Friedrich-Alexander-Universität
Erlangen-Nürnberg

FAU

CISO Sprechstunde

02.10.2024

Aktuelles aus der FAU

Aktuelles aus der FAU

Das FAU-Security-Team wächst

- Katharina Schiller
- Marion Liegl

ISMS

- Informationssicherheitsleitlinie und –richtlinie weiterhin in Abstimmung mit Kanzlerbüro und GPR

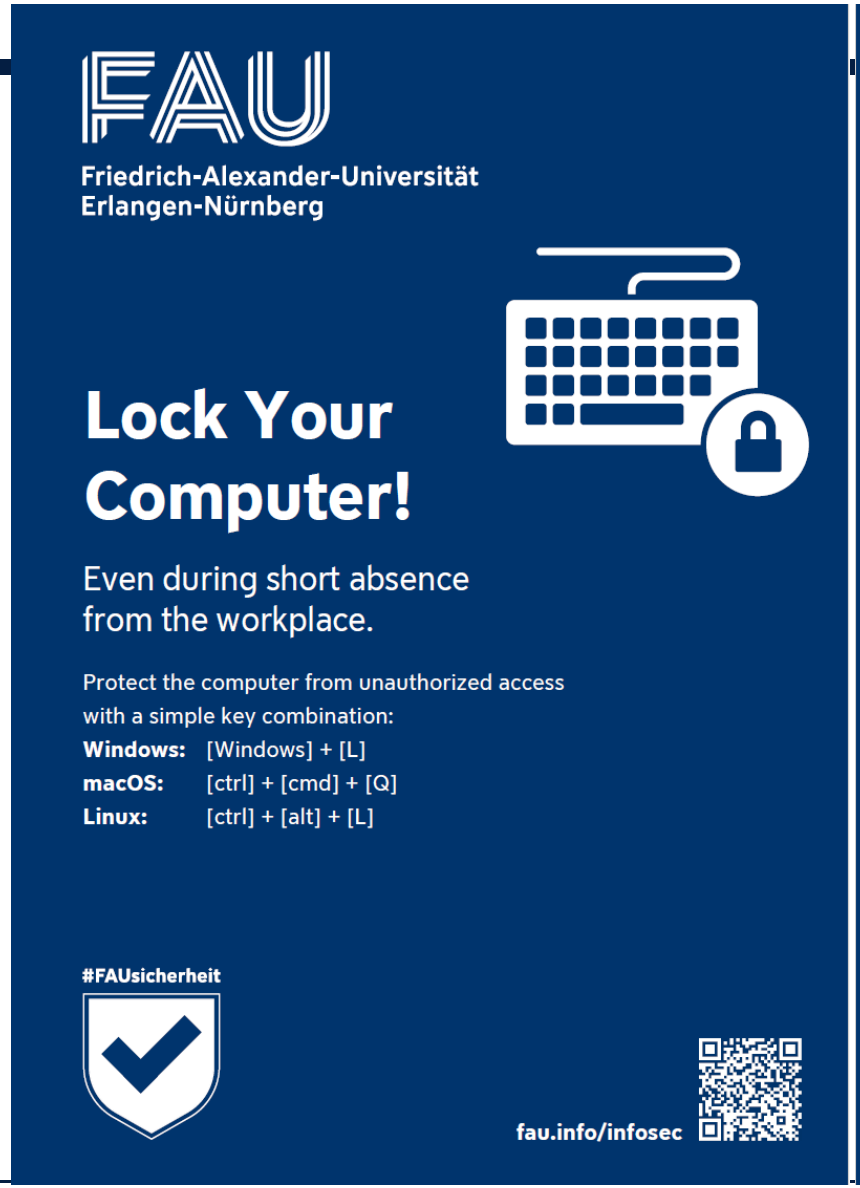
Angriffserkennung

- Dienstvereinbarung für den Testbetrieb eines SIEM und IDS/IPS ist in Bearbeitung durch Kanzlerbüro und wird anschließend mit GPR besprochen

Proof of Concept
Anschließend erfolgt ein Proof of Concept mit der Fa. Elastic
(Perspektive auch auf End Point Protection)

