Wie wir mit Daten sicher und nachhaltig umgehen können

Minimale Grundkenntnisse im Umgang mit Daten sind für jeden Bürger und jede Bürgerin notwendig, um bewusst und sicher im Cyberspace handeln zu können. Die Broschüre zeigt fünf Themen, in denen Bürgerinnen und Bürger selbst aktiv sein müssen, sowie drei Themen, in denen Orientierung für alle wichtig ist, wo aber der Staat verantwortlich ist.

SATW

Schweizerische Akademie der Technischen Wissenschaften
Académie suisse des sciences techniques
Accademia svizzera delle scienze tecniche
Swiss Academy of Engineering Sciences

Glossar

Botnetz Eine Ansammlung von Computern, die mit Malware infiziert (kompromittiert) sind. Diese lassen sich durch einen Angreifer (den Botnetzbesitzer) komplett fernsteuern. Je nach Grösse kann ein Botnetz aus einigen Hundert bis Millionen infizierter Computer bestehen.

Brute Force Lösungsmethode für Probleme aus den Bereichen Informatik, Verschlüsselung und Spieltheorie, die auf dem Ausprobieren aller (oder zumindest vieler) möglichen Fälle beruht.

Denial Of Service (DoS) Eine Denial-of-Service-Attacke hat zum Ziel, einen bestimmten Dienst für dessen Benutzer unerreichbar zu machen oder zumindest die Erreichbarkeit des Dienstes erheblich einzuschränken.

Drive-by Infektion eines Computers mit Malware allein durch Besuch einer Webseite. Oft enthalten betroffene Webseiten seriöse Angebote, sind aber zwecks Verteilung der Malware zuvor infiziert worden. Die Infektion erfolgt meistens durch das Ausnutzen von noch nicht geschlossenen Sicherheitslücken.

Malware (Schadsoftware) Oberbegriff für Software, die schädliche Funktionen auf einem Computer ausführt (beispielsweise Viren, Würmer, Trojanische Pferde).

Man in the Middle Bei einer Man-in-the-Middle-Attacke hängt sich der Angreifer unbemerkt in den Kommunikationskanal zweier Partner ein und kann dadurch deren Datenaustausch mitlesen oder verändern.

Phishing / Spear phishing Spionagemethode, um an vertrauliche Daten von ahnungslosen Internet-Benutzern zu gelangen, etwa Kontodaten von Online-Auktionsanbietern oder Zugangsdaten für das Internet-Banking. Die Betrüger nutzen Gutgläubigkeit und Hilfsbereitschaft ihrer Opfer aus, indem sie ihnen beispielsweise E-Mails mit gefälschten Absenderadressen zustellen.

Spear phishing: Gezielte Phishing-Attacke. Dem Opfer wird etwa vorgegaukelt, mit einer ihm vertrauten Person via E-Mail zu kommunizieren.

Ransomware Malware, mit der die Besitzer der infizierten Rechner erpresst werden sollen (ransom: englisch für Lösegeld). Dazu werden etwa Daten verschlüsselt oder gelöscht, und erst nach Lösegeldzahlungen werden die zur Rettung nötigen Schlüssel vom Angreifer zur Verfügung gestellt.

Skimming Skimming (englisch: Abschöpfen) bezeichnet eine Man-in-the-Middle-Attacke, die illegal die Daten von Kreditkarten oder Bankkarten ausspäht, namentlich indem Daten von Magnetstreifen ausgelesen und auf gefälschte Karten kopiert werden.

Social Engineering Social-Engineering-Angriffe nutzen die Hilfsbereitschaft, Gutgläubigkeit oder Unsicherheit von Personen aus, um beispielsweise an vertrauliche Daten zu gelangen oder die Opfer zu bestimmten Handlungen zu bewegen.

Spam Unaufgefordert und automatisiert zugesandte Massenwerbung, namentlich Spam-E-Mails. Als Spammer bezeichnet man den Absender dieser Mitteilungen, das Versenden selbst als Spamming.

Spoofing Spoofing sind Täuschungsmassnahmen zur Verschleierung der eigenen Identität in Computernetzwerken.

Begriffserklärungen in Anlehnung an das Verzeichnis der Melde- und Analysestelle Informationssicherung des Bundes (MELANI)
www.melani.admin.ch

Wie sollen wir mit der neuen Datenwelt umgehen?

Information wird neben Arbeitskraft, Rohstoff und Kapital als Produktionsfaktor immer wichtiger. Informationen erreichen uns heute über die verschiedensten Kanäle, vom Brief über das Radio bis zum Internet, und basieren sehr häufig auf computergespeicherten Daten. Daten werden von Menschen, immer häufiger aber bereits auch von Maschinen produziert. Die historische Mangelsituation hat sich heute zur Überflusssituation gewandelt. Aktuell verdoppelt sich der weltweite Datenbestand rund alle zwölf Monate: das ist wirklich erstaunlich.

Mit der «Informationsüberflutung» und der dahinterstehenden «Datenexplosion» stellen sich viele Fragen: Wie werden all diese Daten verwertet? Wem sollen sie zur Verfügung stehen? Welche Auswertungen sollen erlaubt, welche verboten sein? Welche Verantwortung haben wir gegenüber der Nachwelt, damit die richtigen Daten archiviert werden und auch lesbar bleiben?

Selbstbestimmung und Demokratie brauchen kritische Auseinandersetzung

Viele Untersuchungen haben ergeben, dass den meisten Menschen eine grundlegende Ausbildung und ein genügendes Verständnis für den «Digitalen Datenraum» fehlen, obwohl sie sich tagtäglich darin bewegen.

