RUHR-UNIVERSITÄT BOCHUM

RUB

RUBinform

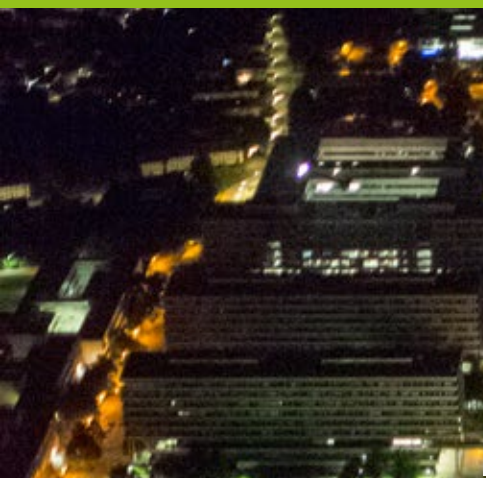
Datenschutz & Datensicherheit

Newsletter 02|16

IN DIESER AUSGABE:

- **NETZWERKDRUCKER** – DIE UNTERSCHÄTZTE GEFAHR
- **STROMAUSFALL** – UND JETZT?
- **COUNTDOWN**
- **USB ATTACKEN**
- INFORMATIVES FÜR **ADMINISTRATOREN**
- **BITS:** URHEBERRECHTSGESETZ § 52A

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



ZUALLERERST

Liebe Leserinnen und Leser,
wir freuen uns, die neue RUBinform präsentieren zu können und danken für das positive Feedback auf die erste Ausgabe. Die Bedrohungslage bleibt angespannt: Ransomware hat in diesem Jahr viele öffentliche Einrichtungen betroffen – auch an der RUB gab es Vorfälle. Gravierende Probleme haben bei uns allerdings veraltete Systeme mit Internetzugriff erzeugt. Das Ergebnis des Selbstversuchs von Tom Liston gilt nach wie vor: „Wer mit einem ungepatchten System surft, hat schnell Ärger." Bedenken Sie dies auch beim Auspacken Ihrer Weihnachtsgeschenke! Frohe und friedliche Festtage wünschen

Brigitte Wojcieszynski
Beauftragte für Informationssicherheit (ITSB)

Kai-Uwe-Loser
Behördlicher Datenschutzbeauftragter (bDSB)

NETZWERK-DRUCKER – DIE UNTERSCHÄTZTE GEFAHR!?

Drucker gelten als eher unscheinbare Geräte, deren Aufgabe es ist, ein digitales Dokument zu Papier zu bringen. Abgesehen von gelegentlicher Aufregung über einen Papierstau wurden sie meist nicht weiter beachtet. Doch vergleichbar mit anderen Gebrauchsgegenständen wie Fernsehern oder Autos haben sich Drucker von mechanischen Geräten mit Mikrochips zu komplexen Computersystemen entwickelt, die oft nur unzureichend geschützt sind. Mediale Aufmerksamkeit erreichte zuletzt ein Vorfall im April dieses Jahres, als massenhaft antisemitische Hetzschriften auf Netzwerkdruckern ausgeduckt wurden. Betroffen hiervon waren vornehmlich US-Universitäten, aber auch verschiedene deutsche Hochschulen. Dies war möglich, weil die Geräte mit öffentlichen IP-Adressen ausgestattet und somit über das Internet erreichbar waren.

Auch Forscher an der RUB beschäftigen sich mit dem Problem der Drucker-Sicherheit. Neben verhältnismäßig harmlosen Angriffen wie unerwünschten Ausdrucken haben sie eine Vielzahl weiterer Schwachstellen in Netzwerkdruckern entdeckt. So lassen sich etwa mit speziellen PostScript-Befehlen die Druckaufträge Dritter mitschneiden und auslesen. Hierdurch kann ein Angreifer an sensible Informationen gelangen – etwa an aktuelle Forschungsergebnisse noch vor ihrer Publikation. Die Sicherheitslücke wird ermöglicht, weil es sich bei der in fast allen Laserdruckern eingesetzten Seitenbeschreibungssprache PostScript um eine vollständige Programmiersprache handelt, die durch ursprünglich nicht vorhergesehene Funktionalitäten erweitert werden kann. Ebenso können Druckaufträgen durch PostScript-Schadcode, welcher sich bis zum Neustart im Hauptspeicher des Druckers befindet, manipuliert werden. So kann ein Benutzer nicht mehr sicher sein, ob das Dokument auf dem Bildschirm tatsächlich dem Ausgedruckten entspricht – oder dieses, etwa durch Zahlendreher, verändert wurde. Bei einigen untersuchten Geräten gelang es sogar, den Arbeitsspeicher und die komplette Festplatte auszulesen oder die physische Zerstörung des NVRAM herbeiführen, jenes Bausteins, der die Speicherung von Langzeit-Einstellungen wie etwa Papierformaten aber auch Passwörtern gewährleistet. Alle Schwachstellen lassen sich ausnutzen, sobald ein Angreifer drucken kann, da sie auf speziellen Befehlen innerhalb eines zu druckenden Dokumentes basieren. Dies ermöglicht es, die Angriffe über einen USB-Stick, per Netzwerk oder sogar über bösartiges JavaScript in einem Webbrowser durchführen.

