RUHR-UNIVERSITÄT BOCHUM

RUB

RUBinform

Datenschutz & Datensicherheit **Newsletter** 02|17

IN DIESER AUSGABE:

LINKS ZU DEN BEITRÄGEN:

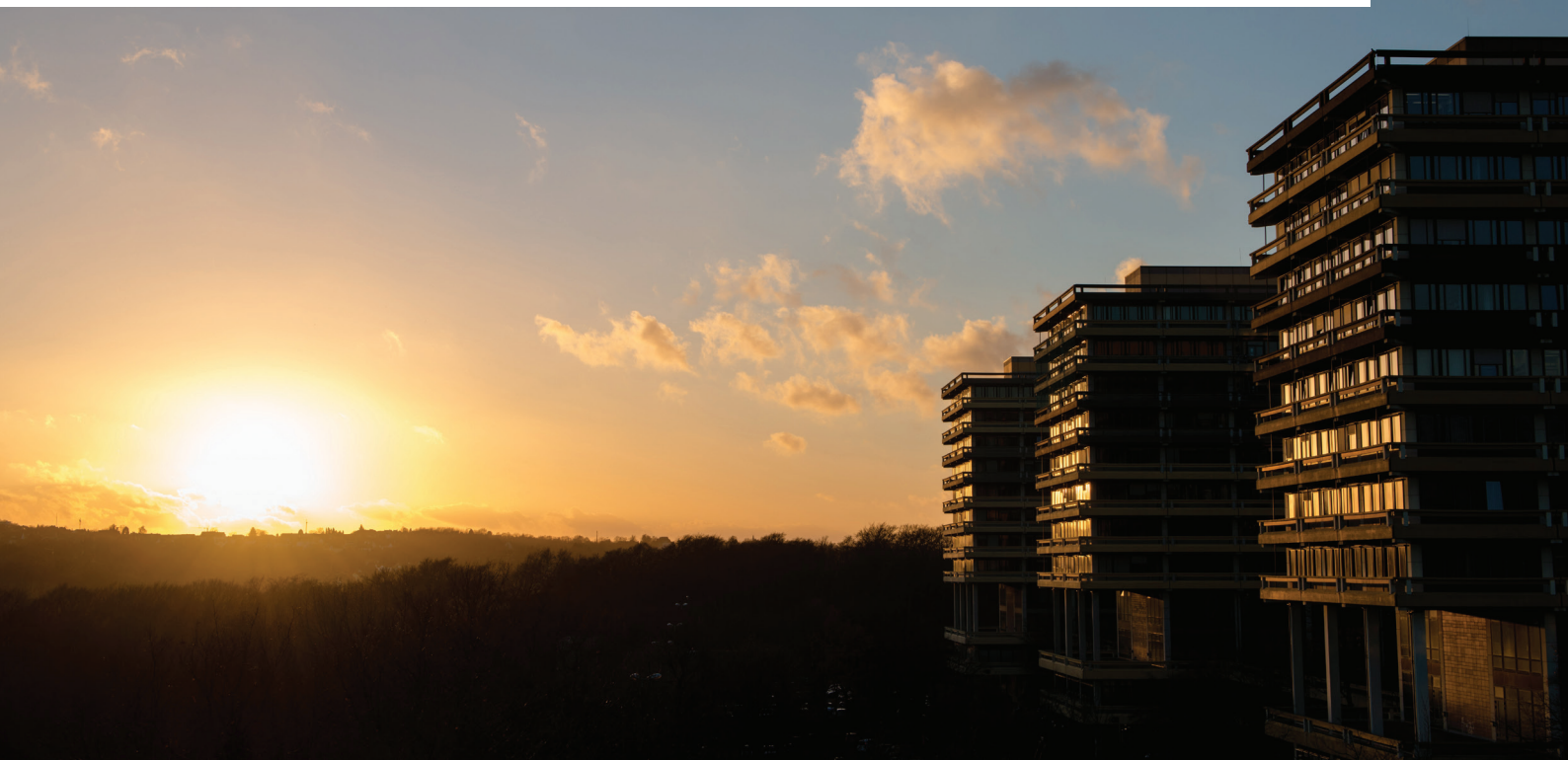
www.rub.de/rubinform

ZUALLERERST

Liebe Leserinnen und Leser,
geht es Ihnen auch so? - die Wintermüdigkeit macht sich breit. Einer Studie des NIST (National Institute of Standards and Technology) zufolge greift dazu auch noch die Cyber-Müdigkeit Raum. Benutzer geben auf - sie sind es leid, sich zig verschiedene Passwörter zu merken, nur durch Überwinden mehrerer Hürden Zugriff auf ihr Benutzerkonto zu bekommen, sie sind es leid, sich über immer neue Taktiken Cyberkrimineller zu informieren. Diese Müdigkeit ist fatal, wirkt doch gerade wegen der immer neuen Herausforderungen das rationale Handeln des Benutzers als letzte Bastion. Glauben Sie uns, geschädigte Benutzer berichten einhellig, dass sie sich plötzlich hellwach in einem real gewordenen Albtraum wiederfanden. *Bleiben Sie wachsam!*

Brigitte Wojcieszynski
Beauftragte für Informationssicherheit (ITSB)

Kai-Uwe Loser
Behördlicher Datenschutzbeauftragter (bDSB)



SCHWACHSTELLE MENSCH

Montagmorgen, eine neue Arbeitswoche im Büro beginnt. Mal schauen, welche E-Mails eingetroffen sind, bevor es an den Papierkram geht. Uff, so viele? Naja, kurz durchblättern. Schau an, eine E-Mail von Irmtraud Mayer <Personalabteilung> - mit einem Rechnungslink? Das kann doch nur ein Irrtum von „Traudl" sein. Mal sehen, an wen die Rechnung eigentlich gehen sollte. Verdammt jetzt klingelt auch noch das Telefon, ... *Griff zum Telefonhörer, Finger klickt, Sophos meldet „Threat erkannt"*. Oh, nein!!! Noch einmal gut gegangen – Sophos hat es gerichtet. Warum sendet Frau Mayer auch einen Link zu blackbox-es.com?
Vier Stunden später, Magen und Kollegen melden sich. Essenszeit! Ach, DHL schreibt gerade, dass mein Paket endlich angekommen ist – Abholschein im Anhang. Ich druck das noch schnell, dann auf in die Mensa – *Sophos schweigt*.

Der Klick-Reflex

