Deutsche Stiftung für Recht und Informatik

Messbarkeit von IT-Sicherheit

Dr. Florian Deusch
ANWALTSKANLEI DR. GRETTER

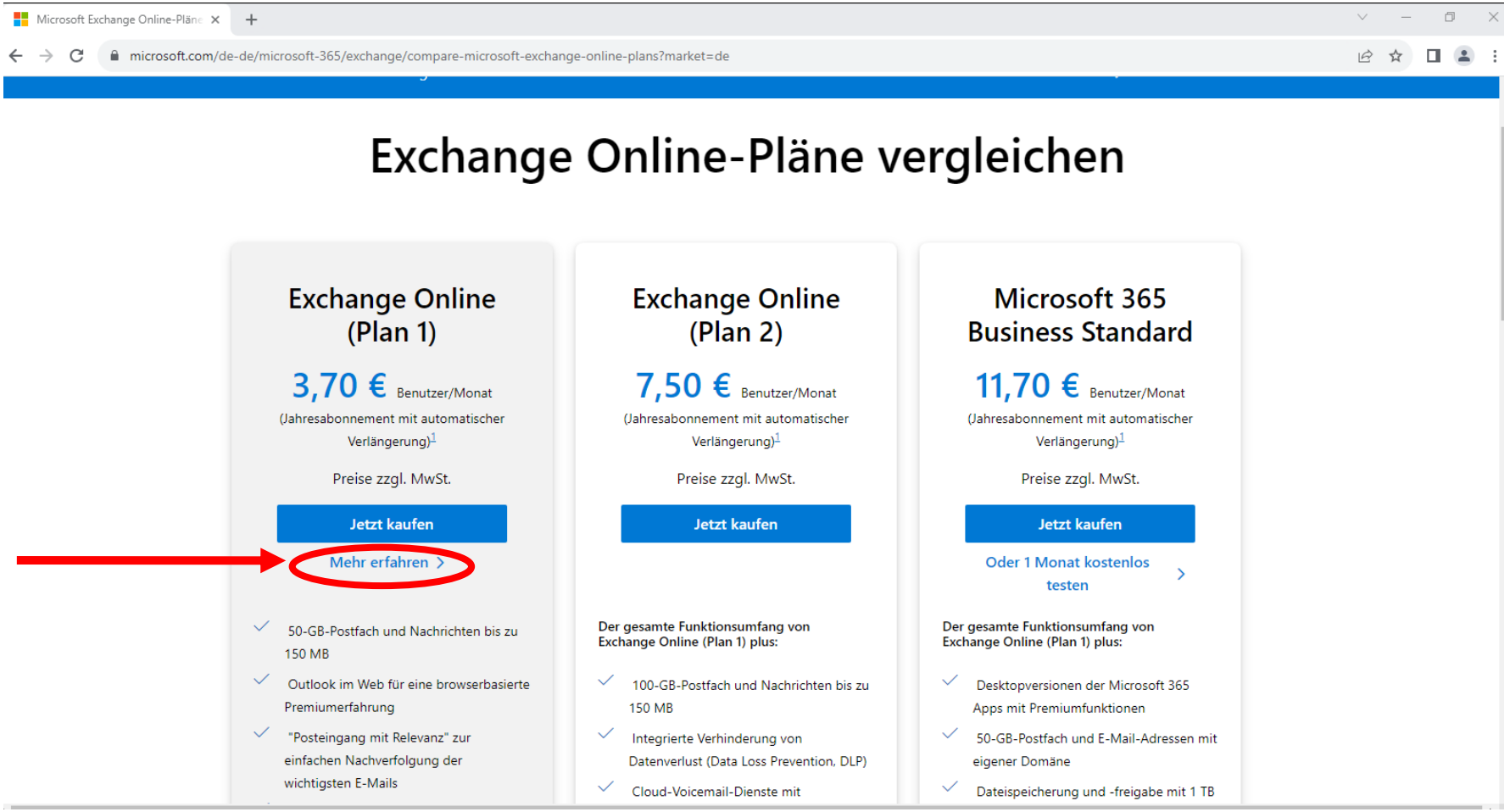
Prof. Dr. Tobias Eggendorfer
Technische Hochschule Ingolstadt

