UNIVERSITÄT BERN

«thinkB4Uclick»

Sicherer Umgang mit IT-Mitteln an der Universität Bern

Stefan Zahnd
Universität Bern
Informatikdienste

Agenda

- Vorstellung
- Ziele
- Informationen (45 Minuten)
  - Grundsätze der IT-Sicherheit
  - Campus Account
  - E-Mail
  - Internet
  - Social Engineering
  - Mobile Geräte
  - Datenschutz
- Fragen / Diskussion

Vorstellung

- Informatikdienste
  - +/- 72 Mitarbeitende
  - Betrieb verschiedener Dienstleistungen für gesamte Universität (Mail, Firewall, Netzwerk uvm.)

- Referent
  - Stefan Zahnd, BSc BFH IT-Security
  - Seit 2002 bei den ID

«thinkB4Uclick» - Grundsätze

- **Zuerst denken, dann klicken/handeln**
- Seien Sie **aufmerksam und skeptisch** (niemand schenkt Ihnen etwas)
- **Verhalten Sie sich im Internet gleich wie im realen Leben** und behandeln Sie andere so, wie Sie selbst behandelt werden möchten
- Behandeln Sie digitale Informationen wie anderes Inventar und **tragen Sie Sorge** dazu

Informationen sind das neue Gold

UNIVERSITÄT BERN

Daten sind das neue Gold

Der Handel mit Daten wird immer lukrativer. Es ist ein neuer milliardenschwerer Markt entstanden. Aber was macht personenbezogene Informationen eigentlich so wertvoll? Und wer interessiert sich für sie?

Berlin. Persönliche Daten gelten als das neue Öl des Internets und die neue Währung der digitalen Welt“: 2009 prägte die damalige EU-Kommissarin für Verbraucherschutz, Meglena Kunewa, dieses seither viel zitierte Bild. Daten sind zum Rohstoff eines Wirtschaftszweiges geworden: personenbezogene Daten wie Name, E-Mail-Adresse, Einkommen oder Foto und auch solche etwa über Verkehrsflüsse oder Stromverbrauch.

Eine Studie im Auftrag der Europäischen Kommission schätzt den Gesamtwert der Datenwirtschaft in der EU auf 300 Milliarden Euro im Jahr 2016 und prognostiziert einen Anstieg auf 740 Milliarden im Jahr 2020. Der Studie zufolge gibt es in der EU sechs Millionen

https://www.haz.de/Nachrichten/Politik/Daten-sind-das-neue-Gold

Ziele

- Sie wissen
  - was mit “IT-Sicherheit” gemeint ist;
  - welche Gefahren im Umgang mit IT-Mitteln lauern;
  - wie Sie sich vor den Gefahren effizient schützen;
  - an wen Sie sich bei Fragen/Problemen wenden können.

- Dieser Workshop ist als Ergänzung / Vertiefung zur Schulung auf ILIAS gedacht
  - https://ilias.unibe.ch/goto_ilias3_unibe_crs_1086873.html

UNIVERSITÄT BERN

Schlagzeilen – Washington State University

Washington State University Settles $4.7M Data Breach Lawsuit

About 1.2 million individuals were impacted by the April 2017 hard drive theft from a storage unit, where the WSU research department kept both personal and health research data.

The suit was filed by victims who claimed WSU's data security was at best 'questionable'. The hard drives were used to create a weekly backup of research data which went through several handoffs. These exchanges were poorly monitored, causing malware.

https://healthitsecurity.com/news/washington-state-university-settles-4.7m-data-breach-lawsuit

UNIVERSITÄT BERN

Schlagzeilen – Australian National University

Australian National University hit by huge data breach

Vice-chancellor says hack involved personal and payroll details going back 19 years

▲ The Australian National University in Canberra has revealed it was the subject of a huge data breach. Photograph: Alan Porritt/AAP

The Australian National University is in damage control after discovering a major data breach a fortnight ago in which a "significant" amount of staff and student information was accessed by a "sophisticated operator".

The university has confirmed an estimated 200,000 people have been affected by the hack, based on student numbers each year and staff turnover.

https://www.theguardian.com/australia-news/2019/jun/04/australian-national-university-hit-by-huge-data-breach

https://www.anu.edu.au/news/all-news/data-breach

Schlagzeilen – Australian National University

UNIVERSITÄT BERN

LESSONS FROM THE ATTACK AND FOLLOW-UP ACTIONS

While, and in part because, the actor was operationally sophisticated and deliberate in their targeting, there are several lessons for the University that have arisen from the data breach and have formed the basis of a range of remediation and hardening measures. Below, personally identifiable information and phishing awareness are called out for special attention, and the remainder are captured in Table One.

Personally identifiable information

The most critical issue arising from the breach has been the protection of affected members of our community and dealing with any repercussions due to the loss of personally identifiable information (PII). As an initial step, ANU provided assistance in this matter through services offered by IDCARE. In addition, enquiries relating to indi

As noted above it is not possible
the lens of the systems which we
knowledge, at the time of the pub
be in the scope of the disclosure.

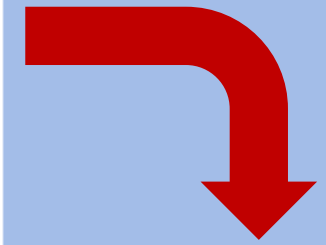
ANU has already instigated data
with PII data kept in its administra
to be undertaken in order to furth
manner, which allows us to remai
chaired by the Chief Privacy Offic
remediation measures.

Before the detection of the breac
for stolen data or credentials that
such activity has been detected.
data or credentials. Should these
prompt notification of any affecte

Phishing awareness

As noted throughout the timeline,
social engineering which underpi
against this form of attack.[16] Give
users, it is clear to us that more e
across the University community.
investment in security culture efforts under the auspices of its forthcoming strategic information security strategy. Work has already commenced with awareness training for high-risk groups.

In addition to security culture, we have invested in stronger safeguards for our mail gateway and are expediting the retirement of legacy mail systems. These measures have already resulted in better technical protection for our mail users, and further investment will follow under the strategic program.