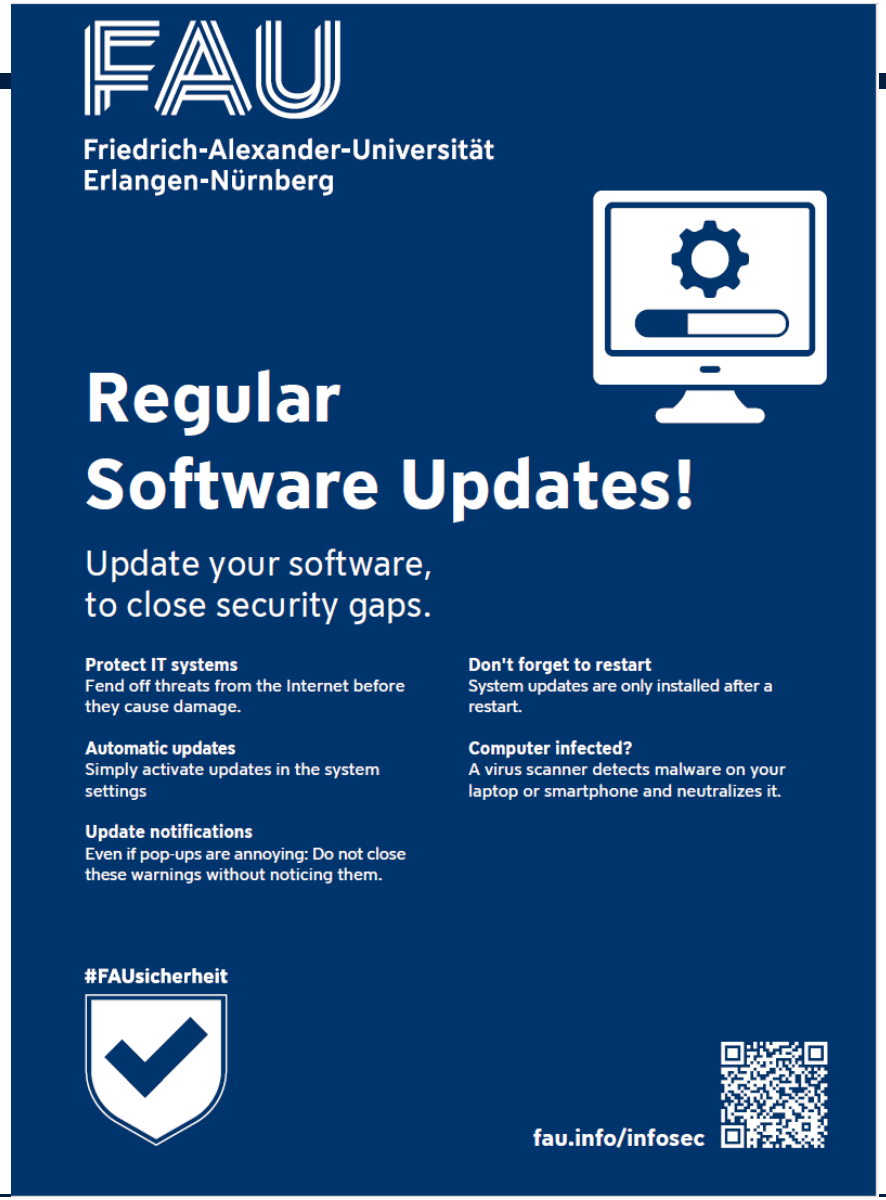
Awareness

- Poster für alle Einrichtungen, CIP Pools, Bibliotheken, Mensen etc.



Aktuelles aus der FAU

Awareness und Schulungsangebote



IT-Krisenstab

- Am 07.10.2024 findet die erste IT-Krisen-Notfallübung statt
  - Notfallhandbuch v1.0 wurde erstellt
  - Drehbuch für die IT-Krise wurde erstellt
  - Ziel: Jedes Jahr eine IT-Krisen-Notfallübung