Einer Untersuchung von Proofpoint (Der Faktor Mensch, 2017) zufolge, haben Kriminelle ihr Angriffsverhalten deutlich, leider auch sehr effektiv verändert. Wurden Benutzersysteme vormals hauptsächlich durch Ausnutzung von Schwachstellen in der Software mit Schadcode infiziert, so setzen die Angriffe jetzt auf menschliches „Fehlverhalten". Es mag an Reizüberflutung, Stress oder Mangel an Risikobewusstsein liegen, wenn Benutzer reflexartig, intuitiv E-Mail-Anhänge öffnen oder auf Links klicken. Dies geschieht selbst (oder gerade) dann, wenn die E-Mail sprachlich eher merkwürdig gestaltet ist. Es genügt dem Empfänger, dass sie einen bekannten Absender hat, oder scheinbar die ersehnte Versand- oder Lieferbestätigung enthält. Ohne genauer zu lesen, kommt es in jedem zwanzigsten Fall zum Klick auf den schädlichen Anhang oder Link, bereits 25% der Klicks erfolgen innerhalb von 10 Minuten nach Empfang. Unter den Top 5 der (Phishing-)Köder sind *Rechnung im Anhang, Ihre Bestellung, Lieferbestätigung, Bitte bestätigen Sie die Transaktion, Fax Report*.

Social Engineering 1x1

Cyberkriminelle haben das Anwenden psychologischer Tricks perfektioniert. Sie legen „Wert" darauf, dass Opfer fehlerfreie E-Mails in gewohnter Sprache erhalten, oft täuschend echt im Design vertrauenswürdiger Firmen. Sie nutzen menschliche Emotionen wie Freude, Furcht, Neugier aus. Absenderadressen vermitteln das Gefühl, es handele sich um die Nachricht eines Vorgesetzten, Freundes oder Kollegen. Nutzer haben sich selten darüber informiert, dass diese Angaben sehr leicht zu fälschen sind (-> E-Mail Spoofing). Auch gefälschte Links lassen sich durch einfache Tricks kaschieren, wie etwa *paypal.de-signin-lang-ger.website* oder *www.ruhr-uni-bochurn.de*. Gezielt auf Opfer zugeschnittene E-Mails ködern am besten – sie enthalten persönliche Daten wie vollständige Namen, Postanschrift, Telefonnummer, Geburtsdatum, Berufsbezeichnung. Kriminelle Akteure (z.B. die Gruppe TA530) generieren neuerdings in großem Stil Personenprofile, indem sie Informationen aus mehreren Quellen verdichten. Vieles ist frei im Internet zu finden und die Datenlöcher z.B. bei Yahoo, Dropbox, Ebay, LinkedIn tun ein Übriges. Selbst beim Versand der schädlichen E-Mails wird das Nutzerverhalten berücksichtigt. Statistisch erfolgen die meisten Klicks direkt nach Dienstbeginn und zur Mittagszeit.