Minimale Grundkenntnisse bezüglich der Datenwelt sind für jeden Bürger und jede Bürgerin dringend notwendig, um die neuen Zusammenhänge zu erkennen, um bewusst und sicher zu handeln und die Konsequenzen ihrer Handlungen zu verstehen.

Fünf Themen, in denen Bürgerinnen und Bürger selber aktiv sein müssen

1. **Persönliches Datenmanagement:** Wie ein nachhaltiges persönliches Datenmanagement aussehen kann.
2. **Archivierung von Daten:** Welche Daten wie archiviert werden sollen.
3. **Vertraulichkeit und Geheimhaltung:** Weshalb Verschlüsselung von Daten und Zugangsberechtigungen wichtige Konzepte zum Schutz von Informationen sind.
4. **Big Data Analytics:** Wie mit Hilfe beliebiger Daten wesentliche statistische Aussagen gemacht werden können.
5. **Privatsphäre ist nicht Privatsache:** Welche Konzepte zum Schutz der Privatsphäre genutzt werden können.

Drei Themen, in denen Orientierung wichtig ist, wo aber der Staat verantwortlich ist

6. **Daten und Öffentlichkeit:** Open Government Data: Wie Datenbestände und Informationen der öffentlichen Verwaltung von Dritten genutzt werden (dürfen).
7. **Achillesferse Informatik der kritischen Infrastrukturen:** Wie der Staat Infrastrukturen, insbesondere kritische Infrastrukturen schützen kann.
8. **Kriminalität im Cyberspace:** Welche Gefahren im Cyberspace lauern.

1 Persönliches Datenmanagement

Wir leben heute in einer Informationsgesellschaft und nutzen Computer und Handy privat und in Beruf und Schule. Da ist es zunehmend wichtig, über die dabei verwendeten Daten den Überblick zu behalten. Eigene Interessen und Kontaktpersonen können wechseln, technische Probleme und Systemwechsel mit der Zeit den Zugang zu den eigenen Daten erschweren oder blockieren; jeder kennt das. Daher ist ein persönliches Datenmanagement nötig, besonders wenn auch Dritte auf eigene oder auf gemeinsame Daten zugreifen müssen. Das Datenmanagement betrifft einerseits die Ablage der Daten und anderseits das langfristige Aufbewahren und Auffinden der Daten.

Erstellen einer Liste der wichtigen Daten: Sie schafft Übersicht und hilft auch bei der Benennung von Dokumenten, Bildern, Passwörtern und Unterlagen aus der Zusammenarbeit mit Kollegen.

Gruppieren der Daten nach Aktivitäten: Datensammlungen sollen gruppiert werden. Professionell erfolgt dies mittels der konsequenten Abbildung von Aktivitäten, zum Beispiel in Projekte, und der konsequenten Zuordnung aller Daten zu jeweils einem Projekt.

Backups machen: Eigene und fremde Datenträger sind anfällig für Störungen. Bei externen Speicherdiensten besteht oft nicht einmal ein formeller Vertrag zur dauerhaften Datenspeicherung. In jedem Fall sollte regelmässig eine Kopie der Daten auf einem vom aktuellen System unabhängigen Datenträger gespeichert werden; dieser Datenträger soll an einem anderen Ort, das heisst möglichst nicht im gleichen Gebäude, gelagert werden. Von Cloud-Daten können lokale Backups automatisiert gespeichert werden und umgekehrt. So bleiben auch alte Daten, die in der Cloud gelöscht werden, zugänglich.

Datensammlungen für mehrere Personen: Daten, die man nicht selbst erzeugt oder für sich selbst speichert, beispielsweise Projektdaten, sollen auch in einer Liste definiert werden, die angibt, welche Datensammlungen für welche Personengruppen wichtig sind, wer darauf zugreifen darf und mit welchen Rechten (Leserecht, Schreibrecht, Recht zum Speichern oder Löschen von Daten, ...).

Empfehlung
Ein konsequentes Datenmanagement ist notwendig, damit sich mehrere Personen in einer Datenablage zurechtfinden, aber auch keinen Schaden anrichten können. Das geeignete Speichern von Daten für ein nachhaltiges Auffinden von länger gültigen Daten (zum Beispiel in PDF) ist ein wichtiger Bestandteil des Datenmanagements.

Rechtlicher Rahmen bei Dokumenten
Der Urheber jedes Dokuments oder Bilds – es wird der Begriff «Werk» verwendet – hat vorerst das alleinige Recht an dessen Weiterverwendung und Nutzung, das so genannte Urheberrecht. Zudem hat jede Person das so genannte «Recht am eigenen Bild» und muss gefragt werden, bevor Fotos von ihr weitergegeben werden. Diese beiden Rechte müssen beim Umgang mit Daten immer berücksichtigt werden, namentlich bei der Veröffentlichung im Internet. Achtung: Bei einigen kostenlosen Online-Diensten wird mit der Nutzungserklärung das Nutzungsrecht an den Dienstleister übertragen

2 Archivierung von Daten

Archivierung bedeutet hier die Langzeitaufbewahrung von Daten, damit diese auch nach Jahren und allfälligen Systemwechseln noch verfügbar gemacht werden können, wobei der Erhalt der Verfügbarkeit meist mit einem zusätzlichen Aufwand verbunden ist. Für die Archivierung gibt es viele Gründe, persönliche, gesetzliche und kulturelle. Ausser für Historiker sind gesetzliche und firmeninterne Gründe die wichtigsten. So müssen bestimmte Daten von Gesetz wegen «so, wie sie sind» (authentisch, revisionssicher, integer) aufbewahrt werden. Diese Anforderung bedingt besondere technische, organisatorische und inhaltliche Massnahmen.

