Disruptionen/Störungen aus Sicht von IT-Security und Privacy

Sebastian Rehms & Stefan Köpsell

Einführung

Eines der zentralen Spannungsfelder von IT-Sicherheit und insbesondere technischem Datenschutz[1] sind Störungen und deren Handhabung. Dies lässt sich vereinfachend auch wie folgt formulieren: „Das Ziel von IT-Sicherheit und Datenschutz ist das Vermeiden von Überraschungen". Gäbe es keine Störungen, gäbe es diese Felder nicht.

Generell lässt sich hier die Hypothese aufstellen, dass sich in IT-Umgebungen immer die Unterscheidung von normativen Forderungen und technischen Tatsachen machen lässt. Erstere werden klassischerweise in Form von „Policies" bzw. Regeln als das gefasst, was der Fall sein soll. Solche Regeln sind nicht immer klar ausformuliert. Häufig ist jedoch zur Möglichmachung der Durchsetzung von Regeln eine formale, zumindest jedoch wenigstens teilweise strukturierte natürlichsprachliche Ausarbeitung erforderlich.

In der Praxis entsteht hier eine Problematik: die normative Anforderungsanalyse eines Systems/ einer Umgebung ist nicht notwendigerweise vollständig oder korrekt. Störungen können insofern einerseits als Abweichungen von Regeln und andererseits als Konsequenz von unvollständig oder unkorrekt formulierten Regeln auftreten.[2] Es lassen sich also Klassen von Störungen unterscheiden.

So gibt es *antizipierte, spezifische Störungen*, deren mögliches Auftreten explizit gemacht wurde, indem die Störungen als positive oder negative Regeln formuliert wurden (insbesondere auch als Abweichung vom gewünschten Normalzustand). Diese Störungen können oft in einer organisatorischen oder technischen Form bearbeitet werden.

[1] Auf eine ausführliche Diskussion zu den Begrifflichkeiten von Privacy, Privatsphäre, Datenschutz usw. wird aus Platzgründen an dieser Stelle verzichtet. Der interessierte Leser wird hier auf die einschlägige Literatur verwiesen.

[2] Der Einfachheit halber wird der Fall der Widersprüchlichkeit der Anforderungen nicht weiter betrachtet. Prinzipiell können Regeln korrekterweise Widersprüche enthalten. Ein Umgang in solchen Fällen ist normalerweise eine Art Abwägung – und wäre ein ganz eigenes Thema, das im Text wiederholt auftauchen, aber bewusst übergangen wird.

DOI: 10.62892/intodis.v1i1.3

Zugehörige Betrachtungen erfolgen im nächsten Abschnitt dieses Textes. Die zweite Klasse sind *antizipierte, unspezifische* Störungen, für die nicht notwendigerweise korrespondierende, konkrete Regeln existieren, für die aber gleichwohl Maßnahmen zur Störungsbehandlung vorgesehen sind. Diese Art von Störungen wird im dritten Abschnitt dieses Textes besprochen. Im vierten Abschnitt wird auf Basis der bisherigen Überlegungen noch eine mögliche dritte Klasse diskutiert. Im Rahmen dessen wird unter anderem durch Bezüge auf Privacy und das Bystander-Problem im Bereich von 6G-Systemen eine nicht weiter untersuchte These zur Diskussion gestellt.

Erste Klasse: Antizipierte, spezifische Störungen

Antizipierte, spezifische Störungen lassen sich oft durch technische Mittel verhindert bzw. entdecken. Beispielsweise kann die konkrete Anforderung der Vertraulichkeit von Informationen, die über einen Übertragungskanal ausgetauscht werden, durch Verschlüsselung sichergestellt werden. Die Anforderung der Vertraulichkeit der Tatsache, dass überhaupt kommuniziert wird, lässt sich durch Steganographie umsetzen. Die gegensätzliche Anforderung wiederum, dass keine Kommunikation stattfinden soll, kann durch Beobachtung von möglichen Kommunikationskanälen, der Analyse der übertragenen Information sowie durch Unterbindung von Kommunikation umgesetzt werden.

