Hochschule für öffentliche Verwaltung und Finanzen
Ludwigsburg
University of Applied Sciences

Informationssicherheit in der Deutschen Verwaltung heute und (hoffentlich) morgen

Ein Handlungsleitfaden für Kommunen in Baden-Württemberg

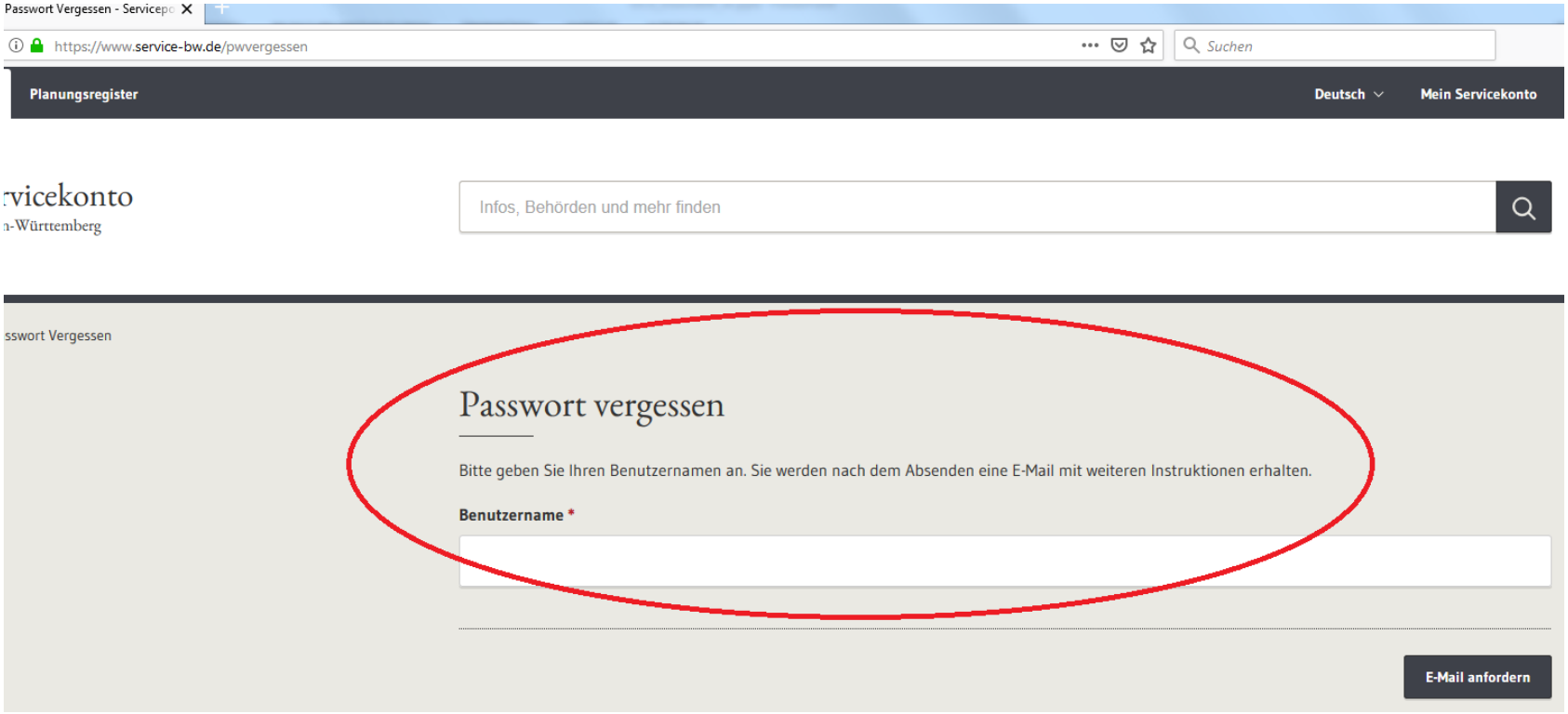
Prof. Dr. Robert Müller-Török

HÖD Berlin, 17. Januar 2019

Agenda

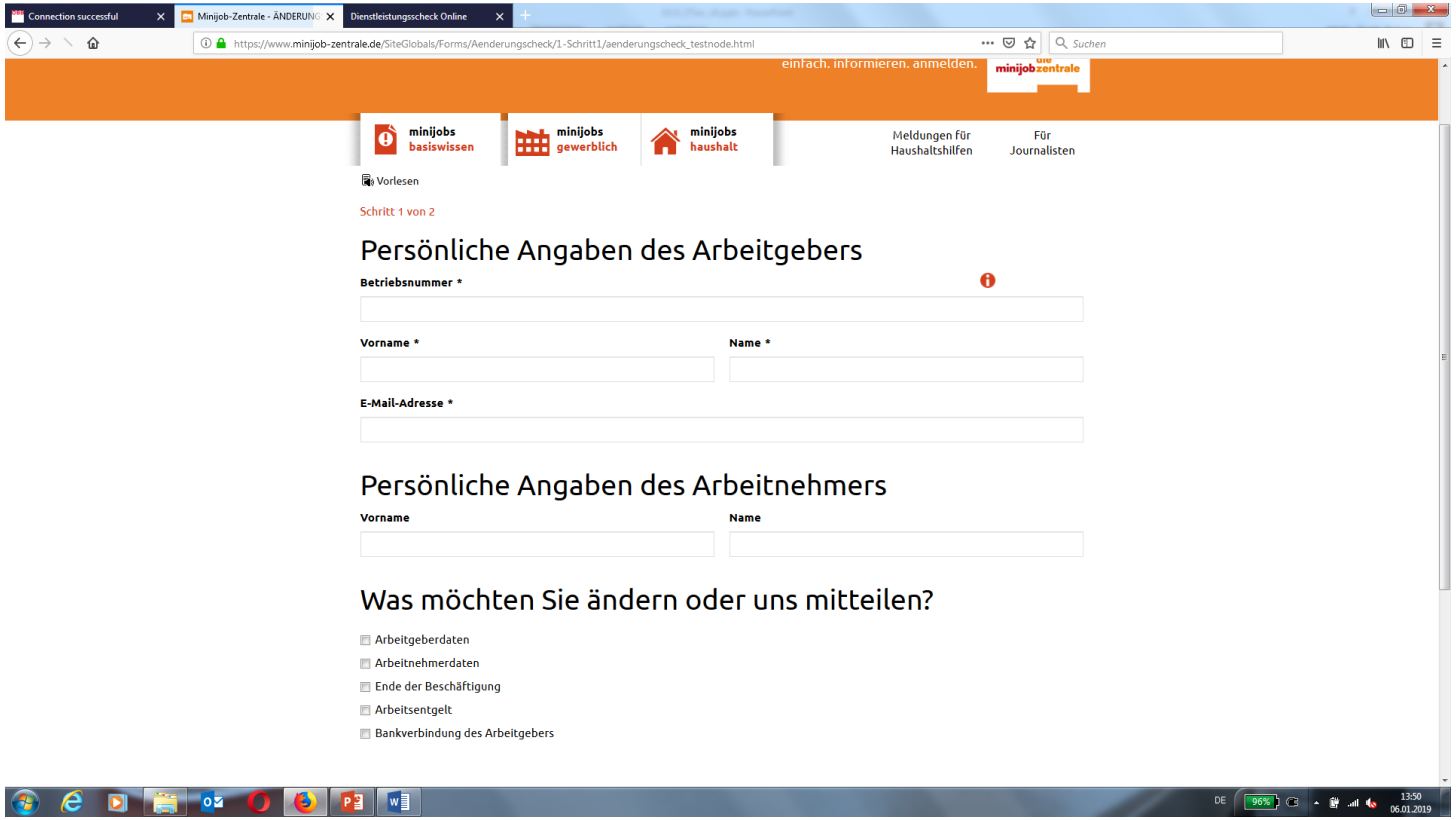
- **Die Situation per heute**
- The Big Picture
- Informationssicherheit am Beispiel E-Mail in der Verwaltung
- Wer soll was tun? Personal- und Organisationsthemen
- Diskussion

Service-BW, das Pendant zu help.gv.at



Da kann man sein Auto abmelden und einen Pass beantragen!

Minijobzentrale – entspricht Dienstleistungsscheck online



Hier konnte ich am 27.12.2018 ohne Login und ohne Identifikation den Beschäftigungsumfang ändern

Wo stehen wir in der Verwaltung in Deutschland heute?

Das Thema elektronische Identifikation ist nicht bzw. nur theoretisch gelöst und die theoretischen Lösungen sind faktisch nicht verbreitet, jedenfalls nicht im Umfang der Bürgerkarte in Österreich.

