Digitale Gesellschaft e. V.
Groninger Str. 7
D - 13347 Berlin

(030) 450 840 18

info@digitalegesellschaft.de
www.digitalegesellschaft.de

Stellungnahme BMI Cybersicherheit

Digitale Gesellschaft e. V.

August 2020

Fragebogen zur Cyber-Sicherheitsstrategie

Die Cyber-Sicherheitsstrategie für Deutschland aus dem Jahr 2016 soll evaluiert und fortgeschrieben werden. Hierbei bitten wir Sie um Unterstützung. Bitte beantworten Sie folgende Fragen:

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

Kryptographie als zentrales Gestaltungsmittel

Bei der Analyse der Sicherheit von Computernetzwerken geht man in der theoretischen Modellbildung von sehr mächtigen Angreifern aus, die alle Nachrichten mitlesen und verändern können. Da das Internet auf der Grundphilosophie von offenem Zugang gründet, ist der Schutz von Daten Aufgabe der Kryptographie. Die in der Praxis eingesetzten kryptographischen Algorithmen haben die interessante Eigenschaft, daß Sie entweder für Niemanden oder nahezu für jeden Motivierten brechbar sind. Diese Eigenschaft verbietet eine Schwächung der Kryptographie. Kryptographie ist in vielerlei Hinsicht das einzig wirksame Werkzeug die Digitalisierung im Geiste einer freiheitlich demokratischen Grundordnung mitzugestalten. Die Grundlagenforschung insbesondere in den Bereichen Kryptographie und sicheres Systemdesign ist auszubauen. Anknüpfend an weltweit anerkannte Initiativen (beispielsweise GNU-Privacy Guard) soll die Förderung von Open Source Lösungen weitergeführt, erweitert und intelligent verstetigt werden.

Bedrohung der Inneren Sicherheit durch Sicherheitslücken

Sicherheitslücken können mit Hilfe von Angriffen ausgenutzt werden, bei denen es sich um kopierbare Programme handelt. Diese gefährlichen digitalen Waffen können selbst aus halbwegs engagierten Einzelpersonen mächtige Angreifer ganzer Wirtschaftssysteme machen. Im Falle von WannaCry ist die Weltwirtschaft nur wegen der diletantischen Programmierung vor einem katastrophalen Schaden bewahrt worden. Aus diesen Gründen scheint seit wenigen Tagen der US-amerikanische Nachrichtendienst NSA seine Veröffentlichungspraxis zu ändern.

Die in Deutschland durch die Gründung des BSI bisher angestrebte Trennung von Schutz der Bevölkerung und der Entwicklung von digitalen Angriffswaffen hat zu einer im Vergleich zu anderen Staaten höheren Vertrauensbildung geführt. Ausdrücklich lobend erwähnt sei die vertrauensbildende Arbeit des BSI im Falle Huawei. Diese hat im Bereiche des aufziehenden Handelskrieges zu einer Deeskalation beigetragen. Dieses Vertrauen sollte in einer immer instabileren Weltlage nicht aufs Spiel gesetzt, sondern gepflegt, ausgebaut und auch institutionell verstetigt werden.

- Das Nichtschließen von Sicherheitslücken bedroht angesichts der weiter fortschreitenden Vernetzung in den Bereichen Industrie und der kritischen Infrastruktur nicht mehr nur im digitalen Sinne Heimat und innere Sicherheit.

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

Systemrelevante Open-Source Softwareprojekte

Die genannten Open-Source Projekte stellen systemrelevante Sicherheitssoftware für den Erhalt der digitalen Souveränität dar. Eine nachhaltige Sicherung dieser Projekte ist wichtig für die digitale Souveränität und damit auch Aufgabe staatlicher Stellen. Aufgrund der vielen ehrenamtlichen Projektteilnehmer sind die entstehenden Kosten gering. Die Offenen Lizenzen garantieren die Nachhaltigkeit

- VeraCrypt: Festplattenverschlüsselung

Firmengeheimnisse und andere vertrauliche Daten sollten immer verschlüsselt gespeichert werden – vor allem, auf mobilen Geräten, die leicht gestohlen werden können. Das früher vielfach genutzte Truecrypt wird offiziell nicht mehr weiterentwickelt, aber die offene Lizenz erlaubte eine Weiterentwicklung unter dem Namen Veracrypt.

