Zentrale Schritte zur Vorbereitung auf mögliche Cyber-Angriffe
Ein Überblick

Malte Dreyer

Humboldt-Universität zu Berlin

Handreichung zur Vorbereitung auf Informationssicherheitsvorfälle

Herausgegeben durch den ZKI e.V.
Arbeitskreis Strategie und Organisation

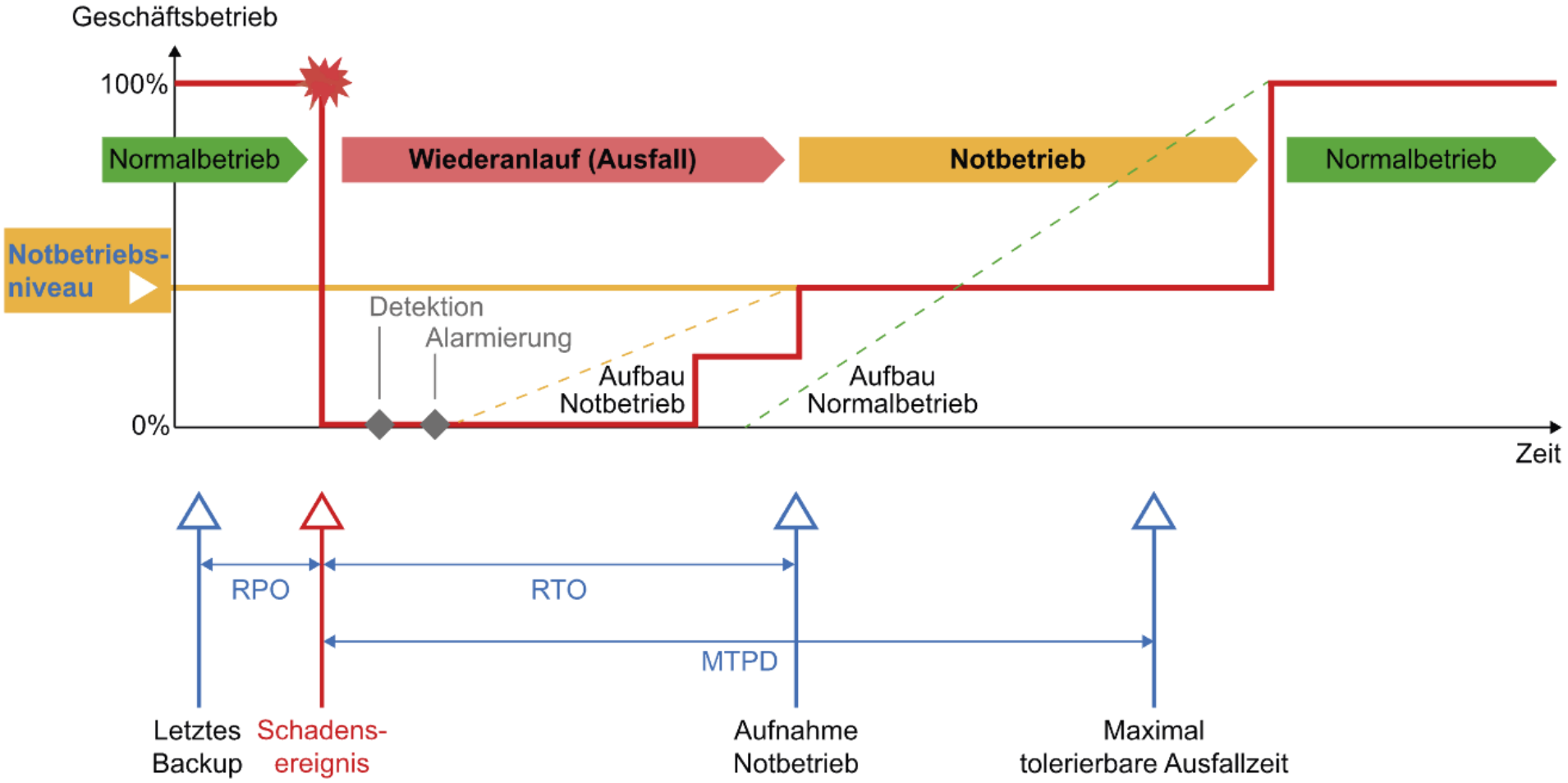
ZKI
Zentren für Kommunikation und Informationsverarbeitung e.V.