Technische Anforderungen an digitale Archive

Viele nehmen fälschlicherweise an, dass Speichermedien wie Festplatten oder CD-ROMs Daten dauerhaft sichern. Das stimmt nur begrenzt, denn die dauerhafte Erhaltung von digitalen Daten und die Sicherstellung ihrer Lesbarkeit sind schon nach wenigen Jahren technologisch nicht mehr gewährleistet, weil neben den Datenträgern auch entsprechende Lese-/Schreib-Stationen und Betriebssysteme einsatzfähig bleiben müssen. Daten müssen redundant, das heisst mehrfach, auf unterschiedlichen Datenträgern und an unterschiedlichen Orten gespeichert werden, um die Gefahr eines (Total-)Verlusts zu minimieren. «Stabile», das heisst neutrale, öffentlich standardisierte, möglichst einfache Dateiformate ermöglichen, dass die Inhalte auch von künftigen technologischen Systemen geöffnet und gelesen werden können. Beispiele für stabile Dateiformate sind für feste Inhalte PDF, für Bilder PNG und JPG, für veränderbare Texte und Tabellen die OpenDocument-Formate (.odt, .ods). Bei Bildern kann es sich lohnen, diese sowohl in einem Bildformat als auch als PDF abzuspeichern. Von der Datenübernahme bis zur späteren Nutzung müssen archivierte Daten geschützt gespeichert werden, das heisst, jede Bewegung der Daten muss aufgezeichnet werden und einer Person zugeordnet werden können (zur Vertraulichkeit siehe Teil 3, Seite 6).

Inhaltliche Anforderungen

Daten sollen möglichst strukturiert – beispielsweise in Ordnern oder in Datenbanken – abgelegt und mit Metadaten beschrieben werden. Metadaten beschreiben die Merkmale von Daten wie inhaltliche Schlüsselwörter, Erstelldatum, Grösse und Dateinamen. Sie erleichtern das spätere Auffinden spezifischer Inhalte.

Der digitalen Archivierung stellen sich derzeit neue Herausforderungen: Dazu gehören etwa die Wiederverwendung der Daten für künftige Forschungsarbeiten, die Auswahl und Bewertung von digitalen Nachlässen und die Aufbewahrung und Vermittlung «komplexer» digitaler Objekte, die über die Struktur der klassischen Inventarisierung hinausweisen.

Internet ein Langzeitspeicher?

Digitale Langzeitarchive wandeln sich von statischen zu dynamischen Systemen, in denen die aufgenommenen Daten nicht mehr nur geordnet, verwaltet und dauerhaft gelagert, sondern auch im Internet zugänglich gemacht und aktiv bewirtschaftet werden. Zunehmend gibt es auch Internet-Archivdienste, die von Organisationen und Privaten genutzt werden können. Dass das Internet selbst vergisst, ist selten. Jedoch kann man sich nicht darauf verlassen, dass dort gespeicherte Daten später wieder zur Verfügung stehen: Dazu braucht es lokale Kopien.

Empfehlung

Verwaltungs- und Geschäftsdaten müssen professionell gespeichert und für digitale Archive zum Beispiel mit Metadaten aufbereitet werden.
Die Daten müssen rund alle fünf Jahre kopiert werden, damit sie lesbar bleiben. Ausserdem sollen für «nachnutzende» Generationen die Daten-Prozesse akribisch dokumentiert werden.

3 Vertraulichkeit und Geheimhaltung

Auch in der computergestützten Welt müssen Menschen und Organisationen vertraulich miteinander verkehren können. Dazu braucht es entsprechende Methoden, um Daten vor unerlaubtem Zugriff angemessen zu schützen.

Klassifizierungsstufen

Mit der Klassifizierung wird festgelegt, welche Vertraulichkeitsstufe ein Dokument haben soll und welchem Personenkreis dieses zugänglich gemacht werden soll. Dementsprechend müssen die Schutzmassnahmen gewählt werden. Bei vielen Dokumenten reicht ein relativ schwacher Schutz wie die Vergabe von Zugangsberechtigungen. Besonders schützenswerte Dokumente müssen verschlüsselt werden.

Schutz durch Zugangsberechtigungen

Eine einfache Möglichkeit, um die Vertraulichkeit von Daten zu gewährleisten, sind Zugangsberechtigungen. Bei Server-Systemen und Cloud-Anbietern werden damit die Daten von Nutzergruppen gegeneinander geschützt. Nach einem Anmeldeprozess, dem Login mit Passwort, ist der Benutzer dem System bekannt und hat Zugang auf die Bereiche, die er exklusiv nutzt oder mit anderen (Abteilung, Firma oder Spezialgruppen) teilt. Zugangsberechtigungen sind für den Alltagsgebrauch ausreichend sicher.