Notfallmanagement

Notfallmanagement

Kategorien

STÖRUNGEN, NOTFÄLLE, KRISEN UND KATASTROPHEN IM VERSTÄNDNIS DES BSI-STANDARDS 100-4

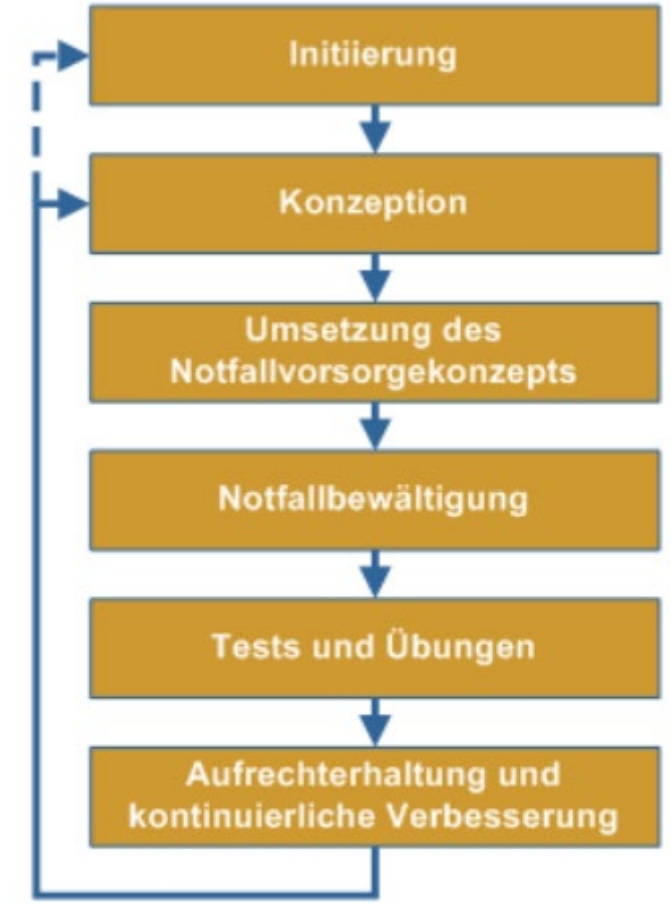
Vorfallsart	Erläuterung	Behandlung
Einfache Störung	Kurzzeitiger Ausfall von Prozessen oder Ressourcen mit nur geringem Schaden	Behandlung ist Teil der üblichen Störungsbehebung
Notfall	Länger andauernder Ausfall von Prozessen oder Ressourcen mit hohem oder sehr hohem Schaden	Behandlung verlangt besondere Notfallorganisation
Krise	Im Wesentlichen auf die Institution begrenzter verschärfter Notfall, der die Existenz der Institution bedroht oder die Gesundheit oder das Leben von Personen beeinträchtigt	Da Krisen nicht breitflächig die Umgebung oder das öffentliche Leben beeinträchtigen, können sie, zumindest größtenteils, innerhalb der Institution selbst behoben werden
Katastrophe	Räumlich und zeitlich nicht begrenztes Großschadensereignis, zum Beispiel als Folge von Überschwemmungen oder Erdbeben	Aus Sicht einer Institution stellt sich eine Katastrophe als Krise dar und wird intern durch deren Notfallorganisation in Zusammenarbeit mit den externen

Notfallmanagement

1. **Initiierung**
   Getragen von der Leitung werden strategische Zielsetzungen festgelegt und grundlegende organisatorische Voraussetzungen für den Notfallmanagement-Prozess in einer Institution geschaffen.

2. **Konzeption**
   Die kritischen Geschäftsprozesse und Ressourcen einer Institution werden ermittelt und die Risiken, denen diese ausgesetzt sind, bewertet. Zu diesen Bewertungen und der Notfallstrategie der Institution passende Notfallvorsorgekonzepte werden entwickelt.

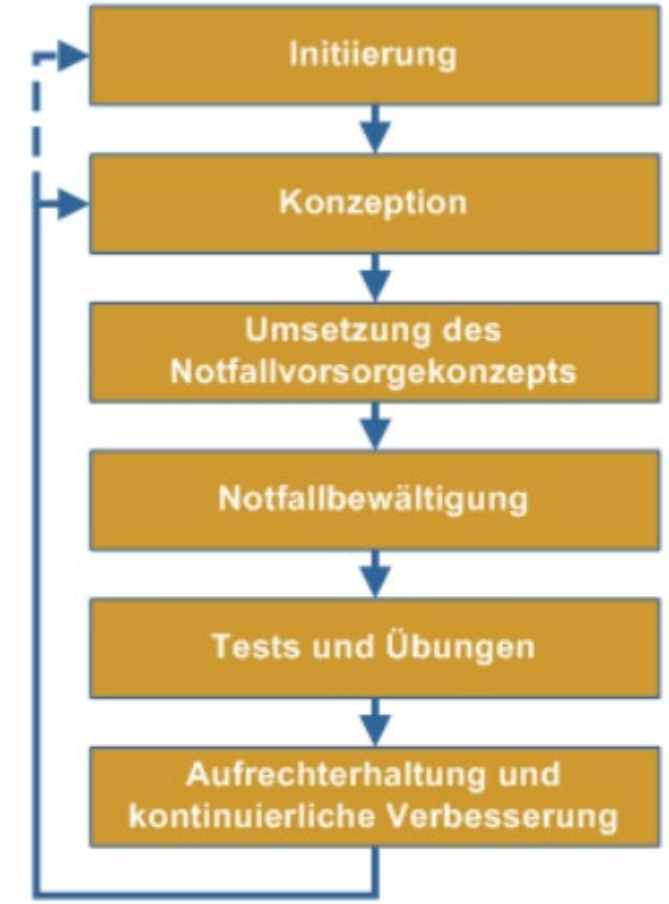
3. **Umsetzung des Notfallvorsorgekonzepts**
   Prioritäten für die Umsetzung der Notfallvorsorgekonzepte werden gesetzt, Ressourcen bereitgestellt, Verantwortlichkeiten festgelegt und gegebenenfalls erforderliche begleitende Maßnahmen identifiziert.



