CISO Sprechstunde

05.02.2025

Aktuelles aus der FAU

SIEM

- DV wird am 11.02.25 mit GPR erstmalig besprochen, weitere Termine werden vermutlich folgen
- DSFA wird erstellt

Allg. Informationssicherheitsrichtlinie

- Abstimmung mit Juristen aus Kanzlerbüro erfolgt aktuell
- Absprache mit GPR 1. Q. 2025?

Friedrich-Alexander-Universität
Erlangen-Nürnberg

FAU

Cyberangriff auf FAU

…

mit besten Grüßen aus Moskau
am 08./09.01.2025

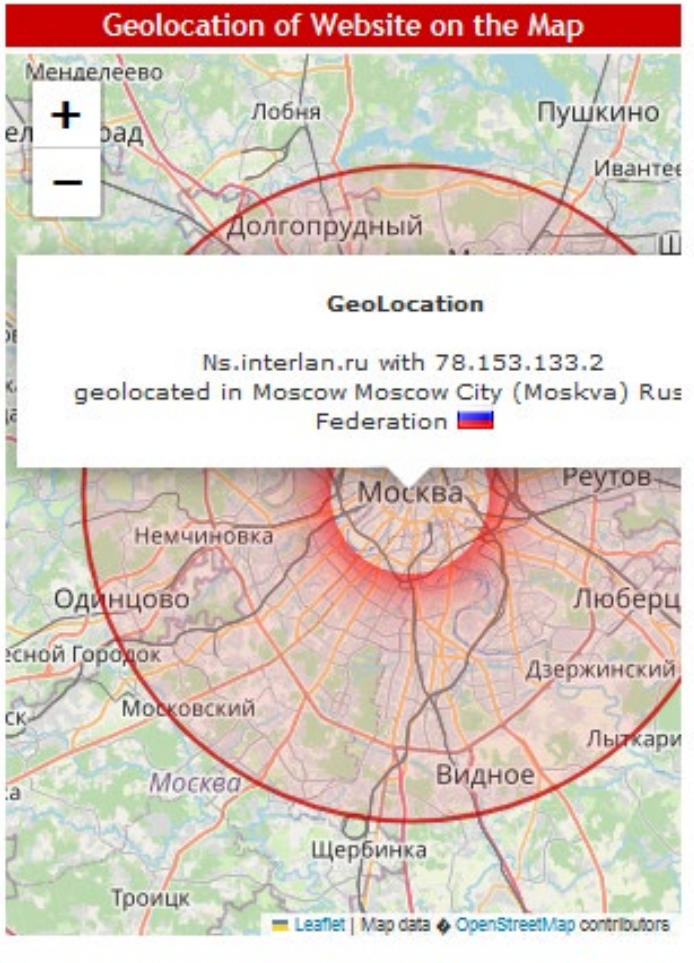
Cyberangriff 08./09.01.2025

… mit besten Grüßen aus Moskau

Webserver der FAU

- Betr. Domain: *b[redacted].org* & *[redacted].fau.de*
- Website erlaubt Upload von Dateien
  - „ *b[redacted].org ist e*ine Wordpress-Instanz mit (zu-)vielen fragwürdigen Plugins“
  - Systemverantwortung unklar (FAU?, TU Dortmund?), zumal Projekt schon lange beendet ist
- Leider auch betroffen: *[redacted].fau.de* die Department-Site

- Beachte, leider FAU-typisch: Keine Netzwerksicherheit für LS-Webserver im Internet (offenes Internet-Segment)



Cyberangriff 08./09.01.2025

Chronologie

04:58:33

- Datei **16710b719d4d.php** auf Webserver hochgeladen
  von IP-Adr. 109.237.99.63 [ISP „interlan.ru“]

