RUHR-UNIVERSITÄT BOCHUM

RUB

RUBinform

Datenschutz & Datensicherheit

Newsletter 01|19

IN DIESER AUSGABE:

- WIE KANN ICH DA **SICHER SEIN?**
- **MÄRCHEN** WERDEN MANCHMAL **WAHR**
- **DAS SMARTE ZUHAUSE**
- DIE CLEVERE ALTERNATIVE: **SCIEBO**
- **FIREFOX-ADDONS**

LINKS ZU DEN BEITRÄGEN:

www.rub.de/rubinform

ZUALLERERST

Liebe Leserinnen und Leser,
ein 20-jähriger Schüler narrte zur Jahreswende Politiker und Prominente durch illegale Veröffentlichung privater Daten. Kurz danach fanden sich mehrere Tausend RUB-Nutzer auf den Passwort-Sammlungen Collection#1 bis #5 wieder. Erbeutete Daten wurden zusammengetragen und verdichtet, um dann z.B. in Erpressungsmails Anwendung zu finden. Auch hielt uns Emotet auf Trab: Auf infizierten Systemen analysiert der Trojaner Kontakte und E-Mails. Mit diesen Informationen gezielt erstellte und mit Schadcode versehene E-Mails verleiten ihre Opfer zum unbedachten Öffnen. *Bleiben Sie wachsam!*

Stabsstelle für Informationssicherheit und behördlicher Datenschutz

WIE KANN ICH DA **SICHER SEIN?**

Verschlüsselung im praktischen Einsatz

VERSCHLÜSSELN & DS-GVO

Alle Stellen der RUB, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben technische und organisatorische Maßnahmen (TOM) zu treffen, die erforderlich sind, um die Schutzziele des Datenschutzes zu gewährleisten. Erforderlich sind nur solche Maßnahmen, deren Realisierungsaufwand in einem angemessenen Verhältnis zum Schutzzweck steht. Art. 32 DS-GVO stellt dabei insbesondere die Verschlüsselung personenbezogener Daten als eine dem Stand der Technik angemessene Maßnahme heraus. So gelten die verschlüsselte Übertragung von Webseiten, insbesondere Formular- und Zugangsdaten, und transportverschlüsselte Mailübertragung als Mindeststandards.

RUB-Dienste im Vorteil

Zentrale Web- und E-Mail-Dienste der RUB erfüllen diese Anforderungen selbstverständlich. Daneben genügen diese und weitere RUB-Dienste in der Regel auch weitergehenden Anforderungen an Ausfallsicherheit und Datensicherheit. Wer statt Eigenentwicklungen oder vermeintlich günstigen, externen Online-Lösungen die zentral bereitgestellten oder vermittelten Dienste nutzt, ist also klar im Vorteil: die Verantwortung für die Einhaltung von Sicherheits- und Datenschutz-Anforderungen liegt beim Betreiber. Zur Dokumentation der technischen Maßnahmen reicht hier ein kurzer Verweis. Der Nachweis der Maßnahmen obliegt den zentralen Dienstleistern.

Auch bei Transport oder Ablage schützenswerter Daten in externen Netzen oder mit privaten Geräten sind geeignete Schutzmaßnahmen zu treffen, z.B. Verwendung eines VPN-Tunnels oder Datenträger-/Dateiverschlüsselung. BS

Sie verwenden starke Passwörter, halten Hard- und Software aktuell? Sie agieren umsichtig im Internet und sichern regelmäßig Ihre Daten? Prima! Damit sind Sie in puncto Sicherheit bereits gut aufgestellt. Wir erklären, wie Sie im Netz noch sicherer vorgehen. Welche Tools gibt es? Worauf gilt es zu achten? Diese und andere Antworten, praktische Tipps und Hintergrundwissen finden Sie im Dossier Verschlüsselung auf unserer Homepage.

