RUHR-UNIVERSITÄT BOCHUM

RUB

RUBinform

Datenschutz & Datensicherheit

Newsletter 01|17

IN DIESER AUSGABE:

- **ERST DENKEN,** DANN POSTEN
- **GOLDENE** UND **GRÜNE WEGE**
- **CLEVER**, GEWITZT, CHIC - **EBEN SMART**
- LISTEN, **LISTEN**
- (K)EIN TEURES **NUTZUNGSERLEBNIS**

LINKS ZU DEN BEITRÄGEN:

www.rub.de/rubinform

ZUALLERERST

Liebe Leserinnen und Leser,
seit Anfang 2017 sind alle Fakultäten und zentralen Einrichtungen aufgerufen, Koordinatoren für Informationssicherheit und Datenschutz zu benennen. Es ist an der Zeit, ein vertrauensvoll zusammenarbeitendes Netzwerk aufzubauen, in dem sich *alle* aktiv an der Gestaltung der Informationssicherheit beteiligen: Wir sind von einer verlässlichen IT abhängig und die im Mai 2018 in Kraft tretende EU-Datenschutzgrundverordnung verpflichtet dazu. Wir danken für die positive Resonanz und werden zeitnah ein Kick-off Treffen organisieren.
Kurzweiliges Lesen!

Brigitte Wojcieszynski
Beauftragte für Informationssicherheit (ITSB)

Kai-Uwe Loser
Behördlicher Datenschutzbeauftragter (bDSB)

ERST DENKEN, DANN POSTEN

Warum *#Boardingpass* keine gute Idee ist

In sozialen Netzwerken sind sie unter dem Hashtag *#Boardingpass* zu finden: Fotos von Bordkarten, die kurz vor einer anstehenden Flugreise stolz gepostet werden. Abgesehen von Name, Flugnummer, Datum und Sitzplatz scheint die Bordkarte keine weiteren Informationen zu beinhalten. Tatsächlich gibt es aber eine weitere – für das menschliche Auge „unlesbare" – Informationsquelle, nämlich den Barcode.

Der Barcode liegt im sogenannten PDF417-Format vor, der von kompatiblen Barcodescannern eingelesen werden kann. Ein Snapshot des geposteten Barcodes reicht, um die enthaltenen Informationen „lesbar" zu machen. Inhalt und Aufbau dieses Barcodes gibt die internationale Luftverkehrsvereinigung (IATA) vor: Er enthält als Pflichtfeld den sechsstelligen alphanumerischen Buchungscode.

Passagiere können bei Fluggesellschaften oder über Webseiten wie „Checkmytrip" und „Travelport" Informationen zu ihrer Buchung einsehen. Dazu ist zwar eine „Validierung" erforderlich, die aber lediglich daraus besteht, Buchungscode und Nachnamen einzugeben. D.h. jeder, der diese Angaben kennt, kann sich einloggen – und ein Snapshot reicht! Einmal eingeloggt kann man nicht nur Informationen zu der Buchung sehen, sondern je nach Airline auch Veränderungen an der Buchung vornehmen: Namensänderung, Sitzplatzreservierung, Umbuchung, Stornierung. Karsten Nohl hat auf dem 33. Chaos Communication Congress vorgeführt, was alles möglich ist – zum Beispiel könnte ein Angreifer den Flug umbuchen, sich einchecken, eine Bordkarte drucken und mit dieser den Flug antreten.

In der Buchung ist eine Vielzahl an Informationen sichtbar, u.U. auch die E-Mail-Adresse und Anschrift. Diese könnte ein Angreifer für eine Phishing-Attacke nutzen: eine vermeintlich von der Fluggesellschaft stammende E-Mail mit der Aufforderung, Zahlungsdaten erneut zu übermitteln, damit das Flugticket nicht verfällt. Mit den authentischen Daten des Passagiers erscheint eine Phishing-Mail wesentlich glaubwürdiger. Unter Kenntnis der Anschrift und der Reisedauer weiß außerdem ein potenzieller Einbrecher, wann die Wohnung der Person vakant sein könnte. Jeder, der also etwas ins Internet

postet, sollte vorher überlegen, ob es dahin gehört. Sonst gibt man Fremden einen sehr tiefen Einblick in die persönlichen Daten und damit eine Vielzahl an Möglichkeiten, diese missbrauchen zu können.