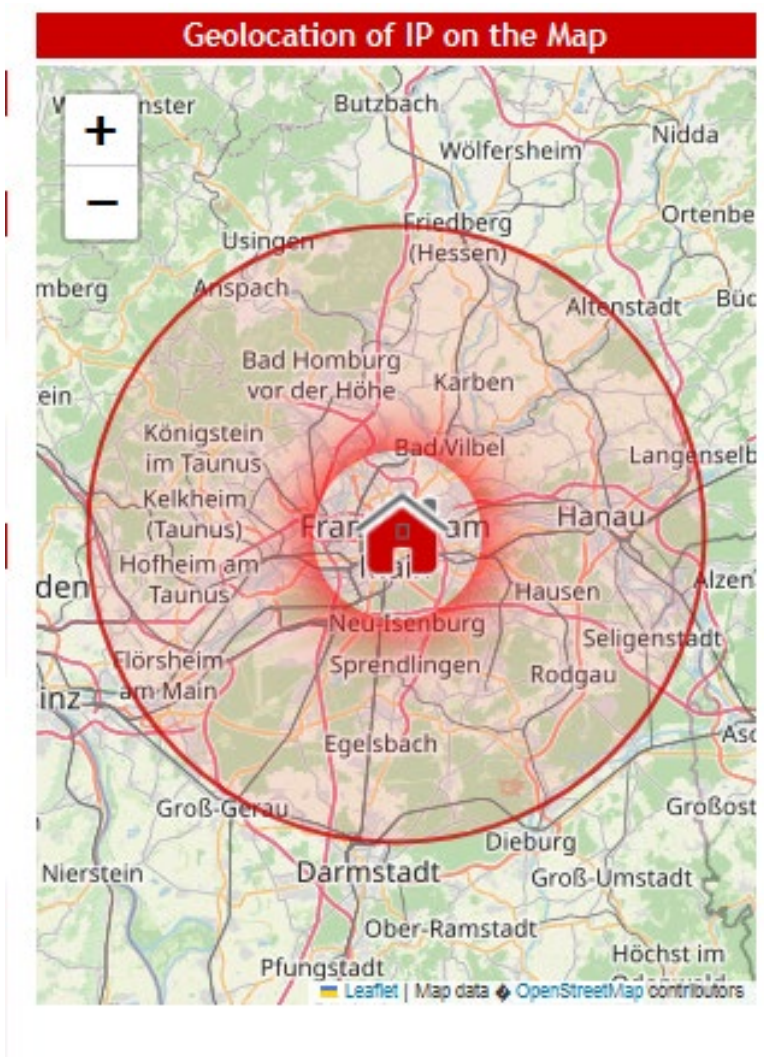
05:51:07 Datei **3ea958ed0f.php** auf Webserver hochgeladen

- 09:19:41 Datei **hplfuns.php** auf Webserver hochgeladen
- 09:21:41 durch die internen Verzeichnisse iteriert und Versionsstände abgefragt
  über Script **accesson.php**
- 09:38:09 Datei **16710b719d4d.php** auf Webserver modifiziert
- 10:03:37 Datei **.htaccess** auf Webserver hochgeladen und damit die
  Website final übernommen

09.01.25

- 00:13:34 bis 01:29:55 Anmeldeversuche auf test3 (BruteForce) mit unterschiedlichen
  IP-Adressen (aus GER und RU)
- 00:13:35 bis 07:00:49 Anmeldeversuche auf [redacted]*fau.de* (BruteForce) mit unterschiedlichen
  IP-Adressen
- 01:09:14 Modifikation der **index.php** von *b*[redacted]*.org*

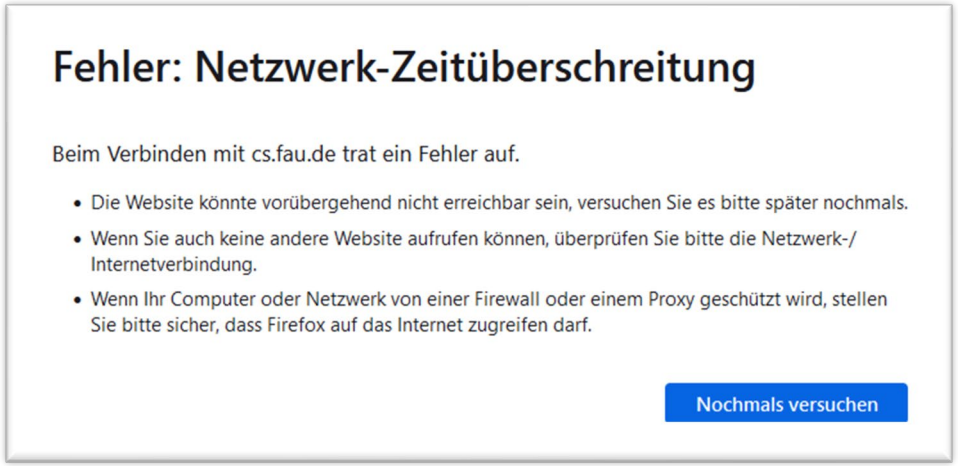
Hinweis: es wurde auf die Zertifikate zugegriffen!