- Open SSH: Kommunikations-Sicherheit

Open SSH dient unter anderem der abhör- und fälschungssicheren Übermittlung von Steuerinformationen an eingebettete Systeme oder Internetserver.

- Open SSL: Datentransport-Sicherheit

TLS (Transport Layer Security) ist das im Internet am meisten genutzte Sicherheitsprotokoll. Leider gibt es immer wieder Sicherheitslücken im TLS-Protokoll, oder in einzelnen TLS-Bibliotheken. Open SSL ist die meistgenutzte und deshalb wichtigste TLS-Bibliothek.

- GNU Privacy Guard: Anwendungs-Sicherheit

Der GNU Privacy Guard wurde zum Versenden von verschlüsselten und unterschriebenen E-Mails nach dem Open PGP Standard entwickelt. GnuPG ist auch wichtig, um die Herkunft und Echtheit von Sicherheitsupdates zu überprüfen.

- Das TOR Projekt: Anonym Surfen

Mit Hilfe des TOR-Browsers kann man im Netz surfen, ohne seine Identität zu verraten. Das TOR Projekt wird momentan vorwiegend vom US Verteidigungsministerium finanziert.

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?

Fragen um die Digitalisierung des Gesundheitssystems sind zwar nicht erst nach dem Jahr 2016 entstanden, aber es erscheint uns wichtig, diese Fragen im Kontext der Cyber-Sicherheit verstärkt in den Blick zu nehmen.

Der Verlust von Zugangsdaten ist immer heikel und macht die Verletzlichkeit in der digitalen Welt deutlich. Der „Verlust“ von Gesundheitsdaten kann erhebliche Konsequenzen mit sich bringen. Die Informationen gehen dabei selbstverständlich nicht verloren, sondern sie werden im Gegenteil öffentlich und können unbegrenzt kopiert werden. Das kann einen tiefgreifenden Einschnitt bedeuten, der den Rest des Lebens verändert. Reisemöglichkeiten könnten eingeschränkt werden, Versicherungen stehen nicht mehr zur Verfügung, die Aussicht auf einen Job wird gemindert … Wenn in der Computer-Sicherheitsforschung die Meinung vorherrscht, dass Daten auf vernetzten Computersystemen generell als hackbar anzusehen sind, dann bedarf der Umgang mit Gesundheitsdaten ganz besonderer Aufmerksamkeit.

Soweit mit der Telematik-Infrastruktur eine sichere Kommunikation im Gesundheitsbereich geschaffen werden soll, ist diese Absicht zu begrüßen. Das Projekt scheint jedoch technisch nicht ausgereift und bedarf einer grundlegenden Überarbeitung. Im September 2019 schrieben wir in unserer Stellungnahme zum Entwurf eines Gesetzes für eine bessere Versorgung durch Digitalisierung und Innovation (Digitale Versorgung-Gesetz – DVG):

> *“Angesichts der Tragweite der vom DVG betriebenen Veränderungen und des Ausmaßes der Probleme beim Aufbau der Telematik-Infrastruktur fordern wir ein Moratorium in der Digitalisierung des Gesundheitswesens. (...) Zunächst muss über den Aufbau einer sicheren Telematik-Infrastruktur mit einem angemessenen Datenschutz- und Sicherheitskonzept befunden werden, bei dem die Interessen der Versicherten im Mittelpunkt stehen.”*
> https://digitalegesellschaft.de/2019/09/gegen-den-ausverkauf-der-gesundheitsdaten-fuer-ein-moratorium-in-der-digitalisierung-des-gesundheitswesens/

Mit dem im Juli 2020 verabschiedeten Patientendaten-Schutz-Gesetz ist die das Konzept verantwortende Gematik von der Verantwortung für Datenschutzverletzungen und Datenverlust freigestellt worden. Verantwortung kann aber in einem solchen Kontext nicht auf die (z.B. Arztpraxen) abgeschoben werden, die den Umgang mit den Gesundheitsdaten nicht beeinflussen können.