Für Drucker gilt prinzipiell dieselbe Regel wie für alle Netzwerkkomponenten: Sofern kein direkter Zugang von außen benötigt wird, sollte dem Gerät auch keine öffentliche IP-Adresse (134.147.x.x) zugewiesen werden. Alternativ können Netzwerkbetreuende durch entsprechende Konfiguration von ACLs (Access Control Lists) den Zugriff auf das Gerät über das Internet einschränken. Weiterhin sollten Drucker durch geeignete Maßnahmen wie das Setzen von Gerätepasswörtern geschützt werden, was zumindest einen Teil der Angriffe erschwert.

JENS **MÜLLER**, MA

STROMAUSFALL – UND JETZT?

Ohne entsprechende Pressemeldungen hätte die Welt den Stromausfall am 15./16. April 2015 in der RUB gar nicht bemerkt: Alle zentralen IT-Systeme liefen dank Notstromversorgung weiter, die RUB war im Internet präsent, von außen waren alle IT-Dienste verfügbar. Für die Betreuer dieser Systeme keine Überraschung: Schließlich wurden alle Geräte aus dem Diesel-Notstromnetz versorgt, die betriebswichtigen Systeme sogar über redundante Stromversorgungen mit mindestens einem Bein im Diesel-Notnetz!

Mit mindestens einem Bein – das wurde den Beteiligten am 13. August 2016 schmerzlich bewusst, als die Diesel-Notstromversorgung der RUB im Gebäude NA im Rahmen einer Umbaumaßnahme für 4 Stunden außer Betrieb genommen werden musste. Davon war auch der zentrale IT-Maschinenraum der RUB betroffen: 75% seiner Stromabnahme erfolgt aus dem Diesel-Notnetz, 20% aus dem Normalnetz und 5% aus dem Labornetz. Und damit alles ganz sicher war, hingen mehrere Systeme gleich mit beiden (redundanten) Netzteilen am Diesel-Notstrom – zwar in unterschiedlich abgesicherten Verteilerfeldern, aber doch an der gleichen Einspeisung (Notstrom ist ja schließlich immer gewährleistet!).

Und so kamen auf die Mitarbeiter des Datacenter-Teams vor der Abschaltung zwei stressreiche Wochen zu. Die Elektroversorgung aller IT-Systeme und Datennetz-Elektroniken des Maschinenraums musste überprüft und die zugehörige Dokumentation aktualisiert werden, um dann die Verkabelung im Sinne einer redundanten Versorgung zu optimieren. Die hierfür vorhandenen Kapazitäten der Normalnetz- und Labornetz-Versorgungen waren aber nicht ausreichend. Nur mit Hilfe einer zusätzlich, schnell organisierten Notversorgung mit Baustellen-Verteilern durch die zentrale Betriebstechnik gelang dies.

Und dann war da noch die Raumklimaanlage. Natürlich Diesel-notversorgt, Redundanz war damals noch kein Thema. Dank der RUB-Betriebstechnik konnte aber auch hier eine temporäre Versorgung aus einem der anderen Stromnetze gesichert werden.

Mit diesen Vorarbeiten haben wir schließlich die Abschaltung weitestgehend störungsfrei überbrücken können. Und unser Kunde IT. SERVICES verfügt jetzt über einen Plan, welche IT-Systeme den technischen Anforderungen nicht mehr genügen und bei nächster Gelegenheit ersetzt werden müssen.