Man kann also generell beschreiben, wie die Welt sein soll oder wie sie nicht sein soll. Dies umfasst das Beschreiben von Phänomen welche in einer unerwünschten Welt auftauchen, um so eine Abweichung vom Gewünschten ausdrücken zu können. Ein Beispiel für die Vermeidung zugehöriger Störungen ist das Suchen nach konkreten unerwünschten Mustern etwa Viren-Signaturen im Falle von Antiviren-Programmen. In allen genannten Beispielen existiert entweder eine „positive“ Regel (welche den Soll-Zustand beschreibt, etwa, dass bestimmte Nutzer bestimmte Daten lesen können) oder eine „negative“ (welche eine Abweichung vom Soll-Zustand beschreibt, etwa dass die Signatur einer bekannten Schadsoftware beobachtet wird).

Ein weiteres Beispiel wäre Zugriffskontrolle: das betrifft etwa Rechte, die virtuellen Nutzern gegeben werden und die meist mit Standardwerten initialisiert werden: eine Datei, die ein Nutzer erstellt, soll auch von diesem lesbar sein. Daher wird die Datei in der Praxis einfach direkt mit entsprechenden Rechten versehen. Dies geschieht oft so

DOI: 10.62892/intodis.v1i1.3

natürlich, dass die Differenz zwischen normativer Forderung und technischer Durchsetzung auf Systemebene schnell unsichtbar wird. Hier soll eine möglichst unauffällige oder automatische Integration der störungsvorbeugenden Sicherheitsmechanismen in den Alltag von Mensch und/oder System passieren.

Im Ergebnis dessen kann aber gewissermaßen das Gegenteil vom Gewünschten erreicht werden: die automatisierte Behandlung von antizipierten, spezifischen Störungen führt zu neuen Störungen. Im konkreten Fall kann die Vergabe von Rechten zur Verhinderung von Sicherheitsrisiken (Störungen) den Nutzer in seinen Möglichkeiten einschränken, etwa, weil nun eine Installation von Software nicht mehr durch den Nutzer, sondern nur noch durch den Administrator möglich ist. Die automatisierte Behandlung von Störungen führt also zu neuartigen Störungen, die dann umso verstörender sind.

In solchen Fällen nimmt hier die „Störungsbearbeitungsstruktur" die Rolle einer Störenden ein. Die Natur von Sicherheit und Privatsphäre ist in vielen Fällen eine Begrenzende: Es soll nur möglich sein, was normativ der Fall sein soll – und sonst nichts. Dinge zu verhindern, verhindert oftmals auch Erwünschtes, was mitunter als störend empfunden wird. Insbesondere, wenn unterschiedliche logische Ebenen involviert sind, auf denen Störungen auftreten bzw. auf denen den Störungen vorgebeugt werden sollen. Dies verstärkt sich noch, wenn nicht (einfach) nachvollziehbar ist, wie diese Ebenen ineinandergreifen. Dass Störungsbearbeitungsstrukturen (im Sinne von Sicherheits-maßnahmen) aus dem Bereich der IT-Sicherheit und Privatsphäre oft stören (oder so wahrgenommen werden), ist wohl selbstevident (Bsp.: Cookie-Banner).

Zweite Klasse: Antizipierte, unspezifische Störungen

Am Beispiel der Zugriffskontrolle wurde eingeführt, dass es an sich legitime Aktionen geben kann, die jedoch in der implementierten Regelmenge nicht als erlaubte abgebildet wurden und von einer existierenden Regel blockiert werden. Die legitimierende Regel existierte bestenfalls als normative Forderung, war aber nicht Bestandteil der technischen Durchsetzung auf Systemebene.

Allgemeiner lässt sich die Struktur so beschreiben, dass Umstände eintreten können, die nicht ohne weiteres vorhersehbar sind und daher nicht in einer „flachen" Form von Regeln eingefangen werden können. Für das oben erwähnte Beispiel existieren üblicherweise

DOI: 10.62892/intodis.v1i1.3

Wege der Konfliktlösung: es steht etwa ein Administrator zur Verfügung, der die Installation durchführen kann. Will man dies mit dem obigen Regelbegriff einfangen, so ist eine gewisse „Regeltiefe“ bzw. „Regelkomplexität“ notwendig, die es ermöglicht, einen „Lösungsweg“ für komplexere Probleme auszudrücken.

Noch allgemeiner gewendet handelt es sich hier um Störungen, die zumindest auf einer Meta-Ebene *bearbeitbar* sind: man nimmt an, dass „Etwas“ schief gehen kann und erlaubt Lösungen – ohne genau zu wissen, was das „Etwas“ eigentlich konkret ist.