Gary **Lee,** B. Sc.

GOLDENE UND **GRÜNE WEGE**

Open Access

Wer kennt das nicht – bei der Recherche im Internet stößt man auf einen wichtigen Artikel zur eigenen Forschungsfrage, doch der direkte Zugriff auf den Volltext ist nur gegen Zahlung einer hohen Gebühr möglich. Die eigene Bibliothek hat das Journal nicht abonniert und eine Bestellung per Fernleihe geht nicht schnell genug, weil der Aufsatz aus Gründen des aktuell geltenden Urheberrechtsgesetzes nur als gedruckte Kopie ausgeliefert werden darf. So entstehen Barrieren für den wissenschaftlichen Austausch, die sich erhöhen, je stärker die Zeitschriftenpreise steigen und je mehr Abonnements deswegen von den Bibliotheken gekündigt werden müssen. Ein Teufelskreis.

„Der Schlüssel zum Erfolg heißt: Open Access" – so steht es in der Open Access-Strategie des Bundesministeriums für Bildung und Forschung (BMBF) vom September 2016. Unter Open Access versteht man den freien Online-Zugang zu Forschungsergebnissen ohne rechtliche, technische oder finanzielle Barrieren. Es handelt sich um eine breit aufgestellte Initiative aus der Wissenschaft für die Wissenschaft, die von der Politik unterstützt und von den Forschungsförderern empfohlen (DFG, BMBF) oder sogar eingefordert wird (EU, HORIZON2020). Open Access hat viele Vorteile: Forschungsergebnisse sind sichtbarer, werden schneller verbreitet, verwertet und häufiger zitiert, kurz: der wissenschaftliche Austausch wird verbessert. Die gesellschaftliche Teilhabe an Forschung, die mit öffentlichen Mitteln finanziert wurde, ist somit sichergestellt.

Angebote der RUB

Es gibt mehrere Wege, Open Access zu publizieren. Koordiniert durch die Universitätsbibliothek leistet die RUB hierbei Unterstützung. Die Erstveröffentlichung in einer Open Access-Zeitschrift wird der *Goldene Weg* genannt. Der Artikel ist direkt nach Erscheinen frei zugänglich, die Qualitätssicherung erfolgt durch ein Begutachtungsverfahren. In vielen Fällen wird für die Bereitstellung im Netz eine Publikationsgebühr berechnet – im Gegenzug fallen keine Kosten für die Nutzung an. An der RUB gibt es seit 2014 einen DFG-geförderten Publikationsfonds, aus dem RUB-Mitglieder Fördermittel für Publikationen in Open Access-Zeitschriften beantragen können.

Als *Grünen Weg* bezeichnet man die Zweitveröffentlichung eines bereits in einem zugangsbeschränkten Journal publizierten Aufsatzes. Viele Verlage erlauben eine solche zeitversetzte Open Access-Veröffentlichung, Auskunft darüber gibt der Verlagsvertrag. Das seit Januar 2014 geltende Zweitverwertungsrecht sieht unter bestimmten Bedingungen ein unabdingbares Recht zur Zweitveröffentlichung nach einem Jahr vor – allerdings nur für Publikationen, die mindestens zur Hälfte mit öffentlichen Mitteln finanziert wurden. Zweitveröffentlichungen können über den Dokumentenserver der RUB publiziert werden. Darüber hinaus unterstützt die UB Wissenschaftlerinnen und Wissenschaftler bei der Herausgabe eigener Open Access-Zeitschriften durch die Bereitstellung der Plattform Open Journal Systems.