Zugleich werden immer neue zentrale Sammlungen von Gesundheitsdaten ermöglicht und weitere Auswertungen dieser Daten erlaubt. So wurde mit dem Gesetz für eine bessere Versorgung durch Digitalisierung und Innovation (DVG) ein Forschungsdatenzentrum geschaffen, in dem nach § 303d die Gesundheitsdaten aller Versicherten gespeichert, ausgewertet und einer langen Liste von Nutzungsberechtigten zur Verfügung gestellt werden. Die Daten sollen im Forschungszentrum

lediglich pseudonymisiert gespeichert werden. (siehe unseren Brief an die Bundestagsabgeordneten: https://digitalegesellschaft.de/2019/11/presseinformation-offener-brief-an-die-bundestagsabgeordneten-keine-zentrale-speicherung-von-gesundheitsdaten/)

Als Beispiel für die immer weitergehende Auswertung von Gesundheitsdaten sei darauf verwiesen, dass im Patientendaten-Schutz-Gesetz kurzfristig und ohne öffentliche Diskussion eine Regelung aus dem Digitale-Versorgungs-Gesetz geändert wurde. Bisher durften die Krankenkassen die Daten der Versicherten für eine marktorientierte Bedarfsanalyse auswerten. Ein individualisiertes "Angebot" sollte erst nach Zustimmung der Versicherten möglich sein, und damit auch die individualisierte Auswertung der Daten. Nach § 68b Abs. 3 SGB V (neu) darf die Krankenkasse jetzt individualisiert auswerten, und individualisierte Angebote unterbreiten. Der Versicherte hat nur die Möglichkeit dem nachträglich zu widersprechen. Der Bundesrat hatte schon bei Verabschiedung des ersten Gesetzes vor der „Gefahr der Diskriminierung von einzelnen oder bestimmten Risikogruppen" durch „individuelle Gesundheitsprofile" gewarnt.

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

5. Welche Anregungen haben Sie für den anstehenden Fortschreibungsprozess?

Da das Internet auf der Grundphilosophie von offenem Zugang gründet, ist der Schutz von Daten Aufgabe der Kryptographie. Die in der Praxis eingestzen kryptographischen Algorithmen haben die interessante Eigenschaft, daß Sie entweder für Niemanden oder für jeden Engagierten brechbar sind. Diese Eigenschaft verbietet eine Schwächung der Kryptographie. Kryptographie ist in vielerlei Hinsicht das einzig wirksame Werkzeug die Digitalisierung im Geiste einer freiheitlich demokratischen Grundordnung mitzugestalten. Die Grundlagenforschung insbesondere in den Bereichen Kryptographie und sicheres Systemdesign ist auszubauen. Anknüpfend an weltweit anerkannte Initiativen (beispielsweise GNU-Privacy Guard) soll die Förderung von Open Source Lösungen weitergeführt, erweitert und intelligent verstetigt werden.

Grundlagenforschung Kryptographie und Systemdesign

Die Grundlagenforschung insbesondere in den Bereichen Kryptographie und sicheres Systemdesign ist auszubauen. Anknüpfend an weltweit anerkannte Initiativen (beispielsweise GNU-Privacy Guard) soll die Förderung von Open Source Lösungen weitergeführt, erweitert und intelligent verstetigt werden.

Post-Quantum Kryptographie zwingend notwendig

- Mathematische Grundlagenforschung im Bereich der Post-Quantum-Kryptographie ist die einzige praktische Herangehensweise für mittel bis langfristige sichere Verschlüsselung und Signierung.