Für IT-Sicherheit und Privatsphäre sind hier auch Aspekte wie die Begrenzung von Schaden angezeigt – etwa durch Isolation von Netzen, um eine Lateralbewegung von Angreifern zu erschweren, wenn diese einmal eingedrungen sind. Weitere Beispiele sind die Erholung im Schadensfall (z. B. Backups) oder Redundanz, um Funktionalität auch im Schadensfall sicher zu stellen (im Sinne der Argumentation lässt sich hier auch etwas vereinfacht 2-Faktor-Authentifizierung als Beispiel nennen). Man kann auch eine „Bearbeitung durch nicht-Bearbeitung“ ansetzen: es ist gängige Praxis, Risiken zu akzeptieren (und möglicherweise die entstehenden Kosten im Schadensfall einfach in Produkten oder Prozessen einzupreisen).

Dritte Klasse: Störungen, die nicht zur ersten oder zweiten Klasse gehören

Das Problem sind hier möglicherweise Störungen der Störungsprävention, oder anders formuliert, Störungen in Störungskontrollstrukturen, d. h., dass aktuell keine Möglichkeit bekannt ist, eine Bearbeitung vorzunehmen. Im Falle der Risikoakzeptanz sind Störungen gemeint, deren Akzeptanz nicht möglich ist.

Man kann versuchen, solche Situationen strukturell folgendermaßen zu fassen: Zunächst muss im Sinne des Textes eine normative Forderung bestehen, damit etwas als Störung gelten kann. Sie muss weiter die Form einer allgemeinen Forderung bezüglich eines unterspezifizierten Ziels haben, z. B. „Personenbezogene Daten sind zu schützen“. Zuletzt muss eine Situation eintreten, z. B. die Verfügbarkeit einer neuen Technik oder Technologie, die unter die Anforderungen fällt, jedoch unter den gegebenen Bedingungen (aktuell) eben nicht bearbeitbar ist.

Als Beispiel sei hier „Joined Communication and Sensing“ als intendiertes Feature des kommenden Mobilfunkstandards 6G genannt. Hier sollen die elektromagnetischen

DOI: 10.62892/intodis.v1i1.3

Wellen zur Kommunikation gleichzeitig als Radar zur Erfassung der Umwelt und der Objekte inklusive der Menschen und deren physischen Eigenschaften und Situationen genutzt werden. Dass dies potentielle Privatheitsprobleme impliziert ist offensichtlich. Rechtliche Prinzipien greifen schwer, da hier die Bearbeitung hauptsächlich über den Mechanismus des „Informed Consent" (also Zustimmung durch die Betroffenen) abgedeckt wird – was natürlich bei einer ubiquitären Verbreitung einer solchen Technologie als wenig praktikabel erscheint. Technische Möglichkeiten zur Lösung sind nur begrenzt verfügbar und weit von einer hinreichenden Verbreitung entfernt. In den Vorschlägen der ITU[3] wird das Privatsphäre-Problem nur am Rande und insbesondere nur für Teilnehmer der Infrastruktur erwähnt – was offensichtlich viel zu kurz greift, da jede Person Gegenstand von Radarvermessung werden kann, unabhängig davon, ob sie an der Telekommunikation teilnimmt oder nicht (Bystander). D. h. sowohl auf rechtlicher als auch auf technischer sowie – so kann man argumentieren – auf Bewusstseinsebene mangelt es an einer Möglichkeit der Bearbeitung. Alte Muster und Ansätze halten nur sehr bedingt unter solchen Bedingungen und eine Abschätzung von dem, was in einer Störungssituation der 3. Klasse passiert, ist kaum möglich.

Ein Ziel der Arbeit von IT-Sicherheits-und Privatsphären-Forschung liegt darin, durch geeignete (Schutz)maßnahmen, Störungen der Klassen ineinander zu überführen: Klasse 3 in Klasse 2 oder 1, Klasse 2 in Klasse 1.

Zusammenfassung

Ein wesentlicher Aspekt von IT-Sicherheit und Datenschutz ist die Bewältigung von Störungen. Die Anwendung des aktuellen Stands von Wissenschaft und Technik verursacht dabei neue Störungen. Eine wesentliche Herausforderung besteht also darin, Sicherheitsmechanismen zu entwickeln, die störungsfrei Störungen bewältigen können.

[3] International Telecommunication Union

DOI: 10.62892/intodis.v1i1.3