Herbstakademie 2023

Überblick

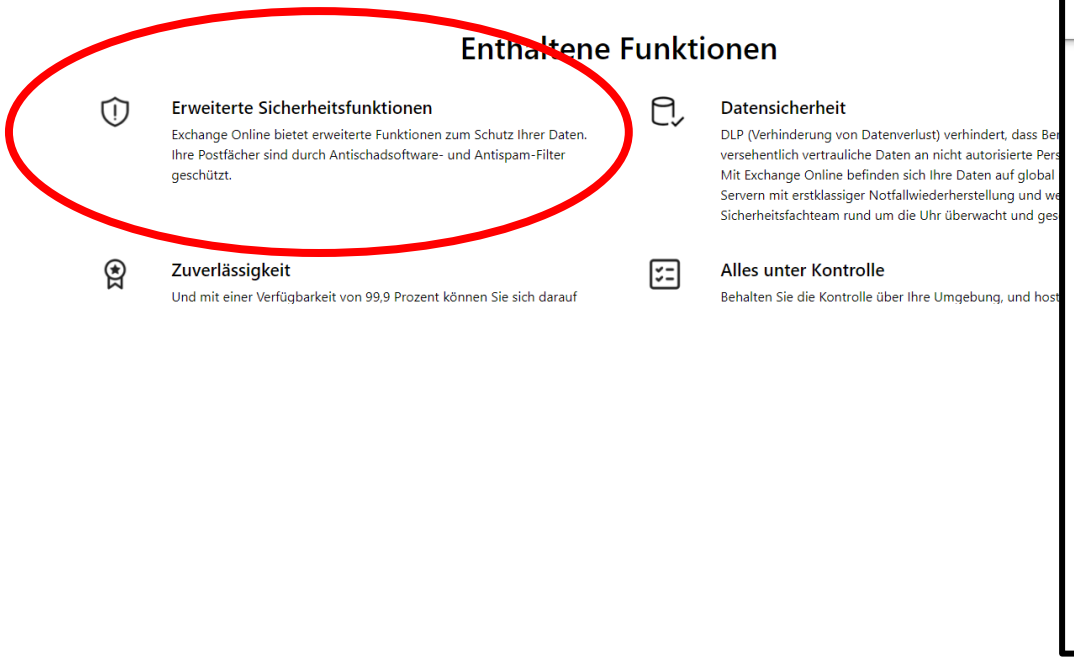
- Verfügbare Aussagen zur IT-Sicherheit von Software
- Fehlende Messbarkeit von IT-Sicherheit: rechtliche Folgen
- Technische Lösungsansätze zur IT-Sicherheitsmetrik
- Rechtliche Auswirkungen einer IT-Sicherheitsmetrik: Zertifizierungen
- Zusammenfassung und Fazit

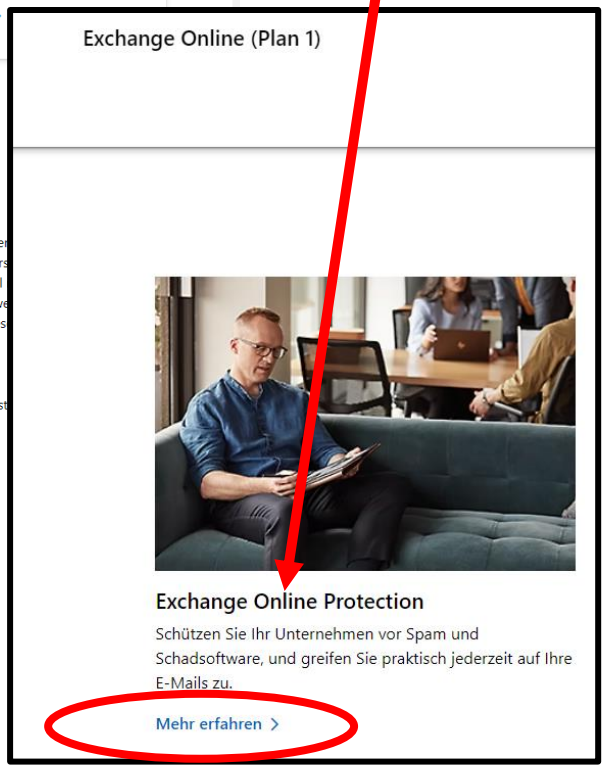
Aussagen zur IT-Sicherheit: Herstellerangaben (1)