Sicherheitsproblem Industrievernetzung: Gefahren über die Digitale Welt hinaus

Die Sicherheitslage ist im Bereich des Internet-of-Things (IoT) aus einer Reihe von Gründen deutlich schlechter als in der klassischen Computerindustrie. Viele Geräte adressieren einen Markt mit sehr geringen Stückpreisen oftmals im einstelligen Eurobereich. Ein organisiertes Netzsicherheitsmanagement, welches die PC-Industrie über viele Jahre mit erheblichem Aufwand

aufbaute, ist im Massenanlagenbau meist nicht zu finden. Oftmals bestehen nicht einmal ausreichende Update-Möglichkeiten. Verschärft wird dies durch eine im niedrigpreisigen Gerätemarkt geringere Kundenbindung der Hersteller, so dass die Verbraucher nicht befriedigend über nötige Sicherheitsupdates informiert werden. Weiterhin haben viele eingebettete Systeme eine weit längere Einsatzzeit als persönliche Computersysteme. Diese kann beispielsweise bei smarten Heizungssteuerungen viele Jahre betragen. Schließlich ist auch bei vielen Verbrauchern oft nicht einmal das Wissen vorhanden, dass das wegen seiner Funktion angeschaffte Gerät einen wartungsintensiven Internet-Teilnehmer darstellt.

- Industriesteuerungen

  Von unsicheren IoT Geräten gehen Gefahren nicht nur für die digitale Welt aus. So können Störungen in industriellen Anlagen Katastrophen auslösen. Auch innerhalb der Hausvernetzungen liegen etwa bei der Heizungssteuerung nicht zu unterschätzende Gefahrenpotentiale vor. Zahlreiche Autoren demonstrierten, wie Angreifer bestimmte IoT-Geräte dazu bringen können, eine Infektion durch ein Schadprogramm weiterzugeben. Innerhalb weniger Minuten können sich Zehntausende von ungeschützten IoT-Geräten in einer Stadt zu einem einzigen, von den Angreifern kontrollierten Botnetz zusammenschließen.

- Haftung für Schäden

  Die seit geraumer Zeit vermehrt auftretenden Angriffe mit Millionen übernommener IoT Geräte zeigen eine neue Dimension des Problems. Für den Verbraucher entsteht unter anderem auch das Problem, dass mit übernommenen Geräten angerichtete Schäden die IP-Adresse des Besitzers als Angriffsherkunft hinterlassen. Dies kann sowohl juristische Folgen, als auch Folgen für die technischen Systeme haben. Abwehrmaßnahmen der angegriffenen Systeme können zu Störungen der unwissend für Angriffe missbrauchten IoT Systeme führen.

  - Aus Sicht des Verbraucherschutzes ist eine Klärung der Haftung für von IoT Geräten verursachte Schäden und eine stärkere Inverantwortungnahme der Hersteller herbeizuführen.
  - Umgekehrt muss von Verbrauchern verlangt werden, dass Sie für Geräte, die die Sicherheit der Allgemeinheit gefährden, die Verantwortung übernehmen und zumindest die Sicherheitsupdates der Hersteller auch einspielen, so es welche gibt.

- Sicherheitsupdates und Nachhaltigkeit

  Die Erfahrung der letzten Jahre lehrt, dass alle Kommunikationsgeräte zu einer Gefahr für ihre Nutzer und für die Allgemeinheit werden können, wenn nicht regelmäßig entdeckte Sicherheitslücken durch Sicherheitsupdates geschlossen werden. Ein wichtiger Grundsatz ist deshalb, dass während der gesamten Lebenszeit eines Gerätes Sicherheitsupdates geschrieben und installiert werden müssen. Eingebettete und IoT Geräte sind da keine Ausnahme. In der Praxis ist die Einhaltung dieses Grundsatzes ein Problem. Erstens haben die Hersteller, wenn sie ihre Geräte einmal verkauft haben, oft kein ökonomisches Interesse an einer weiteren Pflege und dem Erstellen von Sicherheitsupdates. Zweitens ist, vor allem bei kleinen Herstellern, nicht klar, wie lange dieser Hersteller am Markt sein wird, bzw. wie lange es eine verantwortliche Firma gibt, die Sicherheitsupdates erstellen kann. Um dieses Problem zu lösen, schlagen wir das Folgende vor.