Auch an der RUB?

Mehrere Tausend Benutzer waren von den genannten Datenlöchern betroffen. In Wellen sind mehr oder weniger gut personalisierte Köder-E-Mails in den Postfächern gelandet. Durch Aktivieren des Spamfilters hätte sich mancher Benutzer Ärger erspart. Weder Spamfilter noch Anti-Malware-Toolkit sind jedoch Allheilmittel. Im realen Szenario von oben hatte Sophos einen Teil des Schadcodes erkannt, aber andere Teile sind installiert worden - der Abholschein enthielt einen Trojaner. Erst Monate nach den Vorfällen wurden die LoginIDs der Betroffenen zum Spam-Versand missbraucht. Letztlich hilft nur ruhiges, rationales Denken und Handeln, weg vom Klick-Reflex und im Zweifel keine Scheu nachzufragen. Unter www.itsb.rub.de finden sich weitere, ausführliche Informationen zu diesem Thema. **BW**

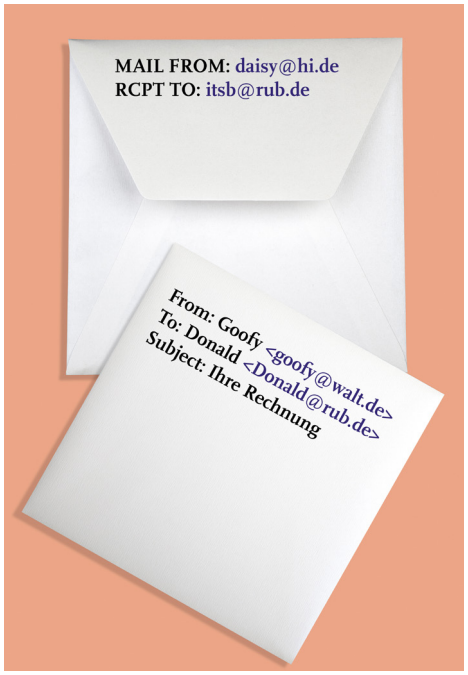
E-MAIL **SPOOFING**

Unter E-Mail Spoofing versteht man das Fälschen von Adressangaben einer E-Mail. Angreifer nutzen dies, um vorzutäuschen, dass sie scheinbar von einer bekannten Firma, einem Bankinstitut oder Kollegen stammt.

Um zu verstehen, wie dies möglich ist, muss man sich nur an die gute alte Zeit zurückerinnern, als Briefe noch per Briefpost versandt wurden. Der Briefbogen enthält im Briefkopf Angaben zu Ziel- und Absenderadresse, Datum, Betreff und den eigentlichen Brieftext. Der Briefbogen wird in einen Umschlag gesteckt, auf dem ebenfalls eine Absenderangabe und ein Adressat stehen. Adressangaben im Briefkopf können sich von denen des Umschlags unterscheiden.

Eine E-Mail ist ganz ähnlich aufgebaut. Sie besteht aus einem virtuellen „Briefbogen" mit Adressangaben (To: From:) im sogenannten Header und dem Brieftext (Body). Header und Body werden im E-Mail-Programm angezeigt. Die E-Mail wird mitunter über mehrere Mailserver zum Ziel transportiert. Zur Zustellung des Briefes wird von den Mailservern ein virtueller Umschlag (Envelope) genutzt, der ebenfalls Adressangaben enthält (MAIL FROM: RCPT TO:). Den Umschlag bekommt der Empfänger nicht zu sehen, nur Teile dieses „Umschlags" z.B. Eingangsstempel der Mailserver (Received:) werden an den Anfang der E-Mail kopiert. Diese zusätzlichen Informationen kann man sich z.B. in Outlook bei geöffneter E-Mail durch *Datei -> Eigenschaften -> Internetkopfzeilen* anzeigen lassen.