Kommunikation im Internet und Datenspeicherung erfolgen in der Regel ungeschützt: Wer Zugriff auf einen Rechner, eine Speicherkarte oder auf das Rechnernetz erlangt, kann Informationen abgreifen oder verändern. Seit Edward Snowden wissen wir, wer an unseren Daten interessiert ist. Staatliche Stellen verschaffen sich Hintertüren oder nehmen Online-Dienste in die Pflicht. Der Zugriff auf Nutzer-Daten gehört gelegentlich gar zum Geschäftsmodell. Meist kann Verschlüsselung helfen, Kommunikation und Datenspeicherung sicher und privat zu gestalten. Kryptographie, die Wissenschaft der Verschlüsselung, stellt Verfahren zur Verfügung, Informationen unverständlich für Außenstehende aufzubereiten. Nur Eingeweihte können mit Hilfe sogenannter Schlüssel oder Codes Daten wieder verständlich darstellen. Auf verwendete Codes gilt es aufzupassen, da ohne sie verschlüsselte Daten praktisch nutzlos sind.

Sicher im Netz

Die Übertragung von Daten erfolgt immer öfter über verschlüsselte Verbindungen. Damit Passwörter, E-Mails und Daten nicht manipuliert oder mitgelesen werden, sollten Webseiten möglichst über https angesteuert und Mailtools über STARTTLS/SSL verbunden werden. Die Schlüssel zur Kommunikation werden von den beteiligten Geräten ausgehandelt. Rückschlüsse auf die Reputation eines Dienstes lässt die Transportverschlüsselung indes nicht zu. Auf den beteiligten Servern und Kommunikationsstellen selbst liegen Dokumente oder E-Mails in der Regel unverschlüsselt.

Thema E-Mail

Die Ende-zu-Ende-Verschlüsselung sorgt dafür, dass verschlüsselte E-Mails erst vom Adressaten entschlüsselt werden können. Weder Mailprovider noch andere Kommunikationsstellen können diese Mails entschlüsseln. Angehörige der RUB können sich zu diesem Zweck kostenlos S/MIME-Zertifikate ausstellen lassen. Die Entschlüsselung einer Mail erfolgt je nach verwendetem Mailprogramm teils automatisch, da der notwendige Schlüssel bereits zuvor installiert wurde.

Digital signierte E-Mails werden von Mailprogrammen automatisch auf Unversehrtheit und Authentizität des Absenders überprüft. Empfänger können die Echtheit einer Mail damit leichter beurteilen.

Geräte, Medien und Daten sichern

Sind einzelne Dateien zu schützen, sollte man sich nicht auf die Verschlüsselung in gängigen Office-Programmen verlassen, deren Schutz häufig mit einfachen Mitteln zu brechen ist. Sinnvoller ist der Einsatz von Verschlüsselungstools. Empfänger der verschlüsselten Daten müssen neben dem Verschlüsselungstool auch den Zugangscode kennen. Die Daten bleiben geschützt, solange sie nicht in einem anderen Format gespeichert oder entpackt werden.

Zum Schutz der Daten bei Verlust, Diebstahl oder im Wartungsfall bietet sich die vollständige Verschlüsselung von mobilen Geräten, Festplatten und Speichermedien an. Dabei sind sämtliche Daten, temporäre Dateien, Profile und Einstellungen verschlüsselt. Nach erfolgreicher Anmeldung am System sind die angeschlossenen Medien entschlüsselt einsatzbereit. Je nach Software und Bedarf kann man auch die erneute Eingabe des Zugangscodes nach eigenen Zeitfenstern einstellen. An anderen IT-Geräten können die verschlüsselten Medien nur nach Eingabe des Zugangscodes verwendet werden. Werden Dateien eines verschlüsselten Laufwerks versendet oder auf ein unverschlüsseltes Laufwerk kopiert, wird die Verschlüsselung entfernt.

Speichern in der Cloud

Wer Cloud-Speichern misstraut, ist gut beraten, nur verschlüsselte Inhalte in der Cloud abzulegen. Verschlüsselungstools stellen die unverschlüsselten Daten als Laufwerk auf dem eigenen Rechner bereit, während die Übertragung in die Cloud stets nur verschlüsselt erfolgt. BS

DAS SMARTE ZUHAUSE

Der Mensch des 21. Jahrhunderts träumt von einem smarten Zuhause, in dem Fernseher, Videorecorder, Heizung, Lampen, Kühlschrank, Rollläden, Türschließsystem, Videoüberwachung, Staubsauger, Rasenmäher und viele Dinge mehr übers Internet per Smartphone-App oder Sprachassistenten ferngesteuert werden können. Dies „Internet der Dinge (IoT)" verspricht Arbeits- und Zeitersparnis, mehr Lebensqualität, Sicherheit und Komfort. Der US-Marktforscher Gartner prognostiziert, dass im nächsten Jahr 20 Milliarden Geräte weltweit vernetzt sein werden.

