Arne Schönbohm

/// Informations- und Cyber-Sicherheit für den Bürger

Gefahren kennen, Privatsphäre schützen

Eine erfolgreiche Digitalisierung wird es ohne Cyber-Sicherheit nicht geben. Denn Informationssicherheit ist die Voraussetzung für Vertrauen in die digitalen Services. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) setzt sich dafür ein, dass Bürger dieses Vertrauen entwickeln und diese zu ihrem Vorteil sicher nutzen.

Informationssicherheit als Voraussetzung

Die Digitalisierung durchdringt unseren Alltag in nahezu allen Lebensbereichen: Smarte Navigations-Apps manövrieren uns am Stau vorbei, der Sprachassistent steuert die Heizung und dank vernetzter, mobiler Geräte können wir jederzeit und überall arbeiten. Im Bereich Bürgerkommunikation sorgen zunehmend partizipative Angebote für Transparenz und schaffen Raum für den Dialog. Mithilfe erster Bürgerservice-Apps können direkt Ideen eingebracht werden, in Chats gibt die Verwaltung Auskunft zu aktuellen Themen und in den Sozialen Medien kann jeder Einzelne mit Abgeordneten und Regionalpolitikern in Kontakt treten.

Jeder Einzelne kann über die Sozialen Medien in Kontakt mit Politikern kommen.

Doch während uns die digitalen Dienste immer mehr politische Teilhabe ermöglichen, nimmt die Anzahl und Qualität der Cyber-Angriffe auf staatliche und zivile Ziele eklatant zu. Verstärkt sind auch die kritischen Infrastrukturen im Fokus der Angreifer. Im Jahr 2018 waren allein 800 Millionen Schadprogramme im Umlauf, täglich kamen etwa 390.000 Varianten hinzu.[1] Eindrucksvoll verdeutlichen diese Zahlen eine hohe Dynamik bei der Weiterentwicklung von Angriffswegen. Mit jedem neuen Smartphone, Laptop

oder smarten Haushaltsgerät wird die verfügbare Angriffsfläche größer. Kriminelle entwickeln regelmäßig Methoden, um das smarte Zuhause anzugreifen. Ihr Ziel ist es, ins Heimnetz einzudringen, Daten zu stehlen oder Web-Transaktionen zu manipulieren. Anfang des Jahres 2019 konnten wir beobachten, wie vor allem politische Funktionsträger und öffentliche Persönlichkeiten Ziel einer Doxing-Attacke waren. Von ihnen wurden Daten zusammengetragen und gegen ihren Willen veröffentlicht. Dieses Beispiel zeigt: Identitätsdiebstahl ist längst ein Alltagsphänomen geworden, vor dem Anwender besser geschützt werden müssen.

Einen umfassenden Datenschutz kann es nur mit Datensicherheit geben.

Wenn Manipulation und Datendiebstahl jedoch keine Seltenheit mehr sind, stellt sich unmittelbar die Frage: Ist es unabwendbar, dass die grundgesetzlich geschützte Privatsphäre im digitalen Alltag verletzt wird? Die Antwort lautet natürlich: Nein, so ist es nicht. Doch unsere Privatsphäre ist stark angreifbar und nur, wenn wir die Informationssicherheit weiter ausbauen, wird uns die Digitalisierung gelingen. Denn einen umfassenden Datenschutz kann es nur mit Datensicherheit geben. Dafür werden wir allerdings an einigen Stellen unser Verhalten ändern müssen. Es geht darum, zu lernen, wie wir uns besser schützen – aber auch Dienstanbieter und Verwaltung sind in der Pflicht, Informationssicherheit so zu gestalten, dass wir Vertrauen in neue Technologien und Dienstleistungen entwickeln können.

Als nationale Cyber-Sicherheitsbehörde gestaltet das BSI Informationssicherheit in der Digitalisierung für Staat, Wirtschaft und Gesellschaft durch Prävention, Detektion und Reaktion. Durch seine integrierte Wertschöpfungskette der Cyber-Sicherheit identifiziert das BSI aus unterschiedlichen Quellen Bedrohungen, findet Lücken in bestehenden Systemen, warnt die Zielgruppen vor diesen Lücken und lässt diese Erkenntnisse bei der Neuentwicklung von Systemen einfließen. Es schafft Mindeststandards und verfolgt unter anderem das Ziel, das selbstbestimmte, sichere Handeln von Bürgern zu unterstützen. Das ist die Grundlage einer digitalen Bürgerkommunikation, denn nur im gesicherten Cyber-Raum können digitale Partizipationsansätze gelingen.

Datenschutz durch Datensicherheit

Um unsere Daten zu schützen, brauchen wir technische Standards, denen wir vertrauen können und die so nutzerfreundlich sind, dass wir sie auch anwenden. Zudem benötigen Privatanwender eine Orientierung, um selbst beurteilen zu können, welches Risiko sie bereit sind einzugehen und auf welche Weise sie ihre Daten sichern wollen. Diese Ansätze werden im Rahmen des digitalen Verbraucherschutzes vom BSI mit Nachdruck verfolgt.