Vertraulichkeit durch Verschlüsselung

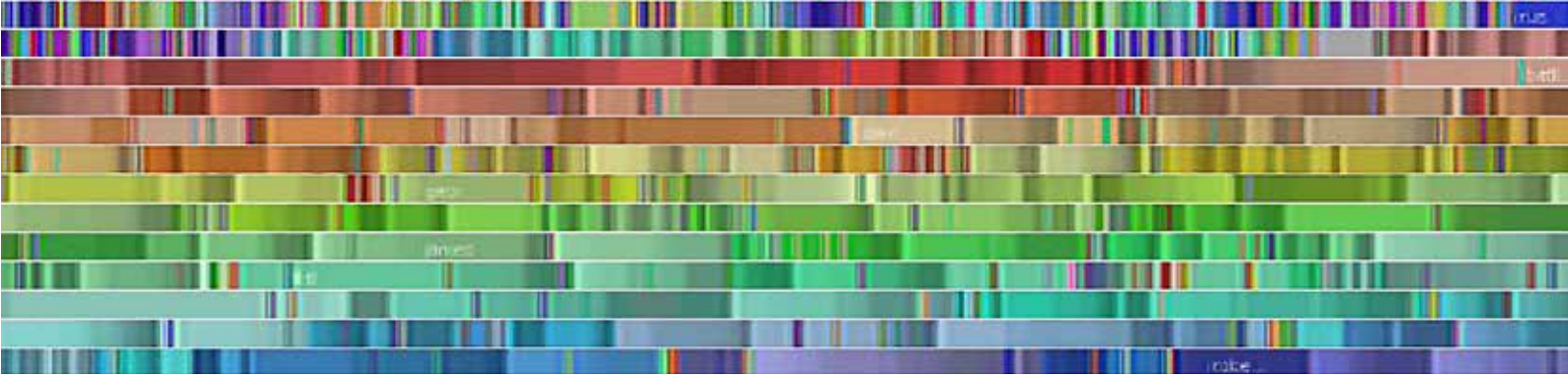
Daten-Verschlüsselung mit einem zweckmässig langen «Schlüssel» schafft stärkeren Schutz. Der Rechenaufwand, um einen solchen Schlüssel zu knacken, ist so gross, dass dieser in vernünftiger Zeit und mit üblichen Rechenanlagen nicht geknackt werden kann. Auch Verschlüsselung bietet allerdings nur einen relativen Schutz, der nicht ewig hält, weil die Rechenleistung stetig zunimmt und billiger wird.

Starke Verschlüsselung ist sehr wirkungsvoll: Sie gibt Organisationen – allerdings auch kriminellen oder terroristischen – die Möglichkeit, ihre Kommunikation geheim zu halten. Lässt der Staat diese Geheimhaltung zu, gewährleistet er zwar die Vertraulichkeit, kann aber Bürgerinnen und Bürgern nicht gleichzeitig den grösstmöglichen Schutz zum Beispiel vor Kriminalität bieten. In der Vergangenheit wurde dieses Dilemma so gelöst, dass die Schlüssel aufgeteilt wurden in einen Teil, der dem Staat bekannt ist, und einen Teil, der nur der vertraulich kommunizierenden Gemeinschaft bekannt ist. Besteht aus Sicht des Staates in ganz spezifisch definierten Situationen eine Notwendigkeit, kann er so auch auf verschlüsselte Daten zugreifen. Gegenüber Dritten sind die Daten aber immer noch geschützt. Doch unproblematisch ist diese «Lösung» nicht: Wenn der Staat rein technisch auf vertrauliche Kommunikation einer Gemeinschaft zugreifen kann, müssen die Regeln, in welchen Fällen der Staat von dieser Möglichkeit Gebrauch macht, klar festgelegt und kommuniziert werden.

Für sehr wertvolle Daten wie Informationen zu Bankkonten, Forschungsresultate von Firmen und Daten aus Leitsystemen von kritischen Infrastrukturen (Teil 7, Seite 10) genügen einzelne Massnahmen nicht. Für diese Daten muss ein Sicherheitsdispositiv erstellt werden, das wertvolle Objekte durch eine Vielzahl von Massnahmen und permanente Isolation gegenüber anderen Systemen direkt schützt.

Empfehlung

Daten müssen zweckmässig geschützt werden, damit die Vertraulichkeit gewahrt werden kann. Geeignete Massnahmen sind Zugangsberechtigungen für den Alltagsgebrauch und Verschlüsselung für besonders schützenswerte Daten. Mit der Klassifizierung wird die Vertraulichkeitsstufe eines Dokuments festgelegt. Für besonders schützenswerte Daten muss ein Sicherheitsdispositiv erarbeitet werden.



4 Big Data Analytics

Die verarbeiteten Datenmengen und die Vernetzung von Informatikanwendungen wachsen ständig: Versuche, das menschliche Hirn zu simulieren, weisen auf die Komplexität von neuen Anwendungen hin. Mit der ungebrochenen Regel, dass elektronische Bausteine alle 18 Monate ihre Speicherkapazität und damit auch die Computerleistungsfähigkeit verdoppeln, ist davon auszugehen, dass weiterhin völlig neuartige Anwendungen entstehen.

Heute werden auf die immer grösser werdenden Datenmengen, Big Data genannt, neue Verfahren, so genannte Big-Data-Analytics-Methoden, angewendet, um neuartige Erkenntnisse gewinnen zu können. Dazu wird die Gesamtheit der Daten, die für einen spezifischen Fragenkomplex massgebend sind, zusammengezogen **(Aggregation)**. Bisher wurden für Analysen und Prozesse primär strukturierte Daten aus Datenbanken ausgewertet; mit Big Data Analytics können dafür heute auch unstrukturierte Daten mit ausgefeilten statistischen Algorithmen ausgewertet werden. Diese Auswertungen liefern **Korrelationen**, das heisst, sie stellen Ähnlichkeiten fest. So können grosse Mengen von unbedeutenden Daten zu interessanten und sehr sinnvollen Aussagen führen. Jedoch sind die dargestellten Zusammenhänge nur statistischer Natur und erlauben keine Aussagen über Einzelfälle.