Schönheitsfehler und Sicherheitslücken

Laufend kommen neue Produkte auf den Markt, alles quasi kleine Computer mit Internetanschluss. Dabei stehen die leichte Bedienbarkeit und schnelle Platzierung auf dem Markt bei den Herstellern eher im Fokus als die Sicherheit der Systeme. Schwachstellen im „Betriebssystem" oder ein unzureichender Schutz des Zugangs sind leider keine Seltenheit. Angreifer können so Systeme kompromittieren und Benutzern direkt Schaden zufügen, etwa durch Sabotage der Gerätefunktion (Erpresserbotschaft statt Fernsehprogramm). Die Intention der Kriminellen liegt aber auch darin, diese Systeme möglichst unbemerkt zu verwenden, um damit Angriffe auf weitere Ziele durchzuführen: Millionen Systeme werden zu Botnetzen zusammengefasst, die für DDos-Attacken (Überlastung von Internet-Diensten) genutzt werden.

„Oh shit"

Das sagte nicht nur Daniel K., das denkt sicher auch der stolze Eigentümer, wenn unerwartet die Polizei vor seiner Tür steht.

Daniel K. hatte sich mithilfe des Schadcodes Mirai ein eigenes Botnetz aufgebaut. Er flog Ende 2016 beim Versuch dieses zu erweitern auf: durch einen „Programmierfehler" waren Router der Telekom lahmgelegt und hunderttausende Nutzer vom Internet abgeschnitten worden. In Deutschland wurde er zu einer Bewährungsstrafe verurteilt und direkt aus dem Gerichtssaal an das Vereinigte Königreich ausgeliefert. Dort sitzt er eine Gefängnisstrafe von 32 Monaten ab. Danach wird er mutmaßlich an die USA ausgeliefert – er hat eben weltweit agiert.

Smart und sicher

Ein smartes Zuhause will fachgerecht administriert sein. Dabei sollten bei der Kaufentscheidung nicht nur Bequemlichkeit oder besser Begehrlichkeit den Ausschlag geben. Im März beschloss die EU den Cybersecurity Act, demnach sollen in Zukunft Systeme mit einem Gütesiegel versehen werden. Dies soll garantieren, dass Hersteller einen Mindeststandard an Sicherheit einhalten. Das BSI fasst in wenigen Schritten zusammen, wie ein Zuhause smart und sicher wird. **BW**

DIE CLEVERE ALTERNATIVE

sciebo – die Campus-Cloud

In der Reihe „Die clevere Alternative" werden wir Online-Dienste vorstellen, die an der RUB genutzt werden können und die eine Alternative zu gängigen Diensten großer Anbieter darstellen. Über die direkte Anmeldung mit der RUB-LoginID lassen sie sich einfacher in den Alltag der Hochschule einbinden und bieten zudem einen besseren Datenschutz. Die Nutzung für dienstliche Zwecke ist ebenso zulässig.

Cloudspeicher-Dienste für Fotos, Videos und Dateien aller Art sind aus unserem privaten Alltag nicht mehr wegzudenken. Neue Fotos werden direkt mit der Familie über die gemeinsame iCloud geteilt und alle wichtigen Dokumente in der Dropbox abgelegt. Auch im Hochschulalltag bietet das einfache Synchronisieren und Teilen von Dateien und das gemeinsame Erstellen und Bearbeiten von Dokumenten viele Vorteile. Bei der Nutzung gibt es doch einiges zu beachten, um die Anforderungen zu erfüllen, die aus Sicht des Datenschutzes und der IT-Sicherheit an Cloud-Dienste gestellt werden. Beispielsweise werden Verträge zur Auftragsdatenverarbeitung erforderlich und zusätzlich „geeignete Garantien", wenn ein internationaler Datentransfer vorliegt, z. B. in die USA zu einem der großen Cloud-Dienste.

Seit Oktober 2017 nimmt die RUB an sciebo (Ski-Boh gesprochen) teil. Eine von mehreren Hochschulen in NRW gemeinsam betriebene Lösung auf Basis von Owncloud. Jede/r Studierende der teilnehmenden Hochschulen bekommt ein Speicherkontingent von 30 GB zur Verfügung gestellt, MitarbeiterInnen können dieses auf 500 GB erhöhen. Zusätzlich lassen sich für einzelnen Projekte sogenannte „Projektboxen" anlegen.

