RUHR-UNIVERSITÄT BOCHUM

RUB

RUBinform

Datenschutz & Datensicherheit

Newsletter 02|**19**

IN DIESER AUSGABE:

LINKS ZU DEN BEITRÄGEN:

www.rub.de/rubinform

ZUALLERERST

Liebe Leserinnen und Leser,
in diesem Jahr gab es an der RUB sehr viele erfolgreiche Phishing-Angriffe zu verzeichnen: E-Mails, die auf den schnellen Blick scheinbar aus vertrauenswürdiger Quelle stammen. Sie fordern den Empfänger auf, einem Link zu folgen, etwa um eine Rechnung oder Account-Daten zu verifizieren. Spätestens jetzt lohnt sich ein aufmerksamer Blick auf die E-Mail. Auch wenn Phishing-E-Mails oft täuschend echt aussehen, lassen sie sich meist entlarven. Gehen Sie achtsam mit sich und Ihren Daten um!

Stabsstelle für Informationssicherheit und behördlicher Datenschutz

KOMPROMITTIERT – WAS NUN?

Der Duden kennt zwei Bedeutungen: bloßgestellt/blamiert oder – im IT-Kontext – Opfer einer Computermanipulation oder Ausspähung von Daten zu sein. Betroffene merken es häufig schnell, wenn Beschwerdemails strömen und E-Mail, Eduroam oder Internet nicht mehr funktionieren. Werden Limits beim Verbindungsaufbau oder Mailversand überschritten, greifen oftmals automatische Sperren. Dann ist es jedenfalls passiert - der Mail-Account oder ein Gerät sind kompromittiert und werden zum Versand von Spam oder Schadsoftware missbraucht. Unter Umständen werden eigene und anderer Leute Daten gestohlen oder verfälscht.

UND DER DATENSCHUTZ?

Die Kompromittierung einer Mailbox oder eines IT-Geräts, das personenbezogene Daten enthält, stellt bereits eine Verletzung des Schutzes dieser Daten dar. Das Datenschutzgesetz NRW und die DS-GVO verpflichten die RUB, solche Datenschutz-Verletzungen in ihrem Verantwortungsbereich und daraus folgende Risiken zu beurteilen und adäquat zu handeln. Diese Aufgaben nehmen der Datenschutzbeauftragte und die Stabsstelle für Informationssicherheit für die RUB wahr. Die Stabsstelle stellt Meldewege und passende Vordrucke zur Klärung der Datenschutz-Fragen zur Verfügung. Je nach Risiko sind Betroffene oder Aufsichtsbehörden fristgerecht zu informieren.

Um weiteren Schaden für den Account-Inhaber und die Ruhr-Universität abzuwenden, werden Mail-Account oder Netzwerk-Ressourcen umgehend gesperrt. Betroffene Nutzer oder Netzbetreuer werden schnellstmöglich informiert. Auch um den Schaden und mögliche Risiken zu beurteilen, ist deren Mitwirkung unerlässlich. Was kann passiert sein?

Unbefugte kennen mein Passwort

Ist der Mail-Account kompromittiert, so hat der Nutzer im einfachsten Fall sein Passwort weitergegeben oder es ist Unbefugten durch eine Phishing-Mail zugänglich gemacht worden. Das Passwort neu zu setzen, bietet sofort Abhilfe. Ist der Account bereits gesperrt, hilft das Servicecenter von IT.Services.

Hilfe, mein Rechner spinnt

Ist die Ursache nicht so leicht nachzuvollziehen, so ist in der Regel ein IT-Gerät mit Schadsoftware befallen, versendet Spam oder fällt durch ungewöhnliches Verhalten auf. Mitunter treibt die Schadsoftware auch im Verborgenen ihr Unwesen, liest Passwörter mit oder spioniert Daten aus. Ob ein böswilliger E-Mail-Anhang oder der Besuch einer verdächtigen Webseite ursächlich sind, wissen Nutzer häufig nicht mehr genau. Auch bei der Überlassung in fremde Hände kann Schadsoftware installiert worden sein – beispielsweise im Rahmen von Kontrollen bei Grenzübertritt. Der Verdacht einer Infektion kann durch geeignete Analysetools bestätigt werden. Eine restlose Bereinigung von Schadsoftware ist aber häufig nicht möglich – auch wenn Antivirus-Tools dies gerne versprechen. Niemand weiß, welche Schadsoftware womöglich nachgeladen wurde oder von Analysetools noch nicht erkennbar ist. Die einzig sichere Möglichkeit besteht in einer vollständigen Neuinstallation von Original-Installationsmedien.

