Bundesverband IT-Sicherheit e.V.

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens "IT Security made in Germany". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Kommentierung

(Fragebogen des BMI zur Evaluierung der Cyber-Sicherheitsstrategie für Deutschland)

2020-08

1. Welche Schwerpunktthemen und Ziele der CSS 2016 haben sich bewährt? Welche Verabredungen, Strukturen und Maßnahmen wirkten sich positiv auf die Zielerreichung aus?

Alle vier Handlungsfelder waren in der Vergangenheit und sind in der Zukunft im Prinzip wichtig:

1. Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung
2. Gemeinsamer Auftrag Cyber-Sicherheit von Staat und Wirtschaft
3. Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur
4. Aktive Positionierung Deutschlands in der europäischen und internationalen Cyber-Sicherheitspolitik

Dennoch müssen wir feststellen, dass der Level an Cyber-Sicherheit und die notwendige Robustheit unserer IT-Infrastrukturen noch nicht hoch genug ist. Die Herausforderungen sind in den letzten vier Jahren größer und nicht kleiner geworden. Daher müssen die Handlungsfelder und deren Maßnahmen mit deutlich mehr Energie bearbeitet werden. Ein Ziel zu definieren reicht nicht aus, es muss auch mit konkreten, nachhaltigen Maßnahmen und einer geeigneten Struktur umgesetzt werden.

Aus diesem Grund sollte mit Hilfe einer sehr gut ausgestatteten Task Force eine geeignete Struktur aufgebaut werden, bei der mit allen Stakeholdern gemeinsam die Fortschreibung der Cyber-Sicherheitsstrategie durchgeführt und auch getragen wird. Durch die gemeinsame Verantwortung werden die notwendigen Maßnahmen auch konkreter, wirkungsvoller und nachhaltiger umgesetzt.

Weitere Aspekte

■ Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung

Digitale Kompetenz bei allen Anwendern fördern:
Digitale Systeme durchdringen inzwischen alle Bereiche der Gesellschaft. Das führt dazu, dass immer mehr Menschen mit digitalen Systemen konfrontiert werden und mit ihnen umgehen müssen, ohne die dazu nötigen Kenntnisse oder auch nur das nötige Grundverständnis zu haben. Ein gutes Beispiel ist die durch die Corona-Pandemie plötzlich eingeführte Nutzung von Online-Konferenzen in Schulen. Vielen, wenn nicht den meisten Lehrern fehlen Kenntnisse und Erfahrungen im Umgang mit diesen Werkzeugen und mit der Vermittlung von Lehrinhalten auf diesem Weg.

Voraussetzungen für sichere elektronische Kommunikation und sichere Webangebote schaffen:
Die Voraussetzungen sind sowohl aus technischer wie auch aus rechtlicher Sicht weitgehend gegeben. Es fehlt an der tatsächlichen Umsetzung in der Praxis. Förderinitiativen zur Sicherung (im Sinne der IT-Sicherheit) bestehender digitaler Angebote vor allem im KMU-Bereich könnten helfen.

Sichere elektronische Identitäten:
Technisch und rechtlich sind wir sehr weit. Es fehlt an der tatsächlichen Umsetzung. Die öffentliche Hand könnte hier viel bewirken, u.a. durch breite Nutzung des digitalen Personalausweises oder Technologien wir die Smartphone Bürger-ID bei behördlichen Angeboten im Netz (Bürgerportale).

■ Gemeinsamer Auftrag von Staat und Wirtschaft

Kritische Infrastrukturen sichern:
Das ITSiG hat da vieles bewegt und zum Positivem verbessert. Eine Ausweitung des Geltungsbereichs von ITSiG auf weitere Branchen, weitere Dienste und auch kleinere Betreiber (mehr in die Breite) ist mittelfristig nötig - evtl. unter Senkung der Anforderungen in weniger kritischen Bereichen.

