RUHR-UNIVERSITÄT BOCHUM

RUB

RUBinform

Datenschutz & Datensicherheit

Newsletter 01|**16**

IN DIESER AUSGABE:

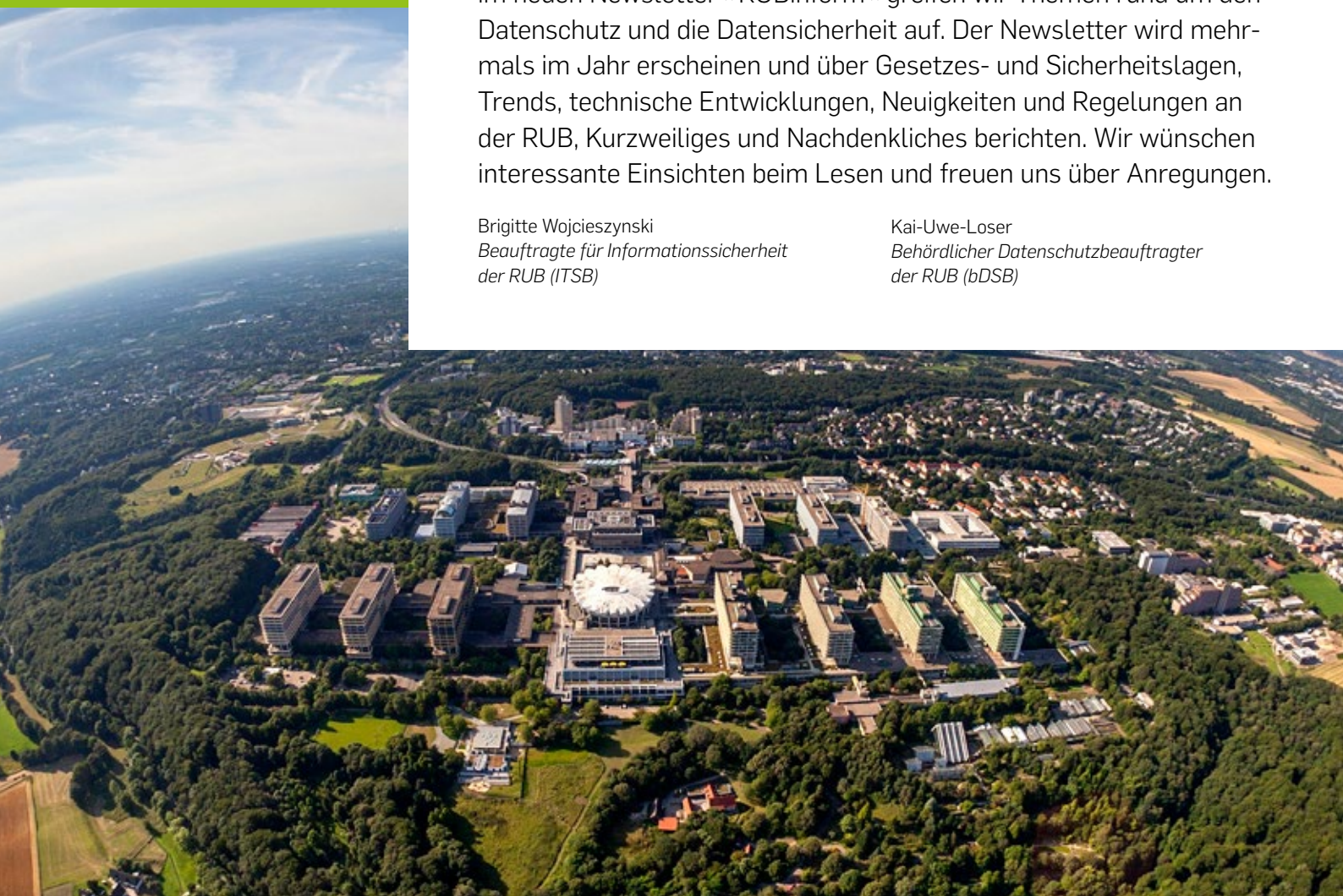
LINKS ZU DEN BEITRÄGEN: *www.rub.de/rubinform*

ZUALLERERST

Liebe Leserinnen und Leser,
im neuen Newsletter »RUBinform« greifen wir Themen rund um den Datenschutz und die Datensicherheit auf. Der Newsletter wird mehrmals im Jahr erscheinen und über Gesetzes- und Sicherheitslagen, Trends, technische Entwicklungen, Neuigkeiten und Regelungen an der RUB, Kurzweiliges und Nachdenkliches berichten. Wir wünschen interessante Einsichten beim Lesen und freuen uns über Anregungen.

