CISO Sprechstunde

03.06.2026

Aktuelles aus der FAU

Phishing-Handout

Phishing-Handout

Das **Handout zum Schutz vor Phishing** kann gern ausgedruckt und an Mitarbeitende oder Studierende verteilt werden. Es steht als PDF zum Download bereit.

https://www.intern.fau.de/informationstechnik-it/infosec/awareness/

https://www.intern.fau.de/files/2026/05/2026_05_29_Phishing-Handout.pdf

FAU Friedrich-Alexander-Universität Erlangen-Nürnberg

Phishing-Schutz

Auf dem Stand der Technik bleiben

- **Email-Zertifikate:** Signaturen nutzen, auch für Funktionskonten & Newsletter!
- **MFA** nutzen
- **Phishing-resistente MFA**: Passkeys / FIDO2 (wenn möglich nutzen)
- **IT-Grundhygiene beachten:** Regelmäßige Updates, starke Passwörter, etc.

Social Engineering erkennen

- **Angst**: „Konto gesperrt!"
- **Freude**: „Sie haben gewonnen!"
- **Hilfsbereitschaft**: „Bitte ..."
- **Dringlichkeit**: „Sofort handeln".

Absender prüfen

- Absenderadresse statt nur Anzeigenamen prüfen: Antworten (ohne abzusenden!) oder Adresse in den Editor kopieren.
- Auch eine legitime Absenderadresse schützt nicht sicher. Absenderaccount kann kompromittiert sein.
- Bei Verdacht auf Scam-Anruf auflegen oder ggf. nach Rückrufnummer fragen, aber nicht darauf zurückrufen – nur über offizielle Kanäle erlangte Nummern nutzen.

Inhalte prüfen

- Link prüfen: Hovern (ohne Klick) oder URL in den Editor kopieren.
- Im Zweifel über einen nicht in der Mail erwähnten Kanal nachfragen
- Im Zweifel keine Anhänge/Links öffnen
- Vorsicht bei der Abfrage vertraulicher Daten

Domain-Spoofing prüfen

- rnicrosoft.com statt microsoft.com, VV statt W, großes i statt kleines L, Null statt O
- Unicode-Homoglyphen (Unicode-Inspector / ASCII-Validator)
- Beispiel: *paypal.us.com* – Hauptdomain ist *us*, nicht *paypal.*

Im Zweifel prüfen lassen

Als Anhang an postmaster@fau.de weiterleiten (soc@fau.de in Kopie). So bleiben Header und Originalinhalt erhalten.

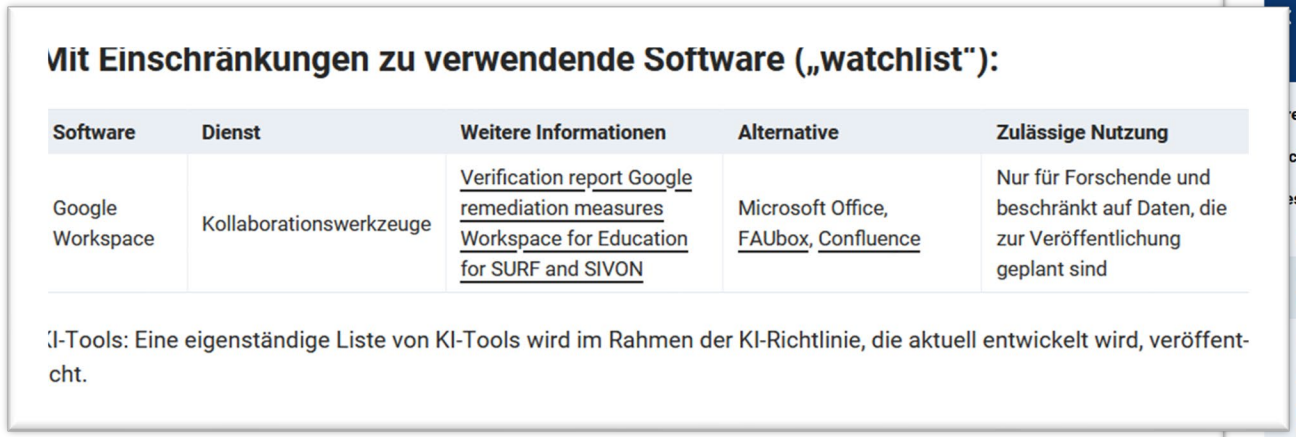
Bei verdächtigem Verhalten auf Ihrem Computer ...

