Ein Angebot von IJAB

WEBDAYS 2017 DEINE DATEN. DEINE SICHERHEIT. DEINE MEINUNG.
03.-05.11.2017 WANNSEEFORUM, BERLIN

Agenda

Jugendgerechter Daten- und Verbraucherschutz in der digitalen Welt

Verfasst von 60 Jugendlichen zwischen 16 und 21 Jahren
im Rahmen der IJAB-Jugendkonferenz „WebDays 2017“
vom 03. bis 05. November 2017 in Berlin

Workshop „Fairness im Netz“

Für uns bedeutet Fairness im Netz die Schaffung eines gesellschaftlichen Klimas, das von gegenseitigem Respekt geprägt ist. Wir fordern ein Internet, in dem die Demokratie frei ausgelebt wird und der Pluralismus unterstützt wird.

Dafür braucht es konkrete Unterstützung durch den Staat (z.B. Fortbildungsmaßnahmen für die Exekutive, bessere technische Unterstützung, Ressourcen und Mittel, um die bestehenden Gesetze umzusetzen) sowie die Förderung einer lebendigen, konstruktiven Debattenkultur (z.B. mit dem Fokus auf Digitalisierung in der Gesellschaft), sowohl online als auch offline.

Um die Debattenkultur im Netz zu fördern, sollte die Bildung lokaler Diskussionsgruppen unterstützt werden. Den Bürger/-innen muss vermittelt werden, dass sie ein Mitspracherecht haben und dies auch nutzen können. Zudem sollten Onlineportale eingerichtet werden, die Vernetzung und Verabredungen ermöglichen.

Vorhandene Online-Beteiligungsprojekte und Strukturen zur Vernetzung sollten zielgruppengerecht beworben werden. Dazu sollte eine konkrete Infrastruktur gefördert werden, auf die Projekte zugreifen können, um ihr Marketing zu unterstützen und so gezielt Gruppen erreichen zu können.

Im Zuge eines digitalen Generationenvertrages fordern wir die altersgerechte Aufklärung für jung bis alt. Dadurch sollen Vorurteile und Ängste im Umgang mit digitalen Medien abgebaut werden, ohne bestehende Risiken zu relativieren.

Es ist notwendig, bestehende Begriffsdefinitionen zu diskutieren und zu entwickeln. Dadurch wollen wir eine inflationäre Nutzung von Begriffen wie Hate Speech oder Fake News verhindern, damit sie durch zu häufigen Gebrauch nicht entwertet werden sondern der Wirklichkeit digitalen Geschehens entsprechen.

Workshop „Hacker Ethik“

Alle "nicht persönlichen" Daten sollten für die Öffentlichkeit jederzeit zugänglich und abrufbar sein (vgl. Informationsfreiheitsgesetz). Als öffentliche Daten sind nur solche anzusehen, die die Bürger/-innen bilden und informieren. Alle anderen persönlichen und privaten Daten sind schützenswert.

Jede/r Bürger/-in hat ein Anrecht auf den Schutz der Privatsphäre und persönlicher Daten im Internet. Denn auch hier müssen Grundrechte gewahrt werden, sodass beispielsweise Chatverläufe der Geheimhaltung unterliegen und nicht publiziert oder von Dritten mitgelesen werden dürfen. Bereits in der Schule sollte für den Umgang mit dem Internet und dessen Gefahren und Chancen sensibilisiert werden (z.B. in Seminaren, regelmäßigen Unterrichtseinheiten). Wichtig ist dabei, dass der Fokus auf dem verantwortungsvollen Umgang mit Medien liegt.

Wir fordern, dass staatlich geförderte Institutionen als öffentliche, anonyme Meldestelle für Sicherheitslücken dienen. Diese sollen den Bürger informieren und vor gemeldeten Sicherheitslücken schützen.

Diese Institution muss folgende Kriterien erfüllen:

- Sie muss die Bürger/-innen über Sicherheitslücken informieren.
- Bei Meldungen wird zuerst das Unternehmen informiert und eine Frist zum Schließen der Sicherheitslücken gesetzt. Wird diese Frist nicht eingehalten, wird eine Pressemitteilung veröffentlicht, welche über das gesamte Ausmaß der Sicherheitslücke informiert.
- Falls durch eine Veröffentlichung ohne Rücksprache mit dem Unternehmen ein Schaden entsteht, muss der/die Publizist/-in selbstverständlich die Verantwortung in Form einer angemessenen Strafe übernehmen.