Open Access, Urheberrecht und Lizenzen

Open Access-Publikationen sind wie jede andere geistige Schöpfung vom Urheberrecht geschützt. Außerdem spielt die Übertragung von Nutzungsrechten, die im Verlagsvertrag geregelt ist, eine wichtige Rolle. Hier ist die Übertragung ausschließlicher Nutzungsrechte eher die Regel. Was viele nicht wissen: Jede/r hat die Handhabe individuell mit dem Verlag zu verhandeln. Beim Open Access-Publizieren wird dem Verlag nur ein einfaches Nutzungsrecht eingeräumt, die Rechte verbleiben bei Autorinnen und Autoren. Durch Vergabe von Lizenzen ist es möglich, Dritten Rechte für die Nachnutzung und Weiterverbreitung einzuräumen. International verbreitet sind hierbei die Creative Commons-Lizenzen (CC), deren Verwendung von der Allianz der deutschen Wissenschaftsorganisationen empfohlen wird.

Kathrin **Lucht-Roussel,** Universitätsbibliothek

CLEVER, GEWITZT, CHIC

eben smart

Im Duden finden sich viele Synonyme zu „smart" – auch gerissen, durchtrieben. Eine sinngemäß smarte Geschäftsidee steckt hinter Erpressungstrojanern, auch als Ransomware bezeichnet. Sie blockieren den Zugriff auf Daten und Systeme und geben diesen erst nach Zahlung eines Lösegeldes (engl. ransom) wieder frei. Die Blockade kann auf diverse Art erfolgen, z.B. durch Veränderung des Benutzerpasswords oder sichere Verschlüsselung von Daten. Betroffene zahlen in vielen Fällen das geforderte Lösegeld, um wieder Zugang zu den Ressourcen zu bekommen.

Freie Fahrt dank Ransomware

Das Geschäft mit der „digitalen" Erpressung ist nicht neu, aber seit 2015 zu einer weltweiten Plage geworden, Privatnutzer, Krankenhäuser, Behörden, Forschungseinrichtungen (auch die Ruhr-Universität) waren betroffen. Im Dezember bescherte eine Attacke auf das Bezahlsystem des öffentlichen Nahverkehrs von San Francisco allen Fahrgästen freie Fahrt.

Die Schadsoftware wird u.a. über komprimittierte Webseiten oder Werbebanner verteilt – ausgenutzt werden Sicherheitslücken in Browser- oder Viewersoftware, um ein System „nebenbei" zu infizieren. Spam E-Mails kommen als Bestellbestätigung, Rechnung oder wie im Falle von „Goldeneye" als vermeintliche Bewerbung daher und verleiten Benutzer durch psychologische Tricks, Anhänge auszuführen oder auf präparierte Links zu klicken. Auch soziale Netzwerke eignen sich naturgemäß für derartige Tricks. Im Cisco Cybersecurity Report 2017 rangieren betrügerische Facebook-Seiten auf Platz drei der Quellen für Schadcode-Verteilung.

Bot-Netze (fernsteuerbare Netzwerke aus kompromittierten Systemen) helfen dabei, grosse Mengen von Ransomware in Umlauf zu bringen. Die Malware Locky erreichte so eine Infektionsrate von mehr als 5000 Systemen pro Stunde. Gleichzeitig kann der Angreifer den Code schnell anpassen, um unter dem Radar von Anti-Virus-Toolkits zu bleiben.

Ransomware greift inzwischen nicht nur Endbenutzersysteme an, sondern nutzt auch Schwachstellen in Serversystemen aus.

Make your own Ransomware

Als smarte Zweit-Einnahmequelle bieten Kriminelle Baukastensysteme (Exploit-Kits) an, mit Hilfe derer sich jeder Laie „gegen Gebühr" seine individuelle Malware zusammenklicken kann. Technisches Wissen darüber, wie sich Schadsoftware über Sicherheitslücken in ein System einschleusen lässt, ist nicht von Nöten – dieses „Feature" wird mitgeliefert. Auf der RSA Conference 2017 zeigte James Lyne die Bedienung eines solchen Kits auf unterhaltsame Weise.

Cisco zufolge haben die Betreiber des Kits „Angler" jährlich 30 Millionen Dollar allein an Lösegeld „verdient".

