Datenschutz durch Technik — wie viel Technikkompetenz braucht eine vernünftige Netzpolitik?

micu

Barcamp zum netzpolitischen Kongress der grünen Bundestagsfraktion

14. November 2010

Zitat zum Einstieg

Prof. Dr. Hannes Federrath[1]:

> Das Schlimmste daran ist – das ist das, was mir immer wieder zu denken gibt, wenn ich in solchen Anhörungen als Sachverständiger geladen bin –, dass durch die Befürworter einer solchen Technologie immer sehr schnell all das, was dagegen spricht, weggewischt wird.
>
> Es wird – das erlebe ich unter den Sachverständigen auch in unserer Runde – nicht zugehört. Es schmerzt förmlich, wenn ich technische Argumente vorbringe, die anschließend – zum Beispiel zehn Minuten später – nicht mehr zur Kenntnis genommen werden. Es wird so getan, als ginge es doch irgendwie. Wir müssten nur die Augen vor den negativen Seiten verschließen, dann wird es schon gut gehen. Das ist leider die Tendenz, die ich immer dann, wenn es technisch wird, bemerke.

[1] In der Anhörung zum JMStV im sächsischen Landtag (13.09.2010), `http://is.gd/gWZU9`

Struktur

Zum Verhältnis von Technik und Recht

Angelehnt an **Prof. Dr. Andreas Pfitzmann († 23.09.2010)**[2]:
Ziel: Datenmissbrauch verhindern oder zumindest erkennen ⇒
Allgemeinplatz, dass Recht alleine zu wenig ist?

Besonderheiten (digitaler) Daten

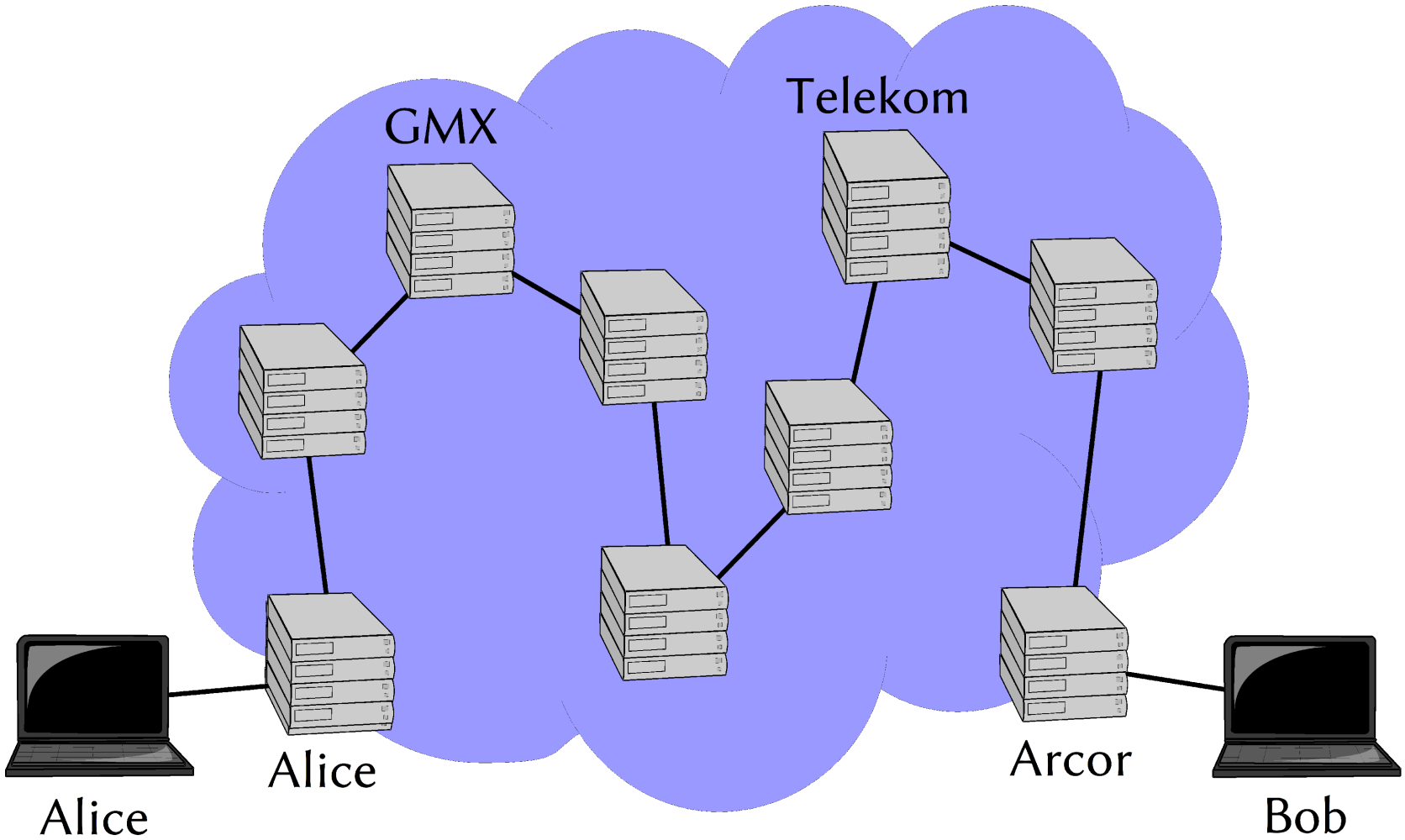
- I.d.R. keine Spuren beim Datendiebstahl ⇒ oft nicht einmal bemerkt.
- Wenn bemerkt/vermutet: ordnungsgemäße Löschung nicht überprüfbar.

