5.7 Cybersicherheitsfragen und -antworten

[Dr. Sandro Gaycken | Freie Universität Berlin]

5.7.1 Muss man sich mit Cybersecurity beschäftigen?

Absolut. Mindestens als Politiker und Entscheider. Denn Cyber Security ist eine wichtige Aufgabe. Und die aktuelle Phase des Problems ist überaus relevant. Die meisten großen Spieler bringen jetzt ihre Figuren in Stellung. Mischt man erst später mit, wird man sich zu einem Gutteil mit bereits geschaffenen Fakten auseinandersetzen müssen. Und viele Entscheidungen (oder Nicht-Entscheidungen) werden teilweise drastische Auswirkungen auf andere Werte wie Frieden, Freiheit und Wohlstand haben. Kümmern muss man sich aber auch als Zivilist und Demokrat. Denn gerade weil Politiker und Entscheider sich in diesem Bereich ungern entscheiden – und weil an allen Ecken und Enden viel Geld und Einfluss im Spiel sind – tummeln sich hier Lobbyisten aller Couleur, die das Problem in alle möglichen Richtungen drehen und wenden, mit reichlich künstlerischer Freiheit. Den meisten Entscheidern kommt das entgegen.

Der Ansatz der Übergabe der Entscheidungen an interessierte Profiteure ist sogar explizierter Trend: „Multi-Stakeholder" ist das Entscheidungsmodell der Stunde, wenn es um Cybersicherheit geht. Bei Cybersicherheit führt das dazu, dass die Produzenten von IT und Sicherheitsprodukten die Entscheidungen treffen, die eigentlich demokratisch getroffen werden müssten. Der demokratische Bürger muss hier also besonders aufmerksam sein, sich belesen, Politik und Wirtschaft beobachten.

5.7.2 Was muss man über Cybersicherheit wissen?

Um ein tragfähiges Urteil zu bilden, braucht man eine Basis, von der aus man bewerten und schließen kann. Das braucht man in diesem Fall auch bereits vor der Anamnese der Fakten, denn die sind bereits häufig sehr tendenziös. Was also muss man als Grundlage über Cybersicherheit wissen? Man muss die Risiken kennen; man muss die Optionen kennen, um diese Risiken beherrschbar zu machen; und man muss einige der beharrlichen Probleme kennen, die sich auf die Realisierbarkeit der möglichen Optionen auswirken. Bevor diese Punkte aber angesprochen werden können, muss noch eine wichtige Eingangsbemerkung gemacht werden. Wissen muss vermittelt werden. Und leider gibt es gerade in diesem Bereich nur noch wenige neutrale Vermittler. Wie findet der Lernende also heraus, wer hier Bären aufbindet und wer nicht? Dies führt zu einer wichtigen Wissensbasis in diesem Bereich.
Bevor man sich an die Lektüre von Mengen von Fakten und Kausalitäten aus den Federn potentieller Ahnungsloser oder Betrüger macht, muss man vor allem wissen, welche Art von Interessent welches Interesse verfolgt. Erst vor diesem Hintergrund kann man Ereignisse und fremde Bewertungen und Verbindungen treffend einordnen und bewerten. Welche Interessenten also gibt es zu Cyber Security? In aller Kürze lassen sich vier Typen unterscheiden, die mit ihren Interessen gleichzeitig vier immens wichtige, nicht-technische Kernprobleme der Cyber Security darstellen.

- **IT-Firmen, Internet-Firmen und etablierte IT-Sicherheitsfirmen** haben meist ein hohes Interesse an „Business As Usual". Sie akzeptieren Cybersicherheit als Problem, möchten aber jede tiefer gehende Veränderung an Technologien und Organisations- oder Regulierungsmodellen verhindern oder auf ungefährliches Terrain lenken, da ihre Produkte sonst nicht mehr in der gleichen Form marktfähig sind.
- **Kritische Infrastrukturen** und viele Teile der Wirtschaft können aufgrund mangelnder Transparenz über Angriffe entstehende Kosten durch Betrug oder Spionage leicht an die Kunden abgeben, wenn diese überhaupt in den vier Jahren des jeweiligen Vorstands zu erwarten sind, während die Kosten für hohe IT-Sicherheit dagegen konkreter und höher sind. Das führt also bei diesen Stakeholdern ebenfalls zu einer „Business As Usual"-Haltung, oft ergänzt durch eine aggressive Vortäuschung falscher Tatsachen.
- **Projektmittelabhängige Experten** tendieren stark dazu, das Problem in ihre Richtung zu definieren, so dass eben gerade ihre Expertise als Ausweg unablässlich wird, oder sie hängen über Projekte doch wieder am Tropf der Wirtschaft und werden das Lied singen, das ihre Geldgeber beglückt.
- **Staaten** als Interessenten erzählen zum Teil strategische Narrative, die sie als Werkzeuge brauchen, um bestimmte Sicherheitsmodelle oder Strategien zu etablieren. Eine andere Variante des Staates als Interessent sind Cyber Security-Bürokraten, die naturgemäß zu vorsichtigen, kleinteiligen Entscheidungen tendieren und die um diese Entscheidungen zu rechtfertigen oft selbst Narrative entwickeln.