Unternehmen sollten verpflichtet werden, Pentesting[1] durch unabhängige Institutionen durchzuführen. Hierfür müssen Standards entwickelt und umgesetzt werden. Zudem sollten "Bug Bounty"-Programme[2] gefördert werden.

Wir fordern eine politische Auseinandersetzung mit "GrayHat-Hacking"[3], um neue Wege für die Sicherheitsforschung zu öffnen.

Wir fordern, dass Vereine und Institutionen (wie z. B. der Chaos Computer Club) unterstützt werden, damit sie besser an der IT-Sicherheit arbeiten können.

---

[1] *Pentesting ist ein Test, bei dem die Sicherheit eines Rechners oder eines Netzwerks mit Mitteln und Methoden geprüft wird, die ein Angreifer (umgangssprachlich „Hacker“) anwenden würde, um unautorisiert in das System einzudringen.*

[2] *Ein Bug-Bounty-Programm ist eine Initiative von z.B. Unternehmen oder Regierungsstellen, bei der für die Behebung und Bekanntmachung von Software-Fehlern Sach- und/oder Geldpreise für die Entdecker vergeben werden.*

[3] *Ein Gray-Hat-Hacker (wörtlich: ein Hacker mit grauen Hut”) ist jemand, der ohne Vorsatz oder bösen Willen ethische Standards oder Prinzipien verletzt (anders als ein „Black-Hat-Hacker“, also ein Hacker mit schwarzem Hut). Häufig tragen diese Hacker dazu bei, Sicherheitsfehler festzustellen.*

Wir fordern, dass unabhängige IT-Fachleute bei der politischen und juristischen Entscheidungsfindung stärker einbezogen werden, um dem Internet als #Neuland in der Politik entgegenzuwirken.

Workshop „Fake News“

Gefälschte Nachrichten sind ein immer stärker werdendes Problem. Allerdings ist der Grat zwischen gefälschter Nachricht und der nach Artikel 5 des Grundgesetzes geschützten Pressefreiheit dünn. Wir fordern daher die Stärkung und Erhaltung der Pressefreiheit in vollem Umfang.

Die Aufklärung über Fake News in Medien wird immer wichtiger. Deshalb sollte das Thema in die Lehrpläne aufgenommen werden (z.B. Wie erkenne ich Fake News?). Zudem sollten Gelder für Aufklärungsarbeit in Jugendeinrichtungen zur Verfügung gestellt werden.

Wir fordern, dass Fake News in jedem sozialen Netzwerk konkret gemeldet werden können (z.B. über Buttons auf der Startseite). Geteilte Artikel sollen auf falsche Inhalte hin überprüft werden.

Soziale Netzwerke sollten dafür sorgen, dass eine einseitige Informationsbeschaffung („Filterblase“) vermieden wird, indem die im Netzwerk gezeigten Interessen von mehreren Quellen gespeist werden und bspw. auf der Timeline vorgeschlagen werden.

Viele Hoster der Webseiten befinden sich im EU-Ausland, was eine Strafverfolgung erschwert. Deshalb fordern wir auf europäischer Ebene eine stärkere Kooperation in Bezug auf die Strafverfolgung von auf Fake News spezialisierten Webseiten.

Workshop „Digitale Selbstbestimmung“

Unternehmen sollten verpflichtet werden, die Allgemeinen Geschäftsbedingungen, Datenschutzrichtlinien und alle weiteren Bestimmungen ihrer Webseiten in vereinfachter Form darzustellen.

Dies bedeutet, dass sie die Aspekte des Datenschutzes und der Privatsphäre zusammenfassen und in Form von rechtlich nicht bindenden "AGBs" in sogenannter "Einfacher Sprache" darstellen. Dabei sollte darauf geachtet werden, dass die Übereinstimmung zwischen den rechtlich bindenden AGBs und jenen in "Einfacher Sprache" möglichst groß ist.

Sobald Daten von den Verbraucher/-innen auf Webseiten erhoben werden, sollten Unternehmen transparent auf die Möglichkeit eines Auskunftsverfahrens nach den Paragrafen 19 und 34 des Bundesdatenschutzgesetzes hinweisen.

Aufgrund der globalen Reichweite des Internets brauchen wir auf internationaler Ebene Lösungen zur Verbesserung des Datenschutzes. Hierfür könnte der Schutz der persönlichen Daten als Menschen- oder Bürgerrecht im EU-Recht und perspektivisch im Völkerrecht verankert werden.

