Die Bekanntmachung in Zahlen

22
KLEINE UND MITTLERE UNTERNEHMEN

16
MILLIONEN EURO FÖRDERVOLUMEN

16
PROJEKTE

Impressum

Herausgeber
Bundesministerium für Bildung und Forschung (BMBF)
Referat Kommunikationssysteme; IT-Sicherheit
53170 Bonn

Bestellungen
schriftlich an
Publikationsversand der Bundesregierung
Postfach 48 10 09, 18132 Rostock
E-Mail: publikationen@bundesregierung.de
Internet: http://www.bmbf.de
oder per
Tel.: 030 18 272 272 1, Fax: 030 18 10 272 272 1

Stand
Februar 2017

Gestaltung
VDI/VDE-IT, AZ

Druck
MKL Druck GmbH & Co. KG, Ostbevern

Bildnachweis
Bonsum: Goodcoin
CISPA: PROMISE, SmartPriv
Fotolia.com:
Alphaspirit: Titel, maxsim: AN.ON-Next, Maksim Kabakou: AndProtect, bernardbodo: MoPPa, Velikov: PARADISE, gena96: VVV, Andrey Popov: SIOC, weerapat1003: PGuard
Fraunhofer SIT, Darmstadt: SeDaFa
Dr. Volker Roth: enzevalos
Presse- und Informationsamt der Bundesregierung, Steffen Kugler:
Porträt Prof. Dr. Johanna Wanka
Thinkstock:
LDProd: Die Bekanntmachung in Zahlen, myneData: Hemera, Wavebreakmedia Ltd: TRINICS, .sepy: SyncEnc
Universität Hamburg: AppPETs

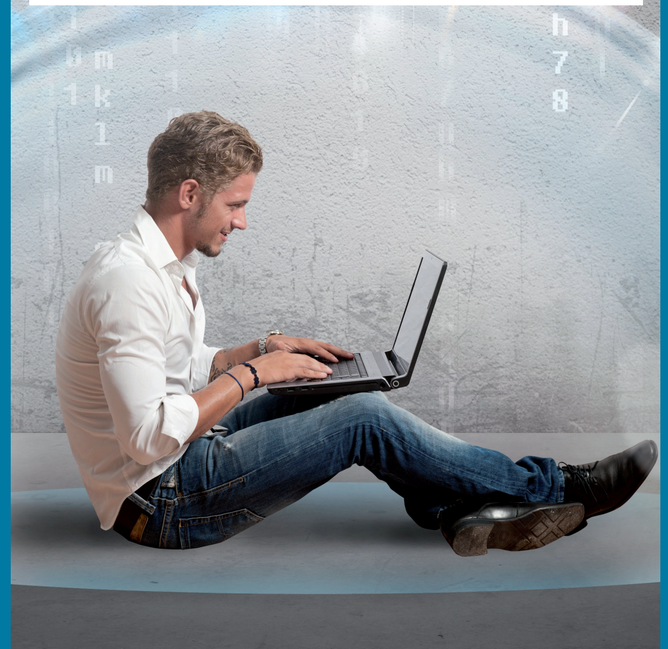
Mehr Informationen:
https://www.bmbf.de/de/informationsgesellschaft-weichen-fuer-die-zukunft-stellen-847.html

Bundesministerium
für Bildung
und Forschung

DIE NEUE HIGHTECH STRATEGIE
Innovationen für Deutschland

Sicher surfen im Internet

Datenschutz: selbstbestimmt in der digitalen Welt



Projekte für einen stärkeren Selbstdatenschutz

In Deutschland nutzt jede Person im Durchschnitt bereits mehr als zwei mobile Endgeräte. Unsere moderne Kommunikation hinterlässt dabei digitale Spuren, die wir regelmäßig in Kauf nehmen, um Dienste jederzeit und von jedem Ort aus nutzen zu können.

Anbieter von digitalen Dienstleistungen können so jedoch Profile der Nutzerinnen und Nutzer erstellen und erhalten potenziell tiefe Einblicke in das Leben der Betroffenen mit möglicherweise negativen Konsequenzen – oft, ohne dass diese es erkennen oder steuern können. So können beispielsweise in Folge einer Profilbildung Nachteile bei Versicherungs- oder Kreditabschlüssen entstehen oder die Stellen- und Wohnungssuche erschwert werden.

Die Bundesregierung hat im Rahmen des Forschungsprogramms für IT-Sicherheit „Selbstbestimmt und sicher in der digitalen Welt" die Erforschung neuer Ansätze und zukunftsfähiger Lösungen für den Selbstdatenschutz als Schwerpunkt gewählt. Die Projekte der Bekanntmachung „Datenschutz: selbstbestimmt in der digitalen Welt" sollen dazu beitragen, dass jeder die Kontrolle über seine personenbezogenen Daten behält und entscheiden kann, wer wann welche Daten zu welchem Zweck verwenden darf. So sollen alltagstaugliche Möglichkeiten für den selbstbestimmten Umgang mit sensiblen Daten eröffnet und geschaffen werden.

„Angesichts immer neuer technischer Möglichkeiten, Daten zu erheben und auszuwerten, müssen wir die zunehmende Besorgnis über die Sicherheit von privaten Daten ernstnehmen. Der Schutz der Privatsphäre muss in der digitalen Welt zur Selbstverständlichkeit werden."