1. Damit hat jede eGov-Anwendung ein eID-Problem

2. Erschwerend gibt es 16 Landes- und ein Bundes-verwaltungsverfahrensgesetz, somit keine Prozesse

3. Zuständigkeiten und Verantwortlichkeiten völlig zersplittert

4. Keinerlei rechtsverbindliche Vorgaben für IT-Sicherheit von einer zentral verantwortlichen bzw. zuständigen Stelle

Agenda

- Die Situation per heute
- **The Big Picture**
- Informationssicherheit am Beispiel E-Mail in der Verwaltung
- Wer soll was tun? Personal- und Organisationsthemen
- Diskussion

Was bedeutet Informationssicherheit?

Inhaltlich (in Anlehnung an IT-Grundschutz BSI)

1. Geräte, Netze, Infrastruktur
2. Systeme (v.a. Berechtigungsverwaltung und Administration)
3. Organisation und Personal
4. Kryptographie und Identifikation
5. Auditing
6. Etablierung eines ISMS

Organisationskulturell

1. SENSIBILISIERUNG!!!
2. Schulung und Training
3. Kulturwandel hin zu Whistleblowing, Fehler aufzeigen, „Beobachten und Melden“ anstatt beschwichtigen und schönreden!

Wer wir sind

Hochschule für öffentliche Verwaltung und Finanzen Ludwigsburg
(zentrale Ausbildungsstätte der Kommunal- und Finanzbeamte gemeinsam mit einer Schwesterhochschule in Kehl)

ITEOS (entspricht dem BRZ auf Ebene der Baden-Württembergischen Kommunal- und Landesverwaltung)

Wirtschaftsuniversität Wien, Department of Information Management

National Cybersecurity Academy an der Nationalen Universität für den öffentlichen Dienst Ungarns

Was wir erreichen wollen

- Diffusion des Handlungsleitfadens sowie ergänzend Informationsveranstaltungen in Baden-Württemberg
- Sensibilisierung auf Entscheiderebene und Einleitung von Audits zur Standortbestimmung
- Erhöhung der Risk Awareness und Aufsetzen entsprechender Projekte

Das ist der 4. Handlungsleitfaden für Kommunen

2016. E-Government Gesetz Baden-Württemberg
2017. EU-DSGVO
2018. Open Data
2019. Informationssicherheit

Agenda

Die Situation per heute

The Big Picture

Informationssicherheit am Beispiel E-Mail in der Verwaltung

Wer soll was tun? Personal- und Organisationsthemen

Diskussion

Echte Erlebnisse im Jahr 2016 in Baden-Württemberg

- Vortrag vor Organisations- und Hauptamtsleitern von Kommunen zum EGovG BW

- Livedemonstration, wie man eine E-Mail des Ministerpräsidenten kretschmann@stm.bwl.de versendet mithilfe von https://anonymousemail.me

- Erklärung, wie der Weg einer E-Mail funktioniert, wie ein SMT-Protokoll aussieht und wie man so eine Mail problemlos fälschen kann

Ergebnis:

Entsetzte Gesichter, weil bislang E-Mails von „Bürgern“ und „Behörden“ für bare Münze genommen wurden.

Prank email sending service.

Free anonymous email service !
Anonymailer
Anonymailer.net

471 Tweet

Gefällt m

G+1 4

NEW Sign up now!

Only $19/year

Home | How it works | Send email free | Sign up | Tools | Contact us

Stats of last hour:
104 active paid members.

Sign-In
Username:
Password:
Sign In
Sign up
Forgot your password?

Visitors
US 317,765
IN 111,615
GB 67,273
DE 39,715
CA 37,425

Send fake email.

Online web tool for sending prank emails.
No download required! It is virus free.

From Name	:	(Optional)
From E-mail *	:	
To Email *	:	
Subject of the email	:	(Optional)

E-Mail-Sicherheit heute

- Verbindungsnetz (Netz des Bundes, NdB) existiert
- Landesverwaltungsnetz (LVN) existiert, betrieben von BITBW
- Kommunalverwaltungsnetz (KVN) existiert, betrieben von ITEOS

Ob die konkrete E-Mail diesen Weg geht, ist nicht klar. So geht bspw. eine E-Mail von der Hochschule an das Wissenschaftsministerium NICHT gesichert diesen Weg, ebenso wenig eine E-Mail einer Gemeinde an die Hochschule. Die Verbindung zum NdB bspw. ist optional auswählbar bei Erstanbindung an das KVN.