Unternehmen in Deutschland schützen:
Noch besser wäre es, die Unternehmen würden sich selbst schützen. Das korrespondiert mit "Digitale Kompetenz bei allen Anwendern fördern". Der Schutz der Unternehmen durch den Staat bzw. staatliche Organe ist wichtig - besser wäre es aber, die Unternehmen zu befähigen, sich selbst hinreichend zu schützen. Das Augenmerk muss dabei besonders auf KMU liegen, die mit dieser Aufgabe bisher noch meist überfordert sind.

■ **Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur**

Strafverfolgung im Cyber-Raum intensivieren:
Es fehlt an wirksamen Mitteln der internationalen Strafverfolgung (siehe "Aktive Positionierung Deutschlands in der europäischen und internationalen Cyber-Sicherheitspolitik"), Frühwarnsystem gegen Cyber-Angriffe aus dem Ausland:

Datensouveränität:
Informationelle Selbstbestimmung des Dateneigentümers über die Verwendung seiner Daten und damit den generellen Schutz von Daten vor unberechtigtem Zugriff und Manipulation

Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung:
Insbesondere das Fördern digitaler Kompetenzen und Investition in digitale Bildung

Kooperation Staat und Wirtschaft:
Kritische IT-Infrastrukturen sollten von vertrauenswürdigen, sicherheitszertifizierten deutschen / europäischen Unternehmen bereitgestellt und abgesichert werden sollten. In diesem Zusammenhang sind europäische Initiativen zu begrüßen, um die Abhängigkeit von internationalen Anbietern zu reduzieren, ebenso wie der Auf- und Ausbau eines sicheren 5G-Netzes sowie ein flächendeckender Breitbandausbau.

2. Welche Schwerpunktthemen und Ziele der CSS 2016 erachten Sie als erreicht bzw. für überholt und bedürfen nach Ihrem Kenntnisstand zukünftig weniger Beachtung?

Die Aktivitäten im Umfeld des "Bundestrojaners“ durch die ZITiS im Handlungsfeld "Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur“ sollten umgehend gestoppt werden, weil sie allen anderen Maßnahmen entgegenwirkt und damit die Cyber-Sicherheitsstrategie unglaubwürdig erscheinen lässt.

3. Welche Schwerpunktthemen und Ziele sind seit der Fortschreibung der CSS im Jahr 2016 aus Ihrer Sicht hinzugekommen und bedürfen einer zusätzlichen Erwähnung? Welche Verabredungen, Strukturen und Maßnahmen können Staat, Gesellschaft und Wirtschaft festlegen und vereinbaren um die von Ihnen genannten Ziele zu erreichen?

Der Bundesverband IT-Sicherheit würde es begrüßen, wenn mehr Initiativen für die Verschlüsselung werthaltiger Daten von Unternehmen und zum Schutz der Privatsphäre umgesetzt würden, weil es für die fortschreitende Digitalisierung ein wichtiger und mit hohem Schutzpotenzial nutzbarer Sicherheitsmechanismus ist. Außerdem glauben wir, dass es dringend notwendig ist, eine vertrauenswürdige, digitale Cyber-Sicherheitsinfrastruktur aufzubauen, die z.B.:

- extended Zertifikates für mehr Vertrauen von Webanwendungen einfach zur Verfügung stellt,
- eine Alternative zu "Let´s Encrypt“ (mit einer Identitätsüberprüfung) schafft und
- für eine einfache Verschlüsselungen von E-Mail-Sicherheit, Chats, usw. sorgt.

TeleTrusT würde es begrüßen, wenn die Initiative GAIA-X für die Schaffung von mehr Unabhängigkeit und höhere Cyber-Sicherheit und Datenschutz als gemeinsames Ziel definiert würde.