Ransomware of Things

Der moderne Mensch lebt im „Internet of Things" – Fernseher, Videorecorder, Heizungen, Lampen, Rolladen und viele Dinge mehr sind via Internet fernsteuerbar. Zugegeben, dem Reiz der einen oder anderen technischen Neuerung kann man erliegen. Über den Nutzen anderer – wie die Steuerung der Kühlschranktemperatur vom Supermarkt aus, die Tablettendose, die zur Einnahme per SMS mahnt oder die G***-Box, die die Klingen für den Herrn online nachbestellt – muss man vielleicht länger nachdenken. Laufend kommen neue „smarte" Produkte auf den Markt, alles quasi kleine Computer mit

Internetanschluss und häufig mit gefährlichen Sicherheitslücken. „Betriebssystem"-Schwachstellen, fehlende oder schwache LoginID/Passwort-Kombinationen (admin/admin, admin /1234) sind leider keine Seltenheit. Schadsoftware wie Mirai oder Bashlight nutzen diese Achillesferse aus, um Schadcode auf IoT-Systeme zu installieren. Millionen davon werden zu mietbaren Botnetzen zusammengefasst, die für DDos-Attacken (Überlastung von Internet-Diensten) genutzt werden. Erpressungspotential steckt auch darin, die Funktion von IoT-Systemen zu stören: Erpresserbotschaft statt Fernsehprogramm; Licht an, Licht aus; Blockierte Heizungssteuerung. Diese Beispiele muten eher wie Schabernack an. Dass fehlende Sicherheit aber auch sehr ernsthafte Konsequenzen haben kann, zeigt die Warnung des US. Gesundheitsministeriums vor Schwachstellen in smarten Herzschrittmachern. BW

LISTEN, **LISTEN**

Und noch mehr Listen

Immer wieder tauchen Fragen zum Datenschutz rund um die (Studierenden-)Listen auf, die im Alltag an Universitäten so präsent sind. Klarzustellen ist zunächst, dass Matrikelnummern personenbezogene Daten sind, d.h. auch Listen, die lediglich Matrikelnummern enthalten, sind den Datenschutz-Anforderungen entsprechend zu behandeln. Eine wesentliche Grundregel ist, dass Listen, die Name *und* Matrikelnummer enthalten, keinesfalls öffentlich gemacht werden dürfen. Diese Zuordnung ist als vertraulich einzustufen – auch wenn sich einzelne Studierende in eigener Verantwortung dagegen entscheiden.

Auch mit der (beschränkten) Schutzwirkung des Pseudonyms „Matrikelnummer", dürfen No-

tenlisten nicht für viele erreichbar sein. Die Bekanntgabe einer Liste dieser Art stellte eine Übermittlung personenbezogener Daten an Dritte dar. Es bestehen zudem datenschutzfreundlichere Möglichkeiten, die vorzuziehen sind. Der optimale Weg ist, jedem Studierenden ausschließlich sein eigenes Ergebnis mitzuteilen. Wege dazu bestehen in FlexNow, Campus und selbst Moodle bietet hierzu Möglichkeiten. Allenfalls in bestimmten Fällen kann es noch vertretbar sein, Notenlisten, dann in zumindest per Passwort zugangsbeschränkten Bereichen, bekanntzumachen. Bei solchen Überlegungen spielen die Verfahrensweisen in den Fakultäten und Prüfungsämtern die wesentliche Rolle.

Damit sind bereits die entscheidenden Apekte benannt. Für andere Listen sind abgeleitete Varianten umzusetzen. Zum Beispiel Gruppenverteilungen auf Übungsgruppen sollten ebenfalls zugriffsbeschränkt sein und eher den Namen als die Matrikelnummer enthalten. Kontaktaufnahmen zwischen Studierenden lassen sich dann über die Lehr-/Lernplattformen realisieren. Auch dort sollten Matrikelnummern nicht einsehbar für andere Studierende gemacht werden. Zum Nachweis der Teilnahme an Veranstaltungen werden häufig Anwesenheitslisten geführt. Aber – die verpflichtende Teilnahme ist im Hochschulzukunftsgesetz (§ 64 Abs. 2a HG NRW) auf wenige Fälle beschränkt worden. Damit dürfen auch diese nur noch in speziell zu begründenden oder rechtlich geregelten Fällen (etwa bei Sicherheitsunterweisungen) gesammelt werden. KUL