Mit sciebo können Dateien und Ordner mit einzelnen Personen oder mit Gruppen geteilt werden. Zusätzlich können über wahlweise passwortgeschützte private und öffentliche Links auch größere Gruppen außerhalb von sciebo beteiligt werden. Des Weiteren ist auch eine Textverarbeitung integriert, die ein gemeinsames und gleichzeitiges Bearbeiten von Dokumenten erlaubt.

Alle Informationen, um direkt mit sciebo loslegen zu können, finden Sie auf der Informationsseite von IT-Services. Dort sind auch die Hinweise der Stabsstelle für Informationssicherheit zur Nutzung verlinkt sowie Hinweise zum geeigneten Einsatz von Verschlüsselungen.

CHRISTOPHER **LENTZSCH**, INSTITUT FÜR ARBEITSWISSENSCHAFT

MÄRCHEN WERDEN MANCHMAL **WAHR**

Am 10. Februar hatte der BLB den Wettbewerb für die Planung und Errichtung des RUB-Datacenters ausgeschrieben. Bis Ende April werden aus den eingereichten Bewerbungen maximal drei Bewerber ausgewählt und zur Abgabe eines Angebots aufgefordert. Das Angebot soll die komplette Ausführungsplanung, das Einholen der erforderlichen Genehmigungen und die Bauausführung abdecken.

Als Grundlage der Planung haben RUB und BLB gemeinsam ein Lastenheft erarbeitet, das den für die IT-Anwendungen der RUB erforderlichen hohen Schutz- und Verfügbarkeitsbedarf abbildet. In parallellaufenden Verhandlungen mit den Bietern sollen deren Planungen mit den speziellen Erfordernisse der RUB in Übereinstimmung gebracht werden. Dieses rekursive Verfahren von Planung, Kostenermittlung und Überarbeitung endet Mitte Oktober mit der Abgabe der finalen Angebote, auf deren Basis dann der Zuschlag erteilt wird.

Der ausgewählte Bieter wird für das gesamte Genehmigungs- und Bauverfahren verantwortlich sein und das Datacenter schlüsselfertig übergeben. Die Realisierung der Schutz- und Verfügbarkeitsziele soll durch ein unabhängiges Gutachten zertifiziert werden.

RAINER **WOJCIESZYNSKI**

FIREFOX-ADDONS

XSS, XSRF, Drive-By-Downloads, ... es existieren zahlreiche Angriffsmöglichkeiten auf Browser, die eine Bedrohung der Privatsphäre und Datensicherheit darstellen. Kreditkartendaten, Logins für Online-Banking oder E-Mail-Accounts sind lukrative Ziele für Angreifer: Die erbeuteten Daten werden in der Regel schnell weiterverkauft. Es ist also sinnvoll, den Browser nicht ungeprüft jeglichen Code ausführen zu lassen, den er lädt. Alles zu blockieren funktioniert in der Praxis aber kaum, weil so manche Website ohne aktiviertes JavaScript überhaupt nicht funktioniert.

Im Folgenden geht es daher um einen möglichst guten Kompromiss aus Sicherheit und Bedienbarkeit mit nur wenigen Addons. Die hier vorgestellten Addons habe ich in der Kombination seit längerer Zeit im Einsatz und sie haben sich als relativ unauffällig aber wirksam erwiesen. Sie alle verankern sich mit einem Icon in der Symbolleiste der Browsers, worüber Statusinformationen angezeigt und Einstellungen vorgenommen werden können.

Die Addons gibt es übrigens auch für Google Chrome. Einige Optionen können im Detail zwar anders aussehen, im Prinzip sollte das Ergebnis aber wie beim Firefox funktionieren.

