das Thema (Umweltsünder, Regierungen, dominante Firmen, …) vorgegeben oder wird spontan bestimmt. Die Akteure sind hochmotiviert und verfügen mitunter auch über professionelles Wissen in ihren Reihen. Leicht entsteht eine unkontrollierbare Eigendynamik in der Gruppe.

Social Media	Wir erwarten vermehrt spontane Kampagnen oder durch Social Media koordinierte Attacken gegen Ziele, welche direkt oder indirekt mit dem auslösenden Thema in Verbindung stehen.

4.5 Vandalen, Skript Kiddies

Vandalen und Skript Kiddies sind nicht-professionelle Angreifer welche aus Langeweile oder Geltungsdrang mit einfach verfügbaren Tools Attacken und „Experimente“ durchführen. Dabei steht kein bestimmtes Ziel im Vordergrund, sondern vielmehr die Möglichkeit, mit minimalen Mitteln und Wissen durch eine Cyber-Attacke Ansehen zu erlangen. Entsprechend sind die Zielauswahl und der Angriffszeitpunkt hier eher als zufällig zu erachten.
Solche Attacken sind als permanentes Grundrauschen im Internet zu betrachten und entsprechend zu behandeln. Der Grundschutz aller vernetzten Systeme muss solche Attacken automatisiert abwehren können. Durch die vermehrte Verfügbarkeit von Informationen und einfach zu bedienender Angriffstools werden solche Attacken nicht abnehmen – der Basisschutz muss permanent überprüft und angepasst werden.

5 Bedrohung durch die Vernetzung der Gesellschaft

5.1 Orientierungsverlust

Technische Innovationen sowie neue Anwendungen des Internets werden in hohem Tempo eingeführt. Nischenplayer können innert weniger Jahre zu dominanten Anbietern werden, was bisherige Businessmodelle und Sicherheitsannahmen bedroht. Dies stellt hohe Anforderungen an die Menschen und die Wirtschaft, da ganze Zweige über Nacht in Frage gestellt werden (z.B. Taxigewerbe vs. Uber, Hotels vs. AirBnB). Naturgemäss hat das Bekämpfen, Verschliessen oder sogar eine Umkehr dieser Entwicklung langfristig nicht viel Aussicht auf Erfolg.

„**Because there is no army that can hold back an economic principle whose time has come"**
John Donovan, AT&T

Es besteht weiterhin die Gefahr, dass wir als Wirtschaft, Gesellschaft, in der Rechtsfindung und der Ausbildung mit der Dynamik, welche durch das Internet eingeführt wurde, nicht mehr werden mithalten können; mit fatalen Folgen für künftige Generationen.