Handlungsvorschläge IoT-Sicherheit

- Hersteller sind während der gesamten Lebenszeit eines IoT Gerätes dazu verpflichtet,

Sicherheitsupdates zu schreiben und an die Nutzer zu verbreiten.

- Wollen die Hersteller sich, nach Ablauf einer angegebenen Lebenszeit, dieser Verpflichtung entziehen, müssen sie spätestens zu diesem Zeitpunkt ihre Quelltexte als Open-Source veröffentlichen. Damit soll sichergestellt werden, dass zumindest Dritte das Schreiben und ggf. Verbreiten von Sicherheitsupdates übernehmen können.
- Soweit die Quelltexte der Hersteller anfänglich nicht Open-Source sind, müssen sie bei einem Treuhänder hinterlegt werden. Kommt ein Hersteller den genannten Verpflichtungen nicht nach oder existiert der Hersteller nicht mehr, sorgt der Treuhänder für die Veröffentlichung der Quelltexte als Open-Source.

Die Notwendigkeit der Datensparsamkeit

Beginnend mit dem Volkszählungsurteil des Bundesverfassungsgerichts (1983) hat sich in Deutschland ein weltweit beachtetes Datenschutzrecht in Gesetzgebung und Rechtsprechung entwickelt. Datensparsamkeit ist die verfassungsrechtlich und höchstrichterlich geforderte einzuhaltende Norm.

- Datenverzicht

  Heute müssen sich Datenschutzexperten daher auch in hoch konfliktäre Diskussionen einbringen. Das hier leider vorherrschende politische Diskussionsklima schreckt dabei verständlicherweise viele Wissenschaftler ab. Dennoch gebietet es die gesellschaftliche Verantwortung, darauf hinzuweisen, wenn technische Entwicklungen, wie eine allumfassende Überwachung oder die praktische Angreifbarkeit von Computersystemen, juristische Datenschutzsicherungen praktisch unwirksam werden lassen. In der Computer-Sicherheitsforschung herrscht die Meinung vor, dass Daten auf vernetzten Computersystemen generell als hackbar anzusehen sind.

  - Wenn man nicht bereit ist, das Risiko einer möglichen Veröffentlichung von vertraulichen Daten einzugehen, darf man die Daten gar nicht erst speichern.

- Daten von besonders gefährdeten Personengruppen

  Wer Daten speichert, oder eine Verpflichtung zum Speichern bestimmter Daten einführt, muss die Vorteile, die sich aus einer Speicherung ergeben, mit den Nachteilen, die sich aus einer Veröffentlichung der Daten ergeben würden, abwägen – selbst wenn eine Veröffentlichung der Daten nicht vorgesehen ist. Es genügt keinesfalls, die Daten nur rechtlich zu sichern (also, ihre Veröffentlichung zu verbieten bzw. unter Strafe zu stellen). Es genügt nicht einmal, die Daten, zusätzlich zu dem juristischen Schutz auch technisch zu schützen, mit Maßnahmen, die dem Stand der Technik entsprechen. Denn nicht einmal die Kombination von rechtlichen und technischen Sicherungsmaßnahmen gibt eine Garantie dafür, dass die Daten auf Dauer geheim bleiben. Erwachsen aus einer möglichen Veröffentlichung besonders schwere Nachteile für die Betroffenen, oder sogar eine Gefahr für Leib und Leben, müssen die Vorteile einer Speicherung diesen Nachteilen und Gefahren gegenübergestellt werden.