(K)EIN TEURES **NUTZUNGSERLEBNIS**

Effizientes Arbeiten und das perfekte Anwendungserlebnis sind Microsofts Versprechen für Windows 10: Personalisierung der Oberfläche, kostenfreie Features und Updates, gezielte Werbung, bequeme Speicher- und Synchronisierungstools. Den gesteigerten Komfort bezahlt der Nutzer – mit seinen Daten: angefangen von Kontakt- und Standortdaten, über Termine, Zahlungsinformationen, Passwörter, Browserverlauf, Spracheingaben bis hin zu Inhalten aus Dokumenten und E-Mails – alles wird gesammelt. Ob aus Misstrauen oder zum Schutz der Privatsphäre - wer sich nicht auf das „Erlebnis“ einlassen will, kann die Geschwätzigkeit des Systems gezielt einschränken.

Aufgepasst bereits bei der Ersteinrichtung! Vermeiden Sie die Express-Installation oder ein Standard-Upgrade auf Windows 10; beides aktiviert eine Vielzahl von Datenübermittlungen an Microsoft. Bei den benutzerdefinierten Einstellungen sollten Sie die relevanten Schieberegler auf *Aus* stellen, um möglichst wenige persönliche Informationen zu übermitteln. Falls Sie bereits mit den Express-Einstellungen das System eingerichtet haben – don't panic. Alle Einstellungen können Sie auch noch nachträglich ändern; sie sind in der Regel unter → ⚙ → *Datenschutz* zu finden.

Es wird persönlich

Der Wert von Daten steigt, sobald sie miteinander verknüpft und Personen zugeordnet werden können; dem Microsoft-Konto kommt daher besondere Bedeutung zu. Verzichten Sie nach Möglichkeit auf die Anmeldung mit einem Microsoft-Konto und verwenden Sie eine lokale Benutzeranmeldung. Vermeiden Sie möglichst auch bei anderen Microsoft-Diensten (z.B. MSN, Outlook.com) die Verwendung eines Microsoft-Kontos. Die Werbungs-ID, auf die Microsoft und eine Vielzahl anderer Unternehmen und Applikationen zugreifen, ermöglicht zudem personalisierte Werbung. Die Verwendung dieser ID sollte sowohl in Apps wie auch in jedem verwendeten Browser ausgeschaltet werden. In den Datenschutzeinstellungen ist dazu der Link zur Verwaltung von Microsoft-Werbung zu finden.

Cortana will dich kennenlernen

Die digitale Assistentin erkennt gesprochene Fragen und Anweisungen sowie Tastatureingaben. Sie sammelt fleißig Informationen: Geo-Position, Kontakte, Spracheingaben, Inhalte aus Webrecherche, Kommunikation und Apps. Die Verwendung von Cortana sollte bereits bei der Einrichtung abgelehnt werden. Dennoch wird Cortana für die lokale, nicht personalisierte Suche weiterhin verwendet. Derzeit sind Cortana und die standardmäßige Websuche mit Microsofts Suchmaschine Bing nur durch Änderung von Gruppenrichtlinien abzustellen (Rechtsklick → *Ausführen, gpedit.msc, Administrative Vorlagen→Windows-Komponenten→Suche→Cortana zulassen* deaktivieren).

Windows sagt Hello

Hello ermöglicht die Benutzeranmeldung zum Betriebssystem und zu geeigneten Apps mit biometrischen Merkmalen wie Fingerabdruck, Gesichts- oder Iriserkennung. Die verwendeten Merkmale – nicht aber komplette Abbildungen – werden nach Microsoft-Aussage allerdings nur auf dem lokalen Rechner gespeichert.