Brigitte Wojcieszynski
Beauftragte für Informationssicherheit der RUB (ITSB)

Kai-Uwe-Loser
Behördlicher Datenschutzbeauftragter der RUB (bDSB)



MALWARE-AS-A-SERVICE

Längst ist das Internet als Tatort von Kriminellen entdeckt worden: Phishing-E-Mails, die darauf abzielen, persönliche Daten, etwa Logindaten oder Kreditkartennummern zu erlangen, sind hinlänglich bekannt. Sie verleiten Nutzer durch psychologische Tricks, auf Links zu gefälschten Webseiten zu klicken oder schädliche E-Mail-Anhänge auszuführen. Wimmelten solche E-Mails bis vor kurzem noch vor Schreibfehlern, kommen sie nun immer öfter stilsicher und täuschend echt als Amazon Bestellbestätigung, T-Online Rechnung oder DHL Tracking daher.

Cybercrime-as-a-Service

Die erbeuteten digitalen Identitäten werden entweder direkt betrügerisch verwendet oder weiterverkauft. Im Untergrund steht ein komfortables Dienstleistungsangebot zur Erleichterung von Internetkriminalität bereit, so dass im Lagebild des BKA gar vom Geschäftsmodell „Cybercrime-as-a-Service" gesprochen wird. Die Bezahlung erfolgt nahezu anonym unter Verwendung digitaler Währungen (z.B. Bitcoins). Zu mieten sind hier auch vielseitig verwendbare Botnetze – ein Zusammenschluss von einigen Tausend bis hin zu Millionen ferngesteuerten kompromittierten Systemen. Mittels Botnetzen können z.B. Server im Internet mit Anfragen überhäuft und somit blockiert (DDoS) werden – berühmtes Beispiel ist die DDoS Attacke auf die Webseite des Bundestages im Januar 2015.

Die breitbandigen Netze der Universitäten sind ein attraktives Ziel, um Systeme für Botnetze zu rekrutieren. Im Datennetz der RUB, insbesondere auch in den Wohnheimnetzen, fallen immer wieder solche Systeme auf. Kompromittiert werden sie häufig durch Drive-by-Downloads. Diese nutzen Schwachstellen in Browsern oder Plug-Ins aus, um Schadcode automatisch und unbemerkt beim Ansehen einer Webseite zu installieren. Laut Lagebericht 2015 des BSI wurden allein in den ersten neun Monaten 847 solcher kritischen Schwachstellen in 11 verbreiteten Produkten gezählt – Spitzenreiter ist der Adobe Flash Player.

Ransomware

Erpressungen unter Einsatz von sogenannter „Ransomware" sind seit 2014 auf dem Vormarsch und gelten auch für 2016 als Renner (McAffee Threat Prediction 2016). Dieser Typ Schadcode verschlüsselt Daten auf der Festplatte des Opfers. Das notwendige „Passwort" zur Entschlüsselung ist gegen Zahlung eines Lösegeldes in Form von digitaler Währung erhältlich. Im April 2015 wurden mittels der Ransomware Cryptowall Korrespondenz- und Abrechnungsdateien auf einem System eines Klinikkonsortiums verschlüsselt (BSI-Lagebericht). Im Dezember 2015 hat TeslaCrypt den großen Wurf gelandet und 12.000 Systeme des Landschaftsverbandes Rheinland sowie Systeme des NRW Innenministeriums befallen. Wohl dem, der durch Backups vorgesorgt hat!

Advanced Persistent Threats (APT)

APT-Angriffe sind gezielte Cyberattacken, über die Angreifer versuchen, längerfristig Zugriff auf Netzwerke zu erlangen. Der individuelle Zuschnitt erfordert ausreichend Recherche über das Angriffsziel und genügend Geldmittel. Oftmals sind solche Angriffe staatlich gesponsert und dienen dem Zweck der Staats- oder Wirtschaftsspionage. Ziele sind auch Forschungseinrichtungen und die Öffentliche Verwaltung. Es dauert oft Monate, bis die Angriffe entdeckt werden. Im April 2014 wurde das Netzwerk des Deutschen Zentrums für Luft- und Raumfahrt (DLR) Opfer einer APT-Attacke, im Mai 2015 das des Deutschen Bundestages. Der initiale Angriff erfolgt häufig per Spear-Phishing, einer personalisierten Form des Phishing. Dazu wird das Arbeitsfeld des Opfer sondiert: Tagungen, Veröffentlichungen, Vorträge etc. Die Phishing E-Mail nimmt darauf Bezug.