Cyberangriff 08./09.01.2025

- Der Angreifer hat in der Nacht vom 08. zum 09. Januar die Website [redacted]*.fau.de* offenbar sehr genau analysiert (siehe department_access.log)
- Es wurde mit diversen Angriffen auch ordentlich an der Webseite „gerüttelt“ (**BruteForce, BufferOverflow)**
- Die Angriffe waren nur bedingt erfolgreich und wurden wohl durch den Admin unterbrochen (Netztrennung)

- Es gibt auch Überlagerungen von anderen Spuren u.a. durch **Bots**, daher können wir nicht alles ganz sauber trennen



Cyberangriff 08./09.01.2025

Maßnahmen CISO:

- *b[redacted].org* wird nicht wieder in Betrieb genommen
- Neuinstallation [redacted].fau.de (nur Webseiten-Inhalte aus Backup vom Dezember)
- Dedizierte Netzwerk-Überwachung durch RRZE von [redacted]*.fau.de* für 14 Tage (Angreifer kommt u.U. wieder)
- Anzeige und Bericht geht zeitnah an die Polizei

Dringende Empfehlung:

- Umzug der [redacted]*.fau.de* ins RRZE (siehe IT-R §5)

➔ Betreuung eines produktiven Dept.-Webauftritts ist am LS ist nicht optimal aufgehoben

Friedrich-Alexander-Universität
Erlangen-Nürnberg

FAU

Phishing Mails aus FAU Postfach

reichlich Phishing Mails aus FAU Postfach

------- Weitergeleitete Nachricht ------

Von: **Fc** el@fau.de>

Datum: Mo. 3. Feb. 2025 um 08:22

Betreff: Offizielle Mitteilung der Universität Erlangen-Nürnberg Verwaltungsbüro

An:

Hallo

Sie haben eine Nachricht von der Universität Erlangen-Nürnberg › Präsident Joachim Hornegger erhalten. Klicken Sie bitte hier, um sie zu lesen.

Vielen Dank.

Alle Ordner sind auf dem neuesten Stand. Verbunden mit Microsoft Exchange Anzeigeeinstellungen 120 %

el Klotz 6 Antworten

Friedrich-Alexander-Universität
Erlangen-Nürnberg

FAU

Datenübermittlung in die USA

Datenschutz

https://www.heise.de/hintergrund/Nach-Trump-Entscheidung-Kippt-das-Abkommen-fuer-Datenuebermittlungen-in-die-USA-10260045.html

Nach seiner offiziellen Ernennung hat US-Präsident Donald Trump die drei demokratischen Mitglieder des Privacy and Civil Liberties Oversight Board (PCLOB) zum Rücktritt aufgefordert, was die Behörde nun bestätigt hat. Das PCLOB ist eine unabhängige Datenschutzaufsichtsbehörde in den USA und ein wichtiges Element bei der Legitimierung von Datenübermittlungen im Rahmen des EU-US-Datenschutzrahmens (Transatlantic Data Privacy Framework, kurz TADPF). Die ersten beiden Versuche eines Datenübermittlungsabkommens zwischen der EU und den USA – Safe Harbour und Privacy Shield – scheiterten in der Vergangenheit nach Klagen der Datenschutz-NGO noyb vor dem Europäischen Gerichtshof.

Im Rücktritt der drei Mitglieder sieht noyb jetzt ein erstes Loch im TADPF. Dieses Abkommen zwischen der EU-Kommission und der US-Regierung ist die zentrale Grundlage für den seit dem 10. Juni 2023 geltenden Angemessenheitsbeschluss für Datentransfers in die USA. Damit wurde ein jahrelanger Zustand der Rechtsunsicherheit beendet. Verantwortliche, die personenbezogene Daten in die USA übermitteln, müssen seitdem keine zusätzlichen Garantien vereinbaren, wenn der Empfänger in den USA nach dem EU-US-Datenschutzrahmen zertifiziert ist. Fällt der Angemessenheitsbeschluss weg, droht erneut erhebliche Rechtsunsicherheit für Unternehmen auf beiden Seiten des Atlantiks.

Vortrag Export Kontrolle muss heute leider entfallen

Ihre Fragen?

Ihre Wünsche?