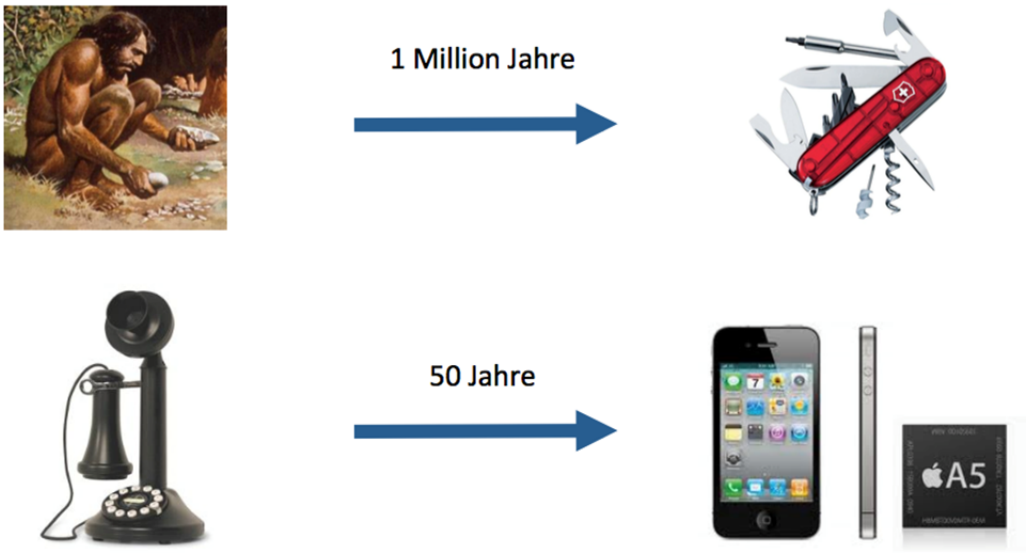

Abbildung 6 – Neue Technologien werden immer schneller eingeführt, was Menschen wie auch die Gesellschaft vor grosse Herausforderungen stellt.

Wir müssen schnell lernen, auf allen Stufen mit dieser hohen Dynamik und Agilität im Internet-Zeitalter adäquat umzugehen. Entwicklungen wie „Cloud Computing", „Shared Economy", Distanzlernen etc. fordern neue Denkansätze, um die Vorteile und Risiken adäquat abzuschätzen. Um nicht kopflos in ungewollte Abhängigkeiten zu geraten,

müssen solche Risiken und Möglichkeiten früh erkannt werden und Mechanismen bestehen, damit das Potenzial ausgeschöpft werden kann.
Vertrautes weicht Neuem, Bestehendes ändert sich dauernd. Die Orientierung in dieser Vielfältigkeit und Informationsflut wird schwieriger.

Bildung	Unser Bildungssystem ist immer noch darauf ausgelegt, vor allem Fertigkeiten zu lehren, wie sie in der frühen Phase der Industrialisierung gebraucht wurden.[5] Die Gefahr, dass wir als Gesellschaft und Wirtschaft mit der Entwicklung nicht mithalten können, erhöht sich.
Politik, Rechtsfindung	Die Rechtsfindung kann mit der Geschwindigkeit der Entwicklungen des Internet-Zeitalters kaum mithalten. Kenntnisse und Verständnis der grossen Zusammenhänge im Cyber-Umfeld sind rar, mit der Gefahr, dass nicht adäquate Gesetzte erlassen werden oder Gesetze bei der Einführung bereits hoffnungslos veraltet sind. Die laufende Debatte um „Intrusion Software" in der *Wassenaar Vereinbarung* illustriert diese Herausforderung sehr gut.[6]
Menschen	Der Mensch wird mit der rasch steigenden Komplexität und Vielfalt von Diensten, Interaktions- und Kombinationsmöglichkeiten zunehmend gefordert und überfordert. Dies gilt sowohl für den Administrator von ICT-Systemen wie auch für die Endbenutzer. Dies eröffnet vielfältige neue Bewegungsräume für Angreifer. Komplexität ist sowohl aus technischer wie auch aus menschlicher und sozialer Sicht der grösste Feind von Sicherheit.

5.2 Erosion der Privatsphäre

Zur Identifikation gegenüber Diensten und Behörden steht jeder Person eine endliche – jedoch kleine – Anzahl von persönlichen Attributen zur Verfügung. Die Anzahl der Internetdienste, die wir täglich und künftig verwenden, steigt stetig an. Mit jedem Datenleck bei einem beliebigen Dienst oder einer Behörde, kommen nach und nach alle identifizierenden Attribute einer Person abhanden. Attribute wie *E-Mail-Adresse*, *Passwort* und *Sicherheitsfragen* können wir nach einem Datenleck relativ einfach ändern.

[5] https://www.youtube.com/watch?v=Optk-gYgFo8
[6] https://www.eff.org/deeplinks/2015/05/we-must-fight-proposed-us-wassenaar-implementation

Statische Attribute wie z.B. *Sozialversicherungsnummer*, *Geburtsdatum*, *Geburtsort*, *Geschlecht*, *Wohnort* etc. lassen sich kaum oder gar nicht ändern. Durch diese Entwicklung, gepaart mit umfangreichen persönlichen Angaben, welche über Social Media einsehbar sind („OSINT"), können persönliche Attribute langfristig nicht geheim gehalten werden[7].