Sicherheitsstandards für Dienstanbieter

Die großen Datendiebstahl-Vorfälle Ende des Jahres 2018 machten deutlich, wie interessant persönliche Online-Accounts für Cyber-Kriminelle sind. Schnell wird klar: Ein sicherer Zugangsschutz zu Online-Diensten ist ein absolutes Muss, doch ein starkes Passwort allein reicht in vielen Fällen nicht aus. Dienstanbieter sind ebenso in der Pflicht, die Daten ihrer Kunden zu schützen. Dazu müssen sie sichere Zugangsverfahren wie etwa eine Zwei-Faktor-Authentifizierung anbieten und ihre eigenen Anwendungen und Systeme noch besser gegen Cyber-Kriminalität schützen.

Ein weiteres Beispiel ist das Internet der Dinge. Mit zunehmender Digitalisierung gelangen immer mehr vernetzte Geräte in die Privathaushalte. Herzstück des heimischen Netzwerks ist der Router. Über dieses Gerät laufen alle Informationen und Daten, die ausgetauscht werden. Wer Zugriff darauf hat, der hat in den meisten Fällen auch Zugriff auf die privaten Daten. Darum erstellte das BSI die Technische Richtlinie „Secure Broadband Router“[2], die ein Mindestmaß an IT-Sicherheitsmaßnahmen festlegt. Dienstanbieter und Provider müssen zum Schutze der Nutzer ein einheitliches, hohes Sicherheitsniveau für ihre Leistungen umsetzen.

Zudem verfolgt das BSI generell das Ziel, dass Angebote standardmäßig sicher eingestellt beim Nutzer ankommen und sicher entwickelt wurden („Security by design“ und „Security by default“). Würden alle Produkte so entwickelt und ausgeliefert, liefen viele der heute erfolgreichen Cyber-Angriffe ins Leere. Und nicht zuletzt muss auch die Frage geklärt werden, wer in welchem Umfang für verwirklichte Risiken haftet.

Orientierung für Bürger

Grundvoraussetzung für eine sichere Partizipation ist die Entwicklung eines Risikobewusstseins, einer Beurteilungsfähigkeit von Problemen und der Kompetenz, dazu auch entsprechende Lösungen zu finden. Wer sich der Gefahrenpotenziale des digitalen Raums nicht bewusst ist, entwickelt kein Interesse an Schutzmaßnahmen. Aus diesem Grund müssen Bürger zielgruppenspezifisch in die Lage versetzt werden, Sensibilität für Informationssicherheit zu entwickeln und diese in ihrer Rolle als Verbraucher auch aktiv nachzufragen. Dazu gehören entsprechende Rahmenbedingungen, die Orientierung schaffen, damit Sicherheitsrisiken besser eingeschätzt und daraufhin Entscheidungen getroffen werden können. Deswegen plant das BSI in enger Zusammenarbeit mit den Verbraucherzentralen die Einführung eines IT-Sicherheitskennzeichens. Dieses soll zukünftig sichtbar machen, wie lange beispielsweise das Betriebssystem eines Routers noch durch Sicherheitsupdates aktuell gehalten wird.

Jeder muss sich der Gefahrenpotenziale des digitalen Raums bewusst sein.

So hat der Verbraucher die Chance, wirklich selbst zu bestimmen, welches Risiko er bereit ist einzugehen. Gleichzeitig wird IT-Sicherheit zum Bestandteil von Kaufentscheidungen. Darüber hinaus können sich alle Privatanwender beim Informations- und Beratungsangebot „BSI für Bürger“ über notwendige Schutzmaßnahmen ihrer Privatsphäre informieren. Dazu gehören neben Handlungsempfehlungen für den digitalen Alltag auch die Vermittlung von Hintergrundinformationen, um ein Verständnis zu Funktionsweisen und Gefahren im Cyber-Raum zu schaffen. Die komplexen Themen der Informations- und Cyber-Sicherheit werden für „BSI für Bürger“ einfach aufgearbeitet und stehen als Checklisten, in Experten-Interviews, animierten Videos und interaktiven Quiz zur Nutzung bereit. Dort sind auch technische Warnungen zu finden, die anlassbezogen zu aktuellen Sicherheitslücken in gängiger Software und zu verfügbaren Updates informieren. Zudem kann auch der Newsletter „Sicher • Informiert“ abonniert werden, der alle 14 Tage über Neuigkeiten aus der Cyber-Sicherheit berichtet. Insgesamt wurden über 16 Millionen Warn-E-Mails im letzten Jahr verschickt, um auf Gefahrensituationen aufmerksam zu machen.[3]

Sichere Strukturen für die Verwaltung

Hauptaufgaben des BSI ist die Abwehr von Cyber-Angriffen gegen die IT-Systeme des Bundes.