Der E-Mail-Versand erfolgt auf Basis eines textbasierten Protokolls, das die oben in Klammern angegebenen Schlüsselwörter für die Verständigung zwischen Klient und Mailserver festlegt. Eine Überprüfung der Angaben hinter den Schlüsselwörtern erfolgt nicht. Im Mailserver-FAQ der RUB ist ein Beispieldialog, der zeigt, wie eine E-Mail „von Hand" verschickt werden kann. Auch wenn es dem Nutzer eines E-Mail-Programms vielleicht seltsam erscheint – alle Adressangaben (To, From, MAIL FROM) können beliebig „kreativ" gestaltet werden - solange die RCPT-TO Angabe des „Envelopes" eine gültige Zieladresse enthält, wird der Brief an diese Adresse zugestellt. Nur durch Analyse der Internetkopfzeilen lässt sich mitunter etwas mehr über die tatsächliche Herkunft einer E-Mail ermitteln. Dies ist allerdings für Laien nicht einfach. **BW**



E-Mail-Zustellung an itsb@rub.de

Outlook:
Von: Goofy <goofy@walt.de>
An: Donald <Donald@rub.de>

INFORMATIONSSICHERHEIT AN DER RUB

An der Ruhr-Universität wurde schon früh die Bedeutung der Informationssicherheit erkannt und eine mehrstufige Organisationsstruktur nach den Empfehlungen des BSI (Bundesamt für Sicherheit in der Informationstechnik) aufgebaut. Die zentrale Stabsstelle berät das Rektorat und die Leitungen der Organisationseinheiten in Fragen der Informationssicherheit, führt ein Meldesystem für Ereignisse, die die Informationssicherheit betreffen, und stellt Anwendern Informationen zur IT-Sicherheit zur Verfügung.

Um ein Konzept zur Informationssicherheit zu entwickeln, fortzuschreiben und dessen Umsetzung zu begleiten, ist seit 2010 ein Koordinierungsausschuss unter dem Vorsitz der Beauftragten für Informationssicherheit aktiv. Diesem Ausschuss gehören auch der behördliche Datenschutzbeauftragte sowie Vertreterinnen und Vertreter der Fachbereiche, der Studierenden, der Personalräte, des zentralen IT-Dienstleisters IT.Services, der Universitätsbibliothek und der Verwaltung an.

Sciebo und die Cloudrichtlinie

In regelmäßigen Treffen erarbeitete der Koordinierungsausschuss eine Leitlinie sowie ein Rahmenkonzept zur Informationssicherheit, die vom Rektorat beschlossen und in den amtlichen Bekanntmachungen veröffentlicht wurden. Das Rahmenkonzept orientiert sich an international anerkannten Standards zur Informationssicherheit und beschreibt strategische Maßnahmen. Es wird konkretisiert durch nachgelagerte Konzepte und Dokumente, z.B. Verfahrensbeschreibungen, Empfehlungen oder Checklisten. So wurde zuletzt die Richtlinie „Nutzung von Cloudspeicherdiensten“ - nicht nur, aber auch - für die Campuscloud Sciebo erstellt. Neben grundsätzlichen Hinweisen erläutert sie für Cloudspeicherung geeignete Daten und gibt Verantwortlichen eine Checkliste zur Auswahl von Cloud-Angeboten an die Hand.

Struktur für Informationssicherheit und Datenschutz

Leitlinie und Rahmenkonzept sehen neben den zentralen Beauftragten und dem Koordinierungsausschuss auch die Etablierung dezentraler Beauftragter vor. Mit der neuen Datenschutzgrundverordnung werden demnächst weitere Datenschutzbelange dezentral zu bearbeiten sein (s. Box). Anfang des Jahres wurden daher alle Einrichtungen der RUB aufgerufen, dezentrale Beauftragte für Informationssicherheit und Datenschutz zu benennen. Die bisherigen Zusammentreffen der dezentralen Beauftragten dienten neben der Diskussion inhaltlicher Belange vor allem der gemeinschaftlichen Erarbeitung eines Tätigkeitsprofils. **BS**