⇒ Diffuse Unsicherheit, überwacht zu werden.

⇒ Datensparsamkeit (durch Technik)

[2] Warum brauchen wir Technik? — Zum Verhältnis von Technik und Recht. In: 20 Jahre Datenschutz — Individualismus oder Gemeinschaftssinn?, `http://is.gd/gX0bm`

Beispiel: Email ohne Verschlüsselung



Grundlagen der IT-Sicherheit

1. Was ist zu schützen? ⇒ **Schutzziele**

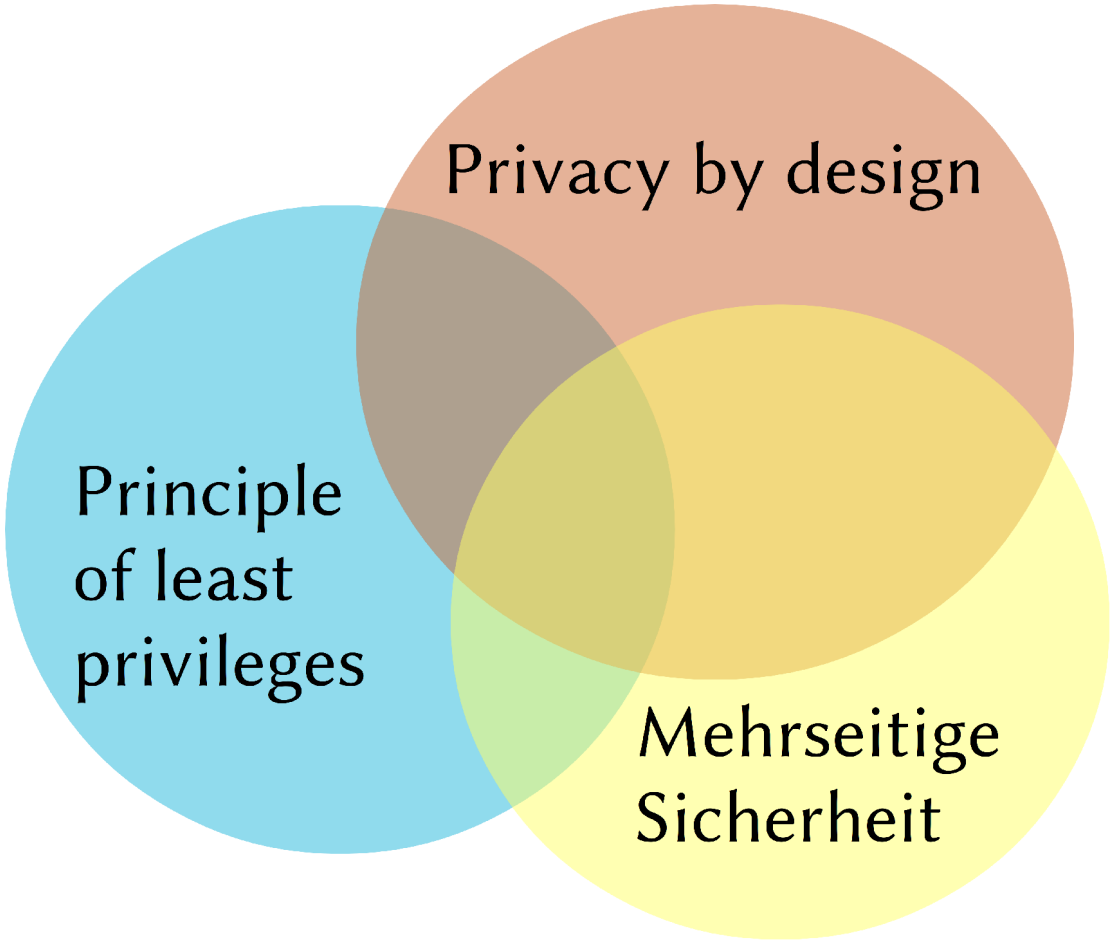
1. Vertraulichkeit (confidentiality)
2. Integrität (integrity)
3. Verfügbarkeit (availability)