Foto: iStock.com/uprightouch

Wann bin ich wieder online?

Nur wenn keine weitere Gefahr von kompromittierten Geräten oder Mailboxen ausgeht, können diese wieder entsperrt werden. Das Servicecenter und die Stabsstelle für Informationssicherheit beraten hierzu Betroffene.

Vermeidungsstrategie

Ständiges Misstrauen und Unsicherheit im Netz sind eher hinderlich. Das Wissen um Gefahren und Risiken unterstützt sicheres Handeln: Warum ist die Phishing-Gefahr gerade auf Smartphones besonders groß? Was muss ich IMMER beachten, bevor ich meine Zugangsdaten eingebe? Über wichtige Sicherheitsmaßnahmen, aktuelle Tipps, Hilfestellungen und Hintergrundinformationen unterrichtet die Homepage der Stabsstelle. BS

DIE CLEVERE ALTERNATIVE

EvaSys – Software für Umfragen

In der Reihe „Die clevere Alternative“ stellen wir Online-Dienste vor, die an der RUB genutzt werden können und 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.

„Wie hat Ihnen unsere Dienstleistung gefallen?“, „Wie viele Sterne vergeben Sie für das Produkt?“. Immer häufiger werden wir mit Umfragen konfrontiert, meistens handelt es sich um Online-Befragungen. Neben der Bitte um Rezensionen und zur Teilnahme an Marktforschungsumfragen finden sich auch immer wieder Einladungen zu wissenschaftlichen Befragungen in unseren Postfächern. Auch bei der systematischen Verbesserung der Lehre an der Ruhr-Universität spielen Studierendenbefragungen und Befragungen der Absolventinnen und Absolventen eine wichtige Rolle. Nicht immer wird aber unmittelbar deutlich, welche Software dahintersteckt und noch weniger, wo die Server stehen, auf denen unsere oftmals personenbezogenen Daten landen, wenn wir an solchen Umfragen teilnehmen. Diese Fragen werden ganz besonders virulent, wenn es um besonders schutzbedürftige Daten geht. Zu diesen Daten gehören beispielsweise politische Meinungen, religiöse oder weltanschauliche Überzeugungen, aber auch Daten mit Gesundheitsbezug (vgl. Art. 9 EU-DSGVO).

Seit Anfang 2013 können RUB-Angehörige die Software EvaSys für eigene Befragungen nutzen. Damit lassen sich nicht nur Online-Umfragen durchführen, sondern auch maschinenlesbare Papierfragebögen generieren, so dass keine manuelle Datenerfassung notwendig ist. Als Output stehen sowohl Rohdaten für die Verarbeitung in SPSS oder Excel, als auch ein standardisierter Ergebnisreport im PDF-Format zur Verfügung. Für Studierende und Promovierende sowie für Lehrprojekte ist die Nutzung kostenlos. Wissenschaftlerinnen und Wissenschaftler, die EvaSys im Rahmen von drittmittelgeförderter Forschung nutzen wollen, kostet die Nutzung 300 Euro im ersten Jahr und in den Folgejahren je 100 Euro.

Für EvaSys spricht nicht zuletzt, dass die Server an der RUB stehen und Befragungsdaten hier verarbeitet werden, obgleich Menschen aus der ganzen Welt an den hier gehosteten Befragungen teilnehmen können. Für die Server gibt es regelmäßige Sicherungen und Updates, so dass Datenverluste extrem unwahrscheinlich sind.

Alle Informationen, um EvaSys nutzen zu können, finden Sie auf der Webseite www.rub.de/evastud. Dort sind auch die Termine der nächsten Einführungsveranstaltungen zu finden.

ANNE **KRÜGER** & DR. FRANK **WISSING**, DEZERNAT 1 (HOCHSCHULENTWICKLUNG UND STRATEGIE)

WENN EINER EINE **REISE** TUT …

Eine gute Reiseplanung kann viel Stress und Ärger ersparen, insbesondere bei Reisen ins Ausland. Über Einreise- und Einfuhrbestimmungen des Reiselandes informiert das Auswärtige Amt der Bundesrepublik Deutschland. Hier erfährt man, welche Gültigkeit Reisedokumente bei Reiseantritt haben müssen, ob es eine Visumspflicht gibt, welche Impfungen erforderlich oder empfehlenswert sind. Eine sorgfältige Beachtung der Einfuhrbestimmungen kann davor bewahren, dass der vergessene Apfel im Proviant bei der Zollkontrolle zu einer sofort fälligen, empfindlichen Geldstrafe führt.