Einer der Hauptaufgaben des BSI ist der Schutz der IT-Systeme des Bundes. Hierbei geht es um die Abwehr von Cyber-Angriffen und anderen technischen Bedrohungen gegen die IT-Systeme und Netze des Bundes. Damit stellt das BSI sicher, dass die verfassungsrechtlichen Aufgaben ausgeübt werden können. So kann ein zuverlässiges, fälschungssicher dokumentiertes Verwaltungshandeln garantiert werden und der Staat mit seinen Bürgern lückenlos und gegen Manipulationen jeglicher Art geschützt kommunizieren. Denn in der digitalen Gesellschaft sind die Informationssysteme der Staatsgewalten zu kritischen Größen für das Funktionieren des Gemeinwesens geworden.

Deswegen setzte sich das BSI zuletzt auch für die Absicherung der Europawahl ein. Durch Beratungsleistungen wurde die Resilienz der Systeme gegen technische Manipulationsversuche im Umfeld der Wahlen erhöht, insbesondere auch durch einen intensiven Dialog mit den beteiligten Akteuren.

Cyber-Sicherheit ist eine gemeinsame Herausforderung

Die Gewährleistung von Cyber-Sicherheit als Voraussetzung für eine gelungene Digitalisierung erfordert eine ständige Überprüfung von Prozessen, Befugnissen und Zuständigkeiten. Daher soll das BSI als unabhängige und neutrale Beratungsstelle in Fragen der IT-Sicherheit für Bund, Länder, Unternehmen und Bürgerschaft mit einem neuen IT-Sicherheitsgesetz gestärkt

werden. Unternehmen und Hersteller von IT-Produkten, die von besonderem nationalen Interesse sind, sollen hierbei stärker in die Pflicht genommen werden.

Cyber-Sicherheit ist nur durch eine Zusammenarbeit zwischen Bund und Ländern zu erreichen.

In der Cyber-Sicherheitsstrategie für Deutschland wurde die Stärkung der Bund-Länder-Zusammenarbeit im Themenfeld der Informationssicherheit festgelegt. In den vergangenen zwei Jahren konnten bereits mit neun Bundesländern Absichtserklärungen für engere Kooperationen geschlossen werden. In diesem Rahmen wird die BSI-Präsenz in der Fläche ausgebaut, um die Länder und die Wirtschaft vor Ort noch besser unterstützen zu können. Mehrere Verbindungsbüros im Norden, Süden, Westen und Osten Deutschlands bringen die Dienstleistungen des BSI, die sich im Bund bewährt haben, noch näher an die Bundesländer heran. Die Beratungs- und Unterstützungsleistungen sind essenziell, um einer Fragmentierung im Bereich Cyber-Sicherheit entgegenzuwirken. Auf diese Weise können sich Bund und Länder gemeinsam der Verantwortung stellen, durchgehend ein qualitativ hohes und einheitliches Cyber-Sicherheitsniveau zu gewährleisten. Auch der globalen Herausforderung stellt sich das BSI durch aktive Mitarbeit in Gremien, darunter bei der EU und NATO, sowie in Zusammenarbeit mit anderen Staaten.

Bereits seit dem Jahr 2016 intensiviert das BSI den gesellschaftlichen Dialog zum Thema Cyber-Sicherheit in dem Projekt „Digitale Gesellschaft: smart & sicher (SuSi)“. Im Nachfolgeprojekt „Institutionalisierung des gesellschaftlichen Dialogs“ werden durch einen Multi-Stakeholder-Dialog neuartige Lösungsansätze entwickelt, wie Cyber-Sicherheit in Deutschland gestaltet werden kann. Der Dialogprozess umfasst eine jährlich stattfindende Denkwerkstatt und themenspezifische Workshops, Veranstaltungen und ergebnisorientierte Arbeitsgruppen.

Aktuell werden darüber hinaus bereits zahlreiche Aufklärungs- und Sensibilisierungsmaßnahmen umgesetzt. Viele davon in Zusammenarbeit mit Organisationen und Initiativen, die sich ebenfalls mit der Cyber-Sicherheit befassen. Darunter zum Beispiel die Verbraucherzentralen, die Polizeiliche Kriminalprävention der Länder und des Bundes sowie der Verein „Deutschland sicher im Netz“. Regelmäßig bringt das BSI auch die Cyber-Sicherheits-Initiativen Deutschlands an einen Tisch. Durch diesen regen Austausch und ein gemeinschaftliches Auftreten können Synergien genutzt und gemeinsame Botschaften breit kommuniziert werden. Denn Cyber-Sicherheit ist eine gemeinsame Herausforderung und kann nur im Zusammenspiel gelingen.

ARNE SCHÖNBOHM
Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI), Bonn

Weitere Informationen zu BSI für Bürger:

- https://www.bsi-fuer-buerger.de/
- https://de-de.facebook.com/bsi.fuer.buerger/

Anmerkungen

1 Bundesamt für Sicherheit in der Informationstechnik (BSI): Die Lage der IT-Sicherheit in Deutschland 2018, https://www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html, Stand: September 2018.

2 Bundesamt für Sicherheit in der Informationstechnik: Secure Broadband Router (BSI TR-03148), https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03148/tr03148_node.html, Stand: 16.11.2018.

3 BSI: Die Lage der IT-Sicherheit in Deutschland 2018.