Phishing awareness

As noted throughout the timeline, phishing emails were a hallmark of the activities of the actor. The social engineering which underpinned these emails highlights the vigilance needed to protect users against this form of attack.[16] Given the methods of the actor and the number of successfully phished users, it is clear to us that more effort is required to help drive awareness and safe user behaviours across the University community. ANU will focus significantly in this area as part of a broader investment in security culture efforts under the auspices of its forthcoming strategic information security strategy. Work has already commenced with awareness training for high-risk groups.

In addition to security culture, we have invested in stronger safeguards for our mail gateway and are expediting the retirement of legacy mail systems. These measures have already resulted in better technical protection for our mail users, and further investment will follow under the strategic program.

Schlagzeilen - Hochschulsektor

Higher education's vulnerability to cyber attacks

Establishing a Written Information Security Program to address exposure

By Charles E. Harris and Laura R. Hammargren
September 6, 2016

— University Business, August 2016

Recent highly publicized cyber attacks have spurred a growing public awareness of the risk that sensitive personal information might be accessed by unauthorized third parties. It is not as well-known that the industry sector with the highest number of breaches is higher education: since 2005, higher education institutions have been the victim of 539 breaches involving nearly 13 million known records. This trend may be due, in part, to the sheer number of personal records kept by these institutions, considering their ever-changing student bodies, as well as the valued open, collaborative environment of most colleges and universities.

https://www.universitybusiness.com/article/0816-wisp

Schlagzeilen – Hochschulsektor

UNIVERSITÄT BERN

SECURITY

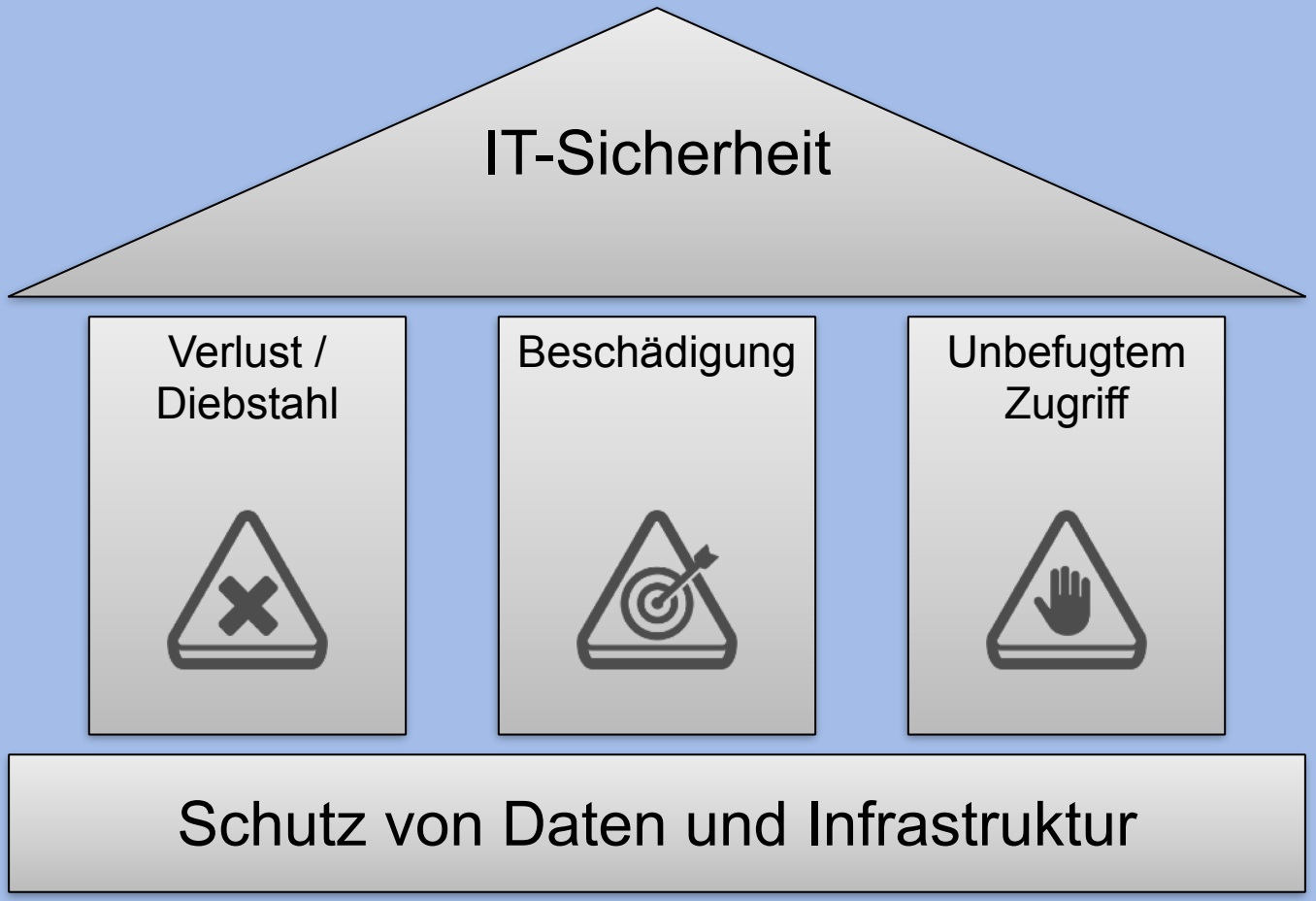
Education Sector Data Breaches Skyrocket in 2017

With breaches up 103 percent, universities will continue to rely on technology and user practices to keep data safe from hackers.