PFLICHT ZUR ERSTELLUNG EINER **VERARBEITUNGSÜBERSICHT**

Die neue EU-Datenschutz-Grundverordnung (DS-GVO) verlangt von „Datenverarbeitern“ wie der Ruhr-Universität, ein sogenanntes „Verzeichnis von Verarbeitungstätigkeiten“ zu führen (gemäß Artikel 30). Das heißt, alle Prozesse, in denen personenbezogenen Daten verarbeitet werden, müssen dokumentiert werden. Die Begriffe „personenbezogene Daten“ und „Verarbeitung“ sind dabei weit ausgelegt. Jegliche Daten, in denen natürliche Personen identifizierbar sein können, sind als personenbezogen anzusehen; ebenso ist jedweder Umgang mit diesen Daten (z.B. auch die Speicherung) als Verarbeitung zu betrachten. Das Verzeichnis ist ein Nachweis dafür, dass Datenschutzbelange bedacht wurden. Es ist auf Anfrage der Aufsichtsbehörde vorzulegen, damit diese Verarbeitungsvorgänge kontrollieren kann. Die Pflicht zur Erstellung der Dokumentation liegt bei den für die Verarbeitung Verantwortlichen - dies sind die jeweils zuständigen Einrichtungen der RUB, Dezernate ebenso wie Fakultäten und Lehrstühle.

Als Grundlage der Dokumentation dient ein Formular, dessen Ausfüllen keine komplexe Aufgabe ist. Es beinhaltet Grundangaben darüber, wer wo Daten verarbeitet, Angaben zum Zweck der Verarbeitung, zu den möglicherweise von den Verarbeitungen betroffenen Personengruppen und zur Art der verarbeiteten Daten. Weitere Details - wohin Daten unter Umständen übermittelt werden und wann sie voraussichtlich gelöscht werden - kommen hinzu. Diese Informationen ermöglichen eine grundlegende Beurteilung des Risikos und der Zulässigkeit der Verarbeitung.

Alle Daten müssen angemessen geschützt sein. Schutzmaßnahmen beschreibt das Konzept zur Informationssicherheit der RUB. Spezifische Maßnahmen eines Verarbeitungsprozesses sind in der Verarbeitungsübersicht gesondert anzugeben. Werden höchst sensible Daten verarbeitet oder wird eine Technologie eingesetzt, die neue Herausforderungen aus Sicht des Datenschutzes darstellt, so kann eine komplexe, sogenannte Datenschutzfolgenabschätzung notwendig sein. Dabei werden anhand einer detaillierten Risikoanalyse Risiken und Schutzmaßnahmen gegeneinander abgewogen und ggf. weitere Sicherheitsmaßnahmen abgeleitet.

Die behördlichen Datenschutzbeauftragten sowie die dezentralen Beauftragten für Informationssicherheit und Datenschutz stehen bei Fragen zur Dokumentation als Ansprechpartner zur Verfügung. Die Stabsstelle Informationssicherheit berät bzgl. geeigneter Maßnahmen zur Informationssicherheit. **KUL**

SERVER **SICHER VERORTET**

Es kommt – das RUB-Datacenter, ein Neubau neben dem Technischen Zentrum. Als „Geburtshelferin“ wirkt die neue „Rechenzentrumsnormenreihe“ DIN EN 50600, die die Anforderungen an ein zeitgemäßes Rechenzentrum normativ spezifiziert. Aufgrund einer Analyse des Schutz- und Verfügbarkeitsbedarfs wird hiernach das RUB-Datacenter ein Rechenzentrum der Schutzklasse 3 und der Verfügbarkeitsklasse 3 sein: Dies spezifiziert einen gesicherten Serverraum für die Bearbeitung von Informationen mit hohem Schutzbedarf, u.a. mit Vorkehrungen zur Brandfrüherkennung und automatischen Brandlöschung sowie mit einer Einbruchmeldeanlage. Die hohe Verfügbarkeit wird durch eine redundante Stromversorgung bis zum Endgerät mit lokaler USV und Netzersatzanlage sowie eine redundant ausgelegte Klimaanlage gewährleistet. Auch die Kommunikationsanbindung wird redundant vom RUB-Backbone bis zum Endsystem ausgelegt. Die Einhausung der umluftgekühlten IT-Systeme wird eine effiziente Klimatisierung ermöglichen. Für Hochleistungsserver mit großer Wärmeerzeugung wird die Installation wassergekühlter Serverracks vorbereitet sein.