Auch zur Gewinnung solcher Auswertungen hat in der Cyberindustrie der Kampf um die Vorherrschaft bei der Speicherung grosser Datenmengen begonnen.

Politprognosen mit Big Data Analytics

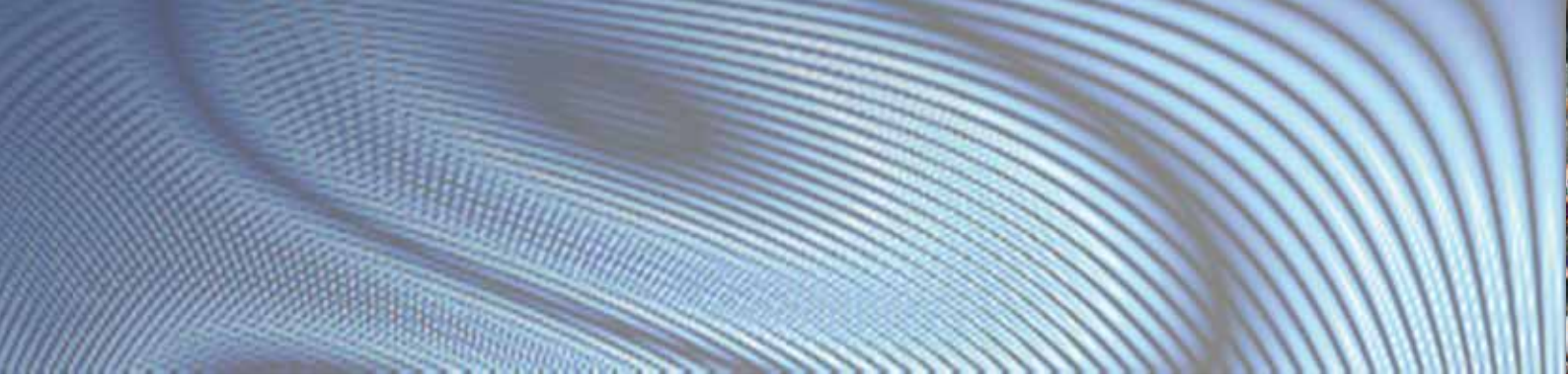
Das Massachusetts Institute of Technology (MIT) hat ein System entwickelt, das Daten aus verschiedenen Cloud-Dienstleistungen wie Blog, Facebook und Twitter nutzt und daraus Prognosen und Trendanalysen verschiedenster Art erstellt. Dieses System wurde erfolgreich für die Präsidentschaftswahl im Iran und in den USA bereits schon für die Nomination des Präsidentschaftskandidaten der Demokraten – Barack Obama oder Hillary Clinton – eingesetzt: Die dabei entstandenen Prognosen waren wesentlich genauer und zuverlässiger als klassische Verfahren.

Das Internet der Dinge

Das so genannte Internet der Dinge (Internet of Things, IoT) ist die kommunikationstechnische Vernetzung eindeutig identifizierbarer physischer Dinge, etwa vom eigenen Auto über den Kühlschrank bis zur heutigen Getränkelieferung, die miteinander kommunizieren und interagieren. Dies geschieht über Sensoren, Aktoren und Kommunikationstechnologie. Mit zunehmender Anzahl der durch das Internet verbundenen Objekte steigen die Möglichkeiten, Informationen zu senden, zu empfangen, zu sammeln, zu analysieren und auf Ereignisse zu reagieren. Bereits heute sind mehr elektronische Sensoren und Aktoren am Internet angeschlossen als von Menschenhand bediente Geräte. Experten gehen davon aus, dass schon bald das Internet der Dinge mindestens zehnmal grösser ist als unser bislang bekanntes Internet. Entsprechend umfangreich sind auch hier die Daten der Dinge, zum Beispiel Stromkonsum, Fahrverhalten von Autos, Standorte und Bewegungen von Smartphones; auch sie werden gesammelt und analysiert.

Empfehlung

Mit Big Data Analytics können aus scheinbar unbedeutenden Daten wesentliche Aussagen gemacht werden, die statistisch von Bedeutung sind, jedoch im Einzelfall nicht zutreffen müssen. Bürger sollen deshalb gut überlegen, welche Datenspuren sie in Speichern hinterlassen, bei denen Big-Data-Analytics-Methoden eingesetzt werden können.



5 Privatsphäre ist nicht Privatsache

Informationen entstehen immer in einem Kontext. Mit der Digitalisierung und Vernetzung werden persönliche Daten leicht aus dem Kontext gerissen. Wenn Sie beispielsweise über eine Krankheit im Internet googeln, weiss der Suchmaschinenbetreiber vermeintlich bald einiges über Sie. Vielleicht haben Sie aber nicht nach Ihrem eigenen Gebrechen gesucht, sondern nach der Krankheit eines Nachbars. Informationen ohne Kontext können also leicht missinterpretiert werden.