A new report from Gemalto found that **the number of lost, stolen or compromised data records went up 164 percent in the first six months of 2017** compared to the last half of 2016, Campus Technology reports.

https://edtechmagazine.com/higher/article/2017/12/education-sector-data-breaches-skyrocket-2017

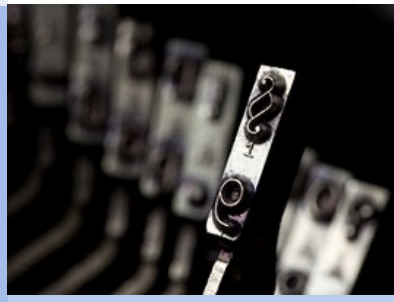
IT-Sicherheit - Grundsätze



IT-Sicherheit an der Universität Bern

UNIVERSITÄT BERN

- Reglemente und Weisungen
  - http://rechtsdienst.unibe.ch > Rechtssammlung > Informatik
    - Weisungen über die Benutzung der IT-Ressourcen an der Universität Bern

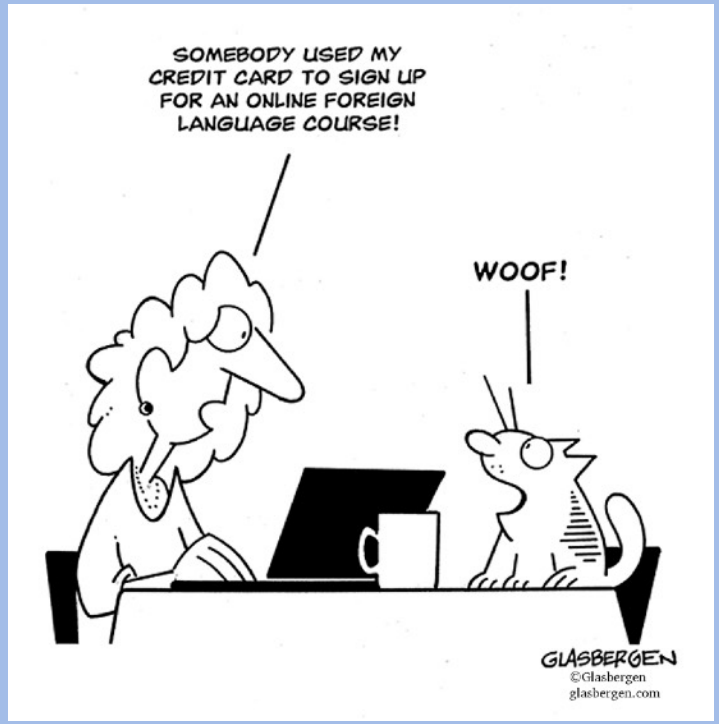


Rechtssammlung der Universität

- Ansprechpersonen Stufe Institut / Abteilung
  - Technik-Verantwortliche
  - Vorgesetzte Stelle
- Ansprechpersonen Stufe Universität
  - Rechtsdienst: info@rechtsdienst.unibe.ch
  - ID (Security-Team):
    - security@unibe.ch
    - http://unibesecure.unibe.ch

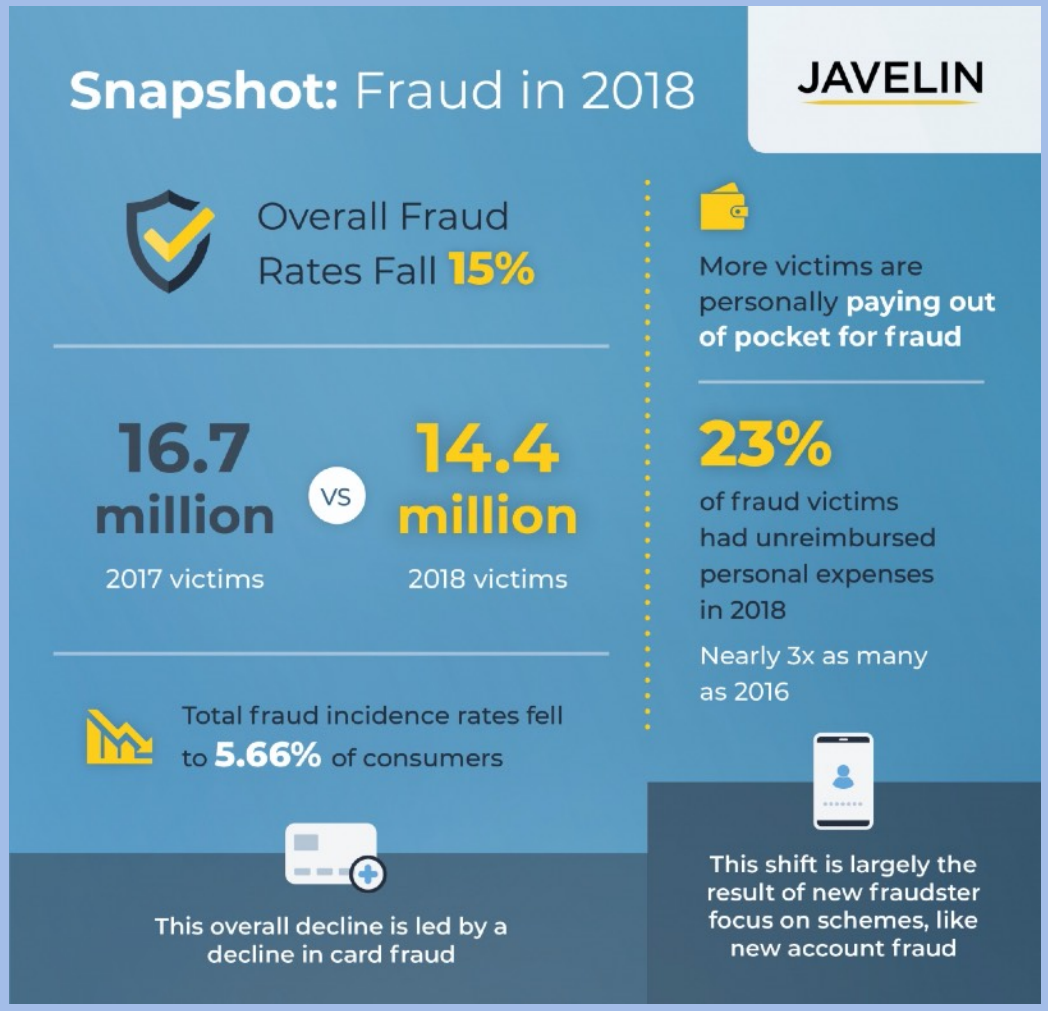
Campus Account (CA)