So geht's richtig

Diagnose- und Nutzungsdaten, die sogenannten Telemetriedaten, geben Auskunft zu installierten Apps und deren Benutzung an Microsoft, aber unter Umständen auch Inhalte von Dateien. Die Übermittlung sollten Sie möglichst einschränken. Nutzer von Windows Home oder Professional können allenfalls Übermittlungsart *einfach* wählen. In der Enterprise-Edition kann die striktere Einstellung *nie* verwendet werden.

Eine umfangreiche Aufstellung aller relevanten Einstellungen und Hinweise zur weiteren Administration beschreibt die Orientierungshilfe des Arbeitskreises Informationssicherheit der deutschen Forschungseinrichtungen (AKIF). Als individuelle Entscheidungshilfe taugen auch die Datenschutzbestimmungen von Microsoft und die in unserer Linkliste aufgeführten Quellen. **BS**

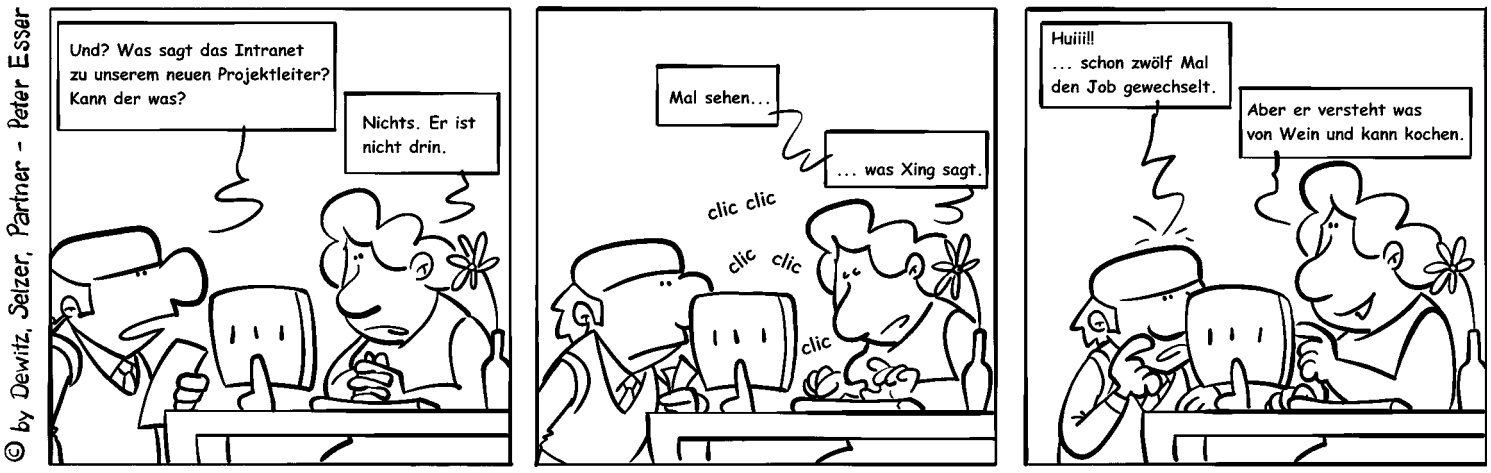
BITS

Schutz gegen Ransomware

Einen hundertprozentigen Schutz gegen Ransomware gibt es nicht. Sicherheitsupdates für Betriebssystem und Softwareprodukte sollte man jedoch zeitnah installieren und den Virenscanner aktuell halten. Darüber hinaus sind die Ratschläge des BSI-für-Bürger zum „Surfen mit gesundem Menschenverstand“ empfehlenswert. Für Opfer einer Ransomware-Attacke stellen sich eigentlich nur drei Fragen: *Gibt es möglicherweise ein bekanntes Entschlüsselungsverfahren?* Für einige Ransomware-Varianten sind mit der Zeit Entschlüsselungslösungen gefunden worden. Eine erste Anlaufstelle ist die Website No More Ransom!. *Habe ich ein aktuelles Backup meiner Daten?* Da Ransomware in der Regel verbundene Fileshares gleich mitverschlüsselt, wird nur ein Offline-Backup nützlich sein. *Zahle ich das Lösegeld?* Es gibt keine Garantie, dass eine getätigte Zahlung tatsächlich zum Ziel führt.