Nachzufragen, welchen Weg die eigenen E-Mails gehen, dazu fehlt es (noch) an Sensibilisierung.

Digitale Signatur im Verwaltungsverfahren – Regelungen des EGovG BW

- Im Verwaltungsverfahren ist jede Behörde nur dann verpflichtet, digital signierte Dokumente entgegenzunehmen, wenn sie dies ausdrücklich wünscht und erklärt hat.

  → Keine Annahmepflicht

- Es besteht kein Rechtsanspruch des Bürgers, schriftformgebundene Dokumente in digital signierter Form an die Behörde senden zu dürfen.

  → Kein subjektives Recht des Bürgers

Ausnahme: Gemeinde als Finanzbehörde

- In Angelegenheiten, wo die Gemeinde Finanzbehörde ist, gilt die AO des Bundes und hier ist sie seit 1.7.2014 verpflichtet, digital signierte Dokumente zu akzeptieren.

  - Grundsteuer
  - Gewerbesteuer
  - Örtliche Verbrauchs- und Aufwandsteuern wie die Hundesteuer

  → Ein Bürger schickt Widerspruch gegen Grundsteuerbescheid und einen Antrag auf Anwohnerparkgenehmigung digital signiert oder per De-Mail: Kann man ernstlich den zweiten Teil zurückweisen?

Elektronische Siegel

Gibt es in der baden-württembergischen Kommunal- und Landesverwaltung nicht.

Zertifikate für E-Mails (fortgeschrittene Signatur) sind ebenfalls nicht verbreitet.

Eine echte Mail >>>

Löschen | Antworten

Mo 17.12.2018 10:56

marieta.munk@landtag-bw.de

UA [redacted] Zeugenvernehmung

An marieta.munk@landtag-bw.de

Cc Silke.Hartmann@landtag-bw.de; sabine.kurtz@cdu.landtag-bw.de

[redacted]

Mit freundlichen Grüßen

Marieta Munk

Marieta Munk
-Staatsanwältin-
Referentin im Plenar- und Ausschussdienst
Untersuchungsausschuss „ [redacted]
Landtag von Baden-Württemberg
Konrad-Adenauer-Str. 3
70173 Stuttgart

Tel. 0711/2063-2206
FAX 0711/2063-142206

E-Mail: marieta.munk@landtag-bw.de
Webseite: www.landtag-bw.de

Notwendige Maßnahmen für Kommunen

1. Klären, ob man an sicheren Netzen teilnimmt

2. Sensibilisierung und Schulung der Mitarbeiter, was mit E-Mail gemacht werden darf/soll und was nicht

3. SIGNATUREN und elektronische SIEGEL einführen!!!

4. Überwachung/Audit im Rahmen eines ISMS definieren und einführen sowie ggf. technische Vorkehrungen treffen wie z. B. Anhangverbot etc.

5. Anpassung der eigenen internen Rechtsvorschriften bzw. Dienstanweisungen

Agenda

Die Situation per heute

The Big Picture

Informationssicherheit am Beispiel E-Mail in der Verwaltung

Wer soll was tun? Personal- und Organisationsthemen

Diskussion

Rahmenbedingungen von Kommunen in Baden-Württemberg

- Die allermeisten Kommunen sind vergleichsweise klein und bescheiden ausgestattet
- IT-Fachpersonal regelmäßig nicht vorhanden
- Verwaltungsbeamte und Kommunalpolitiker üblicherweise rechtslastig ausgebildet und mit vglw. geringer IT-Bildung
- Potenter IT-Dienstleister ITEOS, dem man auch als Zweckverbandsmitglied angehört
- Kaum eigene IT-Anwendungen, zumeist Kunde von Fachanwendungen, die von ITEOS zur Verfügung gestellt werden
- ABER: Nach DSGVO und Kommunalrecht bleibt die Verantwortung stets bei der Kommune, nicht beim Auftragnehmer/Dienstleister