Im Grunde geht es im obigen Beispiel um die Privatsphäre und das Grundrecht auf «informationelle Selbstbestimmung». Sie sollen prinzipiell selber bestimmen können, wer über Sie was weiss. Klar braucht soziale Interaktion persönliche Daten, sonst bleibt Kommunikation oberflächlich. Klar braucht ein Lieferant Ihre Adresse, um Ihnen bestellte Ware zustellen zu können. Klar braucht der Staat persönliche Daten, damit er seine gesetzlichen Aufgaben erfüllen kann. Jedoch ist es europäische Philosophie, dass niemand «alles» über Sie wissen darf – es sei denn, dass Sie dem zustimmen.

Demokratie und Marktwirtschaft brauchen Privatsphäre

Das Gegenteil von Selbstbestimmung ist Fremdbestimmung. Doch damit funktionieren weder unsere Gesellschaft noch der Staat noch die Marktwirtschaft. Die Marktwirtschaft als System ist auf selbstbestimmt handelnde, mündige Konsumentinnen und Konsumenten angewiesen, die auch Manipulationsversuche erkennen können, damit der Wettbewerb wirklich zum Tragen kommen kann. Deshalb sollten wir einer Entwicklung, in der die Privatsphäre zu verschwinden droht, nicht tatenlos zuschauen.

Privatsphäre durch Eigenverantwortung: Selbstdatenschutz

Gratisangebote und Bequemlichkeit verlocken leicht zur Preisgabe von Teilen der Privatsphäre. Kurzfristiger Nutzen einer kostenlosen App, der Sie auf Ihrem Smartphone alle Zugriffsrechte einräumen, kann langfristige Folgen haben. Sind die dabei freigegeben Daten wirklich so «harmlos», dass Sie diese mit der App teilen und die Kontrolle darüber verlieren wollen?

Privatsphäre durch Technik: Anwendung eines Systemdatenschutzes

Moderne Computeranwendungen, auch viele Apps, unterstützen oft den Schutz der Privatsphäre der Benutzer, aber häufig erst nach sorgfältiger Einstellung ihrer Benutzungsparameter. Daher Vorsicht bei Neuinstallationen; nachträgliche Einstellungsveränderungen sind oft schwierig und unsicher.

Privatsphäre durch Recht

In allen Industrieländern gibt es Datenschutzgesetze für den Persönlichkeitsschutz in Informatiksystemen bis hin zu Auskunfts- und Berichtigungsrechten für die einzelnen Betroffenen. Aber diese Gesetze sind national ausgerichtet, sodass im globalen Cyberspace Regulierungslücken verbleiben, die straffrei ausgenützt werden können. Daher sind Anstrengungen im Verbund, zum Beispiel auf europäischer Ebene, notwendig, um Recht durchsetzen zu können.

Empfehlung

Selbstbestimmt handelnde, mündige Bürgerinnen und Bürger beziehungsweise Konsumentinnen und Konsumenten brauchen Privatsphäre. Für den Selbstdatenschutz ist jeder selbst verantwortlich. Dabei empfiehlt es sich, dem Prinzip der Datensparsamkeit zu folgen, das heisst, nur Daten bekannt zu geben, die wirklich von der Gegenpartei gebraucht werden.

Der Staat soll mit Anforderungen für den Systemdatenschutz sowie im Datenschutzrecht den Rahmen für eine sichere Privatsphäre schaffen.

6 Daten und Öffentlichkeit: Open Government Data

Behörden benötigen umfangreiche und qualitativ gute Datenbestände, um ihre gesetzlichen Aufgaben erfüllen zu können. Das so genannte Öffentlichkeitsprinzip verpflichtet die Behörden darüber hinaus, der Öffentlichkeit Informationen zur Verfügung zu stellen, die für die Meinungsbildung und für die Wahrung der demokratischen und rechtsstaatlichen Belange wichtig sind. Dies können beispielsweise Massnahmenpläne, Rechtsgutachten oder Rechenschaftsberichte, aber natürlich auch statistische Daten sein. Die Forderung von «Open Government Data» (OGD) ist die freie Zugänglichkeit und Wiederverwendung von Behördendaten als Teil der Umsetzung des Öffentlichkeitsprinzips. OGD sind ein junges, aber wichtiges Element im globalen Datenraum: OGD verstärkt die demokratische Kontrolle durch alternative Auswertungsmöglichkeiten und fördert die Erzeugung von neuem Wissen und Innovation.

OGD als Sekundärnutzung von Behördendaten

Die Veröffentlichung und Sekundärnutzung von Behördendaten ist in der Schweiz in Gesetzen, Verordnungen und Weisungen auf allen drei föderalen Staatsebenen geregelt, aber leider bisher nicht einheitlich, denn der Bund hat keine Gesetzgebungskompetenz für die kantonalen und kommunalen Verwaltungen. Datenschutz und Öffentlichkeitsprinzip sind auf Bundesebene, in den Kantonen und in grossen Gemeinden unterschiedlich gestaltet, was die Sekundärnutzung schwieriger macht.

Die Open-Data-Bewegung

Die Open-Data-Bewegung, welche die Freigabe von Behördendaten in den letzten Jahren wesentlich vorangetrieben hat, nahm ihren Ursprung vorab in den USA und verbreitete sich dann rasch weltweit. Aktivisten, denen der freie Zugang zu Daten, Informationen, Wissen und Software ein Kernanliegen ist, haben die Bewegung ursprünglich gegründet. Medienschaffende, Grafiker und weitere interessierte Kreise vorwiegend aus dem akademischen Umfeld haben sich der Bewegung angeschlossen und sind bereit, im Interesse der Allgemeinheit unentgeltliche Arbeit in die Aufbereitung und Nutzung frei zugänglicher Daten zu investieren. Tim Berners-Lee, der Erfinder des WWW und prominentester OGD-Promoter, propagiert bereits seit einigen Jahren die globale Vernetzung offener Datenbestände zu einem so genannten «Web of Data» mit neuen und wertschöpfenden Anwendungen.