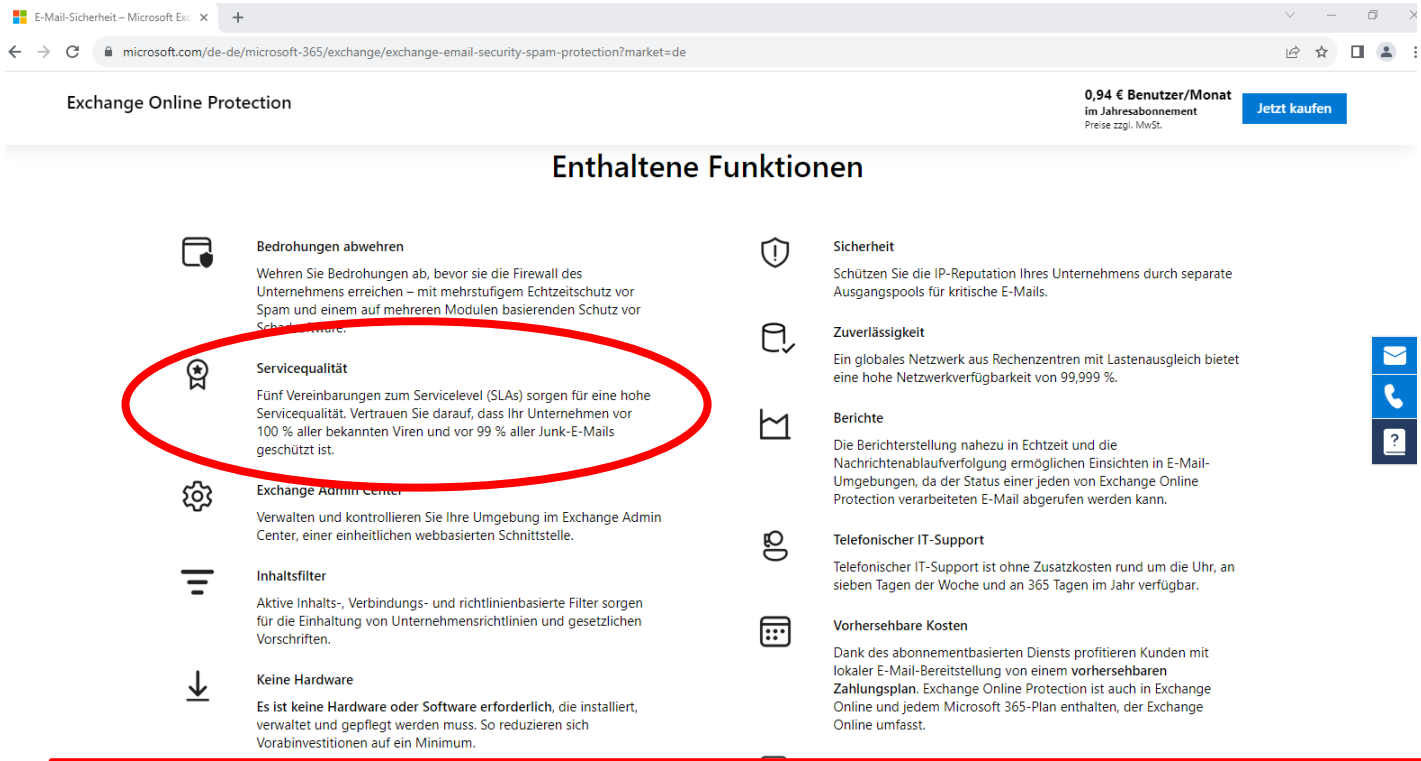
Aussagen zur IT-Sicherheit: Herstellerangaben (2)

nach unten scrollen:





Aussagen zur IT-Sicherheit: Herstellerangaben (3)



E-Mail-Sicherheit – Microsoft Exc

microsoft.com/de-de/microsoft-365/exchange/exchange-email-security-spam-protection?market=de

Exchange Online Protection

0,94 € Benutzer/Monat
im Jahresabonnement
Preise zzgl. MwSt.