Was Reisende oftmals auch nicht wissen: In einigen Ländern ist der Zoll befugt, bei der Einreise elektronische Datenträger wie Smartphone, Tablet, Notebook und Digitalkamera zu durchsuchen, die Daten zu kopieren oder gar die Geräte zu beschlagnahmen.

Achtung: Datenkontrolle

Beispielsweise ermächtigt der Customs and Excise Act 2018 den neuseeländischen Zoll zur Durchsuchung von Datenträgern. Wer hierzu Passworte nicht herausgeben will, dem drohen Geldstrafen von bis zu 5.000 NZD. Bei Einreise in die USA führt die dortige Zoll- und Grenzschutzbehörde (CBP) strenge Kontrollen durch. Die CBP Directive No. 33340-049A erlaubt eine anlasslose Durchsuchung und Beschlagnahme von Datenträgern. Mangelnde Kooperation des Besitzers kann im besten Fall zu einer Verweigerung der Einreise führen. Mit derartigen Kontrollen ist auch in weiteren Staaten wie Australien, Großbritannien, Israel, Kanada, Russland und der Türkei zu rechnen. Die Süddeutsche Zeitung berichtete, dass an zwei Grenzübergängen von Kirgisistan nach China sogar Ausspäh-Trojaner auf Handys von Reisenden installiert werden.

Kontrollen elektronischer Datenträger werden im Augenblick noch nicht regelmäßig, sondern eher selten, stichprobenartig durchgeführt und man mag denken, Kirgisistan ist weit weg – doch im universitären Leben ist „die Welt ein Dorf". So verwundert es nicht, dass es auch schon entsprechende Erfahrungsberichte an der RUB gibt.

Foto: iStock.com/kunertus

Informationsschutz auf Reisen

Kontakte, E-Mails, Bilder und Nachrichten, die über Messenger-Dienste ausgetauscht wurden, verraten mehr über das persönliche Leben als Dinge, die in Handgepäck oder Koffer vorzufinden sind. Daher möchte man diese vielleicht noch nicht einmal dem besten Freund zugänglich machen, geschweige denn mit dem Grenzschutz „teilen". Viel schlimmer ist es noch, wenn man Systeme mit sich führt, auf denen sich sensible, vertrauliche Informationen befinden. Die Allianz für Sicherheit in der Wirtschaft (ASW) hat in Zusammenarbeit mit dem Bundesamt für Verfassungsschutz eine Checkliste „Informationsschutz auf Reisen" zusammengestellt. Die Bürgerrechtler der Electronic Frontier Foundation (EFF) haben ein englischsprachiges Whitepaper *Digital Privacy at the U.S. Border* herausgegeben. Beide Dokumente beschreiben Verhalten und technische Maßnahmen, die dienlich sind, um Geräte und Daten bei der Einreise zu schützen.

Mentale Vorbereitung

Generell ist es ratsam, die Menge der mitgeführten Daten zu reduzieren. Falls möglich sollte man ein Reise-Notebook und -Handy nutzen, auf denen ausschließlich die Daten sind, die man benötigt. Ein Backup ist nützlich, damit die Daten nach etwaiger Beschlagnahme von Geräten noch zugänglich sind. Aus E-Mail-, Cloud- und Social-Media-Apps sollte man sich ausloggen und gecachte Inhalte sowie gespeicherte Login-Informationen löschen. Aber Vorsicht: Wer scheinbar unbenutzte, komplett neu installierte Systeme präsentiert, muss eventuell längere Befragungen über sich ergehen lassen.