Der Vorfall lenkt die Aufmerksamkeit aber auch auf eine andere Entwicklung: Die Motoren für den Diesel-Notstrom sollen Ende 2018 außer Betrieb genommen werden. Für die personelle Sicherheit in den Gebäuden (Aufzüge, Fluchtwege-Beleuchtung, ...) bei Stromausfall werden aktuell auf den einzelnen Hochhäusern Netzersatzanlagen installiert. Eine Elektro-Notversorgung für IT-Systeme, Kühlschränke, Dauerversuchseinrichtungen usw. ist im neuen Liegenschafts-Energiekonzept der RUB nicht vorgesehen.

Fazit: Das geplante RUB-Datacenter wird alle Notversorgungen für die in ihm betriebenen IT-Systeme lokal vorhalten müssen. Und vielleicht noch wichtiger: Allen Beteiligten ist bewusst geworden, wie wichtig ein aktuelles Kabelinventar ist und dass man dieses regelmäßig auf Schlüssigkeit überprüfen muss!

RAINER **WOJCIESZYNSKI**

COUNTDOWN 2018

EU-Datenschutzgrund-verordnung stellt neue Anforderungen für den Datenschutz

Die Ruhr-Universität unterliegt dem DSG NRW. Dort stellen Hochschulen in der Breite der öffentlichen Einrichtungen in den Ländern einen recht kleinen Sonderbereich dar. Es sind nur wenige besondere spezialisierte Regelungen vorhanden. Ansonsten werden Hochschulen wie z.B. ein Einwohnermeldeamt behandelt. Das führt nicht selten zu Brüchen in der Rechtsanwendung. Im Mai 2018 treten durch die EU-Datenschutzgrundverordnung (DS-GVO) an Hochschulen, Unternehmen und Behörden einheitliche Regeln in Kraft.

Die Mitgliedsstaaten können in verschiedenen Bereichen Änderungen vornehmen. Grobe Linien sind schon absehbar, wie 30 Datenschutzbeauftragte an Hochschulen in einem Workshop festgestellt haben, der am 7. und 8. Oktober an der RUB stattgefunden hat. Der Zeitrahmen für die Umsetzung wird eng werden: Die nationalen Umsetzungsgesetze werden erst kurz vor dem Stichtag in Kraft treten. Die Landesgesetzgeber arbeiten derzeit gemeinsam an einem harmonisierten Entwurf für ein einheitliches Landesdatenschutzgesetz.

Die Verarbeitung personenbezogener Daten zu wissenschaftlichen Zwecken besitzt in der DS-GVO einen Sonderstatus. Der Datenschutz soll Forschung zulassen, allerdings sind Schranken zur Auflösung des in den verschiedenen Grundrechten angelegten Konflikts formuliert. Die Privilegierung der Forschung sieht im Grundsatz eine abgestufte Berechtigung zur Verarbeitung von personenbezogenen Daten vor. Die Teilnahme von Personen an der Forschung ist grundsätzlich freiwillig. Es besteht für Wissenschaftler das Gebot, anonym zu forschen. Falls dies nicht möglich ist, ist zu prüfen, ob pseudonyme Verarbeitungen möglich sind. Und nur als letztmöglicher Fall sind mit Begründung der Erforderlichkeit personenbezogene Verarbeitungen in der Forschung erlaubt. Die pseudonyme Verarbeitung erfordert bereits die Einwilligung. Diese Abstufung ist dann im Verlauf der weiteren Forschung wiederum so früh wie möglich auf die Daten anzuwenden: Also pseudonymisieren, sobald möglich, anonymisieren bzw. löschen sobald möglich.

Zuletzt hat der EU-GH nochmals die Begrifflichkeit des Personenbezugs konkretisiert. Die Einstufung ist streng, es ist und bleibt sauber zu durchdenken, ob Daten (auch in Einzelfällen) deanonymisiert werden können.

Einwilligungen bleiben ein wesentlicher Bestandteil des Datenschutzes. Positiv ist anzumerken, dass der Wildwuchs zwischen den unterschiedlichen Landesgesetzen 2018 endet. In einer Erklärung haben sich die Datenschutzbehörden bereits jetzt geäußert, dass bestehende Einwilligungen weitgehend auch unter den Änderungen der DS-GVO gültig bleiben.