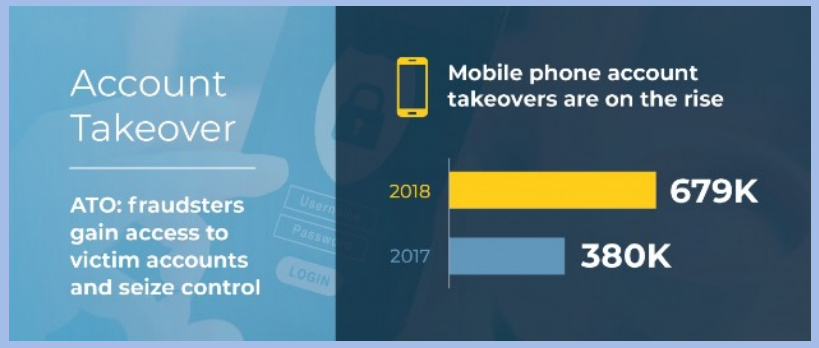
- Gefahr
  - Identitätsmissbrauch



UNIVERSITÄT BERN

Identitätsdiebstahl in Zahlen





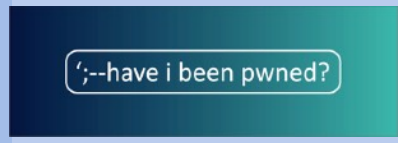
https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-report-fraudsters-seek-new-targets-and-victims-bear-brunt

Campus Account (CA)

- Do's
  - Behandeln Sie Ihren CA und Ihre UniCard wie Ihren **Hausschlüssel**
  - Schützen Sie Ihren CA mit einem
    - **Passwort**
      - 12 Zeichen, Sonderzeichen usw.
    - **Passphrase (Pass-Satz)**
      - `MeinHuthat3EckenundmeineKatze2blaueAugen`
  - Verwenden Sie ein **separates Passwort** für Ihren CA
    - Verwenden Sie einen Passwort-Manager
- Dont's
  - **Geben Sie das Passwort Ihres CA niemals weiter**, auch nicht an Freunde, Kollegen, Verwandte, Vorgesetzte usw.
  - Lassen Sie **niemals eine andere Person mit Ihrem CA arbeiten**

Wie wählt man ein starkes Passwort?

Einzigartigkeit und Passwort Manager



Wurde mein Konto gestohlen?

Häufigste Passwörter

UNIVERSITÄT BERN

Die 25 häufigsten Passwörter gemäß SplashData

Rang	2011[6]	2012[7]	2013[4]	2014[8]	2015[9]	2016[3]	2017[10]	2018[11]	2019[12]
1	password	password	123456	123456	123456	123456	123456	123456	123456
2	123456	123456	password	password	password	password	password	password	123456789
3	12345678	12345678	12345678	12345	12345678	12345	12345678	123456789	qwerty
4	qwerty	abc123	qwerty	12345678	qwerty	12345678	qwerty	12345678	password
5	abc123	qwerty	abc123	qwerty	12345	football	12345	12345	1234567
6	monkey	monkey	123456789	123456789	123456789	qwerty	123456789	111111	12345678
7	1234567	letmein	111111	1234	football	1234567890	letmein	1234567	12345
8	letmein	dragon	1234567	baseball	1234	1234567	1234567	sunshine	iloveyou
9	trustno1	111111	iloveyou	dragon	1234567	princess	football	qwerty	111111
10	dragon	baseball	adobe123	football	baseball	1234	iloveyou	iloveyou	123123

https://de.wikipedia.org/wiki/Listen_der_h%C3%A4ufigsten_Passw%C3%B6rter

E-Mail

- Gefahren
  - Infektion mit Schadsoftware (Malware)
  - Diebstahl von Benutzername, Passwort, Kreditkartendaten usw.
  - Bekanntgabe von Personendaten an Dritte

E-Mail ist kein sicheres Übertragungsmedium!