⇓

»Grundrecht auf Gewährleistung der **Vertraulichkeit** und **Integrität** informationstechnischer Systeme«

2. Vor wem ist es zu schützen ⇒ **Angreifermodell**

Nicht trennscharf — Überschneidungen



Privacy by design

- Unschärfstes der drei Prinzipien
- Privatsphäre als Standard (Privacy by default)
- Privatsphäre eingebaut — nicht im Nachhinein aufgepfropft
- Je nach Verständnis auch: Privatsphäre per Entwurf des Systems technisch sichergestellt

Principle of least privileges

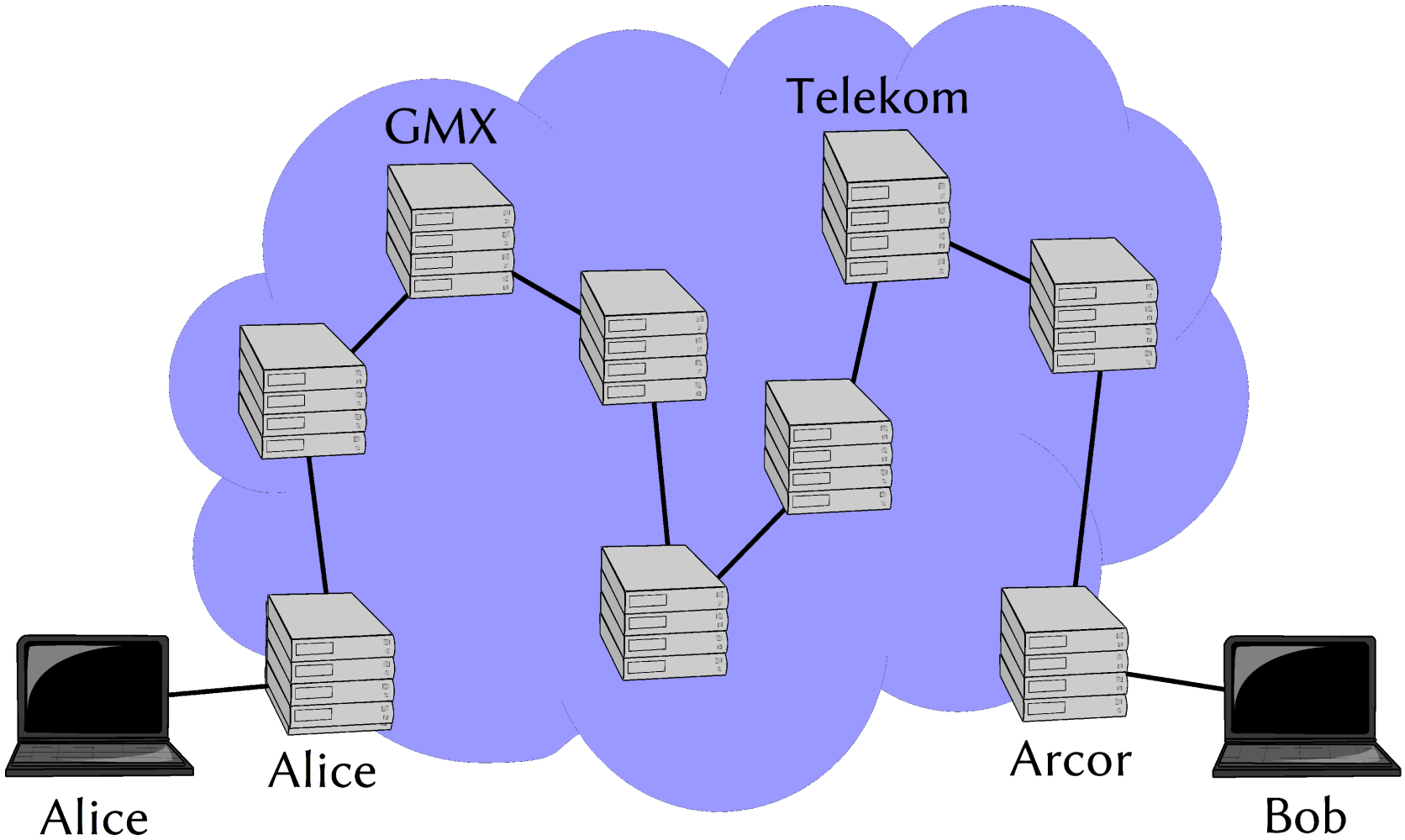
Definition aus der englischen Wikipedia[3]