Die EFF rät, sich mental auf die Grenzkontrolle vorzubereiten, stets ein respektvolles Verhalten zu zeigen und mit den Beamten zu kooperieren. Bei Beantwortung von Fragen sollte man keinesfalls lügen, denn das ist eine Straftat. Soweit möglich sollte man Passwörter nicht herausgeben, sondern die Systeme selbst entsperren. Musste man Passwörter dennoch herausgeben, sind diese anschließend schnellstens zu ändern. **BW**

WIE **COOKIE-HINWEISE** ZUR ZUSTIMMUNG DRÄNGEN

Die Medienaufmerksamkeit rund um die Einführung der Datenschutzgrundverordnung (DSGVO) in 2018 hat dazu geführt, dass viele Unternehmen sich (erstmals) Gedanken darüber machten, ob und wie sie Datenschutz auf ihren Webseiten umsetzen. Doch anstatt weniger Daten zu sammeln, haben viele nur zusätzliche Cookie-Hinweise eingebunden, die aus Sicht der Nutzer*innen vor allem nerven und dabei rechtliche Vorgaben nur unzureichend umsetzen. In mehreren Studien haben Wissenschaftler*innen der RUB und der University of Michigan Cookie-Hinweise und deren Einfluss auf Nutzer*innen untersucht.

Die Zahl von Cookie-Hinweisen auf Webseiten hat rapide zugenommen. In Deutschland stieg ihre Anzahl im ersten Halbjahr 2018 von 26 % auf 49 %. Aber das bloße Vorhandensein eines solchen Hinweises heißt noch lange nicht, dass eine Webseite gut mit den Daten der Besucher*innen umgeht. Eine Analyse vom August 2018 zeigt, dass nur 14 % der Webseiten in ihrem Cookie-Hinweis überhaupt die Möglichkeit bieten, sich für oder gegen Cookies zu entscheiden. Von diesen benutzen über die Hälfte subtile Verfahren, um Nutzer*innen zur Einwilligung zu drängen, indem die Option zur Zustimmung grafisch hervorgehoben ist oder Auswahlfelder bereits angekreuzt sind.

Um zu verstehen, wie Nutzer*innen Cookie-Hinweise wahrnehmen, wurden in einer weiteren Studie verschiedene Varianten von Cookie-Hinweisen auf einer realen Website mit über 80.000 Besucher*innen evaluiert. Getestet wurde, wie Nutzer*innen mit Hinweisen interagieren abhängig von deren Position, den angebotenen Auswahlmöglichkeiten und dem dargestellten Text.

Wenig überraschend entscheiden sich nur wenige Nutzer*innen dafür, von beliebigen dritten Dienstleistern wie Google oder Facebook überwacht zu werden. Wenn sie nicht dazu gedrängt wurden, akzeptierten weniger als 1 % der Befragten jegliche Form von Cookies. Wenn allerdings der „Einverstanden"-Button größer und Auswahlhäkchen schon gesetzt waren, akzeptierten mehr als 30 % der Besucher*innen das Tracking. Allerdings gelten solche „Opt-out"-Verfahren als nicht datenschutzfreundlich und sind damit in der Regel nicht erlaubt. Besser wäre es, Webseiten würden auf unnötige Datensammlung einfach grundsätzlich verzichten, dann wären Cookie-Hinweise überflüssig.

DR. MARTIN **DEGELING** & CHRISTINE **UTZ,**
LEHRSTUHL SYSTEMS SECURITY

Details zu den Studien gibt es unter https://www.syssec.rub.de.

NEUES HOCHSCHULGESETZ NRW: **5 GUTE GRÜNDE** FÜR DEN DATENSCHUTZ

Für die datenschutzrechtlichen Regelungen sind seit jeher auch die gültigen Hochschulgesetze (HG NRW) zu betrachten. Der nordrhein-westfälische Gesetzgeber schafft immer wieder Sonderregeln und erlaubt den Hochschulen regelmäßig, über Satzungen ihre Regeln selbst zu bestimmen. Beispiele für besondere Regeln fanden sich zuletzt bezüglich der Nutzung von Daten von Ehemaligen (§ 8 Abs. 5 HG NRW) oder hinsichtlich der Erlaubnis, bestimmte Personaldaten an Drittmittelgeber zu übermitteln (§ 71 Abs. 1 HG NRW). Auch im novellierten HG NRW finden sich wieder neue Regelungen, die die Verarbeitung personenbezogener Daten im Blick haben:

1. Digitalisierung von Lehrangeboten: Die europäische Datenschutzgrundverordnung erlaubt Verarbeitungen personenbezogener Daten, wenn sie zur Erfüllung einer öffentlichen Aufgabe erforderlich sind. So hat der Gesetzgeber an verschiedenen Stellen bisher implizite Aufgaben ausdrücklich in den Gesetzestext aufgenommen. So sind die Onlinelehrplattformen (Moodle) zwar gut herleitbar gewesen, eine Explizierung der Aufgabe, wie sie in § 3 Abs. 3 HG NRW zu finden ist, erleichtert hier die rechtliche Argumentation.