- Nicht in Panik geraten, nicht das System herunterfahren / ausschalten
- Trennen Sie die Netzwerkverbindung
- Nicht ungenehmigt über den Vorfall sprechen
- Nicht versuchen, selbst gegen einen Cyber-Angriff vorzugehen
- Melden Sie das Problem unter 09131-85-67777 / abuse@fau.de

fau.info/infosec

Datenschutzkonforme Lösungen

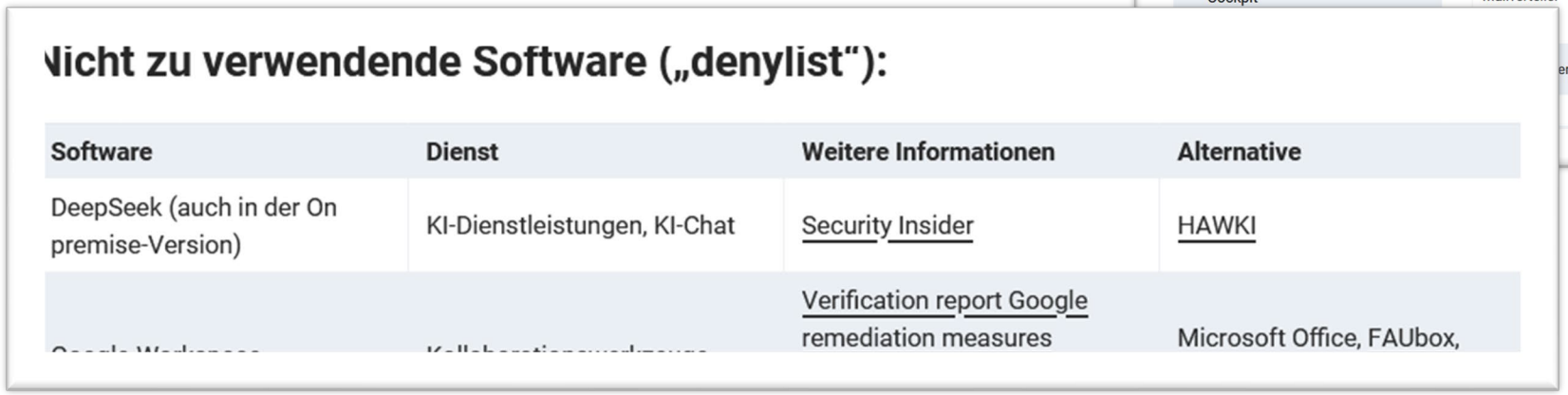
https://www.intern.fau.de/informationstechnik-it/ressourcen-und-anleitungen/datenschutzkonforme-it-loesungen/



Mit Einschränkungen zu verwendende Software („watchlist"):