Auszug aus einer E-Mail an RUB-Mitarbeiter: „Sehr geehrter Herr Prof. ...; Mein Name ist ... ich bin Doktorand bei Prof. ...; In meinen Forschungen befasse ich mit ... . In Ihrer Doktorarbeit habe ich auf Seite 10 einen Fehler entdeckt. Ich habe den Fehler in meinem Forschungsbericht ausgeführt. Sie finden den Bericht im Anhang. .....) Die Archivdatei im Anhang enthielt einen Trojaner des Typs PlugX.

Bleiben Sie vorsichtig! BW

DIE ZUKUNFT DES **DATENSCHUTZES**

Neue EU-Datenschutzgrundverordnung steht vor der Tür

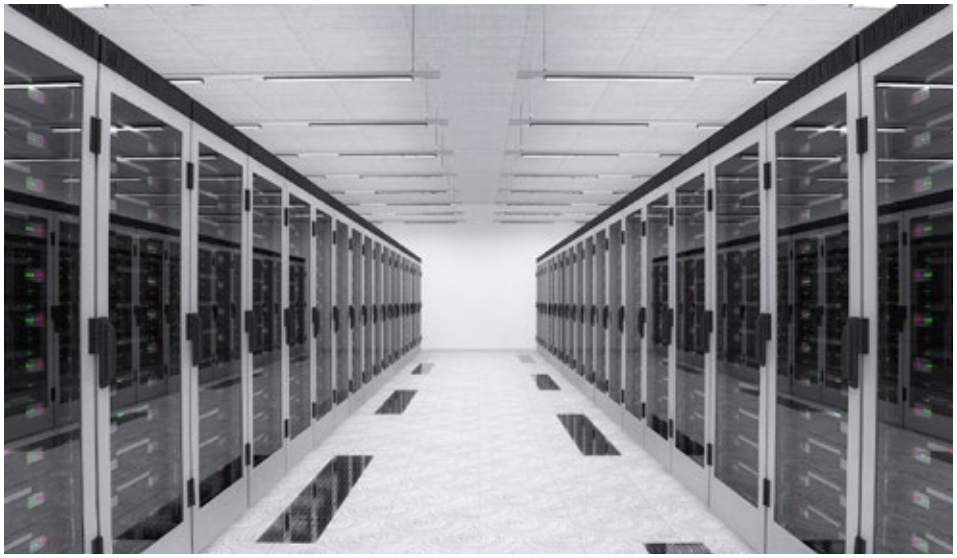
Nach langem Ringen wird es nun eine neue EU-Datenschutzgrundverordnung geben. Sie wird weitgehend alle Regelungen zum Datenschutz in Deutschland ersetzen. Sowohl das Bundesdatenschutzgesetz als auch das Datenschutzgesetz NRW in der heutigen Form wird damit voraussichtlich 2018 außer Kraft treten und nur in Teilen durch einfachere Regelungen für Deutschland und NRW ersetzt.

Was bedeutet das für eine Hochschule in Nordrhein-Westfalen? Veränderungen liegen sicher im Detail und sind derzeit auch noch nicht abschließend geklärt. Für den wissenschaftlichen Bereich sind Öffnungsklauseln enthalten, die es den Mitgliedsstaaten erlauben, spezielle Regelungen für den Forschungsbereich zu treffen. Grundsätzlich bleibt es wie bisher bei einer Stufung, die anonyme Forschung verpflichtend vorschreibt, wenn es möglich ist, die die Pseudonymisierung als Schutzinstrument vorschreibt, wenn das anwendbar ist und die Forschung als dritte Stufe auch in personenbezogener Form erlaubt, wenn das nicht anders möglich ist.