uBlock Origin: Ein effizienter Werbeblocker, der mit Filterlisten arbeitet und auch vor bösartigen Skripten schützt. Sämtliche Inhalte von den in den Filterlisten enthaltenen Quellen werden blockiert. Ich verwende die untenstehende Auswahl, die bereits vorkonfiguriert ist. Einige der Listen sind nach der Installation noch nicht aktiviert, darum lohnt sich ein Blick in die Optionen. Diese erreicht man am schnellsten durch Eingabe von „about:addons“ in der Adresszeile und Klick auf „Einstellungen“. Auf der Registerkarte „Filterlisten“ aktiviert ein Haken links neben dem Namen die gewünschte Liste, sie wird dann zukünftig zur Blockierung von Inhalten verwendet und im Hintergrund automatisch aktualisiert: *uBlock filters, uBlock filters – Badware risks, uBlock filters – Privacy, uBlock filters – Resource abuse, uBlock filters – Unbreak, EasyList, EasyPrivacy, Malware Domain List, Malware domain, Peter Lowe's Ad and tracking server list, DEU: EasyList Germany.*

Ebenfalls in den Optionen aktiviert werden sollte der Punkt „Ich bin ein erfahrener Anwender“ unter „Einstellungen“. Damit zeigt uBlock Origin nach einem Klick auf das Icon in der Symbolleiste die zugelassenen und blockierten Elemente einer Seite nach Quelldomain sortiert an. Falls erforderlich kann man dort auch gezielt Elemente von der Filterung ausnehmen ohne die Filterung komplett deaktivieren zu müssen.

Cookie AutoDelete: Dieses Addon modifiziert die Cookiebehandlung des Browsers folgendermaßen: Standardmäßig dürfen Websites Cookies setzen, diese werden aber automatisch gelöscht, sobald ihr Tab geschlossen wurde. Der Vorteil: Auch auf Cookies angewiesene Sites funktionieren ganz normal. Soll eine bestimmte Site Cookies dauerhaft setzen dürfen, zum Beispiel um Login-Informationen abzuspeichern, kann man sie per Klick auf das Icon in der Symbolleiste entweder zur Greylist (Cookies werden beim Schließen des Browsers gelöscht) oder Whitelist (Cookies bleiben auch nach Schließen des Browsers erhalten) hinzufügen. Die Erlaubnis kann entweder für die gesamte Domain oder nur für einzelne Subdomains gewährt werden.

I don't care about Cookies: Websitebetreiber informieren über die Verwendung von Cookies mit Einblendungen, die per Klick auf „OK“ zu quittieren sind. Dass die Einblendung quittiert wurde, wird wiederum in einem Cookie gespeichert. Wer keine Cookies annimmt oder diese regelmäßig löscht, sieht die entsprechende Information also bei praktisch jedem Seitenaufruf. Dieses Addon löst das Problem, indem es die Cookie-Information auf fast allen Websites ausblendet.

Privacy Badger: Dieses Addon ist eine interessante Ergänzung zur Vermeidung von Nachverfolgung durch Tracker. Es ist nicht auf Blocklisten angewiesen, sondern analysiert das Verhalten der aufgerufenen Seiten. Wenn ein Tracker auf mehreren unterschiedlichen Domains zum Einsatz kommt, wird er zukünftig geblockt. Das Addon wirkt also nicht sofort, dafür nach einer gewissen Lernphase sogar für Tracker, die von keiner Blockliste erfasst sind.

DR. MARIUS **MERTENS**, UDE

BITS

Brexit, Brexit, allerorten Brexit

Bei dem derzeit allgegenwärtigen Thema Brexit, wollen auch wir nicht hintanstehen. Nicht jedem ist bewusst, dass an Universitäten das Thema aus Sicht des Datenschutzes ebenfalls relevant ist. Dass der Brexit eben in vielen kleinen Details Folgen hat, zeigt sich auch in unserem Kontext. In einigen Bereichen sind beispielsweise Unternehmen aus Großbritannien mit Datenverarbeitung beauftragt, Rechenzentren stehen auf der Insel. Viele Dienstleister sind deshalb auch bereits auf das europäische Festland umgezogen. Wesentliche Folgen wird es auch für eventuell bereits langfristig bestehende Kooperationen mit britischen Forscher*innen haben. Auch gemeinsam durchgeführte europäisch geförderte Projekte, bei denen personenbezogene Daten ausgetauscht werden, sind hier zu betrachten. Im schlimmsten Fall kann es dazu kommen, dass das Vereinigte Königreich für den Datenschutz als ein „unsicherer Drittstaat“ eingestuft wird, so dass umfängliche Maßnahmen für eine rechtliche Absicherung von Datentransfers nötig werden.