In information security, computer science, and other fields, **the principle of least privilege** [...] requires that [...] every module [...] must be able to access only such information and resources that are necessary for its legitimate purpose.

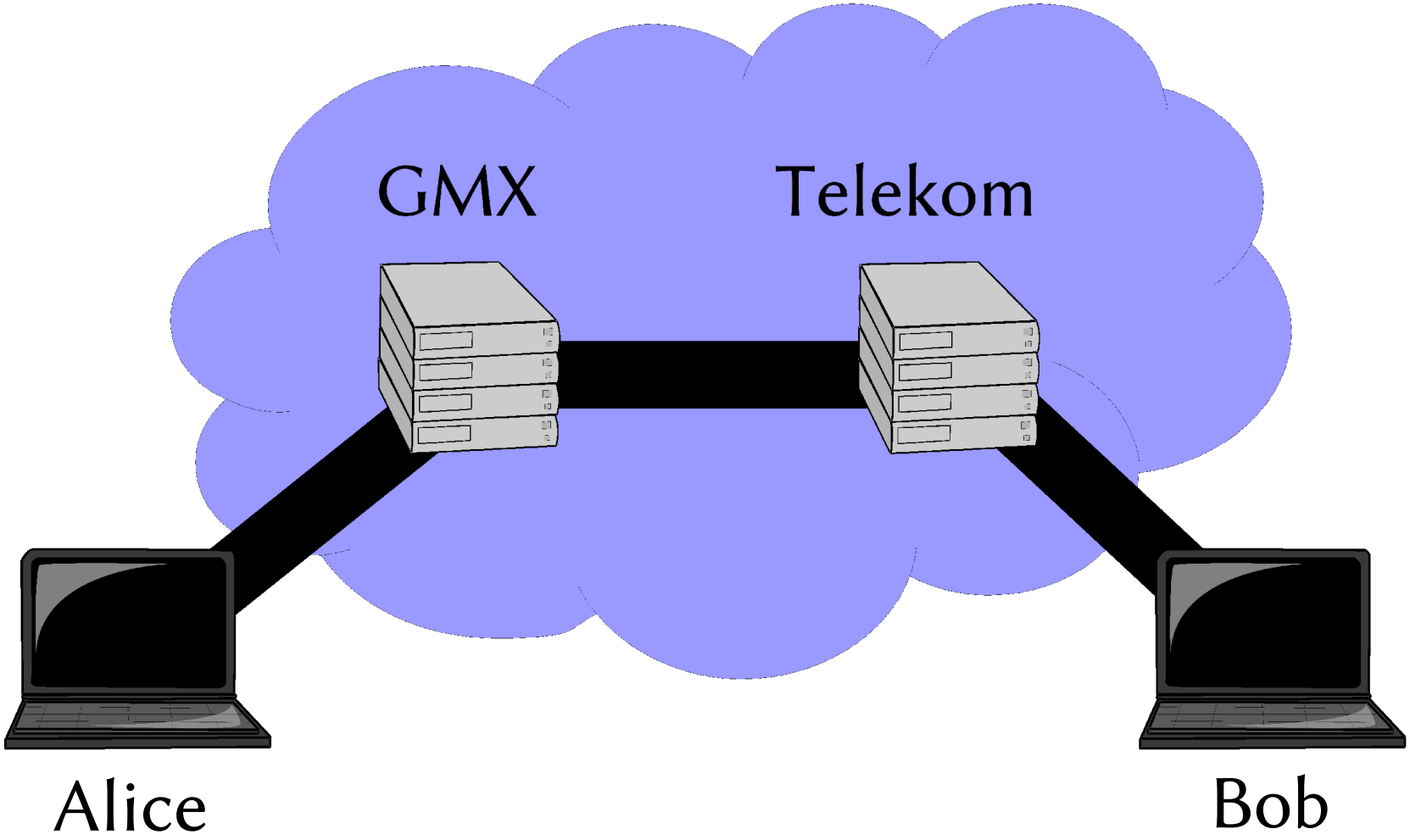
- Beispiel für Verletzung: Browser kann/könnte nach Lust und Laune im Benutzerverzeichnis lesen und schreiben.
- Bsp. für Anwendung in der Politik: De-Mail vs. Ende-zu-Ende-Verschlüsselung (GnuPG).