Das war bisher auch so. Dabei wird aber in jedem Fall von Einwilligungen ausgegangen. Forschungsbereiche, in denen Einwilligungen nicht möglich sind, sind bisher nicht vorgesehen. Hier findet sich noch ein offener Regelungsbereich. An einer Hochschule gelten außerhalb der Forschung in Zukunft die einheitlichen Regeln, die weitgehend in gleicher Weise auch für Unternehmen anzuwenden sind. Die Behandlung der Universitäten als Behörden ist damit beendet, was in einigen Fragen Regeln einfacher zu interpretieren macht. Die EU-Grundverordnung hat sich wesentlich auch die Regelung des internationalen Datenverkehrs vorgenommen, für den auch im Forschungsbereich in Zukunft Aspekte verstärkt zu berücksichtigen sind. Das gilt umso mehr, als in Zukunft eine verschärfte Kontrolle ausgeübt werden soll, die mit deutlich verschärften Strafen einhergeht. KUL

DAS **RUB-DATACENTER**

Ein Gebäude für Maschinen, nicht für Menschen



Es wirkt verwaist – Nur wenn etwas neu installiert, repariert oder abgebaut wird, trifft man hier Menschen. Hinein kommt man nur mit speziellen Berechtigungen. Und ist man drinnen, möchte man eigentlich auch schnell wieder hinaus: Lüfter und Klimaanlage verursachen Lärm, es ist zugig. Eben ein Ort für Maschinen.

Für Maschinen, mit denen wir aber täglich arbeiten: für IT-Systeme, die unsere Online-Dienste und die Daten beherbergen, die wir in Forschung, Lehre und Verwaltung bearbeiten. Die nun in einem Datacenter betrieben werden, das die ihrer Bedeutung und ihrem Wert angemessene Infrastruktur bietet. Das nach anerkannten Sicherheitsstandards zertifiziert ist. Und das damit die Grundlage für die Gewährleistung von Integrität, Verfügbarkeit und Vertraulichkeit legt.

Obwohl derartig abgeschirmt, sind die hier aufgestellten IT-Systeme hochverfügbar: Leistungsfähige Datennetzanschlüsse, redundant über zwei Wege zugeführt, vermitteln das Gefühl, der Server stünde nebenan. Zwei unabhängige Einspeisungen überbrücken unterbrechungsfrei den Ausfall einer Stromversorgung, machen so unabhängig von Notstromproben und Wartungen. Und eine Brandfrüherkennung hilft, mögliche Schäden gering zu halten.

Zur Administration der IT-Systeme gibt es eine Reihe technischer Hilfen. Jedes hier installierte System ist mit einer speziellen Netzwerkkarte für den Administrationszugang ausgestattet. Damit der Administrator vom Büro aus so arbeiten kann, als ob er mit Tastatur und Monitor direkt am Server säße. Er kann sogar Systemstarts mit alternativen Konfigurationen durchführen. Und falls es doch einmal nötig sein sollte, kann er von Ferne auch den Strom an der Steckdose aus- und einschalten. Dafür steht ihm eine separate DCIM-Software (Data Center Infrastructure Management) zur Verfügung. Hierüber kann er sich jederzeit auch über die Umgebungstemperatur und die Luftfeuchte in seinem Serverrack informieren. Wo das Datacenter dann tatsächlich steht, ist damit nebensächlich geworden. Einzig zur Installation, vielleicht einmal Reparatur und am Ende zur Entsorgung muss der Administrator noch Hand an seine Hardware legen. Trotzdem hat er dank Remote Administrationssoftware volle Kontrolle über seine IT-Systeme.

Alles nur Vision? Nein: Das sind die Ziele, die sich die vom Rektorat eingesetzte Projektgruppe RUB-Datacenter gesetzt hat. Das Datacenter soll bis zur Jahresmitte 2019 fertiggestellt werden. Teile der DCIM-Fähigkeiten werden aber schon vorab im Rahmen der Serverhousing-Dienste erprobt. Und werden damit auch Administratoren zum „Hineinschnuppern" zur Verfügung gestellt.

Neugierig geworden? Unter www.rub.de/datacenter werden wir Sie auf dem Laufenden halten. RAINER **WOJCIESZYNSKI**

DATENSCHUTZ BEI **WINDOWS 10**

Seit Herbst letzten Jahres steht Microsofts Windows 10 für die Angehörigen der RUB kostenlos zur Installation bereit. Auch für die private Nutzung empfiehlt der Hersteller das im ersten Jahr kostenlose Upgrade von Windows 7 oder 8 auf die neueste Version. Während ein Upgrade (und die Installation zukünftiger Updates) in den meisten Fällen ein Mehr an Sicherheit mit sich bringt, enthält Windows 10 auch einige Änderungen, die Datenschützerinnen und Datenschützer kritisch sehen.