5.7.3 Was sind die Risiken?

In der Cyber Security lassen sich Risiken erster, zweiter und dritter Ordnung unterscheiden. **Risiken erster Ordnung** sind die unmittelbar durch Cyberangriffe entstehenden Gefahren wie ein Verlust der Zuverlässigkeit des Systems oder der Geheimhaltung. Diese direkten Gefahren äußern sich meist in konkreten monetären oder strategischen Kosten. Diese Risiken sind allerdings systemisch, indem sie meist Prozesse betreffen sind, die ihrerseits in Netzwerke anderer Prozesse und Ziele eingebunden sind. So entstehen **Risiken zweiter Ordnung**, bei denen systemweite Gefahren entstehen, die sich zeitlich oder räumlich oder auch prozessual weit ausdehnen können, die aber auch als Folgeschäden wie Reputationsverlust auftreten können. **Risiken dritter Ordnung** schließlich entstehen durch fehlerhafte oder anderweitig problematische Schutz- und Gegenreaktionen, die weitere monetäre oder strategische Kosten auslösen.
Weiterhin lassen sich die Risiken nach Verwundbarkeit, Schaden und Wahrscheinlichkeit auflösen.
Die **Verwundbarkeit** ist das bei weitem herausragendste und historisch einmalige Phänomen der Cyber Security. Computer sind generell verwundbar gegen Angriffe. Diese dauerhafte Eigenschaft steht im Kontrast zu ihrer weiten Verbreitung in kritischen Prozessen. Je höher qualifiziert der Angreifer, desto schlimmer die Verwundbarkeit. Aktivisten und Kleinkriminelle machen dabei die unterste Stufe der Angreifer aus. Sie verfügen über wenige Fachkenntnisse, geringe Ressourcen, arbeiten meist opportunistisch mit bekannten Angriffen an bekannten Verwundbarkeiten und haben nur mäßige Möglichkeiten der Organisation. Kleinere organisierte Kriminelle, große Unternehmen und hochqualifizierte Einzelhacker machen eine mittlere Stufe aus. Diese Stufe kann in einigen Bereichen auf Spezialwissen zugreifen, kann neuartige Verwundbarkeiten finden und nutzen, verfügt

über einige Ressourcen, kann bereits komplexere, mehrstufige Angriffe bauen, hat Zeit und Muße, ist begrenzt organisiert und kann in Einzelbereichen exzellent sein. Nachrichtendienste, Militärs und sehr gut ausgestattete weitere Organisationen machen die höchste Stufe aus. Dieser Typ Angreifer ist dauerhaft wesentlich besser als jeder Verteidiger, verfügt über herausragend hohe Ressourcen, über vollständige und hochwertige Kenntnisse über Technik, Organisation und Mensch, kann auf vielen verschiedenen Vektoren verschränkt angreifen, kann eigene Verwundbarkeiten in Systeme einbringen und ist umfassend organisiert. Die Verwundbarkeit kann etwas verallgemeinert entlang dieser Kategorien beschrieben werden. Niedrigstufige Angreifer werden generell leicht bemerkt, können nur temporäre, mäßige Schäden anrichten und können mit gängigen, marktüblichen Maßnahmen und Strafverfolgung abgewehrt werden. Mittelstufige Angreifer sind ohne aufwendige Spezialtechnologien nicht zu bemerken, können hohe und lange Zeit unsichtbare Schäden über längere Zeiträume anrichten und können nur sehr begrenzt mit Spezialtechnologien und besonders hochwertiger Strafverfolgung abgewehrt werden. Die höchststufigen Angreifer sind ein neuartiges Problem, da erst in den letzten Jahren ein breites Interesse dieser Kategorie Angreifer an Hacking entstanden ist. Gleichzeitig sind sie aber das größte Problem, denn diese Angreifer sind nicht detektierbar oder identifizierbar, sie kommen überall rein und raus, können sehr hohe monetäre und geostrategische Schäden anrichten (etwa ganze Wirtschaften ruinieren), und es gibt gegenwärtig keine technischen oder strafverfolgungstechnischen Gegenmaßnahmen gegen sie. Historisch gesehen ist der Schutz vom niedrigstufigen Angreifer aus gewachsen, hat jetzt über die letzten Jahre die mittlere Stufe in Teilen und in speziellen Bereichen wie dem Bankenwesen mit aufgenommen und beginnt gegenwärtig langsam, den höchststufigen Angreifer wahrzunehmen (als „unlösbares“ Problem).