Rollen und Prozesse

- Informationssicherheitsbeauftragten auswählen (Qualifikation!) und einführen

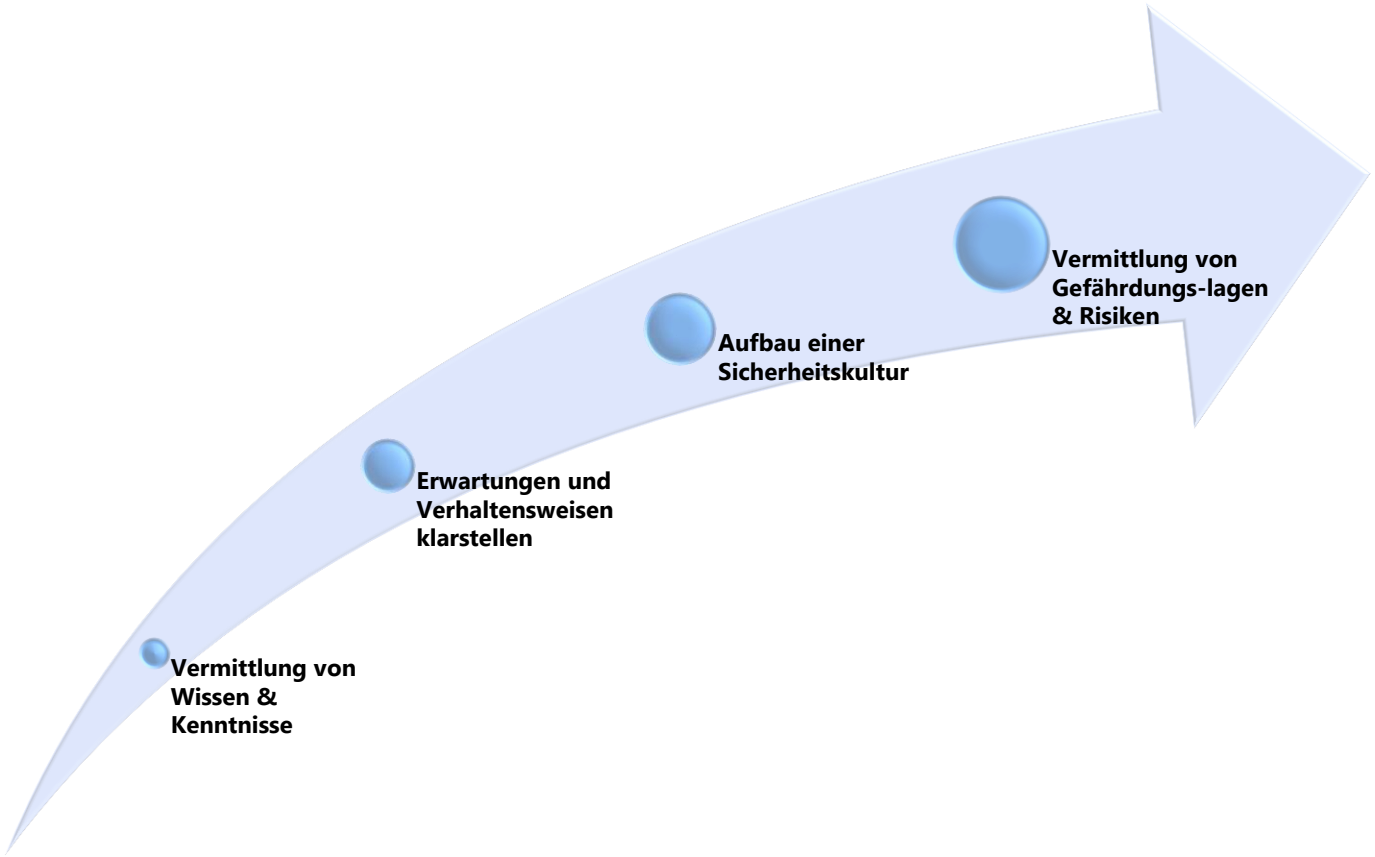
- Rollen im Haus definieren (auch bei kleinen Häusern!)
  - Wenigstens Administrator, Change Manager, Compliance Manager, Behördenleiter, Benutzer, Datenschutzbeauftragter, Fachverantwortlicher und Externer

- Abläufe defínieren und festschreiben
  Lieber weniger, dafür das auch trainieren, sensibilisieren und verinnerlichen