In einer 45-seitigen Erklärung erläutert Microsoft, welche Daten zu welchem Zweck erhoben werden. Neben dem Versprechen der einfacheren Bedienbarkeit, durch die Nutzung von Microsofts-Clouddiensten, werden auch Daten für Werbezwecke gesammelt oder auch nur zum Vorteil des Unternehmens erhoben. Durch die Standardinstallation werden alle Datensammlungen erlaubt. Daher empfehlen wir allen Nutzerinnen und Nutzern das System datenschutzfreundlich einzustellen.

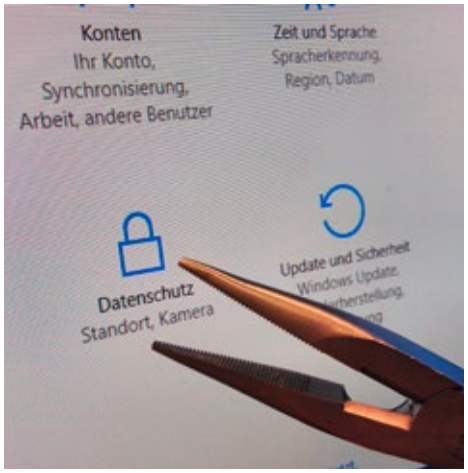
Welche Daten werden gesammelt?

Wird bei der Einrichtung des Rechners ein Microsoft Konto genutzt, vermeintlich zum Vorteil der Nutzerinnen und Nutzer, werden Standort (wenn das Gerät diesen ermitteln kann), Browser Verlauf und Lesezeichen und sogar WLAN Passwörter an Microsoft gesendet und gegebenenfalls mit anderen Geräten synchronisiert. Auch „Daten zur Eingabe-Personifizierung" werden an Microsoft übertragen, wenn die Spracheingabe Cortana oder die Handschriftenerkennung verwendet wird.

Zusätzlich erstellt Microsoft für alle Benutzerinnen und Benutzer eine eindeutige Werbe-ID: diese dient dazu, das Nutzungsverhalten in Apps und im Internet zu verfolgen, um daraus abgeleitet maßgeschneiderte Werbung zu platzieren. Zudem sendet Microsoft regelmäßig Daten zur Nutzungsdauer des Systems und der einzelnen Apps an die eigenen Server, um statistische Auswertungen durchzuführen (Telemetrie).

Datenschutzeinstellungen anpassen

Bei der Neuinstallation sollte darauf geachtet werden, nicht die „Express-Einstellungen" zu übernehmen, sondern die Einstellungen anzupassen. Im weiteren Verlauf der Installation kann ausgewählt werden, dass der Rechner „einer Domäne beitreten" soll. So muss kein



Microsoft-Konto angelegt werden, der Rechner funktioniert aber auch ohne Domäne. Wer ein Upgrade seines Systems durchführt, kann viele Einstellungen im Nachhinein im Menü „Einstellungen → Datenschutz" ändern. Einzig die Übermittlung von Telemetriedaten lässt sich so nicht endgültig unterbinden.

Eine ausführliche und bebilderte Anleitung finden Sie unter: dsb.ruhr-uni-bochum.de

MARTIN **DEGELING**

INFORMATIONS**SICHERHEIT**

Konzepte der RUB

Die Geschäftsprozesse der Ruhr-Universität Bochum in Forschung, Lehre und Verwaltung sind in höchstem Maße von zuverlässig funktionierenden Dienstleistungen der Informations- und Kommunikationstechnik (IKT) abhängig. Verfügbarkeit, Vertraulichkeit und Integrität der Dienste, Systeme und verarbeiteten Informationen muss daher in erforderlichem Maße gewährleistet sein. Zur Erreichung und Aufrechterhaltung eines adäquaten Sicherheitsniveaus in einem komplexen IKT-System wie dem der RUB, ist die Etablierung eines Managementsystems zur Informationssicherheit (ISMS) erforderlich, das die Organisationsstrukturen, Prozesse und Maßnahmen, die zur Planung, Implementierung, Überwachung, und Verbesserung der Informationssicherheit notwendig sind, definiert.