2. Forschungsinformationssysteme (FIS): FIS sind Datenbanken, die ein Verzeichnis der Forscher und Forschungsaktivitäten einer Forschungseinrichtung enthalten. Sie dokumentieren die Leistungen von Wissenschaftlern einer Hochschule. Die Zulässigkeit der Verarbeitung, bei der auch personenbezogene Daten aus unterschiedlichen Quellen zusammengeführt werden, war zuletzt nicht unumstritten. § 8 Abs. 3 HG NRW ermöglicht den Aufbau und Betrieb derselben. Das Ministerium hat dazu allerdings noch weiteres in einer noch ausstehenden Rechtsverordnung zu regeln.

3. Veröffentlichung von (Bild-)Material: Neu ist auch eine Regelung zum sogenannten Bildungsmarketing, welche eine bessere Information der Öffentlichkeit gewährleisten soll (s. § 8 Abs. 6 HG NRW). Damit war intendiert, einige der rechtlichen Unsicherheiten im Bereich Foto- und Videoaufnahmen zu beseitigen. Ob in dieser Vorschrift tatsächlich die erforderliche gesetzliche Erlaubnis zur Veröffentlichung von (Bild-)Material gesehen werden kann und damit gegebenenfalls Einwilligungen der betreffenden Personen obsolet werden, bleibt noch abzuwarten. In die Gesetzesbegründung kann eine solche Intention hineingelesen werden. Durch die Form der Verankerung der Regelung braucht es aber weiter Überlegungen zu den Bildrechten.

4. Elektronische Gremienwahl: Die Zulässigkeit von Online-Wahlen ist nun explizit im Gesetz festgeschrieben (§ 13 HG NRW), womit das Ziel verfolgt wird, eine möglichst umfassende Wahlbeteiligung zu erreichen. Die Anforderungen an online durchgeführte Wahlen sind jedoch im Hinblick auf die Grundsätze der freien, gleichen, geheimen und prüfbaren Wahl komplex. Zur Sicherung dieser Grundsätze will das Ministerium das Nähere zur Stimmabgabe in elektronischer Form durch eine noch zu erlassende Rechtsverordnung regeln.

5. Anwesenheitspflicht in Lehrveranstaltungen: Novelliert wurde weiterhin, dass Prüfungsordnungen nunmehr vorsehen können, dass die Teilnahme an Lehrveranstaltungen verpflichtend ist (§ 64 Abs. 1 HG NRW). Ob dies dem avisierten „sachgerechten Verfahren des innerhochschulischen Diskurses", so die Gesetzesbegründung, zuträglich ist, wird sich in Zukunft zeigen. Das Kursierenlassen von Teilnehmerlisten wird also wieder häufiger der Fall sein. Die Zulässigkeit solcher Listen bleibt aber auf Veranstaltungen beschränkt, für die eine Teilnahmepflicht ausnahmsweise bestimmt wird.

KUL & SABINE **SONNEBORN**

BITS

Auf dem Laufenden

Wer unsere Sicherheits-Warnungen, neue Ausgaben der RUBinform und Nachrichten zur Informationssicherheit nicht mehr verpassen möchte, kann Aktuelles-Meldungen der Stabsstelle für Informationssicherheit jetzt auch als RSS-Feed, RUBinform-Abo oder News-Mailingliste abonnieren. Dringliche Informationen von besonderer Wichtigkeit veröffentlichen wir zudem über das Portal *Einschränkungen an der RUB (ZNE)* und gesonderte E-Mail-Verteiler. **BS**

Bitte lächeln

Den Briten haftet gemeinhin das Stereotyp an, ausnehmend, fast übertrieben gute Manieren zu besitzen. Satirisch beschreibt schon Ephraim Kishon im „Seekranken Walfisch", dass sie sich eher handgreiflich darum streiten, anderen den Vortritt zu lassen, als anderen den Vortritt zu nehmen. Kein Wunder, dass der Londoner Pub „The Underdog" den Segen der Digitalisierung nutzt, um gegen notorische Vordrängelei ins Feld zu ziehen: Gäste, die hier ihr Pint trinken wollen, müssen sich zuvor per Gesichtserkennungssoftware „registrieren". Gesichtsscan und zugeordnete Wartenummer werden offen auf einem Bildschirm angezeigt. Da kann nichts mehr schiefgehen. Die Software ermittelt zusätzlich das ungefähre Alter des Gastes.