Jetzt kaufen

Enthaltene Funktionen

Bedrohungen abwehren

Wehren Sie Bedrohungen ab, bevor sie die Firewall des Unternehmens erreichen – mit mehrstufigem Echtzeitschutz vor Spam und einem auf mehreren Modulen basierenden Schutz vor Schadsoftware.

Servicequalität

Fünf Vereinbarungen zum Servicelevel (SLAs) sorgen für eine hohe Servicequalität. Vertrauen Sie darauf, dass Ihr Unternehmen vor 100 % aller bekannten Viren und vor 99 % aller Junk-E-Mails geschützt ist.

Exchange Admin Center

Verwalten und kontrollieren Sie Ihre Umgebung im Exchange Admin Center, einer einheitlichen webbasierten Schnittstelle.

Inhaltsfilter

Aktive Inhalts-, Verbindungs- und richtlinienbasierte Filter sorgen für die Einhaltung von Unternehmensrichtlinien und gesetzlichen Vorschriften.

Keine Hardware

Es ist keine Hardware oder Software erforderlich, die installiert, verwaltet und gepflegt werden muss. So reduzieren sich Vorabinvestitionen auf ein Minimum.

Sicherheit

Schützen Sie die IP-Reputation Ihres Unternehmens durch separate Ausgangspools für kritische E-Mails.

Zuverlässigkeit

Ein globales Netzwerk aus Rechenzentren mit Lastenausgleich bietet eine hohe Netzwerkverfügbarkeit von 99,999 %.

Berichte

Die Berichterstellung nahezu in Echtzeit und die Nachrichtenablaufverfolgung ermöglichen Einsichten in E-Mail-Umgebungen, da der Status einer jeden von Exchange Online Protection verarbeiteten E-Mail abgerufen werden kann.

Telefonischer IT-Support

Telefonischer IT-Support ist ohne Zusatzkosten rund um die Uhr, an sieben Tagen der Woche und an 365 Tagen im Jahr verfügbar.

Vorhersehbare Kosten

Dank des abonnementbasierten Diensts profitieren Kunden mit lokaler E-Mail-Bereitstellung von einem **vorhersehbaren Zahlungsplan**. Exchange Online Protection ist auch in Exchange Online und jedem Microsoft 365-Plan enthalten, der Exchange Online umfasst.

- Qualität des Programmcodes?
- Sicherheitslücken?
- Wie „sicher“ ist die Softwareanwendung?

Aussagen zur IT-Sicherheit: Realität

heise online > IT > Der

Der Hafniur
Anatomie e

Hätte Microsoft den
verhindern verhinde

Lesezeit: 6 Min. In

heise +

Gestohlene
GAU der Mi

Eine Hackergruppe
Microsoft-Cloud öffn

Lesezeit: 8 Min. In

Microsoft re
Fiasko: Meh

Bislang konnten M3
umfangreiche Protol

Lesezeit: 4 Min. In

(Bild: IB Photography/Shu

Alert!

Patchday: Microsoft repariert Exchange-Sicherheitsupdates

Es sind wichtige Sicherheitspatches für Azure, Teams, Windows & Co. erschienen. Angreifer könnten im schlimmsten Fall Schadcode ausführen.

Lesezeit: 2 Min. In Pocket speichern 5

Aussagen zur IT-Sicherheit: Standards und Zertifizierungen

- Zertifizierung:

  Eine maßgebliche Stelle bestätigt, dass das Prüfobjekt die definierten Anforderungen erfüllt.

- Anforderungsdefinition:

  durch Normen und Standards = Stand der Technik.

- Beispiele:

  → Softwareüberprüfungen zur Ermittlung von Fehlern (Reviews) durch IEEE 1028.

  Fehler: „Abweichen von Erwartungen“: welche?