https://zenodo.org/records/10130339

Einfach umzusetzende Maßnahmen mit großer Wirkung

- Phasen eines IT-Notfalls
- Zeitpunkt des Vorfalls
- Mehrstufiger Krisenstab und Meldeketten (Leitung, Kommunikation, IT)
- Klare Steuerung im Falle eines Vorfalls
- Vertrag mit Incident-Response-Dienstleister
- Externe IT-Ressourcen
- Website der Hochschule für den Notfall
- Trennung vom Internet
- IT-Assetmanagement
- Isolation von Netzsegmenten
- Prioritäten für die IT-Dienste
- Wiederaufsetzplan für Rückkehr zum Normalbetrieb
- Wiederanlauf in den Notbetrieb
- Vergabe neuer Passwörter
- Belastungen für die Beschäftigten

Phasen eines IT-Notfalls



RPO (Recovery Point Objective): beschreibt die Zeitspanne, in der Daten nicht wiederherstellbar sind.
RTO (Recovery Time Objective): beschreibt die Zeitspanne, bis ein Prozess sein Notbetriebsniveau erreicht hat.
MTPD (Maximum Tolerable Period of Disruption): ist die vom Prozess-Verantwortlichen festgelegte, maximal tolerierbare Ausfalldauer dieses Prozesses, bis ein nicht-tolerierbarer Schaden auftritt.

Zeitpunkt des Vorfalls – Unterschiedliche „Jahreszeiten“

- direkt vor oder während der Bewerbungsphase
- direkt vor oder während der Prüfungsphase
- während des Semesters

TO DO: Diskutieren Sie intern die Auswirkungen der unterschiedlichen Zeitpunkte im akademischen Jahr, um die verschiedenen Effekte deutlicher zu identifizieren.

Mehrstufiger Krisenstab

- Krisenstab IT – zur Abstimmung der IT-bezogenen Themen
- Krisenstab Leitung – zur Abstimmung mit der Hochschulleitung
- Team/Krisenstab Kommunikation – für eine gut abgestimmte und gesteuerte Kommunikation der Effekte des IT-Notfalls

- Kommunikation über vorabgestimmte Textbausteine, auch für den Support

TO DO: Etablieren Sie drei Krisenstäbe, testen Sie deren Funktionsfähigkeit und achten Sie darauf, ob alle Status-Gruppen intern und extern adressiert werden.

Klare Steuerung im Notfall

- „Kapitän:in an Deck“
- ToDo-Listen und Rückmeldungen zu jedem Eintrag
- Steuerung z.B. durch
  - 2 Teamleitungen
  - 2 Abteilungsleitungen
  - CISO/IT-Sibe und Abteilungsleitung
- Zentraler Kommunikationskanal – eher mehr Teilnehmende

TODO: Besprechen Sie vorab, wie eine Steuerung und Statuserhebung umgesetzt werden kann und welche Personen dafür infrage komme.

Vertrag mit Incident-Response-Dienstleister

- Externe Unterstützung kann die Abarbeitung professionalisieren
  - Analysiert Spuren und betreibt Forensik
  - Unterstützt dabei, Schäden zu begrenzen
  - Ist erfahren bei den Handlungsnotwendigkeiten
- Onboarding kostet Zeit bei den Beschäftigten und offenbart ggf. Lücken in der Dokumentation
- Jeder Einsatz kostet, z.B. 2200€ pro Einsatztag zzgl. MwSt.

TO DO: Schließen Sie einen Incident-Response-Vertrag und betreiben Sie das Onboarding mit der nötigen Zeit und Aufmerksamkeit.

Externe IT-Ressourcen

- Welche Kriterien gibt es für externe Dienstleister?
  - Technische Anschlussfähigkeit
- Längerfristige Beschaffungen vorbereiten
- Ggf. auch Einbeziehung von externem Fachpersonal
  - Ggf. in Kooperation mit anderen Hochschulen

TO DO: Beschaffen Sie rechtzeitig externe IT-Kapazitäten.

Website der Hochschule für den Notfall

- Notfallwebsites werden gezielt angegriffen
  - Ihr Dienstleister muss hiervon wissen und darauf vorbereitet sein
  - Traffic Limits, Bandbreiten, DDOS-Schutz
- Technischen Rahmen klären
- Übertragung CD/Look-n-Feel vorbereiten
- Wer pflegt und wie erhält man Zugriff?