[3] `http://is.gd/gX7iM`

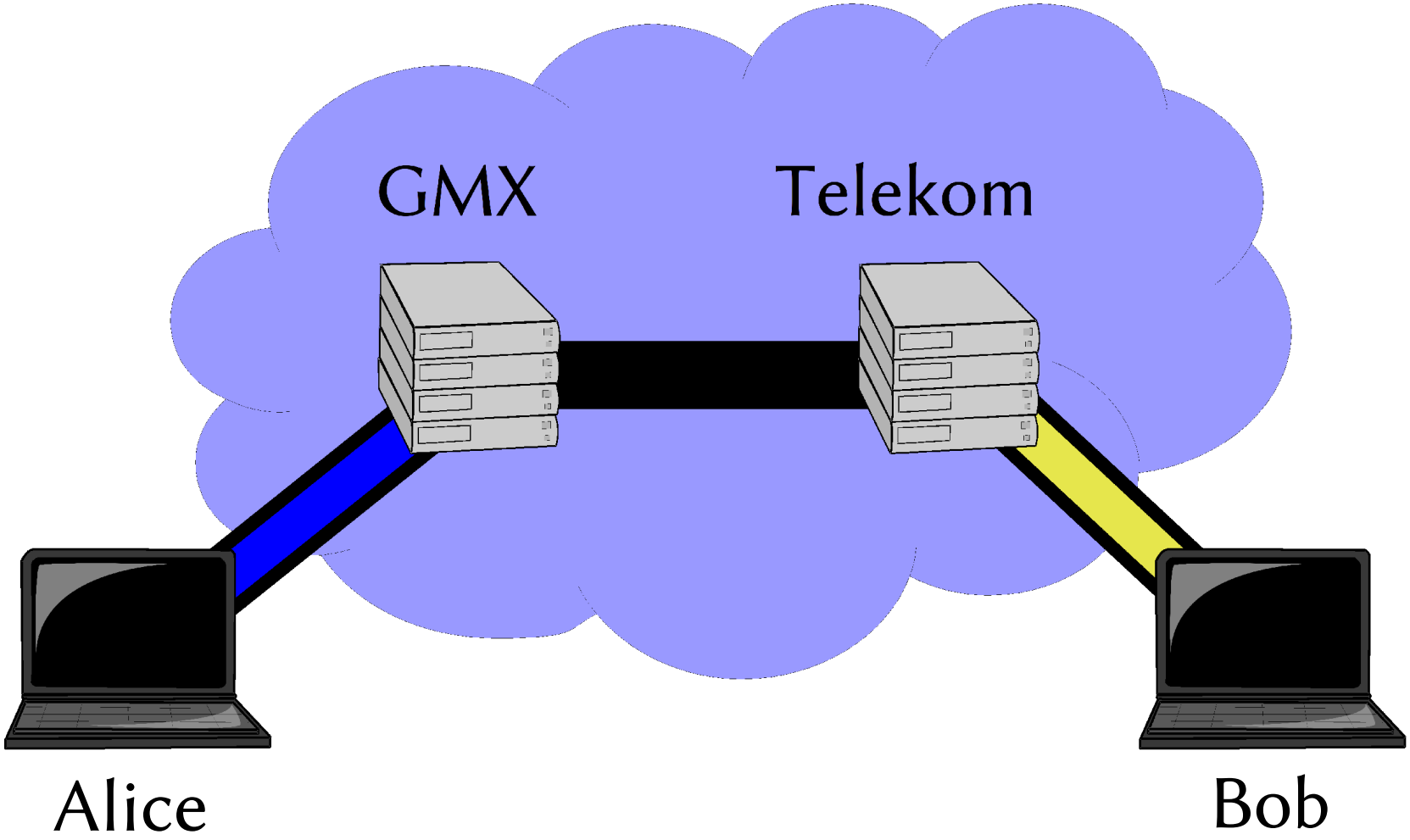
Ohne Verschlüsselung