Auch wenn es noch keine rechtliche Pflicht gibt, ein ISMS an Hochschulen einzuführen, fordert das NRW Wissenschaftsministerium im Rundschreiben vom Juli 2015 „im Interesse einer einheitlichen Sicherheitspolitik" die Informationssicherheitsleitlinie NRW zu berücksichtigen. In dieser wird die Etablierung eines ISMS nach BSI-Grundschutz oder vergleichbaren Standards gefordert. Aufgrund der massiven Angriffe auf Netzwerke von Forschungseinrichtungen (siehe Malware-as-a-Service) fordert die Allianz der Wissenschaftsorganisationen im Oktober 2014 per Rundschreiben von DFG und Hochschulrektorenkonferenz ebenfalls dazu auf.

Wie ist die RUB hier aufgestellt?

Bereits im Mai 2011 hat das Rektorat eine neue Version der Informationssicherheitsleitlinie verabschiedet, die die Prinzipien eines ISMS an der RUB festlegt. Es ist eine mehrstufige Organisationsstruktur sowie ein Koordinierungsausschuss für Informationssicherheit vorgesehen. Der Ausschuss setzt sich aus Vertretern der Fachbereiche, der zentralen Einrichtungen, der Verwaltung, der Personalräte und der Studierendenschaft zusammen und trifft sich seit Dezember 2010 regelmäßig. Er hat die Erarbeitung und Fortschreibung von Sicherheitskonzepten zur Aufgabe. Im Mai 2015 wurde das vom Ausschuss vorgeschlagene Rahmenkonzept zur Informationssicherheit vom Rektorat verabschiedet. Dieses orientiert sich an international anerkannten Standards (DIN ISO/IEC 27001/27002). Es ist ein strategisches Papier und zugleich ein „Fahrplan" dessen, was zur Erreichung eines angemessenen Sicherheitsniveaus in den nächsten Jahren erarbeitet und umgesetzt werden muss.

IT-Risikomanagement

Ressourcen zur Erhöhung der Informationssicherheit müssen wirtschaftlich eingesetzt werden. Es müssen kritische Prozesse (Kronjuwelen) in Forschung, Lehre und Verwaltung identifiziert werden, deren Beeinträchtigung in besonderem Maße zu negativen Auswirkungen für die RUB führen. Das Rektorat hat den Koordinierungsausschuss beauftragt, einen gangbaren Weg für ein IT-Risikomanagement bzw. eine Business Impact Analyse (BIA) zu entwickeln. Erkenntnisse aus einem Pilotprojekt an den Universitäten Paderborn und Dortmund vom letzten Jahr können dank der Kooperationsbereitschaft in die Entwicklung eingehen. Erste Einrichtungen der RUB haben bereits probeweise mit der BI-Analyse begonnen. Die Stabsstelle für Informationssicherheit informiert gerne alle interessierten Einrichtungen über das geplante Vorgehen. Vereinbaren Sie einen Termin.

Der Arbeitskreis Informationssicherheit der Forschungseinrichtungen (AKIF), der sich seit 2014 auch um Mitglieder von Hochschulen erweitert hat, bietet eine deutschlandweite Plattform, über die auch der Austausch von vertraulichen Informationen zur IT-Sicherheitslage im Wissenschaftsumfeld möglich ist. Ebenso ist die Allianz für Cyber-Sicherheit des BSI zu nennen. Eine stärkere Vernetzung auf Hochschulebene wird angestrebt. BW

BITS

Do Not Track
Aktuell erscheint wöchentlich bei Arte-Online eine neue Episode der Webserie „Do Not Track". Dort werden Zusammenhänge rund um das Online Tracking, Big Data und die Gefahren für die informationelle Selbstbestimmung jedes und jeder Einzelnen interaktiv dargestellt und mit kurzen Interviews erläutert.