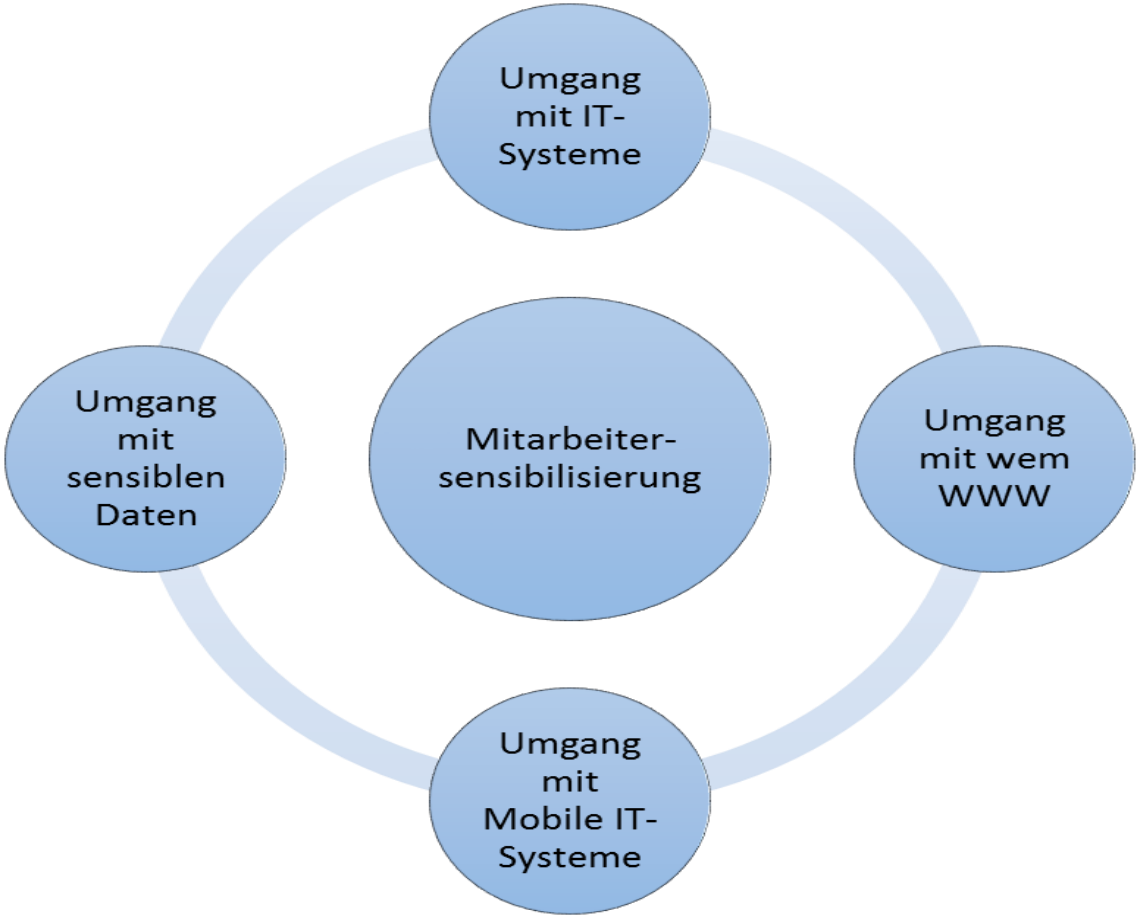
Thema Umgang mit Externen

- Outsourcing gut überlegen
- Dienstleister gut auswählen, v.a. nach Sicherheitsgesichtspunkten
- Saubere Verträge (SLA!!!)
- Kontrolle (Vertrauen ist gut, aber Kontrolle ist besser)
- Pflichten nach DSGVO betrachten (für die Verarbeitung Verantwortlicher gemeinsam mit dem Auftragsverarbeiter!)

Das ALLERWICHTIGSTE: Sensibilisierung



Das ALLERWICHTIGSTE: Sensibilisierung



Inhalte für die Sensibilisierung

- Wie funktioniert das Internet, wie funktioniert E-Mail?
- Wie funktioniert ein Log-In?
- Wie funktioniert ein Virus, ein Hackerangriff, ein Keylogger?
- Warum ist ein Ctrl-Alt-Del zum Bildschirm-Lock notwendig, wenn man den Raum verlässt?
- tbc

Agenda

- Die Situation per heute
- The Big Picture
- Informationssicherheit am Beispiel E-Mail in der Verwaltung
- Wer soll was tun? Personal- und Organisationsthemen
- **Diskussion**

Hochschule für öffentliche
Verwaltung und Finanzen
Ludwigsburg
University of Applied Sciences

Thank you for your attention!

mueller-toeroek@hs-ludwigsburg.de