Totgesagte leben länger – das RUB-Datacenter kommt

Lange war es still um das RUB-Datacenter – jetzt kommt Bewegung in das Projekt! Um die Sanierung des NA-Komplexes nicht zu gefährden, treiben RUB und BLB den Ersatzbau für die zentralen IT-Serverräume nun zügig voran. Mit der Reduktion der Serverstellfläche auf maximal 400 m² soll die Fertigstellung zeitnah zum Freizug des NA-Gebäudes gesichert werden. Vorplanungen anhand der Leistungsanforderungen der RUB hat der BLB bereits beauftragt. Zur Jahresmitte wird der Neubau ausgeschrieben, die Bauarbeiten schließlich sollen im Januar oder Februar 2018 beginnen. Als Standort haben BLB und RUB sich auf einen Neubau neben dem Technischen Zentrum verständigt.



© by Dewitz, Selzer, Partner - Peter Essar

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:

ERST DENKEN, DANN POSTEN

Hashtag #boardingpass auf Instagram: *https://www.instagram.com/explore/tags/boardingpass/*

PDF417 Barcodescanner im Internet: *https://online-barcode-reader.inliteresearch.com/*

BCBP Implementation Guide: *https://www.iata.org/whatwedo/stb/Documents/BCBP-Implementation-Guide-5th-Edition-June-2016.pdf*

Karsten Nohl, 33. Chaos Communication Congress, 12/2016: *https://media.ccc.de/v/33c3-7964-where_in_the_world_is_carmen_sandiego*

GOLDENE UND **GRÜNE WEGE**

Open Access-Strategie des Bundesministeriums für Bildung und Forschung: *https://www.bmbf.de/pub/Open_Access_in_Deutschland.pdf*

Berliner Erklärung: *https://openaccess.mpg.de/Berliner-Erklaerung*

HORIZON2020: *http://www.horizont2020.de/einstieg-open-access.htm*

Directory of Open Access Journals (DOAJ): *https://doaj.org/*

Publikationsfonds: *https://www.ruhr-uni-bochum.de/oa/apply/*

FAQ zum Zweitveröffentlichungsrecht: *http://www.allianzinitiative.de/de/handlungsfelder/rechtliche-rahmenbedingungen/faq-zvr.html*

Dokumentenserver der RUB: *http://hss-opus.ub.ruhr-uni-bochum.de/opus4/home*

Herausgabe eigener Open Access Zeitschriften: *http://www.ub.ruhr-uni-bochum.de/Informationen/publishing.html*

Open Access und Urheberrecht:

https://open-access.net/informationen-zu-open-access/rechtsfragen/urheberrecht/

https://open-access.net/informationen-zu-open-access/rechtsfragen/verlagsvertraege/

Creative Common Lizenzen: *https://creativecommons.org/licenses/*

CLEVER, GEWITZT, CHIC - **EBEN SMART**

Neue Masche: Krypto-Trojaner Locky über Javascript-Dateien verbreitet:

https://www.heise.de/security/meldung/Neue-Masche-Krypto-Trojaner-Locky-ueber-Javascript-Dateien-verbreitet-3113689.html

Ransomware-Virus legt Krankenhaus lahm | heise online:

https://www.heise.de/newsticker/meldung/Ransomware-Virus-legt-Krankenhaus-lahm-3100418.html

Trojaner TeslaCrypt legt deutsche Behörden lahm:

http://www.t-online.de/computer/sicherheit/id_76362038/teslacrypt-erpresser-trojaner-legt-deutsche-behoerden-lahm.html

Locky und die Liga der außergewöhnlichen Schadprogramme:

http://www.zeit.de/digital/datenschutz/2016-03/ransomware-lockey-keranger-tesla-crypt-erfolg