  → ISO 27001, BSI-Grundschutz u.ä.: Management von Informationssicherheit in den geprüften Organisationen.

ABER: Keine Aussage zur Qualität von Programmcode.

Folgen der fehlenden Messbarkeit von IT-Sicherheit (1)

Rechtsunsicherheit für die Anbieter:

- Sachmangel: „sonstige Merkmale einer Sache, einschließlich ihrer Sicherheit“ (§ 434 Abs. (3) S. 2 BGB).
- Sorgfaltsmaßstab für Produkthaftung und deliktsrechtliche Produzentenhaftung.

Folgen der fehlenden Messbarkeit von IT-Sicherheit (2)

Gesetzliche Maßstäbe für die Anwender (Unternehmer):

- Pflicht zur sorgfältigen Geschäftsführung
- Art. 5 Abs. (2), 24 Abs. (1) und 32 DS-GVO
- KRITIS (BSIG, TKG, EnBW)

verlangen den Einsatz „sicherer“ Software.

Betroffen hiervon

- das Unternehmen selbst,
- Unternehmensleitung (Geschäftsführer, Vorstände),
- IT-Sicherheitsbeauftragte,
- Datenschutzbeauftragte.

Außerdem: fehlerhafte Sachverhalte bei Entscheidungen in Gesetzgebung und Rechtsprechung (§ 129 BetrVG).

Technische Lösungsansätze zur IT-Sicherheitsmetrik

KERNFRAGE:
WAS IST ÜBERHAUPT IT-SICHERHEIT?

Ist Sicherheit…

- die Verfügbarkeit von Updates / Patches / Bugfixes?
  - Wenn ja, in welchem Zeitfenster?
- der Einsatz von NIDS, HIDS, IPS, Firewall und Virenscanner?
  - Wenn ja, wieviel davon?
- buntes Buzzword-Bingo wie bei den TOM der DS-GVO?
  - Darf man dem Glauben schenken oder muß Vernunft walten?
- Einsatz von Schlangenöl?

Konzeptioneller Denkfehler bei IT-Sicherheit

- Angreifer erzeugen Sicherheitslücken
  - Nein, die Programmierer waren es.
    Sicherheitslücken sind Programmierfehler.

- Sicherheit kann man mit [teures Produkt] nachrüsten
  - Nein. Bremsfallschirme ersetzen auch keine PKW-Bremse.

- Sicherheit entsteht durch Normen mit (teuren) Audits
  - Die meisten Normen prüfen nicht die Sicherheit, sondern das Vorgehen bei Vorfällen
    (Sinkfestigkeit vs. Verfügbarkeit von Rettungsbooten).

Was eine Sicherheitsmetrik also messen müßte

- Sind Sicherheitslücken im Programmcode?
  - Wenn ja, welche und wieviele?
  - Wie „trivial“ oder „komplex“ sind die Lücken?
  - Aber: Wie messen, ohne sie zu beheben?
  - **Offene Forschungsfrage**
- Gibt es während der Entwicklung Maßnahmen, die Sicherheitslücken vermeiden?
  - z.B. Tests, Code-Reviews, Coding-Standards
  - Wenn ja, welche, wie werden sie durchgesetzt?
- Welche weiteren Meßwerte könnte es geben?
  - **Offene Forschungsfrage**

Fazit zur Messbarkeit aus technischer Sicht

Es gibt noch keine Metrik, aber wir brauchen sie.

Rechtliche Auswirkungen einer IT-Sicherheitsmetrik

- Belastbarer Nachweis zur Erfüllung von IT-Sicherheitspflichten
- Einbindung in gesetzliche Zertifizierungen zur IT-Sicherheit:
  - § 9 BSIG
    → Cyber Security Act (CSA: VO (EU) 2019/881)
  - § 9c BSIG
  - de lege ferenda: Cyber Resilience Act