Notfallmanagement-Prozess gemäß BSI-Standard 100-4

Notfallmanagement

4. **Notfallbewältigung**
   Verantwortlichkeiten, Pläne und Verhaltensregeln für die Reaktion auf und das Handeln in Notfallsituationen werden in einem Notfallplan geregelt.
5. **Tests und Übungen**
   Notfallvorsorgekonzepte und Notfallpläne werden getestet und eingeübt, um mögliche Mängel zu identifizieren und das Verhalten im Notfall zu trainieren.
6. **Aufrechterhaltung und kontinuierliche Verbesserung**
   Angemessenheit und Wirksamkeit der Konzepte und Maßnahmen werden regelmäßig geprüft. Zusammen mit einer Auswertung der Ergebnisse der Tests und Übungen tragen diese Prüfungen zur kontinuierlichen Weiterentwicklung des Notfallmanagement-Prozesses bei.



Notfallmanagement-Prozess gemäß BSI-Standard 100-4

Was tun, wenn die Situation unbekannt ist?

FOR-DEC eine strukturierte Entscheidungsfindung die in der Luftfahrt angewendet wird und vom Deutschen Zentrum für Luft- und Raumfahrt (DLR) entwickelt wurde

Facts	Welche Situation liegt vor?
Options	Welche Handlungsoptionen bieten sich an?
Risks & Benefits	Welche Risiken und Nutzen sind mit den jeweiligen Handlungsoptionen verbunden?
-	
Decision	Welche Handlungsoption wird gewählt?
Execution	Ausführung der gewählten Handlungsoption.
Check	Führt der eingeschlagene Weg zum gewünschten Ziel?

Notfallmanagement

FOR-DEC

•Schritte die zur Entscheidungsfindung führen:

- Facts - Fakten
  - Situationsanalyse, Sammlung von Fakten zur Lage
  - Welche Situation liegt vor?
  - Was ist passiert, und welche Ressourcen, stehen aktuell zur Verfügung?
- Options - Möglichkeiten
  - Entwicklung von Handlungsmöglichkeiten
  - Welche Möglichkeiten sind gegeben?
  - Welche Optionen bieten sich an?
- Risks and Benefits - Gefahren und Chancen
  - Auswahl der Option mit geringstem Risiko und höchster Erfolgsaussicht
  - Welche Risiken und Nutzen sind mit den jeweiligen Handlungsoptionen verbunden?
- -
  - trennt die Phasen der Situationsanalyse vom restlichen Entscheidungsprozeß
- Decision - Entscheidung
  - Auswahl der Option mit geringstem Risiko und höchster Erfolgsaussicht
  - Welche Handlungsoption wird gewählt?
- Execution - Ausführung
  - Konkrete Zuteilung der Aufgaben und Verantwortlichkeiten
  - Wer macht was, wann und wie?
  - Wie wird die Entscheidung umgesetzt?
- Check - Überprüfung
  - Haben sich die Dinge wie erwartet entwickelt?
  - Passen die getroffenen Entscheidungen zur aktuellen Entwicklung?
  - Ist eine Situation eingetreten, die eine Änderung des Planes erzwingt?
  - Führt der eingeschlagene Weg zum gewünschten Ziel?

Quelle: san-erlangen.de

FOR-DEC

Der Bindestrich "-" trennt die Phasen der Situationsanalyse vom restlichen Entscheidungsprozess.

Er symbolisiert quasi einen kurzen Moment des Innehaltens, bevor die favorisierte Option umgesetzt wird.

Dieser Moment kann in Situationen, in denen es auf eine sehr präzise Situationsdiagnose ankommt, verhindern, dass durch Hektik oder starke Vorannahmen (s. u.) wichtige Elemente übersehen werden.

Notfallmanagement

- Wenn in zeitkritischen Situationen Handlungsdruck vorliegt, sollte zunächst eine Option gewählt werden, die di möglichst weitere Zeitreserven bringt.
- Sofortmaßnahmen müssen umgehend ergriffen werden.
- Aktuell findet FOR-DEC hauptsächlich im Luftverkehr und in der Medizin Anwendung (Lehrmeinung).
- Das Prinzip der strukturierten Entscheidungsfindung ist universell anwendbar.

(Quelle Wikipedia)

Ihre Fragen?

Ihre Wünsche?