Weitere Ziele, die in der Cyber-Sicherheitsstrategie eine höhere Bedeutung erlangen sollten, sind:

- Wiederansiedlung von IT-Produktion in Deutschland und Europa, um Versorgung zu sichern und Produkte mit hohen und höchsten Sicherheitsanforderungen unter kontrollierten Bedingungen herzustellen (wie GAIA-X)
- starkes Bekenntnis zu Open Source durch Einsatz (auch und insbesondere in der öffentlichen Verwaltung) und Unterstützung der Open Source Entwicklungsprojekte.
- Forderung nach und Durchsetzung von Komplexitätsreduktion (Komplexität ist der größte Feind der IT-Sicherheit).

- stärkerer Fokus auf Dezentralisierung von IT-Systemen und Verantwortung (insbesondere relevant im Bereich Digitale Identität, Self-Sovereign Identity (SSI), …).
- stärkeren Schwerpunkt auf den Stand der Technik legen (definieren, beschreiben, umsetzen)

Ergänzt werden sollte, dass nicht nur mit Providern und (KRITIS)-Anbietern zusammengearbeitet wird, sondern verstärkt mit den Herstellern und Lieferanten - das sowohl auf Hard- und Software-Ebene. Das ITSiG 2.0 schießt inhaltlich insoweit über die aktuelle Strategie hinaus.

Die Rolle des BSI sollte überdies stärker als bisher in der neuen Strategie Berücksichtigung finden, da sich das ansonsten mit dem zunehmenden Befugnisausbau nicht rechtfertigen lässt.

Das Identitätsmanagement ist ein Schüsselfaktor in jeder sicheren IT-Infrastruktur. Generell ist eine stärkere Berücksichtigung von eID und den in der eIDAS-Verordnung genannten Vertrauensdiensten in Technologie- oder IT-Sicherheitsrelevanten (Gesetzes)Initiativen wünschenswert.

Beim Thema "Sichere elektronische Identitäten“ ist aus unserer Sicht die mobile eID-Funktion zu ergänzen, die eine hochsichere, datensparsame und nutzerfreundliche Ergänzung zur online-Ausweisfunktion des Personalausweises darstellt und ihn über ein mobiles Endgerät - allen voran dem Smartphone - nutzbar macht. Zur Stärkung der sicherheitstechnischen Souveränität und Schaffung innovativer, nutzerfreundlicher und sicherer digitaler Angebote ist es notwendig, dass Sicherheitsmechanismen wie bspw. das Secure Element im Smartphone für die Wirtschaft zugänglich sind und der Zugriff darauf durch die Smartphone-Anbieter nicht verhindert wird.

Zunehmende politische Verunsicherung bei den Großmächten USA und China belasten das Vertrauen in IT-Systeme aus diesen Ländern. Insbesondere für alle kritischen IT-Systeme aber auch für IT-Systeme der Verwaltung generell sollte, soweit wie möglich, auf vertrauenswürdige, sicherheitszertifizierte deutsche/europäische Anbieter zurückgegriffen werden.

Zur Wahrung der digitalen Souveränität Deutschlands ist es unabdingbar Kompetenzen in Zukunftstechnologien wie Künstlicher Intelligenz, Blockchain oder Quantencomputern aufzubauen. Der Staat sollte seine Ressourcen gezielt einsetzen, um in diesen wichtigen Bereichen dem globalen Wettbewerb auf Augenhöhe zu begegnen.

Mobiles Arbeiten ist ein Schwerpunktthema seit Beginn 2020 und wird es für die kommenden Jahre bleiben. Hierdurch ergeben sich neue Sicherheitsrisiken für Firmen, denen sie durch sichere IT-Infrastrukturen sowie sichere Softwarelösungen für Kollaboration begegnen müssen. Bei Hardware, Software sowie Infrastruktursicherheit sollte vorrangig auf vertrauenswürdige, sicherheitszertifizierte deutsche / europäische Anbieter zurückgegriffen werden.

