Friedrich-Alexander-Universität
Erlangen-Nürnberg

FAU

CISO Sprechstunde

07.02.2024

Ihre Fragen?

Ihre Themen?

Informationssicherheit aktuelles

Informationssicherheit

Einschläge kommen näher

Fränkischer Tag

28.01.2024

Erlangen – Die Bezirkskliniken Mittelfranken meldeten am Sonntagabend einen Hackerangriff. Polizei und Staatsanwaltschaft ermitteln.

Am Sonntagabend meldeten die Bezirkskliniken Mittelfranken einen Hackerangriff auf die IT-Systeme, wobei gezielt Daten verschlüsselt worden seien. Aus Sicherheitsgründen habe man alle Systeme vom Netz getrennt. Auch von der Notfallversorgung wurden die Kliniken vorerst abgemeldet. Neben Standorten in Nürnberg und Ansbach gehört auch das Klinikum am Europakanal in **Erlangen** zu dem Netzwerk.

Cyberangriff: Kliniken Mittelfranken verhandeln nicht, Neustart der Systeme

Cyberkriminelle versuchen, ein Lösegeld von den Bezirkskliniken Mittelfranken zu erpressen. Die Klinik will nicht zahlen und derweil die Systeme neu aufsetzen.

01.02.2024 42

Informationssicherheit

Zukunft?

Videokonferenz voller KI-Klone: Angestellter schickt Betrügern 24 Millionen Euro

Bislang werden im Rahmen der "Chef-Masche" Angestellte zumeist von einer Person überzeugt, Geld herauszugeben. Ein Fall in Hongkong hat nun eine neue Qualität.

Lesezeit: **2 Min.** In Pocket speichern 186

(Bild: fizkes/Shutterstock.com)

05.02.2024 08:17 Uhr

Mehr Zugriffschutz für intern.fau.de

https://www.intern.fau.de/2024/02/02/mehr-zugriffschutz-fuer-intern-fau-de/

2. Februar 2024

Zugriff auf die internen Webseiten, Formulare und Downloads nur noch aus dem FAU-Netz

Um die internen Informationen auf www.intern.fau.de besser zu schützen, ist ein Zugriff **ab dem 21. Februar 2024** nur noch aus dem internen FAU-Netzwerk (LAN, WLAN inkl. VPN-Anbindung) möglich.

Auf den internen Webseiten finden Sie wichtige Infos zum Arbeitsleben an der FAU: von Arbeitszeitregelungen und Fortbildungen bis hin zu Vorlagen und Formularen für Buchhaltung, Personaleinstellung und Corporate Design.

Was bedeutet das für mich?

Im lokalen FAU-Netzwerk und bei Verwendung einer VPN-Anbindung (zum Beispiel aus dem Home-Office) werden Sie keinen Unterschied bemerken. Unterwegs vom Smartphone (ohne VPN) ist ein Zugriff allerdings nicht mehr möglich. Weder für Sie, noch für potentielle Hacker oder sonstige Angreifer.

Die Zugriffe auf alle extern bereitgestellten Informationen der Website fau.de sind natürlich aus dem Internet weiterhin wie gewohnt möglich.

Dies ist erfolgt aus den folgenden Gründen:

- **Einhaltung gesetzlicher Vorschriften**: Die Sicherung interner Informationen ist nötig, um gesetzliche Vorschriften und regulatorische Standards einzuhalten, zum Beispiel im Datenschutz.
- **Schutz von Verwaltungsvorschriften und Fehlinformation**: Intern bereitgestellte Informationen beinhalten eine Vielzahl von Verwaltungsvorschriften, Richtlinien und organisatorische Informationen. Ein offener Zugang zu internen Dokumenten kann die Vertraulichkeit unserer internen Abläufe gefährden und zu Missverständnissen führen, sowohl innerhalb der Universität als auch extern.
- **Wettbewerbsvorteil und Schutz vor unerlaubter Nutzung**: Der Schutz interner Informationen sichert das intellektuelle Eigentum unserer Universität vor Diebstahl oder unerlaubter Nutzung und stärkt so unsere langfristige Wettbewerbsposition.
- **Sicherung gegen Cyberangriffe**: Ein effektiver Schutz interner Informationen minimiert das Risiko von Cyberangriffen und Datenlecks, die unter anderem finanzielle Schäden und Imageverluste verursachen könnten.

Inhalte übers Menü finden oder direkt zur Finanzbuchhaltung, Powerpointvorlagen, Sportkursen oder Formularen: intern.fau.de.