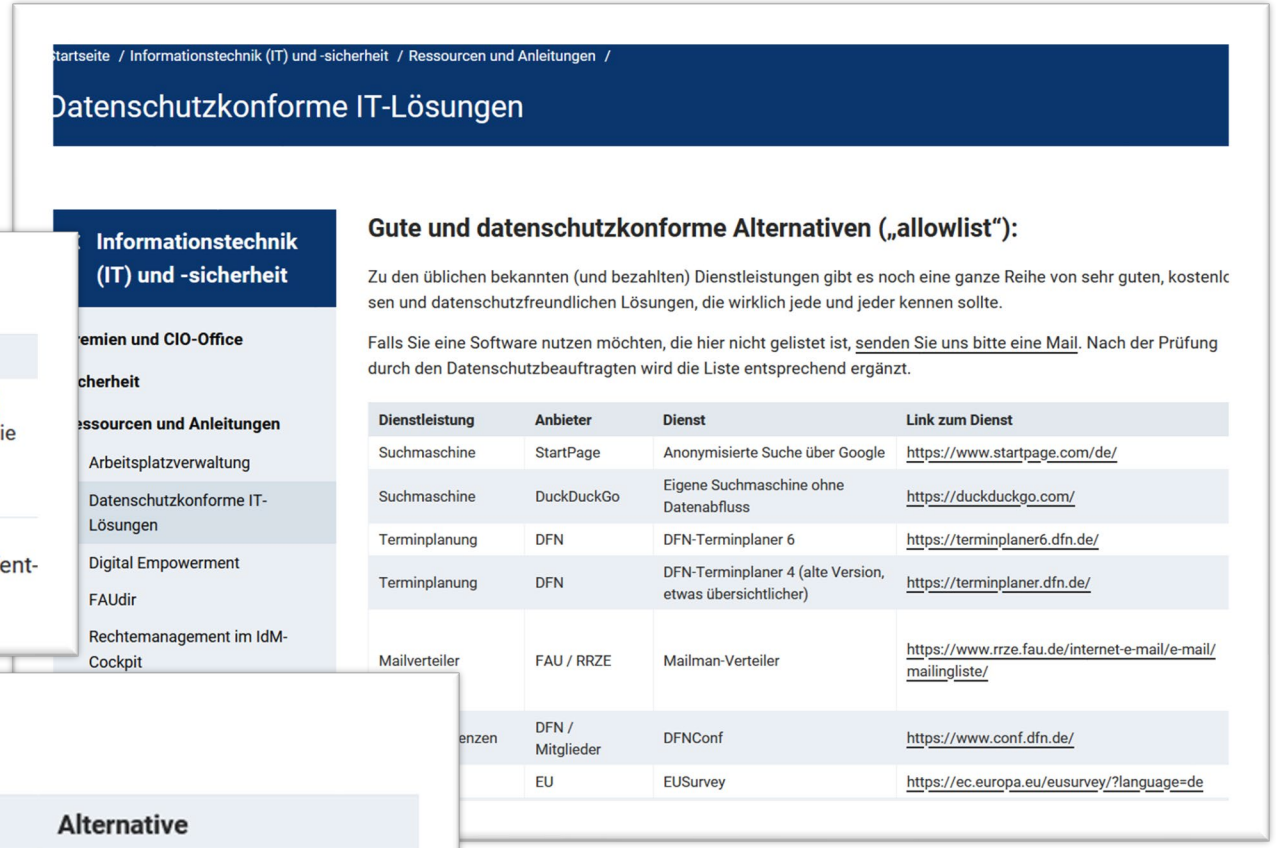
Software	Dienst	Weitere Informationen	Alternative	Zulässige Nutzung
Google Workspace	Kollaborationswerkzeuge	Verification report Google remediation measures Workspace for Education for SURF and SIVON	Microsoft Office, FAUbox, Confluence	Nur für Forschende und beschränkt auf Daten, die zur Veröffentlichung geplant sind

KI-Tools: Eine eigenständige Liste von KI-Tools wird im Rahmen der KI-Richtlinie, die aktuell entwickelt wird, veröffentlicht.



Nicht zu verwendende Software („denylist"):

Software	Dienst	Weitere Informationen	Alternative
DeepSeek (auch in der On premise-Version)	KI-Dienstleistungen, KI-Chat	Security Insider	HAWKI
Google Workspace	Kollaborationswerkzeuge	Verification report Google remediation measures	Microsoft Office, FAUbox,



Startseite / Informationstechnik (IT) und -sicherheit / Ressourcen und Anleitungen /

Datenschutzkonforme IT-Lösungen

Informationstechnik (IT) und -sicherheit

- Gremien und CIO-Office
- Sicherheit
- Ressourcen und Anleitungen
- Arbeitsplatzverwaltung
- Datenschutzkonforme IT-Lösungen
- Digital Empowerment
- FAUdir
- Rechtemanagement im IdM-Cockpit

Gute und datenschutzkonforme Alternativen („allowlist"):

Zu den üblichen bekannten (und bezahlten) Dienstleistungen gibt es noch eine ganze Reihe von sehr guten, kostenlosen und datenschutzfreundlichen Lösungen, die wirklich jede und jeder kennen sollte.