Durch Cyberangriffe auslösbare potentielle **Schäden** sind schwierig prima facie zu beziffern oder auch nur kategorial zu benennen. IT-Systeme sind sehr individuell in verschiedene Strukturen eingebunden und wachsen quasi-organisch über die Zeit in verschiedene Prozesse ein. Tritt ein Verlust oder eine Manipulation bestimmter informationstechnischer Komponenten ein, reagieren die Systeme und die Prozesse sowie die Betroffenen sehr unterschiedlich. Einige Maßnahmen können ergriffen werden, um schadhafte Wirkungen zu begrenzen, allerdings lassen sich diese Wirkungen kaum exakt und vollständig antizipieren, so dass immer Raum für Überraschungen bleibt. Außerdem sind die Schäden gerade hochqualifizierter Cyberangreifer in der Regel keine einfachen und leicht zu bemerkenden Ausfälle, sondern kaum als solche detektierbare Diebstähle oder Manipulationen, die erst viel später und an ganz anderen Stellen Schäden verursachen. Zwei Beispiele dafür sind einmal eine Sabotage, die sich so tarnt, als wäre sie eine Fehlfunktion oder als zweites der Diebstahl von Innovationen, bei dem notorisch unklar ist, ob damit jemals eine ernsthafte Konkurrenzproduktion in Gang gesetzt wird oder nicht. Geht man allerdings von hochqualifizierten Angreifern als Ideal der Bemessung des Schutzbedarfs aus, so müssen die potentiellen Schäden direkt in Relation zur Abhängigkeit der Prozesse vom problemlosen Regelbetrieb der IT ermessen werden. Ist diese Abhängigkeit hoch, so dass etwa wie bei Flugzeugen, kritischen Infrastrukturen oder Produktionsanlagen ein weitflächiger Ausfall der Prozesse einen sofortigen und vollständigen Funktionsverlust nach sich zieht, sind die Schäden entsprechend hoch. Zudem könnten viele Schäden langfristig gestaltet und über viele verschiedene Technologien skaliert werden, indem etwa mit einem Cyberangriff nicht nur ein Flugzeug, sondern alle baugleichen Flugzeuge angegriffen werden, was für den qualifizierten Angreifer nur einen geringfügig höheren Aufwand bedeutet.

Wahrscheinlichkeiten schließlich sind ebenfalls schwierig zu bestimmen. Während die Wahrscheinlichkeiten für kleinstufige Angriffe dauerhaft hoch ist, sind die Wahrscheinlichkeiten für mittel- bis höherstufige Angriffe schwieriger zu determinieren, da hier keine Daten über Angriffe freigegeben werden. Betroffene Unternehmen und Institutionen bemerken diese Angriffe nur schwer und geben sie danach kaum je öffentlich zu. Eine Praxis des Schweigens ist hier sehr weit verbreitet. In der Forschung und der IT-Sicherheitspraxis geht man allerdings davon aus, dass vor allem Industriespionage, Finanzmarktmanipulation und Infrastruktursabotage hohe Risiken darstellen. Industriespionage und Finanzmarktmanipulation stehen mittleren bis hohen Akteuren offen und werden daher als weit verbreitet angenommen, mit hohen kumulativen Schäden, während Angriffe auf kritische Infrastrukturen eher weniger wahrscheinlich, allerdings auch nicht vollkommen ausgeschlossen sind und bei Eintritt unter Umständen hohe Schäden verursachen können.

5.7.4 Warum funktioniert die konventionelle IT-Sicherheit nicht?

Die abgebildeten Verwundbarkeiten insbesondere relativ zu mittleren bis hohen Angreifern sind indikativ für ein allgemein schlechtes Schutzniveau. Die unmittelbaren technischen Gründe für den sehr schlechten Schutz sind zahlreich. Die Computer sind zu komplex, um erfolgreich verifiziert oder transparent bis ins Detail beobachtet werden zu können. Die ausbeutbaren Verwundbarkeiten innerhalb der Software sind zu zahlreich und nicht automatisiert zu erkennen. Zudem wird immer mehr an große Netzwerke gehängt, was viele kritische Bereiche, deren Sicherheitskonzept wesentlich darin bestand, nie ans Internet gehängt zu werden, instantan hochgradig verwundbar und attraktiv macht. Diese universalen Eigenschaften machen „normale“ Computer und Netzwerke per se äußerst angreifbar.