§ 9 BSIG: Deutsches IT-Sicherheitszertifikat

- Erforderlich für gesetzlich definierte Anwendungen, z.B.
  - Einsatz kritischer Komponenten in öffentlichen TK-Netzen mit erhöhtem Gefährdungspotential (5G-Mobilfunk, § 165 Abs. (4) TKG)
  - Smart Meter Gateways (z.B. „intelligente Stromzähler“, § 23 MsBG)
  - Option zum Nachweis für KRITIS-Betreiber (§ 8a BSIG).
- Ist zu erteilen, wenn die definierten Kriterien erfüllt sind (§ 9 Abs. 4 BSIG i.V.m. § 4 BSI-ZertV):
  - Technische Richtlinien des BSI (BSI-TR, auch für freiwilliges IT-Sicherheitskennzeichen § 9c BSIG)
  - Common Criteria

Zertifizierungsrahmen des Cyber Security Act (CSA) – (1)

- Art. 46ff. CSA
- Wird Deutsches IT-Sicherheitszertifikat ablösen.
- Voraussetzung:

  Definition der technischen Anforderungen durch Durchführungsverordnung der EU-Kommission.
- Gilt unmittelbar und zwingend in allen EU-Mitgliedstaaten.
- Bislang:

  zwei Entwürfe der ENISA zu technischen Anforderungen für EU-Durchführungsverordnungen:
  - Certification European Cybersecurity Certification Scheme on Common Criteria – EUCC Scheme)
  - European Scheme for Cloud Services – EUCS.

Zertifizierungsrahmen des Cyber Security Act (CSA) – (2)

ENISA-Entwurf EUCC-Scheme:

- Technische Kriterien zur Zertifizierung von Hard- und Software
- Beruht auf ISO-Norm 15408: Vorgehen zur Evaluierung von IT-Sicherheit
- ISO-Norm 15408 ist durch zwischenstaatliche Vereinbarung in mehreren Staaten als „Common Criteria“ (=CC) anerkannt
- CC:2022 bildet den technischen Inhalt des EUCC-Scheme
- Aber: lediglich Verfahrensbeschreibung, aber keine inhaltlichen Vorgaben für Programmcode.

➢ Erwägungsgrund 77 CSA:

„Die Zertifizierung an sich kann nicht garantieren, dass die zertifizierten IKT-Produkte cybersicher sind.“

IT-Sicherheitsmetrik im Entwurf des Cyber Resilience Act

- CRA-E definiert IT-Sicherheitsanforderungen für alle Produkte mit digitalen Elementen
- Art. 5 Abs. (1) i.V.m. Anhang I:

  Angemessenes Cybersicherheitsniveau, keine bekannten ausnutzbaren Schwachstellen.
- formelle Umsetzung: Konformitätsbewertung (Art.18 CRA-E), wird vermutet bei CSA-Zertifizierung.
- Problem: bisherige Entwürfe zur CSA-Zertifizierung definieren lediglich Verfahren zur Entwicklung von IT.
- Erforderlich sind aber inhaltliche Kriterien zur IT-Sicherheit, z.B. zur Qualität des Programmcodes.

→ Anstrengungen der IT-Sicherheitsforschung verstärken.

Fazit

- Begrenzte Aussagekraft der Herstellerangaben zur IT-Sicherheit.
- Fehlende IT-Sicherheitsmetrik begründet Unsicherheiten bei Herstellern, Anwendern und in der rechtlichen Bewertung und Gestaltung.
- Keine ausreichende Berücksichtigung von inhaltlichen Kriterien zur IT-Sicherheit in gesetzlichen Zertifizierungen.
- Weitere Anstrengungen in der Forschung und Normierung inhaltlicher IT-Sicherheitskriterien und ihrer Messbarkeit erforderlich.

Kontakt

Dr. Florian Deusch
Rechtsanwalt und
Fachanwalt für IT-Recht

Anwaltskanzlei Dr. Gretter
Eisenbahnstraße 41
88212 Ravensburg
Telefon: 0751 / 362 250
Telefax: 0751 / 362 25 30
E-Mail: mail@gretter-rae.de
http://www.gretter-rae.de

Professor Dr. Tobias Eggendorfer
Professor für Sicherheit in vernetzten Anwendungen

TH Ingolstadt
Fakultät für Informatik
Esplanade 10
85049 Ingolstadt

https://www.thi.de/informatik/
https://www.eggendorfer.info