Der Schutz privater Daten, die Dritten verfügbar gemacht wurden, wird immer schwieriger. Angriffe, die unter Verwendung von persönlichen und privaten Daten Vertrauen vortäuschen, um die Zielperson zu bestimmten Handlungen zu bewegen, nehmen weiter zu – sowohl in Anzahl als auch in Raffinesse.

Identitätsdiebstahl	Durch die fortwährende Erosion der Privatsphäre werden Attacken wie Identitätsdiebstahl zunehmen. Die Attacken werden raffinierter (persönlicher) und die Detektion für die Betroffenen wird immer schwieriger, wenn nicht sogar unmöglich.
Missbrauch von Daten	Das umfangreiche und stetig steigende Volumen von persönlichen- wie auch Metadaten bei Staat, Dritten und Dienstanbietern erhöht die Gefährdung durch Missbrauch und Überwachung.
Einbahnstrasse	Persönliche Daten, die auch *nur einmalig* herausgegeben werden (freiwillig oder unfreiwillig), können nicht zurückgenommen werden. Ein Datenleck oder Fauxpas genügt, um die Privatsphäre für *immer* zu kompromittieren. Wir müssen daher davon ausgehen, dass langfristig ein Grossteil unserer persönlichen Daten (z.B. Kontakte) nicht privat gehalten werden können. Viele Apps fragen beispielsweise den Benutzer beim Start um Zugang zu seinen Kontaktdaten. Wird diese Frage auch nur einmal irrtümlich mit „Ja" beantwortet, so kann der Abfluss der Kontaktdaten nicht mehr rückgängig gemacht werden.

5.3 Erosion des Vertrauens

Durch die anhaltende Informationsflut und den vermehrten Missbrauch von privaten und persönlichen Informationen wird allgemein das Vertrauen in Dienste und Informationen erodieren.

[7] http://techzoom.net/Publications/Papers/databreach

Erosion des Vertrauens	Die Erkennung von Angriffen, welche mit raffinierten Methoden und unter Verwendung von persönlichen und privaten Daten Vertrauen vortäuschen, wird schwieriger. Entsprechende Attacken werden zunehmen und immer erfolgreicher sein.

6 Zusammenfassung

Neue Technologien führen anfangs immer zu Unsicherheit. Die Adaptation und der rechte Umgang damit ist ein Prozess, der Zeit braucht. Wir müssen erkennen, welche Risiken wir individuell (als Benutzer oder Organisation) abwehren können und welche Bedrohungen systembedingt bestehen bzw. entstehen und welche nur auf gesellschaftlicher Stufe oder in internationaler Zusammenarbeit nachhaltig adressiert werden können.

Die Erkenntnisse aus diesen Überlegungen:

- Internet-Sicherheit ist vornehmlich ein Problem des Komplexitäts-Managements. Eine Betrachtung der Technologie alleine genügt nicht zum Verständnis der Bedrohungen.
- Hundertprozentige Prävention ist eine Illusion. Sowohl Firmen wie auch Behörden müssen davon ausgehen, dass ihre Infrastruktur kompromittiert wird (oder bereits kompromittiert wurde).
- Organisationen müssen sicherstellen, dass eine erfolgte Kompromittierung möglichst schnell detektiert und mitigiert wird.
- Eine festgestellte Kompromittierung muss in einem definierten und eingeübten Prozess abgearbeitet werden und nicht als Exception Process.
- Das Fehlen eines effektiven Software-Update-Mechanismus in einem Produkt oder einem vernetzten Gerät ist als sicherer Indikator für künftige Attacken und Ausfälle zu werten.
- Wir gehen davon aus, dass gezielte Attacken zunehmen und in Art und Weise sowie Zeitpunkt unvorhersehbarer werden.