Falls Sie eine Software nutzen möchten, die hier nicht gelistet ist, senden Sie uns bitte eine Mail. Nach der Prüfung durch den Datenschutzbeauftragten wird die Liste entsprechend ergänzt.

Dienstleistung	Anbieter	Dienst	Link zum Dienst
Suchmaschine	StartPage	Anonymisierte Suche über Google	https://www.startpage.com/de/
Suchmaschine	DuckDuckGo	Eigene Suchmaschine ohne Datenabfluss	https://duckduckgo.com/
Terminplanung	DFN	DFN-Terminplaner 6	https://terminplaner6.dfn.de/
Terminplanung	DFN	DFN-Terminplaner 4 (alte Version, etwas übersichtlicher)	https://terminplaner.dfn.de/
Mailverteiler	FAU / RRZE	Mailman-Verteiler	https://www.rrze.fau.de/internet-e-mail/e-mail/mailingliste/
Konferenzen	DFN / Mitglieder	DFNConf	https://www.conf.dfn.de/
	EU	EUSurvey	https://ec.europa.eu/eusurvey/?language=de

Instructure mit Canvas-Plattformen

Hack

Zusammenfassung:

- Am 01. Mai wurde der Software-Anbieter Instructure von der Gruppe ShinyHunters gehackt. Es wurden Presseberichten zu folge 275 Millionen Datensätze entwendet. Es sollen rund 9.000 Kunden (Schulen, Hochschulen, Universitäten weltweit) betroffen sein:

https://www.tagesspiegel.de/wissen/hackerangriff-legt-lernplattform-weltweit-lahm-auch-eine-berliner-manager-uni-ist-betroffen-15574936.html.

- Es kursiert im Internet eine Liste, verteilt über X, mit unbekanntem Ursprung:

https://privatebin.net/?f8c17bc224cd9f22#F2qrJM6a2juvQjziJTH8Pbwef5Lsa8TzRbCFW5FMg4uW

- In den darauf folgenden Tagen wurden wohl in einem zweiten Schritt die Canvas-Plattformen von einigen Instructure-Kunden angegriffen
- Die FAU Academy steht mit auf der Liste von den betroffenen Kunden
- Die Daten in der Liste halten wir für NICHT vertrauenswürdig ➔ **dennoch gibt es Hausaufgaben für die FAU**

Linux-Kernel Schwachstellen und generell verkürzte Patch-Fenster

Nachdem die copy.fail Sicherheitslücke (CVE-2026-31431 https://copy.fail) für Aufregung sorgte, tun sich sich weitere, vergleichbar gefährliche Schwachstellen auf:

Local Privilege Escalations mit den Spitznamen „Dirty Frag“ (CVE-2026-43284 / CVE-2026-43500) und Fragnesia (CVE-2026-46300). Mit der Veröffentlichung weiterer Schwachstellen ist zu rechnen.

Bitte beachten Sie dazu folgende Empfehlungen auf der Seite des RRZE:
https://www.rrze.fau.de/2026/05/warnung-neue-lpe-im-linux-kernel-2026-05-08/

*„Laut LSI liegt das Zeitfenster zum Patchen aufgrund der Fähigkeiten von KI-Systemen nun generell bei nur noch **höchstens 10 Stunden**. Absicherung nach dem Stand der Technik wird in vielen Hochschulen zusätzliche Ressourcen für schnelles Patchen erfordern. Weitere Hürden sind u. a. mobile Geräte (Updates oft nur bei WLAN und Ladung), längere Zyklen bei Microsoft-Office-Cloud-Updates sowie Geräte, die wegen Speichermangel o. Ä. keine Updates erhalten. (Hinweise von Johannes Nehlsen, Stabsstelle IT-Recht, Digitalverbund Bayern – Hochschulbereich)*

Daher gibt es derzeit einen Austausch über praxistaugliche Lösungen für zügiges Patchmanagement (HITS IS) und mögliche Mitigationen bis zum Patch. Sobald konkrete Ergebnisse vorliegen, informieren wir Sie.
Bleiben Sie wachsam und schützen Sie Ihre Systeme. „

Schwachstellenmanagement

Tenable SC

- Die neue Lizenz für unseren Tenable scanner liegt in Kürze vor
- Nach Installation kann wieder aktiv nach Schwachstellen gesucht werden
- Nutzen Sie bitte den Client von Tenable für Ihre exponierten Systeme im Internet!
- Kontakt matti.schulze@fau.de oder soc@fau.de

Frage:

Tenable bietet auch die Möglichkeit Systeme automatisch zu patchen. Wäre das für Sie interessant?