Ransomware attack on San Francisco public transit gives everyone a free ride:

https://www.theguardian.com/technology/2016/nov/28/passengers-free-ride-san-francisco-muni-ransomeware

Goldeneye:

https://www.heise.de/security/meldung/Goldeneye-Ransomware-Die-Bedrohung-erkennen-Mitarbeiter-warnen-Infektion-verhindern-3564252.html

Cisco 2017 Annual Cybersecurity Report: *http://b2me.cisco.com/en-us-annual-cybersecurity-report-2017*

You, your endpoints and the Locky virus:

https://medium.com/@networksecurity/you-your-endpoints-and-the-locky-virus-b49ef8241bea#.ym14f4nr2

Krypto-Trojaner Locky wütet in Deutschland: Über 5000 Infektionen pro Stunde:

https://www.heise.de/security/meldung/Krypto-Trojaner-Locky-wuetet-in-Deutschland-Ueber-5000-Infektionen-pro-Stunde-3111774.html

Ransomware-as-a-Service: Mit Satan den eigenen Erpressungstrojaner bauen:

https://www.heise.de/security/meldung/Ransomware-as-a-Service-Mit-Satan-den-eigenen-Erpressungstrojaner-bauen-3605326.html

Reversing the year Let's Hack: IoT, Ransomware and Evasive Payload James Lyne (Sophos Research):

https://www.rsaconference.com/videos/reversing-the-year-lets-hack-iot-ransomware-and-evasive-payloads

Exploit Kit Generating $60M Annually From Ransomware Alone: *http://www.talosintelligence.com/angler-exposed/*

Source Code von mächtigem DDoS-Tool Mirai veröffentlicht:

https://www.heise.de/security/meldung/Source-Code-von-maechtigem-DDoS-Tool-Mirai-veroeffentlicht-3345809.html

Eine riesige Botnet-Schlacht bedroht das Internet: *https://motherboard.vice.com/de/article/eine-riesige-botnet-schlacht-bedroht-das-internet-*

Kriminelle bieten Mirai-Botnetz mit 400.000 IoT-Geräten zur Miete an:

https://www.heise.de/security/meldung/Kriminelle-bieten-Mirai-Botnetz-mit-400-000-IoT-Geraeten-zur-Miete-an-3504584.html

Erpresser-Botschaft in Dauerschleife: Smart TV von LG mit Ransomware infiziert:

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

Philips Hue-Leuchten per Drohne und PKW gehackt:

http://www.borncity.com/blog/2016/11/07/philips-hue-leuchten-per-drohne-und-pkw-gehackt/

Finnland: DDoS-Attacke auf Heizungssteuerung:

https://www.heise.de/security/meldung/Finnland-DDoS-Attacke-auf-Heizungssteuerung-3459730.html

Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication: *https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm*

LISTEN, **LISTEN**

Verbot der allgemeinen Anwesenheitspflicht in Lehrveranstaltungen:

http://www.wissenschaft.nrw.de/hochschule/hochschulrecht/hochschulzukunftsgesetz/verbot-der-allgemeinen-anwesenheitspflicht-in-lehrveranstaltungen/

(K)EIN TEURES **NUTZUNGSERLEBNIS**

Datenschutzerklärung von Microsoft: *https://privacy.microsoft.com/de-DE/privacystatement/*

Microsoft-Werbung und andere Personalisierungsinfos verwalten: *https://choice.microsoft.com/de-DE/opt-out*

Feedback, Diagnose und Datenschutz unter Windows 10: *https://privacy.microsoft.com/de-de/windows-10-feedback-diagnostics-and-privacy*

Orientierungshilfe zur datenarmen Konfiguration von Windows 10; Arbeitskreis Informationssicherheit der deutschen Forschungseinrichtungen (AKIF): *https://www.it-sicherheit.mpg.de/Orientierungshilfe_Windows10.pdf*

BITS: SCHUTZ GEGEN RANSOMWARE

„Surfen mit gesundem Menschenverstand":

https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Menschenverstand/menschenverstand_node.html

No More Ransom!: *https://www.nomoreransom.org/*