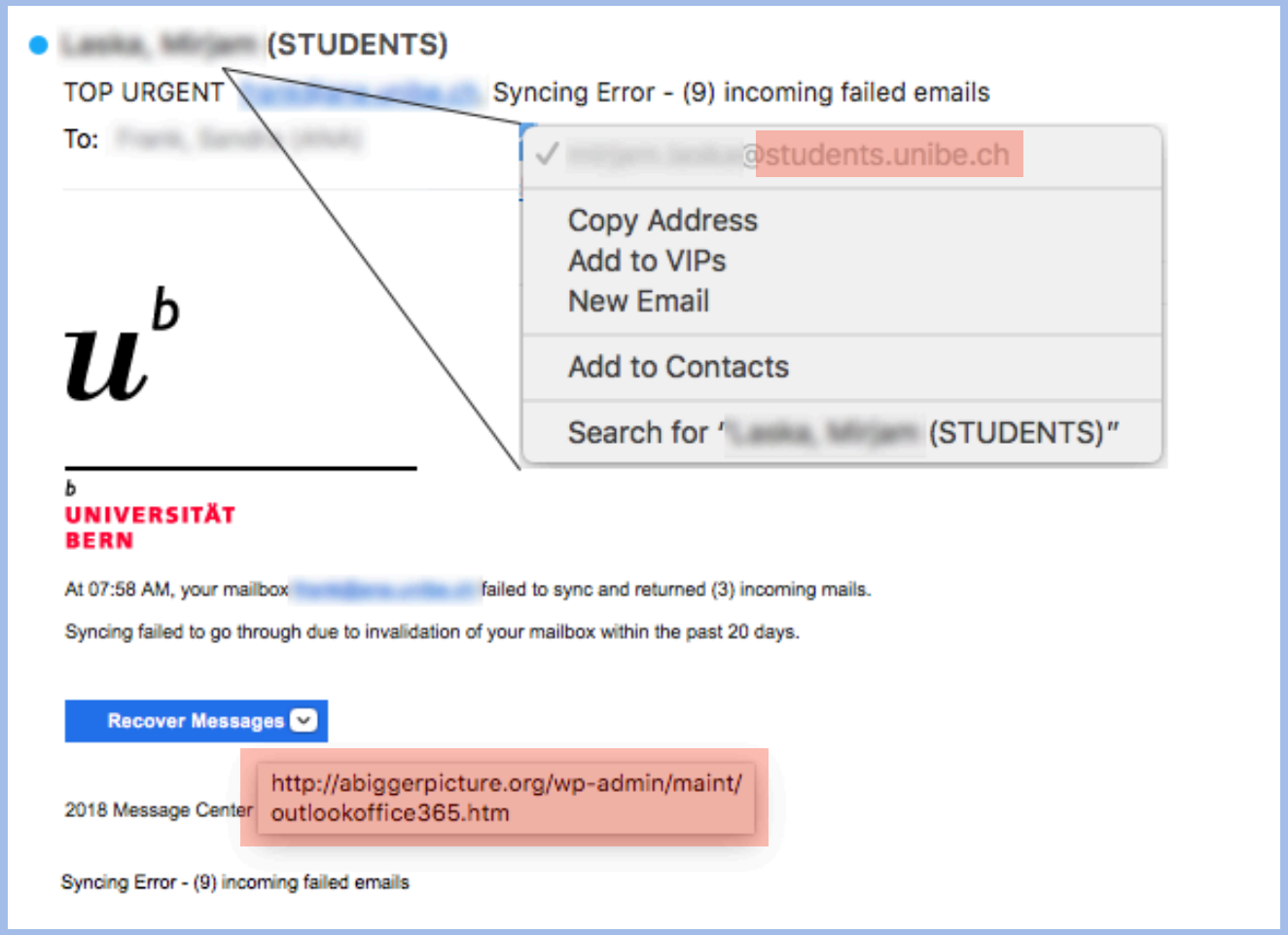
Vorsicht vor dem Angelhaken

- Do's
  - Verwenden Sie **für geschäftliche E-Mails nur die E-Mail-Dienste der Universität Bern**
- Dont's
  - **Reagieren Sie niemals auf E-Mails** in denen Sie aufgefordert werden sich über einen Link anzumelden
  - **Bei Abwesenheit E-Mails nicht weiterleiten**
    - Absender mittels automatischer Antwort auf die Abwesenheit hinweisen und alternative Kontakte angeben
  - Öffnen Sie E-Mail-Anhänge nur, wenn Sie diese von einem Absender erwarten

Was ist Phishing?

Erkennen Sie Phishing?

Phishing von der Universität Bern



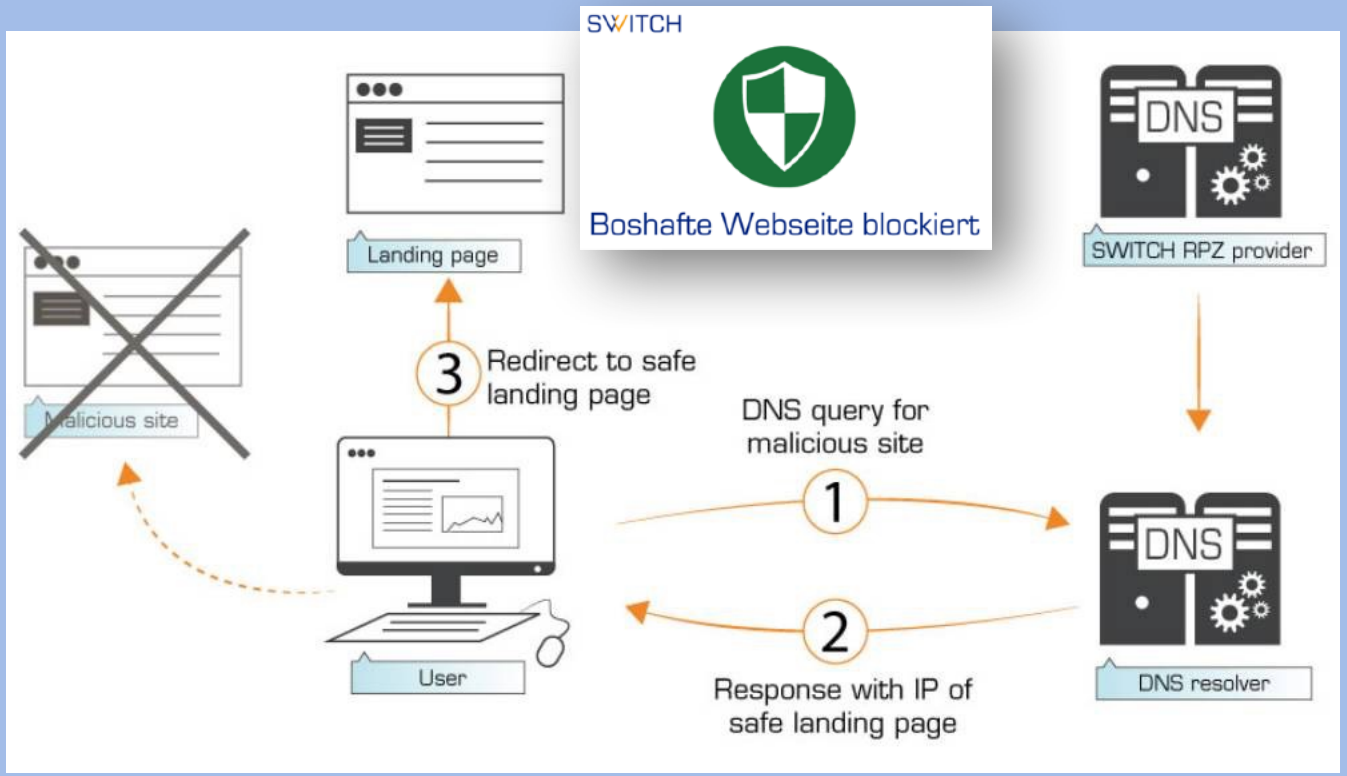
DNS Firewall - Falls man doch klickt

UNIVERSITÄT BERN

SWITCH DNS Firewall
First layer of protection

Erfahren Sie mehr über die DNS Firewall

- Jede DNS-Abfrage von einem Gerät, das mit dem Netzwerk der Universität Bern verbunden ist (inkl. WiFi und VPN) wird auf Risiken geprüft



UNIVERSITÄT BERN

Internet

- Gefahren
  - Infektion mit Malware
  - Diebstahl von Benutzername, Passwort, Kreditkartendaten usw.
  - Angriffe auf die persönliche Integrität