Nutzen für Gesellschaft und Wirtschaft dank OGD-Anwendungen

OGD-basierte Anwendungen können verschiedensten Zwecken dienen. Oft werden dabei Daten aus unterschiedlichen Quellen miteinander kombiniert. Ein zusätzlicher Aspekt betrifft die Verbesserung und Anreicherung der Daten durch die Anwender selbst. Viele OGD-Anwendungen fallen unter die Kategorie «Helfer». Sie erleichtern den Alltag, gestalten den Umgang mit Behörden effizienter oder lassen komplizierte Sachverhalte durch Visualisierung der Daten leichter verstehen. Dazu gehören Anwendungen wie «Cycle hire», die aufzeigt, wo in London Mietvelos noch frei zur Verfügung stehen, und «Wheelmap», mit dem behinderte Menschen im Rollstuhl barrierefreie Wege finden können.

Politisches Diskussionsfeld

Open Government Data OGD können zu einem neuen politischen Verständnis mit mehr Transparenz und neuen Regeln führen. Dieser Prozess und die Veränderungen im politischen Gleichgewicht sollen beobachtet und neue Chancen frühzeitig identifiziert und genutzt werden.

7 Achillesferse Informatik der kritischen Infrastrukturen

Jede hochentwickelte Gesellschaft stützt sich heute auf kritische Infrastrukturen, welche die Verfügbarkeit von essenziellen Gütern und Dienstleistungen (Energie, Kommunikation, Transport, Zahlungsverkehr) sicherstellen. Deren grossflächige Ausfälle wirken sich schwerwiegend auf die Bevölkerung und die Wirtschaft aus; ebenso beeinträchtigen sie die Sicherheit und das Wohlergehen des Staates.

Cyberangriffe

Seit vielen Jahrzehnten werden Informatiksysteme für Betrieb und Überwachung von kritischen Infrastrukturen eingesetzt. Seit ihrer weltweiten Vernetzung über das Internet bilden diese Informatiksysteme jedoch ein neuartiges Angriffsziel für gegnerische Staaten, Terrorgruppen oder gar einzelne Verrückte, und zwar irgendwo auf dem Globus. Die Herkunft von Cyberangriffen ist vorerst unklar; da diese aus jedem Land stammen können. Heutige Ereignisse liegen oft im Graubereich zwischen einer Tat innerhalb des Landes und einem Angriff über die Landesgrenze hinweg. Nur langwierige und kostspielige Untersuchungen können Angriffe eindeutig zuordnen. Dabei stellen sich konkrete Fragen: Wer ist nun zuständig für die Verhinderung solcher Angriffe? Wer für die Aufklärung solcher Angriffe? Es gibt heute noch keine weltweite Vorgabe- und Regulierungsstelle, die mit entsprechenden Kompetenzen ausgerüstet ist. Es gibt jedoch Bemühungen, rechtlich Klarheit zu schaffen, zum Beispiel das Tallinn-Handbuch[1].

Schutzmassnahmen

Seit kritische Infrastrukturen und Dienstleistungen zunehmend privatisiert wurden und in der Wirtschaft zum Alltag gehören, ist der optimale Schutzgrad zum komplexen Diskussionsfeld zwischen Wirtschaft und Staat geworden. Im Falle des Internets möchte die Wirtschaft ökonomische Interessen schützen, während der Staat essenzielle Robustheit und Krisensicherheit fordert.

In der Schweiz existiert seit 2004 mit der Melde- und Analysestelle Informationssicherung MELANI eine Public Private Partnership (PPP) zwischen Bund, Kantonen und Privatwirtschaft, welche die Betreiber von kritischen Infrastrukturen in ihrem Informationssicherungsprozess unterstützt und den Informationsaustausch zu Cyberangriffen unter den Unternehmen fördert. Dazu liefert sie Einschätzungen zur Bedrohungslage, Warnhinweise und vorfallspezifische Informationen. MELANI betreut zurzeit einen geschlossenen Kundenkreis aus sehr wichtigen Organisationen und Unternehmen, die kritische Infrastrukturen für die Schweiz betreiben.

MELANI publiziert einen öffentlichen Halbjahresbericht, der die wichtigsten und aktuellsten Gefahren und Risiken erläutert, die mit den Informations- und Kommunikationstechnologien in der Schweiz und international einhergehen. MELANI leistet hierzu nicht nur eine Beurteilung und Empfehlung der zu treffenden Massnahmen, sondern auch einen Ausblick auf die zu erwartenden Tendenzen.

Politisches Diskussionsfeld
Der Dialog zwischen Wirtschaft und Staat beim Schutz von kritischen Infrastrukturen muss vertieft geführt werden und die Bestimmung der Kostenverteiler von Sicherheitsmassnahmen muss einer nachhaltigen Lösung zugeführt werden.

[1] Tallinn Manual on the International Law Applicable to Cyber Warfare, eine akademische, nicht-bindende Studie, wie das Völkerrecht, insbesondere das «jus ad bellum» und das humanitäre Völkerrecht, auf Cyber-Konflikte und Cyber-Kriegsführung angewendet werden kann.