Alte Anforderungen, wie beispielsweise die Dokumentationspflicht für alle Verarbeitungen personenbezogener Daten, bleiben an Hochschulen herausfordernd. Vorabkontrollen durch den Datenschutzbeauftragten entfallen, können allerdings unter den Bedingungen einer Datenschutzfolgeabschätzung erforderlich werden. Forschungsvorhaben in vielen Bereichen, bei denen besonders sensible Daten verarbeitet werden, haben in Zukunft erhöhte Pflichten.

Neue Regeln gelten natürlich nicht nur für die Forschung, sondern auch für Verwaltung und Lehre. Hier bleibt es weitgehend bei dem Erforderlichkeitsgrundsatz: Daten dürfen verarbeitet werden, wenn das für die rechtmäßige Aufgabe unabdingbar nötig ist. Änderungen, teilweise auch Öffnungen, liegen im Detail.

Für alle Aufgabenbereiche der Hochschule bekommen die Sicherheitsmaßnahmen durch die DS-GVO ein deutlich höheres Gewicht. Für den Schutz muss man sich am Stand der Technik orientieren. Wie schwierig das in der Vielfältigkeit einer Hochschule wie der RUB ist, zeigt sich auch immer wieder in dieser Publikation. Die Risiken und sinnvolle Schutzmaßnahmen ändern sich stetig.

Bis 2018 bleiben diese und noch einige weitere Neuerungen umzusetzen, leider sind noch nicht in allen Bereichen die Details vollständig geklärt. Im kommenden Jahr gilt es aber, sich auf dem Laufenden zu halten und bereits Schritte für die neuen Regeln umzusetzen. KUL

USB ATTACKEN

Alle kennen es: Beim Verlassen des Arbeitsplatzes, wenn auch nur kurz, wird der Computer über die altbekannte Tastenkombination Windows + L gesperrt. Dadurch ist er erstmal vor unbefugtem Zugriff geschützt – eigentlich.

Der IT-Security Berater Mubix “Rob” Fuller hat jetzt eine neue Angriffsmethode vorgestellt.

Mit einem kleinen Minicomputer in USB-Stick Form (z.B. einem „USB Armory“(155$) oder einem wesentlich günstigeren „Hak5 Turtle“(50$) ist es möglich, von einem gesperrten Computer die Zugangsdaten zu entwenden. Diese Minicomputer geben sich, nachdem sie in den Ziel PC eingesteckt und dadurch automatisch gestartet wurden, als Netzwerkadapter aus. Das System versucht, wie bei jedem neuen Netzwerkadapter, eine IP-Adresse zu erhalten, worauf der USB-Stick mit einer gültigen IP-Adresse antwortet. Zusätzlich fordert er das System auf, eine Konfigurationsdatei herunterzuladen. Dazu wird eine Authentifizierung angefordert und der Angreifer erhält somit LoginID und Passwort.

Die Passwörter werden dabei „verschlüsselt“ in Form von Hashes an den Angreifer gesendet, gerade Windows-Hashes lassen sich aber wegen der einfachen Art der Verschlüsselung leicht „knacken“.

Diese Lücke lässt sich nur durch aufwendige Verfahren schließen, z.B. durch Verwendung von Kerberos in einer Netzwerkumgebung oder die Sperrung des USB-Ports. LARS **JENSEN**, BA

INFORMATIVES FÜR **ADMINISTRATOREN**

(IT-)Administratoren planen, konfigurieren, betreiben, überwachen und pflegen IT-Systeme, um die reibungslose Unterstützung von Geschäftsprozessen zu gewährleisten. Sie benötigen dazu ein breitgefächertes technisches Basiswissen, Gespür für die richtige Lösung sowie die ständige Bereitschaft, ihre Kenntnisse in einem sich rasant ändernden Umfeld „auf dem neusten Stand" zu halten.

Allerdings reicht der Fokus auf die rein technischen Kenntnisse nicht aus. Ein Administrator hat gerade auch wegen seiner weitreichenden Zugriffsrechte eine besondere Verantwortung: Er ist zu absoluter Vertraulichkeit verpflichtet, muss einen rechtskonformen Betrieb der von ihm betreuten Systeme sicherstellen und Sicherheitskonzepte unter Risikoabwägung entwickeln. Dazu sind einschlägige gesetzliche Vorgaben (Datenschutzgesetze, Telekommunikationsgesetz – TKG und Telemediengesetz – TMG, Urheberrechtsgesetz), Normen und Quasistandards sowie insbesondere interne Regelungen wie Dienstvereinbarungen und Ordnungen der RUB zu beachten.