7 Glossar

0-Day/Zero-Day Exploit	Software-Exploit, der vor oder mit der ersten Veröffentlichung einer Sicherheitslücke bekannt ist. D.h., der Exploit ist verfügbar, bevor der Software-hersteller einen Sicherheitspatch bereit hat.
API	Application Programming Interface Programmierschnittstelle, die es Programmen erlaubt, mit einer gemeinsamen Sprache direkt Daten auszutauschen (Maschine zu Maschine).
Backdoor	Software-Hintertüre, um unter Umgehung des Zugriffsschutzes auf einen Computer zuzugreifen.
Botnet	Netzwerk einer grossen Anzahl kompromittierter Computer, welche zentral durch einen Botmaster kontrolliert werden.
Defacement	Einbringen von unerwünschten Inhalten in eine gehackte Website.
DOS, DDOS	Denial of Service (DOS) Ein System wird durch eine grosse Anzahl an Anfragen lahmgelegt. Distributed Denial of Service (DDOS) Der DOS Angriff geht gleichzeitig von einer grossen Zahl verteilter Systeme aus (z.B. ein Botnet). Ein einfaches Blockieren des Angreifers ist nicht mehr möglich.
Exploit	Programm, Code oder Befehlsfolgen, mit denen sich Schwachstellen in einer Software ausnutzen lassen.
Exploit Mitigation	Allgemeiner Begriff für Techniken, welche das Ausnutzen von Schwachstellen auf Systemen unterbinden oder erschweren.
GPS	Global Positioning System Globales Satelliten-Navigationssystem zur Positionsbestimmung und genauen Zeitmessung.
ICS	Industry Control System Allgemeine Bezeichnung für Industriekontrollsysteme, siehe SCADA.
ICT	Information and Communication Technology Abkürzung für die Informatik und Telekommunikationsindustrie.
Jamming	Absichtliches Stören von Funkkommunikation.
Kill-Switch	Versteckte Software, die auch auf Befehl von aussen

	reagieren kann, die Funktionsweise eines Systems stört oder das System unbrauchbar macht.
Malware	Software, welche schädliche und nicht gewollte Funktionen ausführt.
Money Mule	Kriminelle verleiten Personen dazu, Geld von „Kunden“ entgegenzunehmen und nach Abzug einer Kommission mit einem Geldüberweisungsdienst weiterzuleiten. Die Person (money mule) glaubt für eine legitime Organisation zu arbeiten.
OSINT	Open Source Intelligence Beschaffung von Informationen unter ausschliesslicher Verwendung von öffentlich zugänglichen Quellen.
Patch Sicherheits-Update	Programmcode der fehlerhafte Software ersetzt, um Sicherheitslücken zu eliminieren.
Phishing	Mit Phishing werden Benutzer durch Tricks (meistens E-Mails mit gefälschten Aufforderungen etwas zu tun) dazu verleitet, sensible Daten preiszugeben.
SCADA	Supervisory Control And Data Acquisition System Systeme zur Überwachung und Steuerung von technischen Prozessen (z.B. Industrieprozessen).
Schwachstelle	Eine Schwachstelle oder Verwundbarkeit in Hard- oder Software, über die Angreifer Zugriff auf ein System erlangen können.
SDR	Software Defined Radio Universelle Hochfrequenzsender und Empfänger, welche die Signalverarbeitung durch Software realisieren und daher durch den Benutzer auf verschiedene Protokolle und Anwendungen adaptierbar sind.
SmartGrid	Intelligentes Stromnetz SmartGrid umfasst die Vernetzung und Steuerung von Stromerzeugern, Speichern, elektrischen Verbrauchern und Energieübertragungs- und Verteilungsnetzen.
SmartHome	Intelligentes Heim Überbegriff für die vernetzte und teilautomatisierte Steuerung von Energie, Unterhaltung und Sicherheit in Wohnungen und Häusern.
Social Media	Webseiten, auf denen sich Benutzer mittels eigens gestalteten Profilen austauschen (z.B. Facebook, Twitter, LinkedIn, Xing).
Spearphishing	Gezielte und personalisierte Phishing-Attacke.
Spoofing	Täuschungsversuche in Netzwerken zur Verschleierung der eigenen Identität.