Internet - Netiquette

Do's	Don'ts
Identifizieren Sie sich (Anrede, Signatur)	**Vermeiden Sie Sarkasmus** (wer Sie nicht kennt, könnte es falsch verstehen)
Geeben Sie einen sinnvollen Betreff an (besonders bei E-Mails)	**Vermeiden Sie SPAM** (bspw. Kettenbriefe)
Respektieren Sie die Privatsphäre anderer (Achtung beim zitieren und weiterleiten von Informationen)	**Unterlassen Sie Beleidigungen**
Formulieren Sie präzise	**Verwenden Sie keine GROSSBUCHSTABEN als Verstärkung** (besser sind *Sternchen*)
Bestätigen Sie den Erhalt von Nachrichten und antworten Sie baldmöglichst	
Achten Sie auf die Rechtschreibung	
Verwenden Sie passende Emoticons (helfen Sie anderen Ihre Meinung / Gefühle besser zu verstehen)	

Sicher im Internet surfen

UNIVERSITÄT BERN

– Geben Sie sensible Informationen wie Anmeldeinformationen und Kreditkartendaten nur auf sicheren Websiten ein

1. Erweiterte Validierung (maximales Vertrauen)

2. Standard Validierung (normales Vetrauen)

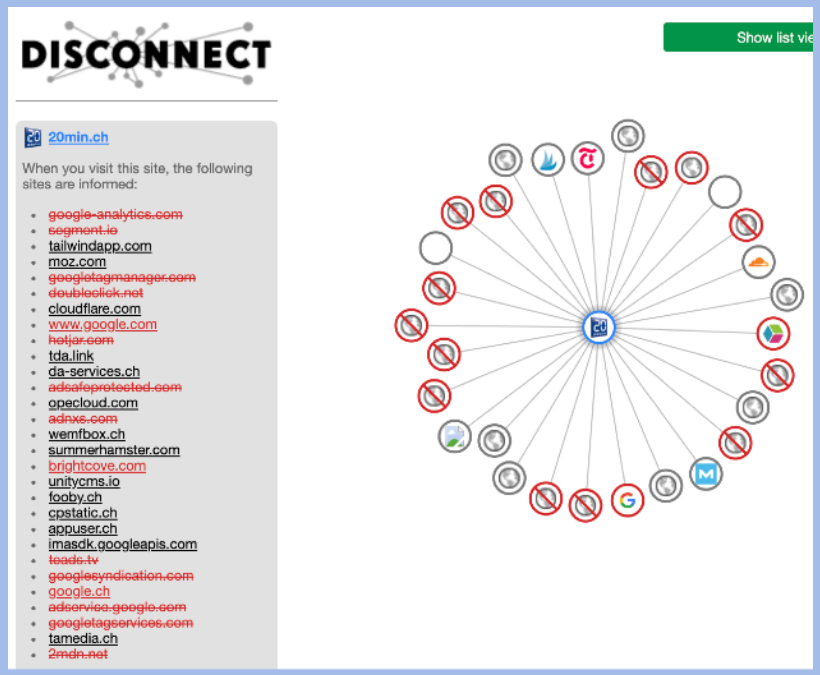
3. Unsichere Webseite (kein Vertrauen)

Internet – Schützen Sie Ihre Privatsphäre

UNIVERSITÄT BERN

- Schützen Sie sich vor ungewollter Datenerhebung beim surfen mit
  - Skript- / Werbeblockern
  - Datenschutzfreundlichen Suchmaschinen

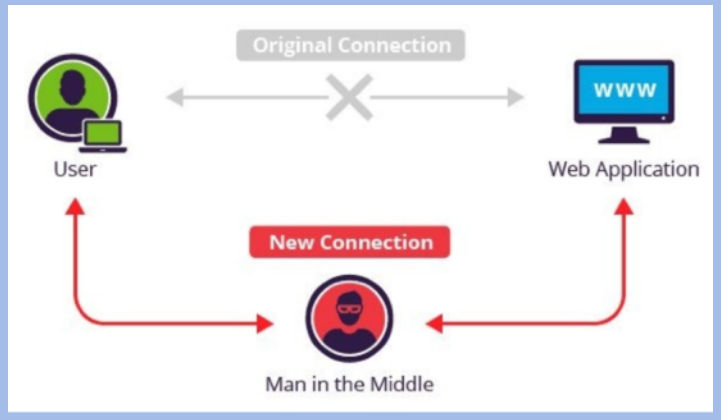
Geschichten aus dem Internet



Internet – Wi-Fi

- Auf dem Campus der Universität Bern
  - **eduroam** = sicher / verschlüsselt
  - **public-unibe** = unsicher / nicht verschlüsselt (ausser HTTPS)

- In der Öffentlichkeit (Hotels, Flughafen, Zug etc.)
  - Webseiten mit HTTPS (kleines Schloss) sind sicher
  - Sichern Sie die Verbindung mit einem VPN (von der UniBE oder ProtonVPN)
  - Registrieren sie sich nicht mit Ihrer UniBE E-Mail-Adresse



ProtonVPN

Kostenloser VPN made by CERN

EUROPOL

Mehr zu den Risiken mit Wi-Fi

Social Engineering / Hacking

- Warum gibt es Social Engineering?
  - Einen Menschen auszutricksen ist einfacher als eine technische Hürde zu umgehen

Bequemlichkeit

Ignoranz

Eile

Angst

Vertrauen

Verhalten

ANGREIFER MACHEN JAGD AUF IHRE MENSCHLICHEN SCHWÄCHEN

Unachtsamkeit

Sympathie

Fähigkeiten

Ego

Gier

Verlangen

Social Engineering / Hacking

UNIVERSITÄT BERN

- 3 Grundtypen von Taktiken

Persönlich

Türöffner
Der Techniker

Telefon

Panik
Ärger

Digital

Phishing
Social Media Phishing

Social Engineering / Hacking - Prävention

UNIVERSITÄT BERN

- Keine vertraulichen Diskussionen an öffentlichen Orten
  - Bus, Plätze, Züge etc.

- Vorsicht in sozialen Netzen
  - Ist es wirklich die richtige Person / Marke?