Datenträger- und Aktenentsorgung
Datenträger und Akten, die personenbezogene oder vertrauliche Informationen enthalten, sind von den Organisationseinheiten eigenverantwortlich und regelkonform zu entsorgen. Zur Unterstützung der Einrichtungen können bei der Stabsstelle Arbeitssicherheit und Umweltschutz Sicherheitsbehälter angefordert werden. Diese werden von einer zertifizierten Firma geliefert, abgeholt und der Inhalt datenschutzkonform vernichtet. Zur Entsorgung kleinerer Mengen stehen an mehreren Orten der RUB Aktenvernichter und Shredder bereit, die in Selbstbedienung nach Voranmeldung genutzt werden können. siehe Link: Aktenvernichtung

pwned?
Immer wieder werden große Mengen von Zugangsdaten zu Onlinediensten – in der Regel E-Mail-Adresse mit zugehörigem Passwort – entwendet. Der Identitätsdiebstahl kann auf vielfältige Weise erfolgen, beispielweise durch Kompromittierung von Benutzersystemen oder Servern der Anbieter. Die Adressen tauchen oft in verschiedensten (Untergrund)foren wieder auf oder werden von den Hackern selbst preisgegeben. Die Betreiber der Websites haveibeenpwned.com und pwnedlist.com sammeln derartige Informationen in Datenbanken. Ein Benutzer kann selbst durch Eingabe seiner E-Mail-Adresse prüfen, ob und welche seiner Zugangsdaten auffällig geworden sind.

HERAUSGEBER Dr. Kai-Uwe Loser (v.i.S.d.P.), KUL, Behördlicher Datenschutzbeauftragte der RUB (bDSB); Brigitte Wojcieszynski (v.i.S.d.P.), BW, 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

LINKS ZU DEN THEMEN DES NEWSLETTERS 01|16

MALWARE-AS-A-SERVICE

Cybercrime Lagebild BKA 2014: http://www.bka.de/nn_204308/DE/Publikationen/Publikationen__node.html?__nnn=true

Digitale Währungen: http://www.heise.de/tp/artikel/40/40750/1.html

Lagebericht 2015 des BSI: https://www.bsi.bund.de/DE/Publikationen/Lageberichte/bsi-lageberichte.html

DDoS-Attacke auf Web-Seiten von Kanzlerin und Bundestag:
http://www.heise.de/newsticker/meldung/DDoS-Attacke-auf-Web-Seiten-von-Kanzlerin-und-Bundestag-2512871.html

McAffee Labs Threat Prediction 2016:
http://www.mcafee.com/us/resources/reports/rp-threats-predictions-2016.pdf

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

Hacker spionierten Luft - und Raumfahrtzentrum aus:
http://www.zeit.de/digital/datenschutz/2014-04/dlr-hacker-angriff-datenspionage-geheimdienst

Der Bundestag ist Offline: http://www.zeit.de/digital/datenschutz/2015-08/hacker-angriff-bundestag-computer-system

Digitale Dilettanten: http://www.sueddeutsche.de/politik/bundestag-digitale-dilettanten-1.2644156

DAS RUB-DATACENTER

Homepage: http://datacenter.rub.de

DIE ZUKUNFT DES DATENSCHUTZES

EU-Datenschutzreform: Pressemitteilung des Europäischen Parlaments:
http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+IM-PRESS+20151217IPR08112+0+DOC+XML+V0//DE

DATENSCHUTZ BEI WINDOWS 10

Links zum Serviceagreement und den Datenschutzbestimmungen:
https://www.microsoft .com/de-de/privacystatement/default.aspx
https://www.microsoft .com/de-de/servicesagreement/default.aspx

Homepage Datenschutz: http://dsb.ruhr-uni-bochum.de

INFORMATIONSSICHERHEIT

Leitlinie zur Informationssicherheit: http://www.itsb.rub.de/leitlinie.html

Rahmenkonzept zur Informationssicherheit (Dokumentenverzeichnis):
http://www.itsb.rub.de/intern/weiterführendeDokumente.html

Rundschreiben des Ministeriums für Innovation, Wissenschaft und Forschung: http://www.itsb.rub.de/intern/leitlinie_nrw.pdf

Rundschreiben der DFG und der HRK:
http://www.itsb.rub.de/intern/eckpunktepapier.pdf

Homepage Informationssicherheit: http://www.itsb.rub.de

BITS

Do Not Track: https://dsb.ruhr-uni-bochum.de/2015/06/02/do-not-track-webserie-zu-online-tracking/

Entsorgung: http://www.itsb.rub.de/entsorgung.html

pwned
Haveibeenpwned: http://haveibeenpwned.com

pwnedlist: http://pwnedlist.com