Zur Orientierung in diesem „Dschungel" stehen RUB Administratoren interessante (kostenfreie) Informationsquellen zur Verfügung. Ohne Anspruch auf Vollständigkeit werden im Folgenden einige davon vorgestellt: Der DFN-Verein bietet mit seinem „Rechtsguide und Wissensbasis" einen guten Einstieg in die Pflichten, die sich aus den wichtigsten Rechtsnormen ergeben. Der monatlich erscheinende „DFN-Infobrief Recht" betrachtet zudem aktuelle Gesetzgebungen und Rechtsprechungen mit Blickrichtung auf das Hochschulumfeld.

Die zentrale Datenschutzstelle der baden-württembergischen Universitäten (ZENDAS) veröffentlicht zahlreiche Informationen und Bewertungen zum Thema Datenschutz. Aus dem Netzwerk der RUB ist der Zugriff auch auf geschützte Inhalte dieses Info-Servers dank des RUB-Abos möglich.

Zur Identifikation von Maßnahmen, die bei der Erstellung eines Sicherheitskonzepts zu berücksichtigen sind, unterstützen die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegeben Grundschutzkataloge oder die international anerkannten Normen DIN ISO/IEC 27001/27002. Während der mehrere Ordner umfassende BSI-Quasistandard detailliert organisatorische, infrastrukturelle, personelle und technische Maßnahmen beschreibt, haben die DIN Normen eher Übersichtscharakter und weisen auf Maßnahmenbereiche hin. Das Angebot des BSI ist öffentlich zugänglich, die DIN Normen können über das Perinorm Angebot der UB eingesehen werden.

Interessierte können im Online Angebot der UB einschlägige Zeitschriften wie „DuD – Datenschutz und Datensicherheit", „Computer und Recht" oder „Multimedia und Recht" finden. Über das e-book Portal der UB sind zudem Fachbücher z.B. zum IT-Risikomanagement einsehbar.

Die Online-Tutorials von video2brain enthalten neben technischen Tutorials auch ein Tutorial über „Rechtsgrundlagen für Administratoren". Video2brain kann mittels der RUB LoginID (Edu-Login) kostenlos genutzt werden.

Last but not least verweisen wir auf das Online-Angebot der Stabsstelle für Informationssicherheit und des behördlichen Datenschutzbeauftragten der RUB. Ach noch etwas: der nächste „Admin Appreciation Day" ist am 28. Juli 2017! BW

BITS

Urheberrechtsgesetz § 52a
Das Urheberrechtsgesetz (UrhG) schützt das Recht eines Menschen an seinen geistigen Werken der Literatur, Wissenschaft und Kunst. Dem Urheber ist es vorbehalten, sein Werk zu verwerten, eine Vervielfältigung oder Veröffentlichung zu veranlassen. Im UrhG sind auch Ausnahmen vorgesehen. Für die Nutzung von geschützten Werken in der Hochschullehre (und Forschung) ist insbesondere der § 52a maßgebend. Kleine Teile eines Werkes, Werke geringen Umfangs sowie einzelne Beiträge aus Zeitungen oder Zeitschriften dürfen zur Veranschaulichung im Unterricht ohne Zustimmung des Autors verwendet und einem begrenzten Kreis zugänglich gemacht werden. Für die Nutzung ist eine Vergütung zu zahlen, die durch Verwertungsgesellschaften (VGs) geltend gemacht wird.

Einzelerfassung bei Sprachwerken
Länder und VGs hatten bisher eine Pauschalvergütung vereinbart, die von den Ländern gezahlt wurde. Bei der Neuverhandlung in 2013 konnten sich alle VGs außer VG Wort (zuständig für Sprachwerke) auf eine Fortsetzung dieser Modalität einigen. Mit VG Wort ist ein separater Rahmenvertrag gültig ab 1.1.2017 ausgehandelt worden, der die geforderte Einzelerfassung der Nutzung vorsieht (0,008 € pro Seite und Teilnehmer). Hochschulen können diesem Rahmenvertrag beitreten. Die Einzelerfassung soll durch die Lehrenden über ein elektronisches Meldeverfahren erfolgen. Zudem sind die Hochschulen direkt für die Vergütung zuständig. Viele Hochschulen haben bereits mitgeteilt, dass sie dem Vertrag nicht beitreten werden und auf Neuverhandlungen hoffen. Entsprechende Beschlüsse hat auch das Rektorat der RUB gefasst und bekanntgegeben. Ab 1.1.2017 dürfen demnach geschützte Sprachwerke nicht mehr zugänglich gemacht werden. KUL/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); Anschrift: Ruhr-Universität Bochum, Geschäftszimmer Stabsstelle Informationssicherheit, NAFOF 03/252, Kerstin Bussmann, 44780 Bochum, Telefon: 0234/32-24888, E-Mail: rubinform@rub.de; Infos: www.rub.de/rubinform; Titelbild: ©Hans Blossey