- Vorsicht bei E-Mails und Dateianhängen
  - Potentielle Malware oder Phishing

- Gesundes Misstrauen gegenüber Fremden
  - Organisieren Sie einen Rückruf und holen Sie in der Zwischenzeit Informationen ein

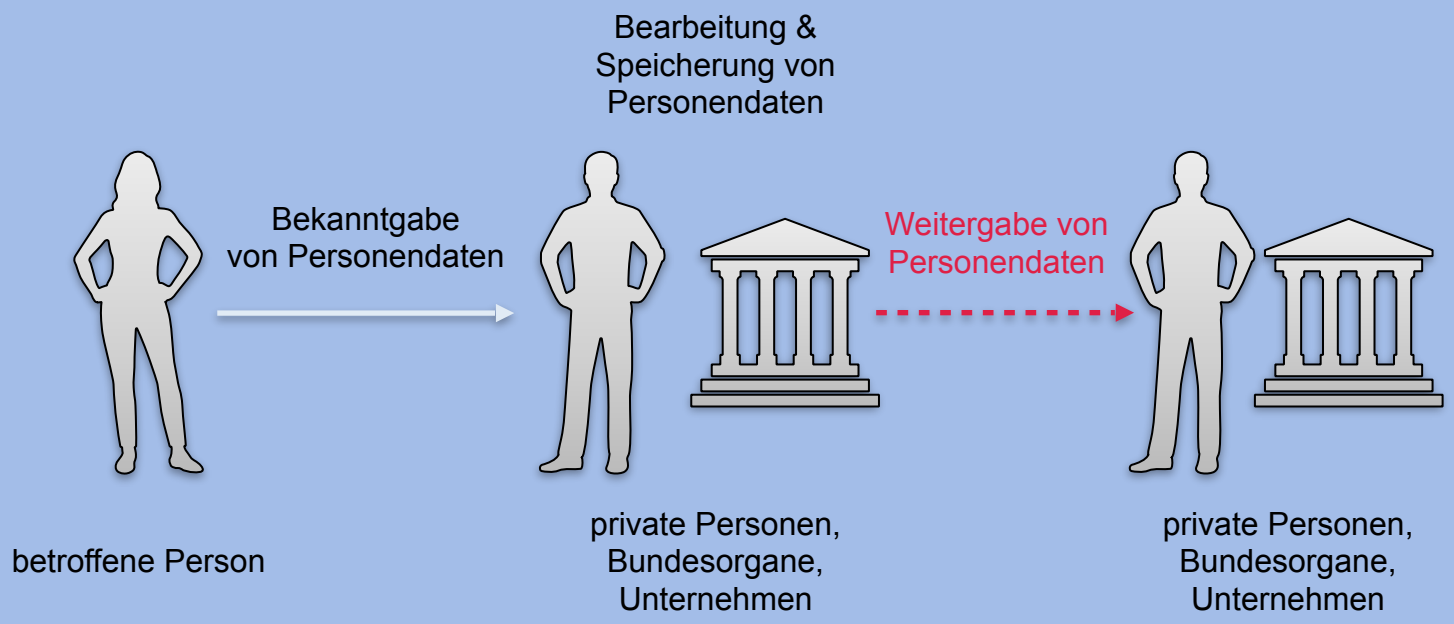
Computer, Laptops, Smartphones und Tablets

- Do's
  - **Aktueller Virenscanner** gehört auf jeden Arbeitscomputer
    - Mac, Windows, Linux
    - Auch zu Hause (Stichwort "Home-Office")
  - **Meldungen des Virenscanners beachten**
  - **Software aktuell halten**
  - **Mobile Geräte** mit einem **Passwort oder Screenlock** schützen
  - **Apps** nur aus den **offiziellen App-Stores installieren**
  - Bildschirm sperren
  - Software korrekt lizenzieren
- Dont's
  - **Mobile Geräte nie unbeaufsichtigt lassen**
  - Keine fremden Datenträger verwenden

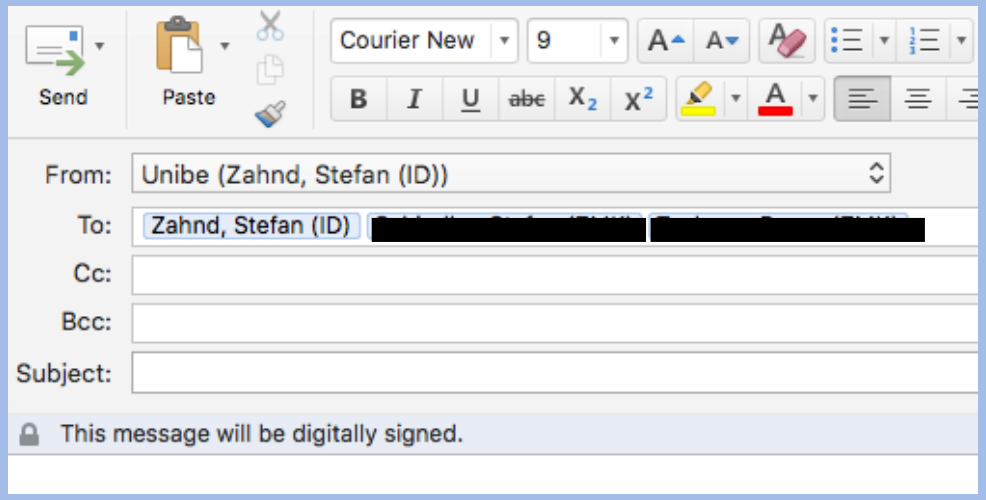
UNIVERSITÄT BERN

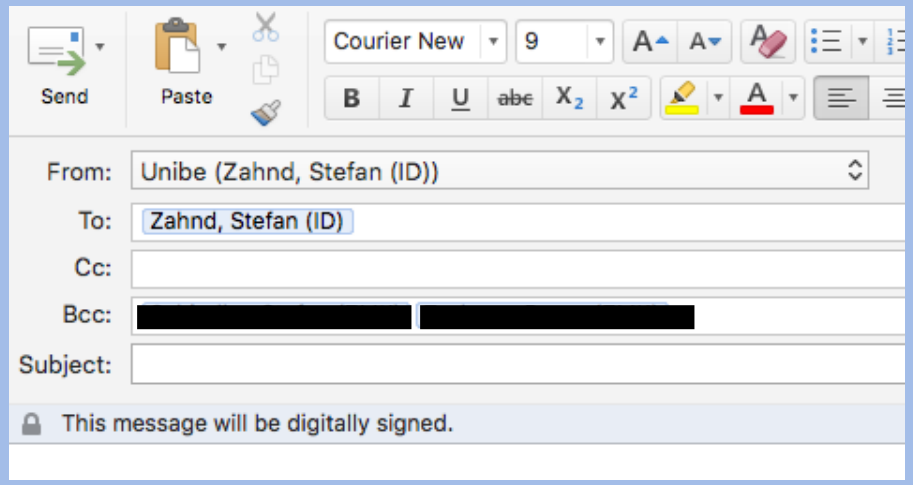
Datenschutz

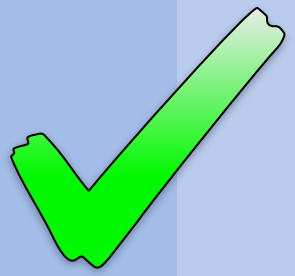
- Gefahr
  - Bekanntgabe sensitiver Informationen an unberechtigte Personen
  - Rechtsverstoss
  - Angriffe auf die persönliche Integrität