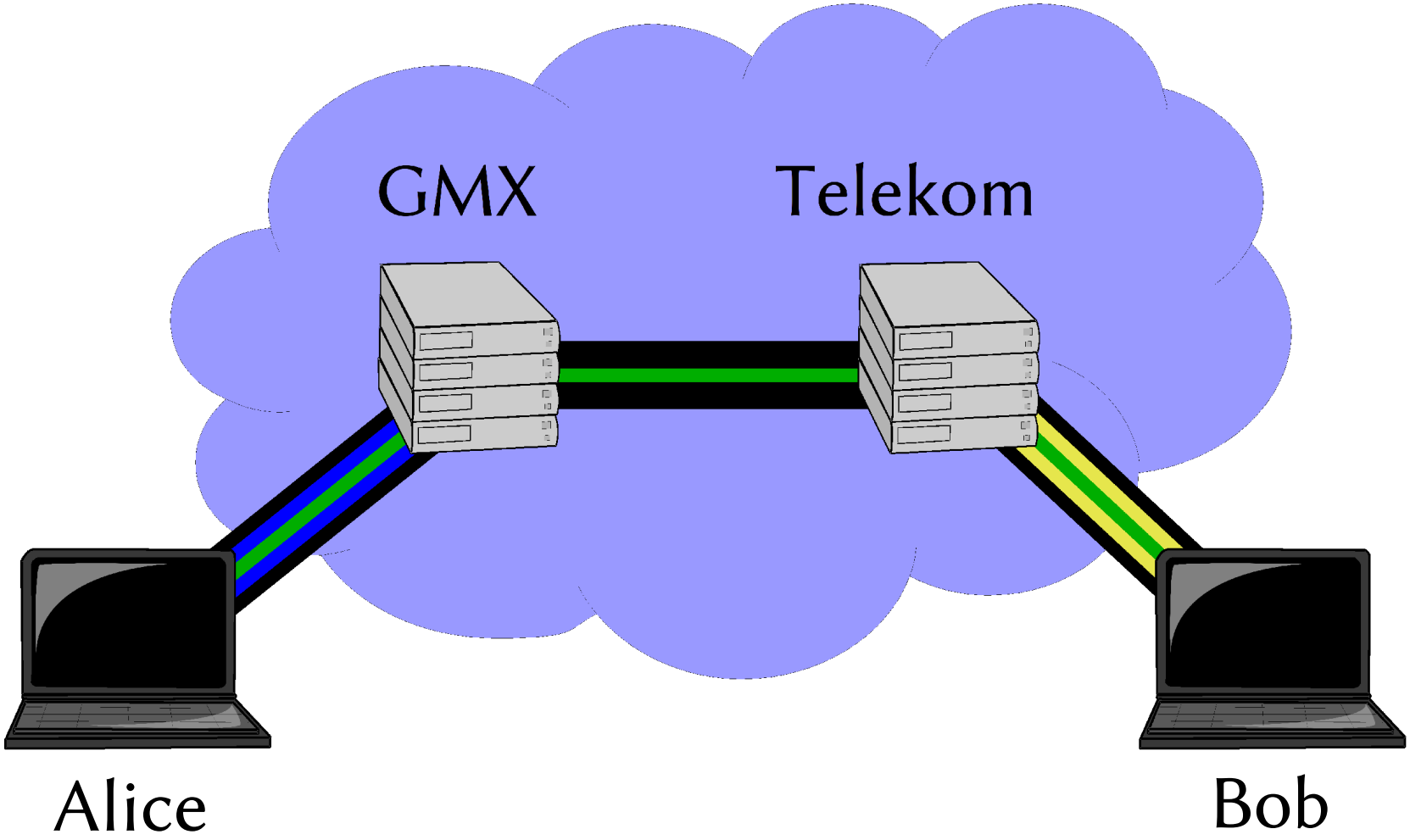
Ohne Verschlüsselung (vereinfacht)