Die Europäische Kommission empfiehlt jetzt die Nutzung von Standardvertragsklauseln, wie sie auch für Drittstaaten Anwendung finden. Konkrete Hilfestellung zur Vorbereitung auf das No-Deal-Szenario gibt ein Leitfaden der European University Association und Universities UK. Links finden sich auf unseren Seiten. KUL

Erpresserische E-Mails

Wie lässt sich mit geknackten Accounts oder gesammelten Daten Geld verdienen? Erpressung scheint die Lösung zu sein. In größerer Zahl erreichen uns Meldungen von Nutzern, die mit angeblich heimlich aufgenommenen Videos pornographischen Inhalts erpresst werden. Um die Mails authentisch wirken zu lassen, werden z. B. vertrauliche Daten oder Passwörter mitgeschickt. In der Regel ist das ein Fake – von einer Zahlung raten wir natürlich ab. BS

HERAUSGEBER Dr. Kai-Uwe Loser (v.i.S.d.P.), KUL, Behördlicher Datenschutzbeauftragter der RUB (bDSB); Brigitte Wojcieszynski (v.i.S.d.P.), BW, Beauftragte für Informationssicherheit der RUB (ITSB); Birgit Steiner, BS, stellv. Beauftragte für Informationssicherheit der RUB (ITSB); Anschrift: Ruhr-Universität Bochum, Geschäftszimmer Stabsstelle Informationssicherheit, NAFOF 03/252, Kerstin Bussmann, 44780 Bochum, Telefon: 0234/32-24888, E-Mail: rubinform@rub.de; Infos: www.rub.de/rubinform; Titelbild: ©Hans Blossey

WEITERE INFOS
ZU UNSEREN THEMEN IM NEWSLETTER:

ZUALLERERST

RUB-Nutzer auf Passwort-Sammlungen: *https://www.itsb.rub.de/aktuelles/meldung00274.html*

Warnung vor Emotet: *https://www.itsb.rub.de/aktuelles/meldung00270.html*

WIE KANN ICH DA **SICHER SEIN?**

Dossier Verschlüsselung: *https://www.itsb.rub.de/themen/verschluesselung.html*

Transportverschlüsselung für RUB-Mailserver: *https://mail.rub.de/mail/anleitungen*

S/MIME-Zertifikate: *https://it-services.rub.de/services/infrastruktur-systeme-it-sicherheit/zertifikatsdienste/beantragung-eines-pers%c3%b6nlichen*

DAS SMARTE ZUHAUSE

US-Marktforscher Gartner: *https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf*

Erpresserbotschaft statt Fernsehprogramm: *https://www.heise.de/security/meldung/Erpresser-Botschaft-in-Dauerschleife-Smart-TV-von-LG-mit-Ransomware-infiziert-3584043.html*

Daniel K. Bewährungsstrafe: *https://rp-online.de/wirtschaft/unternehmen/prozess-in-koeln-britischer-hacker-zu-bewaehrungsstrafe-verurteilt_aid-17700427*

Gefängnisstrafe von 32 Monaten: *https://krebsonsecurity.com/tag/daniel-kaye/*

CybersecurityAct: *https://www.heise.de/newsticker/meldung/EU-Parlament-beschliesst-Guetesiegel-fuer-vernetzte-Geraete-und-warnt-vor-Huawei-4333800.html*

BSI: *https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/willkommen_im_sicheren_smart_home.html*

DIE CLEVERE ALTERNATIVE

sciebo - die Campus Cloud: *https://it-services.ruhr-uni-bochum.de/services/f%C3%BCr-das-studium/sciebo*

Richtlinie zur Cloudnutzung: *https://www.itsb.rub.de/dokumente/intern/cloudrichtlinie_final.pdf*

FIREFOX-ADDONS

uBlock Origin: *https://www.ublock.org/*

Cookie AutoDelete: *https://github.com/Cookie-AutoDelete/Cookie-AutoDelete*

I don't care about Cookies: *https://www.i-dont-care-about-cookies.eu/de*

Privacy Badger: *https://www.eff.org/privacybadger*

BITS

Brexit, Brexit: *https://dsb.ruhr-uni-bochum.de/2019/03/01/brexit-und-die-dsgvo-fuer-universitaeten/*

Erpresserische E-Mails: *https://www.verbraucherzentrale.de/aktuelle-meldungen/digitale-welt/erpressung-per-email-angeblich-porno-geguckt-und-kamera-gehackt-29927*