2FA an der FAU

- Erfreulich wenig manuelle Eingriffe zur technischen Umsetzung
- Akzeptanz scheint hoch zu sein
- Dennoch ca. 600 Nachzügler, die die Frist versäumt haben

Botnets

Drohnen auch an der FAU?

Hier wird hoffentlich unser SIEM mit dem zukünftigen IDS Antwort geben können.

SIEM DV soll in diesem Monat unterschrieben werden.

https://www.heise.de/news/Niederlaendische-Strafverfolger-legen-Botnet-mit-17-Millionen-Drohnen-lahm-11313066.html

heise online > Security > Niederländische Strafverfolger legen Botnet mit 17 Millionen Drohnen lahm

Niederländische Strafverfolger legen Botnet mit 17 Millionen Drohnen lahm

Das niederländische NCSC und die Polizei haben ein Botnet mit 200 Servern und 17 Millionen infizierten Geräten ausgeknipst.

20

(Bild: Portrait Image Asia/Shutterstock.com)

01.06.2026, 09:57 Uhr Lesezeit: 2 Min. | Security

Von Dirk Knop

Ende vergangener Woche ist der niederländischen Polizei zusammen mit dem Nationalen Zentrum für Cybersicherheit (NCSC) des Landes ein Schlag gegen ein großes Botnet gelungen. 200 Server und 17 Millionen infizierte Geräte umfasste das für kriminelle Zwecke genutzte Botnet.

Aktuelles aus der Welt

Android

Patchday

https://www.heise.de/news/Patchday-18-kritische-Sicherheitsluecken-bedrohen-Android-14-15-16-11314546.html

heise online > Security > Patchday: Kritische Lücken ermöglichen Attacken auf Android 14, 15, 16

Alert!

Patchday: Kritische Lücken ermöglichen Attacken auf Android 14, 15, 16

Google hat zahlreiche Softwareschwachstellen in verschiedenen Android-Versionen geschlossen. Es kann Schadcode auf Geräte gelangen.

9

Google Android-Bugdroid vor Schloss-Symbol. (Bild: Primakov/Shutterstock.com)

10:19 Uhr Lesezeit: 2 Min. | Security

Von Dennis Schirrmacher

Sicherheitslücken im Framework, Kernel und System gefährden Smartphones und Tablets mit Android 14, 15, 16 und 16-qpr2. Wer ein noch im Support befindliches Gerät besitzt, sollte sicherstellen, dass die aktuellen Sicherheitsupdates installiert sind.

Home Assistant

Patchday

https://www.heise.de/news/Home-Assistant-Smartphone-Apps-ermoeglichen-Uebernahme-durch-Angreifer-11313360.html

heise online > Security > Home Assistant: Smartphone-Apps ermöglichen Übernahme durch Angreifer

Alert!

Home Assistant: Smartphone-Apps ermöglichen Übernahme durch Angreifer

Die Companion-Apps für Android und iOS reißen ein Sicherheitsleck in Home Assistant. Angreifer könnten Instanzen übernehmen.

24

(Bild: heise medien)

01.06.2026, 11:53 Uhr Lesezeit: 2 Min. | Security

Von Dirk Knop

Wer Home Assistant mit den Companion-Apps unter Android oder iOS steuert, sollte die verfügbare Aktualisierung schleunigst anwenden. Das Update für die Apps schließt eine Sicherheitslücke, durch die Angreifer ein Zugriffstoken abgreifen und damit die komplette Home-Assistant-Instanz übernehmen können.

Was können wir für Sie tun?

Ihre Fragen?

Ihre Wünsche?