Datenschutz - E-Mail-Versand





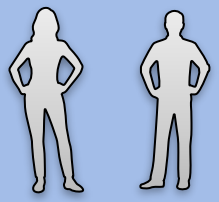


Datenschutz - Personendaten

UNIVERSITÄT BERN

- Personendaten (schützenswerte Daten)
  Bundesgesetz über den Datenschutz (DSG) Art. 3 Buchstabe a)
  - Alle Angaben, die sich auf eine bestimmte[1] oder bestimmbare[2] Person beziehen

Unbestimmte Person: Name + Geburtsdatum =



Bestimmbare Person: Matrikelnummer +

=

Benutzerdatenbank:
Name, Wohnort, Geburtsdatum

Bestimmte Person: Name + Adresse/Wohnort + Geburtsdatum =

[1] *Es wird von einer bestimmten Person gesprochen, wenn ein unmittelbarer Bezug zur Person vorhanden ist.*

[2] *Es wird von einer bestimmbaren Person gesprochen, wenn sich ein Zusammenhang zu einer Person ohne besonderen Aufwand herstellen lässt. Eine Matrikelnummer beispielsweise macht eine Person bestimmbar, wenn auch nur für einen eingeschränkten Benutzerkreis.*

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesgesetz über den Datenschutz (DSG)

Datenschutz - besonders schützenswerte Daten

UNIVERSITÄT BERN

- Besonders schützenswerte Daten
  Bundesgesetz über den Datenschutz (DSG) Art. 3 Buchstabe c)

  - die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten
  - die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit
  - Massnahmen der sozialen Hilfe
  - administrative oder strafrechtliche Verfolgungen und Sanktionen

  - **Achtung**: Photos und Videos sind ebenfalls Daten (bspw. Passfoto auf der UniCard)

Datenarten:

Datenschutz – Handhabung von Daten

- Transfer von Personendaten an Dritte
  - **Grundsätzlich nie** (auch nicht innerhalb der Universität)
  - **Ausnahmen**
    - mit der expliziten Erlaubnis des/der Betroffenen
    - gesetzlich bestimmten Erlaubnis (bspw. AHV-Nummer)
- Übertragung
  - **Nur verschlüsselt** (Vorsicht beim Versand via E-Mail)
  - **Daten voneinander abtrennen** (Informationsdichte reduzieren)
- Aufbewahrung
  - **Nur verschlüsselt** (Arbeitsplatz, Laptop, Datenbank etc.)
  - **Wenn nötig anonymisiert**
  - Prinzip: **So wenig wie möglich, so viel wie nötig, so kurz wie möglich**
- Verarbeitung
  - Immer **Zweckgebunden**
  - Ist der Zweck erfüllt: Daten löschen

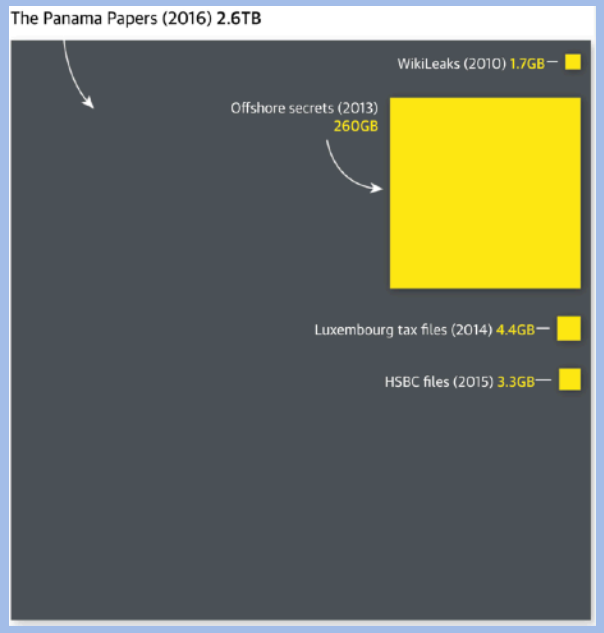
Datenschutz – Cloud-Speicher

- Speichern Sie *niemals* geschäftsbezogene sensible Personendaten auf externen Cloud-Speichern (z.B. Dropbox, OneDrive, Google Drive)
  - Artikel zum Thema:
    - https://www.netzwoche.ch/news/2014-01-31/gilt-das-datenschutzgesetz-auch-fuer-verschluesselte-cloud-daten
    - https://www.boxcryptor.com/en/blog/post/encryption-to-protect-personal-data-in-the-cloud/

- Für den Privatgebrauch
  - Ja, aber bitte verschlüsselt

Panama Papers – Grösstes Datenleck in der Geschichte

- Die Akten enthüllen die Offshore-Konten von 140 Politikern und Amtsträgern aus der ganzen Welt
- Mehr als 240’000 Offshore-Unternehmen tauchen in den Daten auf, die mit Menschen in mehr als 200 Ländern und Hoheitsgebieten in Verbindung stehen.



ICIJ INTERNATIONAL CONSORTIUM OF INVESTIGATIVE JOURNALISTS

Erfahren Sie mehr zu den Panama Papers

https://www.theguardian.com/news/2016/apr/03/what-you-need-to-know-about-the-panama-papers

Fragen / Diskussion

Vielen Dank…

- für Ihre Aufmerksamkeit und
- Ihre Mithilfe

Universität Bern
Informatikdienste

security@unibe.ch
Hotline: +41 31 631 54 55

unibesecure.unibe.ch