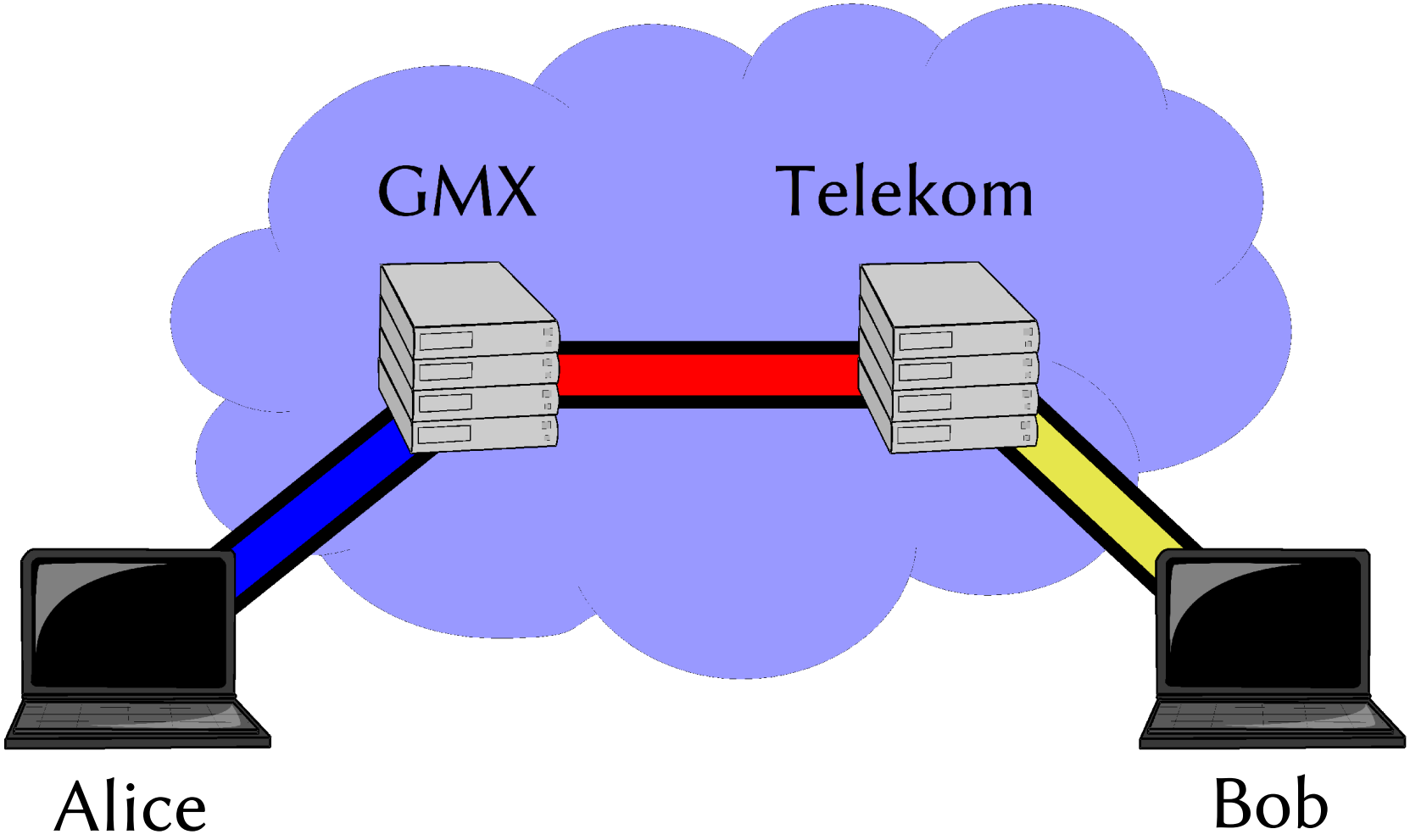
Verschlüsselung zum Server (SSL/TLS)