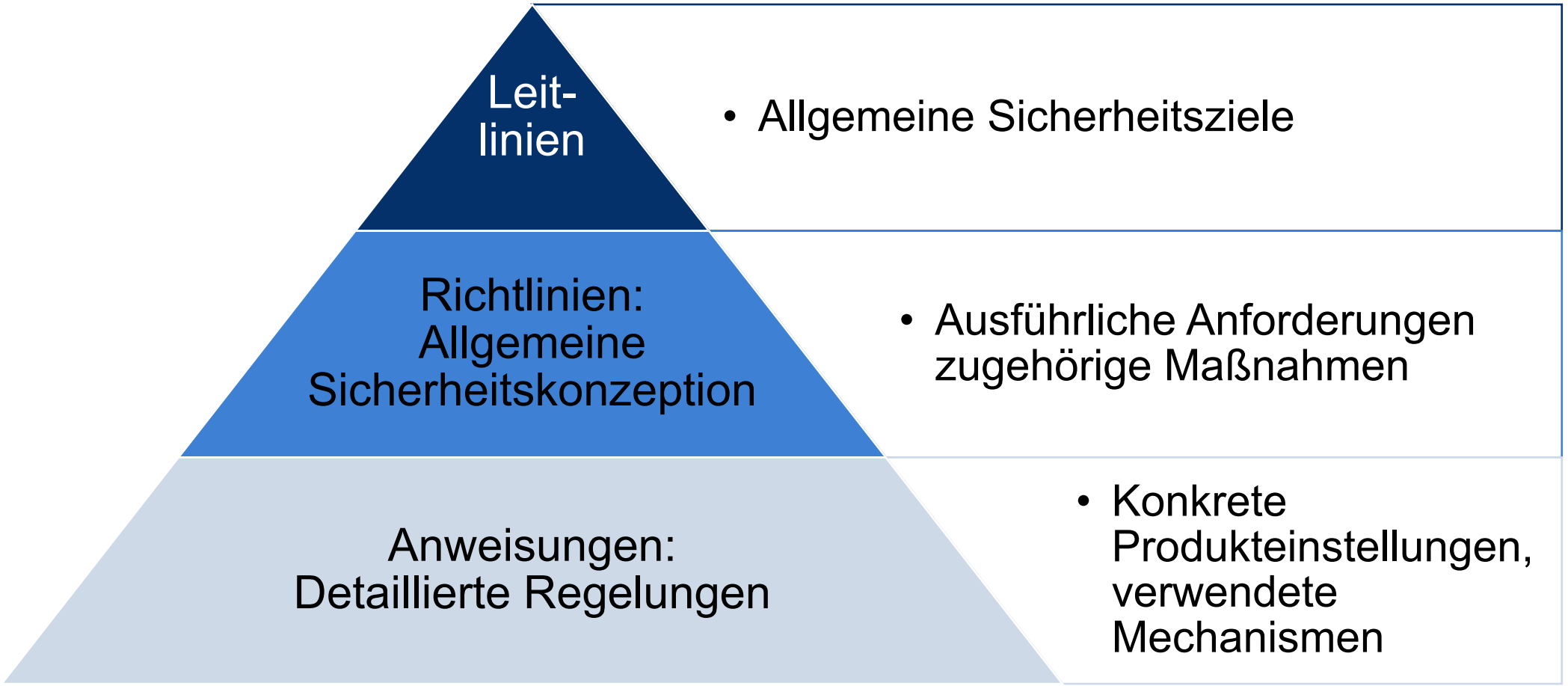
Die Cybersicherheit ist eine sich ständig weiterentwickelnde Herausforderung, und es ist wichtig, stets auf dem neuesten Stand zu bleiben, um potenzielle Risiken zu minimieren. Wenn Sie Fragen haben oder zusätzliche Informationen benötigen, steht Ihnen unser Chief Information Security Officer (CISO) Prof. Dr. Michael Tielemann gerne zur Verfügung.

Anleitung: VPN an der FAU

InfoSec Richtlinie an der FAU

Informationssicherheit

Richtlinien und Regeln



Wichtig sind

- interne Regelungen
- klare Sprachdefinitionen

um Missverständnisse bei Policies, Leitlinien, Richtlinien, Anweisungen, Empfehlungen zu vermeiden.

Radioeteleskopverbund ALMA stellt Forschungsarbeit wegen Cyberattacke ein

Nach einem Cyberangriff am Wochenende ist nicht nur die Homepage des riesigen Observatoriums offline, auch die wissenschaftliche Arbeit wurde unterbrochen.

02. November 2022, 14:34 Uhr 5

Richtlinien, Regeln, Rollen

Hilfreich dabei sind z. B. Modalverben nach RFC 2119 (https://datatracker.ietf.org/doc/rfc2119/)

- In Anlehnung an den RFC 2119 werden die (Sicherheits-) Anforderungen mit den Modalverben MUSS und SOLLTE sowie den zugehörigen Verneinungen formuliert.
- Darüber hinaus wird das Modalverb KANN für ausgewählte Aspekte verwendet.

MUSS / DARF NUR

bedeutet, dass diese Anforderung zwingend zu erfüllen ist. Das von der Nichtumsetzung ausgehende Risiko kann nicht im Rahmen einer Risikoanalyse akzeptiert werden.

DARF NICHT / DARF KEIN

bedeutet, dass etwas zwingend zu unterlassen ist. Das durch die Umsetzung entstehende Risiko kann nicht im Rahmen einer Risikoanalyse akzeptiert werden.

Richtlinien, Regeln, Rollen

SOLLTE

bedeutet, dass etwas umzusetzen ist, es sei denn, im Einzelfall sprechen gute Gründe gegen eine Umsetzung. Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können.

SOLLTE NICHT / SOLLTE KEIN

bedeutet, dass etwas zu unterlassen ist, es sei denn, es sprechen gute Gründe für eine Umsetzung. Bei einem Audit muss die Begründung vom Auditor auf ihre Stichhaltigkeit geprüft werden können.

KANN

bedeutet, dass die Umsetzung / Nicht-Umsetzung optional ist und ohne Angabe von Gründen unterbleiben kann.