Prof. Dr. Johanna Wanka
Bundesministerin für Bildung und Forschung

AN.ON-Next

Digitale Spuren im Internet können dafür genutzt werden, unkontrolliert Personenprofile anzulegen und diese z. B. an Werbenetze zu verkaufen. Um dies zu erschweren, sollen Mechanismen zur Anonymisierung in die Kommunikationsinfrastruktur des Internet integriert werden.

AndProtect

Wer eine App installiert, gewährt oft auch den Zugriff auf Positionsdaten, Kalendereinträge und andere schützenswerte Informationen. Wozu werden die Daten verwendet und welche werden weitergeleitet? Ein Analysewerkzeug soll diese Fragen beantworten.

AppPETs

Apps erfassen und verarbeiten persönliche Daten. Ob die Anbieter sorgsam mit diesen Daten umgehen, ist oft nicht transparent. Das Projekt schafft Abhilfe: Es stellt neue Werkzeuge und Komponenten zur Entwicklung datenschutzfreundlicher Apps bereit.

enzevalos

Um im Netz sicher zu kommunizieren, ist eine Ende-zu-Ende-Verschlüsselung nötig. Diese Technik wird im Projekt alltagstauglich umgesetzt – für eine einfache, benutzerfreundliche E-Mail-Verschlüsselung auf Smartphones.

Goodcoin

Wer eCommerce-Angebote nutzt, kann unfreiwillig zum „gläsernen Kunden“ werden. Eine Abhilfe sollen die sogenannten GoodCoins bieten – digitale Münzen für das anonyme Einkaufen im Internet, die gleichzeitig als Bonuspunkte für getätigte Einkäufe genutzt werden.

MoPPa

Das Privacy Paradoxon beschreibt die Tatsache, dass viele Menschen ihre Daten gerne geschützt wissen, gleichzeitig jedoch im Internet private Informationen preisgeben. Im Projekt wird dieser Sachverhalt aus technischer und psychologischer Sicht betrachtet.

myneData

Ein persönliches Datencockpit soll es Internet-Nutzerinnen und -Nutzern ermöglichen, die Freigabe sensibler Daten zu steuern und an der wirtschaftlichen Verwertung der eigenen Daten beteiligt zu werden.

PARADISE

Sportlerinnen und Sportler müssen bei Doping-Kontrollen sehr große Eingriffe in ihre Privatsphäre dulden. Dass es auch anders geht, zeigt PARADISE. Mit dem im Projekt entwickelten System muss der eigene Aufenthaltsort nur sehr kurz und nur bei Kontrollen offengelegt werden.

PGuard

Viele Apps werten personenbezogene Daten aus und leiten sie weiter. Damit Nutzerinnen und Nutzer dies gezielt einschränken können, werden die Datenströme der Apps ausgewertet und darauf basierend eine individuelle Risikoanalyse zur Verfügung gestellt.

PROMISE

Die Genomanalyse ist ein wichtiges Werkzeug für die Erforschung und Therapie vieler Krankheiten. Im Vorhaben sollen Methoden entwickelt werden, mit denen man die eigenen Genomdaten in der Cloud für Forscher bereitstellen und vor unerlaubtem Zugriff sehr sicher schützen kann.

SeDaFa

Das Internet hat Einzug in die Fahrzeugindustrie gehalten. Damit fallen viele Daten zum Fahrverhalten und zur Mediennutzung an. Im Projekt werden Konzepte entwickelt, um Fahrerinnen und Fahrern eine selbstbestimmte Kontrolle über den Zugriff auf ihre Daten zu ermöglichen.

SIOC

Beim Onlineshopping werden viele persönliche Daten abgefragt und vom Shop gespeichert – doch nicht alle davon sind für einen Kauf nötig. SIOC legt die Kontrolle über die Daten wieder in die Hände der Kaufenden, ohne die Geschäftsmodelle der Onlineshops zu beeinträchtigen.

SmartPriv

Im Projekt wird das Ziel verfolgt, uns allen wieder mehr Kontrolle über unsere persönlichen Daten auf dem Smartphone zu geben. Dazu sollen Interaktionsdialoge verständlich aufbereitet und mit personalisierten Beispielen ansprechender gestaltet werden.

SyncEnc

Das Büro von morgen ist papierfrei. Neben einem Tool werden rechtliche Rahmenbedingungen erarbeitet, die sicheres, kollaboratives Arbeiten im Netz in verschlüsselten Dokumenten ermöglichen: Nur berechtigte Personen können sensible Dokumente sehen und bearbeiten.

TRINICS

Apps nutzen Cloud-Dienste, die oft in Ländern mit niedrigeren Datenschutzstandards betrieben werden. Es wird ein Tool entwickelt, mit dem man die verwendeten Cloud-Dienste und deren Datenschutzrisiko ermitteln kann.

VVV

Verschlüsselung sichert E-Mails vor dem Mitlesen. Zum Entschlüsseln ist ein vertrauenswürdiger Schlüssel notwendig. Der Internetverzeichnisdienst DNS wird so erweitert, dass er im Sinne eines vertrauenswürdigen Adressbuchs genutzt werden kann. Damit wird Verschlüsseln einfacher.