Ende-zu-Ende-Verschlüsselung (GnuPG / OpenPGP)



De-Mail



Mehrseitige Sicherheit = multilaterale Sicherheit

Grobe Definition mehrseitige Sicherheit = multilaterale Sicherheit

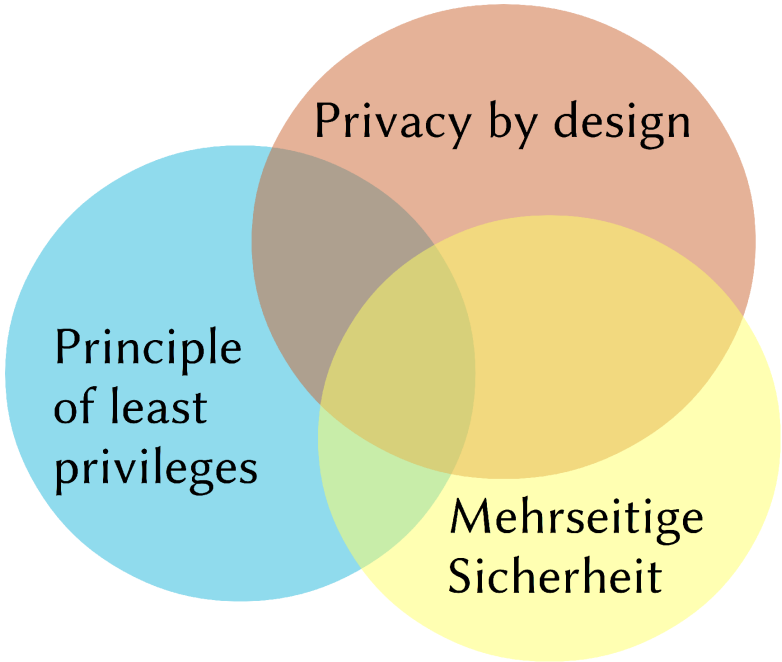
Weg vom SW-Denken „Good Guys“ vs. „Evil Guys“ $\Rightarrow$ viele Teilnehmer mit unterschiedlichen Ansprüchen

Möglichkeiten zur Realisierung

- FOSS
- Aushandlungen im Entwurfsprozess $\Rightarrow$ oft nicht für alle Teilnehmer gleichermaßen möglich
- Politik schafft Ausgleich $\Rightarrow$ Verbraucherschutz

Danke! ⇒ Diskussion

Fragen?



Kontakt

www.micuintus.de
twitter.com/micuintus
identi.ca/micu
micuintus auf gmx punkt net