Die Funktion der technischen Infrastruktur des Datacenters wird laufend überwacht. Störungsmeldungen werden an die ständig besetzte technische Leitwarte der RUB übermittelt. Im Datacenter betriebene IT-Systeme werden remote administriert: Der Administrator kann vom Büro aus direkt auf seine Systeme zugreifen. Für aufwändige Konfigurationsarbeiten steht im benachbarten Technischen Zentrum ein Konfigurationsraum zur Verfügung. Einzig zu Installations- und Reparaturzwecken sind noch vor-Ort-Arbeiten im Datacenter erforderlich. Das neue Datacenter schließt eine Lücke in den Angeboten zur IT-Unterbringung an der RUB: Für Anwendungen zur Bearbeitung sensibler (z.B. personenbezogener) Daten oder bei hohem Verfügbarkeitsbedarf wird es den passenden Installationsort bereitstellen. Die Serverräume in den Gebäuden ID, IC und GD verfügen nicht über die hierfür erforderliche Infrastruktur, sie orientieren sich noch an der Schutzklasse und der Verfügbarkeitsklasse 1 der Norm.

Das Gesamtkonzept zur IT-Unterbringung an der RUB ist gemäß Rahmenkonzept zur Informationssicherheit (Amtl. Bekanntmachung Nr. 1047) in der gerade fertiggestellten Serverraum-Richtlinie formuliert. Dort sind auch Details zur Infrastruktur-Ausstattung nachzulesen. **RW**

POSTKARTE ODER **EINSCHREIBEN**?

Verfahren zum Versenden und Empfangen von E-Mails stammen aus Zeiten, als die Internet-Welt noch in Ordnung war. E-Mails auf dem Transportweg mitzulesen oder zu verändern (-> E-Mail-Spoofing), war schon immer ein Leichtes, da die Übertragung dem Postkartenversand vergleichbar erfolgt.

In unsicheren Zeiten wird die sichere Kommunikation immer wichtiger: Bei einer digital signierten E-Mail wird vom Mailprogramm automatisch die *Echtheit* überprüft, also geprüft, ob sie tatsächlich vom angezeigten Absender stammt. Die Signatur sichert auch die *Integrität*, d.h. dass auf dem Transportweg nichts verfälscht wurde. Digitale Signaturen sind nicht mit textuellen Signaturen oder digitalen Visitenkarten, die Mailprogramme unter eine E-Mail setzen, zu verwechseln. Digital signierte E-Mails sind gegen Manipulation geschützt, können aber unter Umständen auf dem Übertragungsweg von Dritten mitgelesen werden. *Vertraulichkeit* bietet die zusätzliche Verschlüsselung von E-Mails.

Asymmetrische Verschlüsselung

Die am häufigsten eingesetzten Verfahren zum Signieren und Verschlüsseln von E-Mails sind PGP und S/MIME. Beide sind nicht kompatibel zueinander, arbeiten aber nach dem gleichen Grundprinzip, der asymmetrischen Verschlüsselung - es gibt zwei Schlüssel, einen geheimen (privaten) und einen öffentlichen Schlüssel. Der private Schlüssel wird nur vom Eigentümer verwendet und darf niemals aus der Hand gegeben werden. Der öffentliche Schlüssel wird bekannt gemacht, z.B. in einer signierten E-Mail mitgeschickt.

Die Signatur erfolgt mit dem privaten Schlüssel des Absenders – das Mailprogramm eines Empfängers kann dann mit dem öffentlichen Schlüssel des Senders Echtheit und Integrität der E-Mail überprüfen. Zur Verschlüsselung einer E-Mail muss das Mailprogramm den öffentlichen Schlüssel des Empfängers gespeichert haben – z.B. aus einer zuvor vom Empfänger verschickten, signierten Mail. Zur Entschlüsselung wird der Empfänger die E-Mail mit seinem privaten Schlüssel entschlüsseln. Der private Schlüssel muss also auf allen Geräten installiert sein, auf denen man verschlüsselte Mails lesen will.

Persönliche Zertifikate

S/MIME wird von allen gängigen Mailprogrammen auf Desktop- und mobilen Systemen unterstützt. Signatur und Verschlüsselung sind bequem menügesteuert einstellbar.