WEITERE INFOS
ZU UNSEREN THEMEN IM NEWSLETTER:

ZUALLERERST

Tom Liston, Follow the Bouncing Malware:
https://isc.sans.edu/diary.html?date=2004-07-23
Deutsche Fassung: Heise, Schädlingen auf der Spur:
https://www.heise.de/security/artikel/Schaedlingen-auf-der-Spur-270540.html

NETZWERKDRUCKER – DIE UNTERSCHÄTZTE GEFAHR!?

Thousands of Printer Hacked:
https://www.vpnranks.com/news/thousand-of-printer-hacked-for-racist-flyers/
http://fortune.com/2016/03/29/hack-printers-internet-of-things/
Hacker fluten Unis mit antisemitischen Hetzschriften:
http://www.zeit.de/gesellschaft/zeitgeschehen/2016-04/antisemitismus-hacker-universitat-hamburg-tuebingen-drucker

STROMAUSFALL - UND JETZT?

Stromausfall an Ruhr-Uni:
http://www.derwesten.de/staedte/bochum/stromausfall-an-ruhr-uni-groesster-blackout-seit-25-jahren-id10566433.html
RUB Aktuelles:
http://aktuell.rub.de/meldung/2015/04/meld02628.html.de

COUNTDOWN

EU-Datenschutzgrundverordnung (deutsche Fassung):
https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2016/05/CELEX_32016R0679_DE_TXT.pdf
BDSG-Referentenentwurf vom 23.11.2016:
https://www.datenschutzverein.de/wp-content/uploads/2016/11/161123_BDSG-neu-RefE_-2.-Ressortab-Verbaende-Laender.pdf

USB ATTACKEN

Snagging creds from locked machines:
https://room362.com/post/2016/snagging-creds-from-locked-machines/

Informatives Für Administratoren

DFN-Verein, Rechtsguide und Wissensbasis:
https://www.dfn.de/rechtimdfn/rgwb/
DFN Infobrief Recht:
https://www.dfn.de/rechtimdfn/dfn-infobrief-recht/
ZENDAS:
https://www.zendas.de/
BSI Grundschutzkataloge:
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html
Perinorm (UB):
https://www.perinorm.com/search.aspx
Auf nachfolgende Zeitschriften kann aus dem Uninetz zugegriffen werden
DuD-Datenschutz und Datensicherheit (UB):
http://link.springer.com/journal/volumesAndIssues/11623
Computer und Recht (Juris Autologon (UB) -> zur Recherche->Zeitschriften->CR):
http://www.ruhr-uni-bochum.de/jura/zrs/juris/HEBISUBO_autologin_jportalautologin

Multimedia und Recht (UB):
https://beck-online.beck.de/default.aspx?vpath=bibdata%2fzeits%2fMMR%2fcont%2fMMR%2ehtm

E-Books-Portal (UB):
http://www.ub.rub.de/DigiBib/ebooks/
Video2brain:
http://www.it-services.rub.de/software/video2brain
Stabsstelle Informationssicherheit:
www.itsb.rub.de
Behördlicher Datenschutzbeauftragter der RUB:
https://dsb.ruhr-uni-bochum.de/

BITS: Urheberrechtsgesetz § 52A

Meldung RUBeL:
http://www.rubel.rub.de/content/§52a-urhg
Moodle Kurs:
https://moodle.ruhr-uni-bochum.de/m/course/view.php?id=7852
Informationen zur Vertragslage:
https://www.kmk.org/themen/hochschulen/bibliotheken.html
Verträge im Wortlaut:
http://www.bibliotheksverband.de/dbv/vereinbarungen-und-vertraege/urheberrecht-gesamtvertraege.html
VG Wort:
http://www.vgwort.de/einnahmen-tarife/wiedergabe-im-internet-intranet/hochschulen.html