Zudem kommt der Sicherheitsgedanke nur als ad hoc-Konzept auf. Sicherheit soll auf ein bereits existierendes, grundlegend unsicheres System aufgeschraubt werden. Das ist als Gedanke bereits grundlegend defizitär, da so keine strukturellen, architekturellen Veränderungen angestrebt werden, und wird durch weitere Mängel der aufbauenden ad hoc-IT-Sicherheitstechnik noch verschlimmert. Zu diesen ist etwa zu rechnen, dass diese Sicherheitstechnologien weitestgehend reaktiv arbeiten, indem sie bekannte Angriffe oder Angriffsmuster erkennen und abwehren, damit also prinzipiell nur gegen niedrigstufige Angreifer überhaupt funktionieren, dass sie punktuell an besonders verwundbaren Punkten aufgesetzt sind, aber nur selten deckend viele Angriffsvektoren gleichzeitig abdecken und dass sie in ihren Konzeptionen von Angriffen eine statische oder lineare Entwicklung der Angreifermodelle voraussetzen, obwohl diese exponentiell verläuft. Dadurch wirken konventionelle IT-Sicherheitsprodukte vorrangig gegen niedrigstufige Angreifer und prinzipiell nicht oder kaum gegen hochstufige Angreifer. Das Schutzangebot ist umgekehrt proportional zum Schutzbedarf.

National wie international wird gegenwärtig versucht, dieses Manko mit aktiver Verteidigung zu kompensieren, indem Angreifer durch weit verbreitete, feingranulare Internet Überwachung oder fokussierte forensische digitale Spurensuche lokalisiert und identifiziert werden, um so Strafverfolgung oder Rückschläge zur Abschreckung einleiten zu können. Diese kompensative Paradigma krankt allerdings substantiell daran, dass insbesondere mittel- und höherstufige Angreifer nicht lokalisiert und identifiziert werden können. Das Paradigma identifiziert nur die schwächsten oder aufgrund ihrer Stärke ignorante

Angreifer, ist damit de facto nicht funktional, führt aber auf der anderen Seite zu massiver Überwachung und kann bei schlecht oder unbegründeten Anschuldigungen zu konventionellen Eskalationen führen.

5.7.5 Was gibt es für andere Lösungen?

Ein anderer Weg zu einem tragfähigen IT-Sicherheitsparadigma wäre eine deutliche Erhöhung der technischen Sicherheit. Derart nicht-konventionelle IT-Hochsicherheitslösungen sind technisch möglich, könnten das Schutzniveau drastisch erhöhen und sogar höchststufige Angreifer erfolgreich abwehren. Ein Wandel von von-Neumann-Architekturen zu Harvard-Architekturen etwa würde eine deutlich bessere Unterscheidung von Daten und Prozessen ermöglichen, so dass Angriffe nicht mehr als Informationen getarnt werden könnten. Ein Umsatteln auf eindeutigere Computersprachen könnte sprachliche Komplexität drastisch reduzieren und ausbeutbare digitale Missverständnisse verhindern. Eine Reduktion der Komplexität und der Performanz würde einen Einsatz vollständig verifizierter Kerne wie des seL4-Kernels erlauben, der weit weniger Angriffe überhaupt ausführen könnte. Eigene, sicherheitssensible Hardwareproduktionen können eingebaute Hintertüren verhindern. Und viele im Fortschrittsrausch vernetzte Infrastrukturen und Geschäftsprozesse könnten wieder entnetzt werden, um sofort eine deutliche Erhöhung der Sicherheit herzustellen. Allerdings sind diese Lösungen tief gehende architekturelle Eingriffe in den gegenwärtigen Computer und seine Nutzung. Es wäre eine neuartige Informationstechnik, die neue Hersteller benötigte, alte Hersteller obsolet machen würde, die teuer in der Implementierung und geringfügig weniger performant und funktional wäre.

Das alles macht diesen architekturellen Weg prima facie wenig attraktiv und generiert große Widerstände. Secunda facie allerdings hätte eine auf IT-Hochsicherheitslösungen aufbauende Cybersicherheitsstrategie auch signifikante Vorteile. Es wäre eine nachweisbare, deutliche Verbesserung der Abwehr und der Prävention; es wäre stärker rechtskonform, da man völkerrechtlich zuerst zu der bestmöglichen Erhöhung passiven Schutzes verpflichtet ist; es wäre keine umgreifende Überwachung des Internets nötig; aggressive Abschreckungsstrategien wären ebenfalls unnötig, so dass das Eskalationsrisiko begrenzt wäre; an einigen Stellen wie Wartung und Betrieb würde eine neue Informationstechnik auch deutlich weniger laufende Kosten verursachen; und eine neue Informationstechnik wäre außerdem ein gigantischer neuer Markt mit hohem Exportvolumen.