TO DO: Klären und testen Sie, wo und wie Sie eine Notfallwebsite betreiben und pflegen.

Trennung vom Internet

- Zur Schadenseindämmung
- Oft ist dies bei größeren Einrichtungen nicht nur „ein Stecker“
- Reaktionen auf den Vorfall dürfen Problem nicht verschlimmern
  - Auswirkungen vorab durchspielen

TO DO: Prüfen und dokumentieren Sie, was eine Trennung vom Internet für Ihre IT-Strukturen bedeutet und wie diese durchzuführen ist.

IT-Assetmanagement

- Wie sind diese Daten im Notfall erreichbar?
- Welche Arten von Assets sind hier relevant?
  - Räume
  - Racks
  - Server
  - Geräte / Appliances
  - Netzwerkgeräte
  - Dienste
  - IP-Adressen und Netze

ToDo: Verschaffen Sie sich einen Überlick zum Stand des IT-Assetmanagements an der Einrichtung und prüfen Sie stichprobenartig, wie umfangreich und aktuelle die Daten gepflegt sind.

Isolation von Netzsegmenten

- Einzelne Bereiche isolieren, um Ausbreitung zu verhindern
  - Institute
  - Fakultäten
  - Häuser
  - Räume
  - Racks
  - Cluster

TO DO: Prüfen und dokumentieren Sie die Strukturen und Steuerungsprozesse der Netzwerksegmentierung Ihrer IT-Strukturen.

Wiederaufsetzplan für Rückkehr zum Normalbetrieb

- Welche Dokumentation gibt es, um IT-Infrastruktur und –dienste von Grund auf neu aufzubauen?
- Risiken müssen vorab erkundet werden
- Aufbau geschieht parallel zur alten Struktur
  - Dokumentation darf nicht auf später aufgeschoben werden
  - Zielarchitektur für Neuaufbau muss beschrieben und diskutiert sein
  - Bestehende Struktur trotz Zeitdruck reflektieren

TO DO: Entwickeln Sie Pläne und dokumentieren Sie diese, um die Verfügbarkeit von unkompromittierter Infrastruktur zur Administration sicherzustellen.

Prioritäten für die IT-Dienste

- Welche Dienste sind wichtig?
- Nicht zu viele Prioritäten (1-4)
- Abstimmung zwischen IT und Hochschulleitung
- Diese Festlegungen sparen im Fall der Fälle Zeit
  - Und sind auch allgemein für die Bewertung des Dienstportfolios wichtig

TO DO: Erstellen Sie eine Tabelle mit Prioritäten oder Prioritätenklassen für die Bereitstellung von Diensten nach einem Notfall und stimmen Sie diese zwischen IT-Zentrum und Hochschulleitung ab.

Wiederanlauf in den Notbetrieb

- Wie definieren Sie „Notbetrieb“?
- Welche Dienste zählen Sie dazu?
- Notbetrieb ist nicht „Normalbetrieb“
  - Welche Dienste sind für eine basale Funktionsfähigkeit erforderlich?

TO DO: Entwickeln und dokumentieren Sie das gewünschte Niveau für den Notbetrieb.

Vergabe neuer Passwörter

- Ggf. müssen alle Beschäftigen und Studierenden mit neuen Passwörtern versorgt werden
  - Welche Dienstleister können bei Druck und Versand helfen?
  - Ausführung durchspielen

TO DO: Gestalten und prüfen Sie einen Prozess zur Vergabe und Ausgabe neuer Passwörter.

Belastungen für die Beschäftigten

- Auf Belastungen von Beginn an achten
- „Nachtschichten“ helfen nicht, denn es ist eher ein Marathon
- Stress vermeiden
- Auf Frustration bei den Beschäftigten reagieren
- Berichtet wurde auch von Angstzuständen, Panikattacken, Gewichtsverlust, Kündigungen
- **Verlust von Beschäftigten in diesen Phasen ist Ihr größtes Risiko**

TO DO: Führen Sie sich bereits vorab vor Augen, welche Belastungen durch solche Notfälle für die Beschäftigten entstehen, und bereiten Sie entsprechende Maßnahmen vor.

Vielen Dank

dreyer@hu-berlin.de