Angehörige der Ruhr-Universität erhalten kostenlose S/MIME-Nutzerzertifikate. Die Beantragung eines Zertifikats erfolgt über ein Webinterface der RUB-Zertifizierungsstelle. Bei der Beantragung werden ein privater und ein öffentlicher Schlüssel und ein Zertifikat generiert. Das Zertifikat sichert, dass der öffentliche Schlüssel wirklich vom Antragsteller stammt. Es wird erst nach persönlicher Vorlage eines gültigen Ausweisdokuments im Servicecenter von IT.Services ausgestellt. Danach kann im zuvor genutzten Browser das Zertifikat mit dem öffentlichen Schlüssel heruntergeladen und zusammen mit dem privaten Schlüssel im Mailprogramm importiert werden. Unter www.itsb.rub.de finden sich weitere, ausführliche Informationen zu diesem Thema. **BS**

BITS

Oscars für Datenkraken

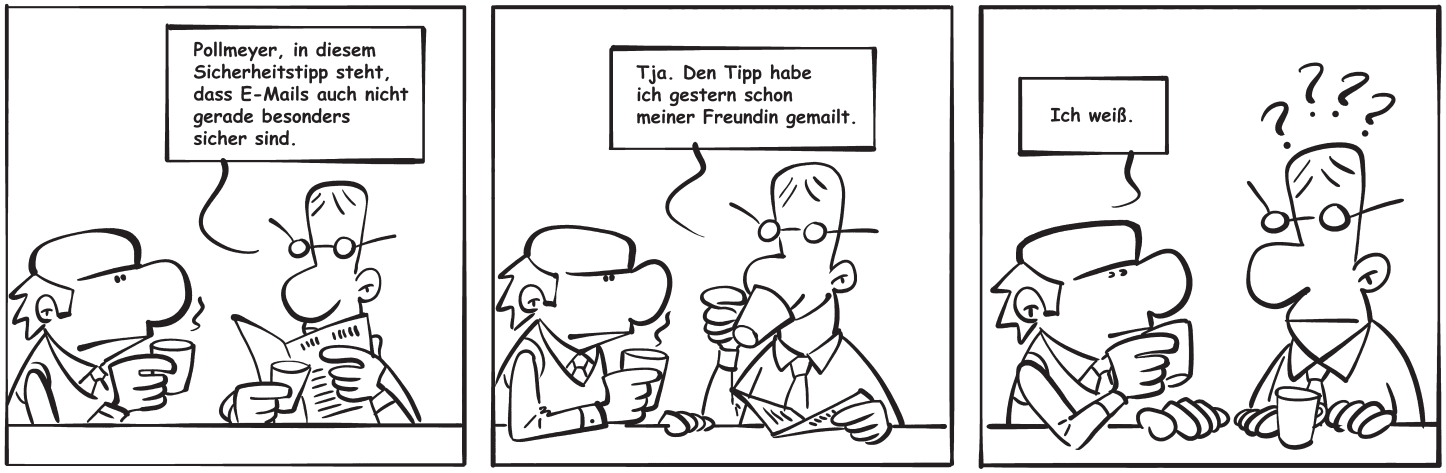
Mit den BigBrotherAwards werden alljährlich Datensünder in Wirtschaft und Politik für fragwürdige Praktiken im Umgang mit personenbezogenen Daten ausgezeichnet. In diesem Jahr haben zwei bekannte Münchener Universitäten die „Ehrung" für ihre Kooperation mit einem Anbieter für „Massive Open Online Courses" (Coursera) erhalten. Zitat aus der Laudatio: „Mit der Verleihung des BigBrotherAwards .. möchten wir die beiden Universitäten und auch alle anderen Bildungseinrichtungen daran erinnern, dass das langfristige Geschäftsmodell von solchen „Bildungsanbietern" daraus besteht, dass die Studierenden durch die Verträge von Coursera nicht die „Kunden" des Online-Bildungsangebotes sind, sondern das Produkt, das verkauft wird."

Urheberrechtsgesetz (UrhG)

Das im März 2018 in Kraft tretende Urheberrechts-Wissenschafts-Gesetz (UrhWissG) dient zur „*Angleichung des Urheberrechts an die aktuellen Erfordernisse der Wissensgesellschaft*". Wesentliche Änderung des UrhG durch das UrhWissG ist die Neugestaltung der gesetzlich erlaubten Nutzungen für den Bereich Unterricht, Lehre und Forschung. Der bisher maßgebliche Paragraph §52 a entfällt und wird durch einen neuen Abschnitt (§60 a-h) ersetzt. Die Arbeitsgruppe Urheberrecht (urheberrecht.uamr.de) gibt schon jetzt einen Ausblick auf die Änderungen. In der nächsten RUBinform wird das Thema ausführlich behandelt.