Standards und Zertifizierung: Wir benötigen EU-weit harmonisierte und anerkannte Sicherheitszertifikate. Deren einheitliche Auslegung und Anwendung schafft Vertrauen in die hiesigen Systeme und stärken die Kompetenz, sichere Systeme und Produkte zu beurteilen. Hier sind eine Vielzahl von Bereichen und Schlüsseltechnologien betroffen, darunter qualifizierte Zertifikate (zum Beispiel für Personen, Webseiten oder Unternehmen), aber auch Standards für die sichere Postquantenverschlüsselung oder sichere Plattformen. Mit der eIDAS-Verordnung wurde bereits ein EU-weiter Standard eingeführt, der nun stärkere Anwendung finden und verbindlich für alle Akteure im Europäischen Binnenmarkt festgeschrieben werden muss. Für mehr Rechtssicherheit, Verbindlichkeit und eine EU-weite Interoperabilität müssen zudem die Methoden und Arbeitsweisen im Rahmen der Anwendung von Standards und Zertifikaten harmonisiert werden. Dies gilt insbesondere für die Arbeit von qualifizierten Vertrauensdiensteanbietern.

Für Datensicherheit und zur Wahrung der Datensouveränität sollte grundsätzlich auf dezentrale Datenhaltung gesetzt werden. Nur beim Austausch, von Daten, zum Beispiel zwischen Behörden, sollte über einen Intermediär, also einen neutralen Dritten, sichergestellt werden, dass Daten im Rahmen geltender Regularien ausgetauscht werden. Weiterhin sollten im Sinne der Datensparsamkeit nur die benötigten Daten ausgetauscht werden. Nicht benötigte Attribute können beispielsweise pseudonymisiert werden.

4. Welche weiteren Änderungen an der CSS würden Sie begrüßen?

(Siehe auch Kommentare zu Frage 3)

Zu ergänzen wäre ein neuer Punkt: "Verstärkung der Kooperation und Vernetzung mit europäischen Einrichtungen, insbesondere der ENISA“, um auch das Thema "nationale Alleingänge“ stärker zu adressieren.

Geprüft werden sollte außerdem, ob man das Thema Transparenz bei der Umsetzung regulatorischer Vorgaben auf EU-Ebene adressiert - siehe auch EU-CSA.

Weitere Aspekte:

- IT-Sicherheitszertifizierungen (Fokus auf IT-Sicherheit 'made in Germany')
- Produkthaftung bei IT-Sicherheitslücken
- staatliche Beschaffung von IT nur mit nachweisbarem IT-Sicherheitsniveau
- Bekenntnis zu einer Cyber-Defensivstrategie, gegen Cyber-Offensivstrategie (keine Hackbacks)

5. Welche Anregungen haben Sie für den anstehenden Fortschreibungsprozess?

Um für die nächsten vier Jahre eine bessere Wirkung der Handlungsfelder und konkrete Maßnahmen zu erzielen, schlägt der Bundesverband IT-Sicherheit vor, die Cyber-Sicherheitsstrategie zusammen mit allen Stakeholdern im Rahmen einer gut aufgestellten und ausgestatteten Taskforce zu erarbeiten und die notwendigen Maßnahmen gemeinsam und nachhaltiger umzusetzen.

Wichtige Stakeholder sind: Anbieter- und Anwenderwirtschaft, Wissenschaft und Forschung sowie Politik und Staat. Die unterschiedlichen Stakeholder sollten direkt oder/und durch Interessenvertretungen aktiv sein. Der Mittelstand und die Nutzer sollten nur durch passende Interessenvertretungen repräsentiert werden.

Die meisten Akteure der Anbieter- und Anwenderwirtschaft wollen einen höheren Level an Cyber-Sicherheit und Robustheit zur Risiko-Minimierung erreichen. Die Budgets sind in der Regel vorhanden, nur die alleinige Vorgehensweise ist oft aufwendiger.

Das gemeinschaftlich mit allen Stakeholdern gleichzeitig zu tun, schafft deutlich mehr Wirkung der einzelnen Maßnahmen und bessere Zielerfüllung der gemeinsamen Cyber-Sicherheitsstrategie. In diesem Sinn würden wir uns eine engere Zusammenarbeit wünschen.