8 Kriminalität im Cyberspace

Cyberkriminalität wird definiert als eine kriminelle Aktivität, die mehrheitlich im Cyberspace (Internet) stattfindet. Cyberkriminelle nutzen Eigenschaften des Internets und die Gutgläubigkeit der Anwender bösartig aus und begehen so Straftaten. Ein informatikgestütztes System zu bauen, dessen Eigenschaften nicht missbraucht werden können, ist aber kaum möglich, denn alle Technologien können für verschiedene Zwecke verwendet werden.

Die Ziele und das Vorgehen von Internetkriminellen sind fast so vielfältig wie das von herkömmlichen Rechtsbrechern. Die Ziele reichen von Bereicherung über Täuschung bis zu Schädigung und Zerstörung. Zum Vorgehen gehören das Ausspionieren (etwa von Passwörtern), das Lügen (etwa mit falscher Identität) und das Übertölpeln (etwa mit unfairen Wetten) sowie das Infizieren ganzer Computernetze mit Schadsoftware (Begriffe siehe Glossar, Seite 2).

Hinter cyberkriminellen Attacken können Einzeltäter stecken, aber auch Gruppen oder bei Angriffen auf kritische Infrastrukturen (Teil 7, Seite nebenan) sogar fremde Staaten. Und selbstverständlich verheimlichen und verschleiern Cyberkriminelle ihre wahre Identität und die eingesetzten Mittel so gut wie nur irgend möglich.

Die Täuschung, die hinter den Lockangeboten und anderen Verführungen in sozialen Netzwerken, Messaging-Plattformen, Diskussionsforen, Dating Sites und Auktionen steckt, lässt sich oft nur sehr schwer erkennen. Kriminelle versuchen auch, mit Zuwendung und Manipulation vorerst Vertrauen zu gewinnen, um finanzielle Vorteile oder sexuelle Handlungen zu erreichen; Kinder und Jugendliche sowie Betagte sind dabei besonders exponierte Gruppen.

Kreditkarten- und Bankkarten-Betrug sowie Diebstahl von vertraulichen Daten werden oft mit **Phishing** ausgeführt, einer gezielten Verführung des Internetnutzers zum Ausführen von Schadcode. Der Kriminelle will dabei eine fremde digitale Identität erschleichen und in deren Namen und aus deren Konto zum Beispiel Geld auf sein Konto überweisen. Phishing nutzt dabei Leichtgläubigkeit, Gier und guten Willen aus.

Mit unzähligen technischen Tricks werden beim **Hacking** Computer angezapft und Daten unberechtigt erschlichen. Es gibt aber auch den schlichten **Diebstahl** von Geräten wie USB-Memory-Sticks, Smartphones und Computern. Noch raffinierter ist es, wenn ein Täter ein Reparaturszenario vortäuscht oder sich als Dienstanbieter ausgibt, um an die gewünschten Daten zu gelangen. In der Schweiz ist bei Internetkriminalität gegen die Bevölkerung die Gemeinde- oder die Kantonspolizei zuständig. Nur in ganz wenigen und wohldefinierten Fällen übernimmt die Schweizerische Koordinationsstelle zur Bekämpfung der Internetkriminalität KOBIK die Untersuchung oder die Koordination.

Politisches Diskussionsfeld
Täter nutzen das Internet für unterschiedlichste Straftaten. Politik und Gesellschaft haben dabei die wichtige Aufgabe, mit Aufklärung, Kontrollen und Strafverfolgung einen sicheren Rahmen zu schaffen sowie unsere verletzlichen Kinder, Jugendlichen und Betagten besonders zu schützen. Erwachsene müssen mit gesunder Skepsis und Wachsamkeit im Internet unterwegs sein und sich über mögliche Gefahren regelmässig informieren.

SATW Geschäftsstelle
Gerbergase 5
CH-8001 Zürich
Telefon +41 (0)44 226 50 11
info@satw.ch
www.satw.ch

Zusammenstellung durch Beatrice Huber, SATW

Die Inhalte basieren auf einer SATW-internen Studie von Ivan Bütler, Adolf Dörig, Stefanie Frey, Solange Ghernaouti-Hélie, André Golliez, Marc Henauer, Marcus Holthaus, Tony Kaiser, Tabea Lurk, Beat Rudin, Gérald Vernez unter Koordination von Bernhard Hämmerli

Broschüre, Studie sowie weitere Informationen zu Cyber Security sind zu finden unter **www.satw.ch/cyber**

Zusammenfassung

Ein sicherer und nachhaltiger Umgang mit Daten ist möglich. Dazu müssen Bürgerinnen und Bürger jedoch aktiv werden und sich mit minimalen Grundkenntnissen des Cyberspace vertraut machen. Diese Broschüre gibt einen Überblick über fünf wichtige Themen in diesem Bereich: **Datenmanagement, Archivierung, Vertraulichkeit und Geheimhaltung, Big Data Analytics sowie Privatsphäre.**

Zusätzlich braucht es Aktivitäten, mit denen der Staat vorsorgt. Dazu sind folgende Themen dargestellt: **Open Government Data, Informatik der kritischen Infrastrukturen sowie Kriminalität im Cyberspace.**

SATW
Schweizerische Akademie der Technischen Wissenschaften
Académie suisse des sciences techniques
Accademia svizzera delle scienze tecniche
Swiss Academy of Engineering Sciences

Mitglied der
Akademien der Wissenschaften Schweiz