Alle Schüler/-innen kommen zwangsläufig in Kontakt mit digitalen Medien und dem Internet. Deshalb ist es elementar, dass die Schule dazu beiträgt, das Wissen und die Fähigkeiten über diese zu fördern und zu erweitern.

Der Umgang mit digitalen Medien sollte neben neuen pädagogischen Konzepten Teil der akademischen Ausbildung der Lehramtsstudierenden sein. Wissen kann nur dann vermittelt werden, wenn es auch selbst erworben wurde.

Der Umgang mit neuen Medien kann nur dann zielführend gelehrt werden, wenn die dazu notwendige Hardware flächendeckend zur Verfügung gestellt wird. Das heißt nicht, dass jede/r Schüler/-in einen tragbaren Computer bekommen muss, aber es darf kein Gefälle bei der technischen Ausstattung der Schulen geben.

Wenn Kompetenzen im Umgang mit den neuen Medien in schulischem Rahmen vermittelt werden sollen, müssen die Kernlehrpläne (Curriculae) angepasst werden. Wünschenswert wäre hierbei ein einheitlicher Maßstab, der länderübergreifend durchgesetzt werden kann.

Es sollte stärker an Konzepten zur Vermittlung von Digitalisierungskompetenzen geforscht werden.

Jugendliche beklagen oft, dass sie nicht genügend Kenntnisse im Umgang mit Verträgen und Gesetzen haben, die aber im Erwachsenenleben sehr wichtig sind. Die Kompetenz im Umgang mit diesen soll an beispielhaft ausgewählten AGBs sozialer Netzwerke demonstrativ erlernt und verdeutlicht werden.

Workshop „Überwachung“

Firmen müssen für bekanntgewordene Sicherheitslücken umgehend Sicherheitsupdates liefern.

Es ist nicht zulässig, diese Lücken offen zu lassen, da sie von anderen ausgenutzt werden können.

Sicherheits- und Funktions-Updates sind stets zu trennen. Die bisherige Kombination gefährdet die Sicherheit, denn viele Nutzer/-innen installieren Updates nicht, weil sie die Funktionalitätsänderungen der neuen Version nicht möchten oder die Notwendigkeit eines baldigen Updates nicht erkennen. Kund(inn)en müssen bei Verfügbarkeit eines Sicherheitsupdates zwingend auf die Notwendigkeit hingewiesen werden, sodass die Kunden die Mündigkeit erhalten, selbst über ihre Sicherheit zu entscheiden.

Sicherheitsupdates sind für die Dauer der Gewährleistung bereitzustellen. Das Ende der Gewährleistung des Produkts ist eindeutig anzugeben. Firmen müssen ein Änderungsprotokoll

(Changelog) ihrer Software bereitstellen. Dieses Changelog muss in der Sprache der Nutzer/-innen (d.h. in einfacher Landessprache) verfasst und ohne technische Vorkenntnisse verständlich sein.

Wir fordern mehr Transparenz und Kontrolle bei der Speicherung und Verarbeitung personenbezogener Daten.

Die Einsicht in die gespeicherten personenbezogenen Daten muss für die Bürger/-innen schneller und unbürokratischer erfolgen, zum Beispiel durch automatisierte Abrufmöglichkeiten. Dabei ist zu prüfen, ob die Möglichkeit besteht, die aktuell geltende Auskunftspflicht in eine Mitteilungspflicht aufzuwerten. Ein entsprechendes Verfahren ist von unabhängiger Stelle zu kontrollieren. Dabei sind auch die von den verarbeitenden Stellen eingesetzten Algorithmen regelmäßig zu prüfen.

Damit die aktuellen Diskussionen über die Überwachung kritisch begleitet werden können, fordern wir, dass der/die Bundesbeauftragte für Datenschutz unabhängig von der aktuellen Regierung wird.

Der/die Bundesdatenschutzbeauftragte darf nicht von der Bundesregierung vorgeschlagen werden. Dieses Vorschlagsrecht soll an die Opposition abgegeben werden oder er/sie soll von der Judikative gestellt werden. Für alle Datenschutzbeauftragten muss es einen verbindlichen Rahmen für die Qualifikation inklusive einer Prüfung mit den Schwerpunkten IT und Recht geben.

Kontakt:

Kira Schmahl
Projektreferentin „WebDays 2016“
IJAB - Fachstelle für Internationale Jugendarbeit der Bundesrepublik Deutschland e.V.
Godesberger Allee 142-148
53175 Bonn
www.ijab.de

Tel.: +49 (0)228 / 9506-104
E-Mail: webdays@ijab.de