Tierisches

Haben Affen auch ein Urheberrecht? Diese Frage hat zu einem jahrelangen Rechtsstreit geführt, der einen Fotografen fast in den Ruin gestürzt hätte. Das selbsternannte „Herrchen" des Wildtieres hatte erbittert um Rechte und Einkünfte des Affen gestritten. Ohne die Frage zu beantworten, wurde der Streit kürzlich außergerichtlich beigelegt.



© by Dewitz, Selzer, Partner - Peter Esser

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: ©RUB, Marquard

WEITERE INFOS
ZU UNSEREN THEMEN IM NEWSLETTER:

ZUALLERERST

NIST (National Institute of Standards and Technology), Cyber-Müdigkeit:

https://www.nist.gov/news-events/news/2016/10/security-fatigue-can-cause-computer-users-feel-hopeless-and-act-recklessly

SCHWACHSTELLE MENSCH

Proofpoint, Der Faktor Mensch:

https://www.adn.de/fileadmin/user_upload/Hersteller/Proofpoint/Datenblaetter/pfpt-de-human-factor-report-2017-a4.pdf

Top 5 Köder: *https://www.proofpoint.com/de/corporate-blog/post/top-5-email-phishing-lures*

TA530: *https://www.proofpoint.com/us/threat-insight/post/malicious-macros-add-to-sandbox-evasion-techniques-to-distribute-new-dridex*

Über drei Milliarden Accounts gekapert: *https://www.heise.de/newsticker/meldung/Ueber-drei-Milliarden-Accounts-gekapert-3373358.html*

Ebay AG Phishing: *https://www.heise.de/security/meldung/eBay-Phisher-gehen-mit-persoenlichen-Details-auf-Opferfang-3194026.html*

Weitere Informationen: *http://www.ruhr-uni-bochum.de/itsb-web/email_betrug.html*

E-MAIL **SPOOFING**

Mailserver-FAQ: *https://mail.ruhr-uni-bochum.de/mail/faq/e-mail_zustellung*

Header-FAQ: *https://th-h.de/net/usenet/faqs/headerfaq/*

INFORMATIONSSICHERHEIT AN DER RUB

Koordinierungsausschuss für Informationssicherheit: *http://www.itsb.ruhr-uni-bochum.de/intern/itsstab.html*

Informationssicherheitsmanagementsystem (Dokumentation): *http://www.itsb.ruhr-uni-bochum.de/intern/weiterführendeDokumente.html*

Dezentrale Beauftragte für Informationssicherheit und Datenschutz: *http://www.itsb.ruhr-uni-bochum.de/intern/dez-beauftragte.html*

PFLICHT ZUR ERSTELLUNG EINER **VERARBEITUNGSÜBERSICHT**

EU-Datenschutz-Grundverordnung: *https://www.lda.bayern.de/media/ds_gvo_de.pdf*

SERVER **SICHER VERORTET**

Rahmenkonzept zur Informationssicherheit: *http://www.uv.ruhr-uni-bochum.de/dezernat1/amtliche/ab1047.pdf*

POSTKARTE ODER **EINSCHREIBEN**

Persönliche Nutzerzertifikate an der RUB:

http://www.it-services.ruhr-uni-bochum.de/services/infrastruktur-systeme-it-sicherheit/zertifikatsdienste/beantragung-eines-persönlichen

Shortguide „Beantragung eines persönlichen Nutzerzertifikats“:

http://www.it-services.ruhr-uni-bochum.de/sites/default/files/shortguide_nutzerzertifikat.pdf

Weitere Informationen: *http://www.ruhr-uni-bochum.de/itsb-web/email_sicherheit.html*

BITS

Oscars für Datenkraken: *https://bigbrotherawards.de/2017/bildung-lmu-tu-muenchen*

Arbeitsgruppe Urheberrecht: *http://www.urheberrecht.uamr.de/*

Monkey selfie copyright dispute: *https://en.wikipedia.org/wiki/Monkey_selfie_copyright_dispute*

Streit über Affen-Selfie beigelegt:

http://www.sueddeutsche.de/panorama/rechtsstreit-um-affen-selfie-streit-ueber-affen-selfie-beendet-1.3662934