Skeptiker mögen hinterfragen, welchen Vorteil dies gegenüber dem klassischen, von Behördengängen bekannten, Wartenummernverfahren hat. Insbesondere Datenschützer sehen die Gefahr, dass die Daten von Hackern abgegriffen werden könnten. Ein Gedanke, der nicht von der Hand zu weisen ist: selbst bei Firmen, die biometrische Zugangssysteme bereitstellen, sind bereits Millionen Daten „geleakt" worden. Wie rückständig, mögen andere denken. In Ländern, die in der Digitalisierung die Nase vorn haben, kann man schließlich schon per Gesichtsscan bezahlen. Cheers! **BW**

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, GAFO 04/622, 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

Phishing-Mails entlarven: *https://www.itsb.rub.de/themen/toptipps.html*

KOMPROMITTIERT - WAS NUN?

Servicecenter von IT.Services: *https://www.it-services.ruhr-uni-bochum.de/kontakt/*

Meldewege und Formulare zum Datenschutz: *https://www.itsb.ruhr-uni-bochum.de/themen/datenpanne.html*

DIE CLEVERE ALTERNATIVE: **EVASYS**

EvaSys an der RUB: *https://www.ruhr-uni-bochum.de/evastud*

WENN EINER EINE **REISE** TUT ...

Hinweise des Auswärtigen Amtes: *https://www.auswaertiges-amt.de/de/ReiseUndSicherheit/reise-und-sicherheitshinweise*

Customs and Excise Act 2018 (NZL): http://www.legislation.govt.nz/act/public/2018/0004/latest/whole.html#DLM7039503

CBP Directive No. 3340-049A (USA): *https://www.cbp.gov/document/directives/cbp-directive-no-3340-049a-border-search-electronic-devices*

Verweigerung der Einreise bei mangelnder Kooperation: *https://theintercept.com/2019/06/22/cbp-border-searches-journalists/*

Ausspäh-Trojaner bei Grenzübertritt: *https://www.sueddeutsche.de/politik/china-ueberwachung-recherche-1.4507615*

Checkliste *Informationsschutz auf Reisen*: *https://asw-bundesverband.de/fileadmin/user_upload/leitfaden_-blatt/LB_Informationsschutz_Reisen_.pdf*

Whitepaper *Digital Privacy at the U.S. Border: Protecting the Data On Your Devices*: *https://www.eff.org/wp/digital-privacy-us-border-2017*

WIE **COOKIE-HINWEISE** ZUR ZUSTIMMUNG DRÄNGEN

Lehrstuhl für Systemsicherheit: *https://www.syssec.rub.de*

NEUES HOCHSCHULGESETZ NRW: **5 GUTE GRÜNDE** FÜR DEN DATENSCHUTZ

Hochschulgesetz des Landes Nordrhein-Westfalen: *https://recht.nrw.de/lmi/owa/br_text_anzeigen?v_id=10000000000000000654*

BITS

Sicherheits-Warnungen als RSS-Feed: *https://www.itsb.ruhr-uni-bochum.de/feed/news.xml*

RUBinform-Abo: *https://www.itsb.ruhr-uni-bochum.de/themen/rubinform-news.html*

Sicherheits-Warnungen als InfoSec-Newsletter: *https://www.itsb.ruhr-uni-bochum.de/themen/infosec-news.html*

Gesichtsscan gegen Vordrängeln:

https://www.derstandard.at/story/2000110944123/londoner-bar-will-mit-gesichtserkennungssoftware-vordraenglern-entgegenwirken

Millionen Daten geleakt:

https://www.derstandard.de/story/2000107405836/millionen-fingerabdruecke-und-daten-zur-gesichtserkennung-unverschluesselt-im-netz

Zahlen per Gesichtsscan:

https://www.deutschlandfunk.de/digitalisierung-in-china-bezahlen-per-gesichtserkennung.766.de.html?dram:article_id=435111