Handreichung zur Vorbereitung auf Informationssicherheitsvorfälle

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

Zentren für
Kommunikation und
Informationsverarbeitung e.V.

Inhalt

Autoren

Malte Dreyer,
Humboldt-Universität zu Berlin

Dr. Frank Kühnlenz,
Humboldt-Universität zu Berlin

Bernhard Brandel,
Katholische Universität Eichstätt

ZKI e.V. unterstützt durch den Vorstand (Torsten Prill – Freie Universität Berlin) und den Arbeitskreis Strategie und Organisation

Zielsetzung der Handreichung

Diese Handreichung soll Hochschul- und IT-Leitungen mit konkreten Handlungsempfehlungen dabei unterstützen, sich besser auf IT-Sicherheitsvorfälle vorzubereiten. Sie zielt dabei im Kern nicht auf die systematische Erhöhung der Reife des Informationssicherheitsmanagementsystems (ISMS), wie sie an den meisten Hochschulen bereits durch Informations- bzw. IT-Sicherheitsbeauftragte adressiert wird.

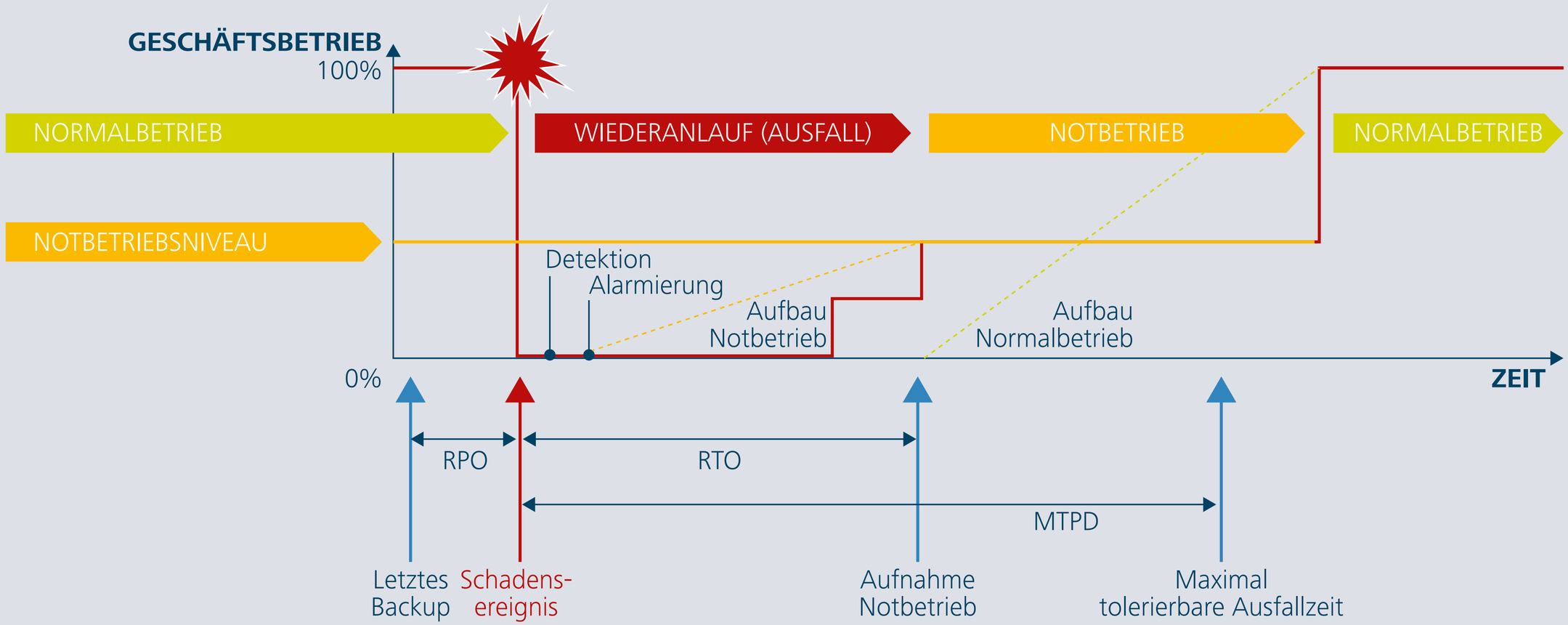
Sie zeigt vielmehr kurzfristige Handlungspunkte mit signifikanter Wirkung auf, die sukzessive durch die Leitung bearbeitet werden können, um einen Einstieg in ein systematisches Notfallmanagement zu ermöglichen.

Hintergrund

Ein Notfall im Fokus der hier beschriebenen Handreichung ist ein Schadensereignis, bei dem IT-gestützte Prozesse oder Ressourcen der Institution nicht wie vorgesehen funktionieren, wie bspw. nach einem erfolgreichen Angriff auf die IT-Infrastruktur. Die Verfügbarkeit der entsprechenden Prozesse oder Ressourcen kann innerhalb einer im normalen Betrieb üblichen Zeit nicht wiederhergestellt werden.

Der Geschäftsbetrieb ist stark beeinträchtigt bzw. überwiegend nicht mehr möglich. Es entstehen beträchtliche bis existenzbedrohende Schäden, die sich signifikant und in nicht akzeptablem Rahmen auf den Haushalt oder die Aufgabenerfüllung auswirken. (IT-)Notfälle können nicht mehr im allgemeinen Tagesgeschäft abgewickelt werden, sondern erfordern eine gesonderte Notfallbewältigungsorganisation.

Phasen eines IT-Notfalls



RPO (Recovery Point Objective)	beschreibt die Zeitspanne, in der Dateien 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 Prozessverantwortlichen festgelegte, maximal tolerierbare Ausfallsdauer dieses Prozesses, bis ein nicht tollerierbarer Schaden auftritt.

Phasen eines IT-Notfalls mit Erläuterung wichtiger Kenngrößen (MTPD, RTO, RPO, Notbetriebsniveau)

Erläuterung zur Illustration

Sobald das Schadensereignis eintritt, endet der Normalbetrieb und wird auf ein besorgniserregendes, undefiniertes Niveau des normalen Geschäftsbetriebs reduziert. Erst mit der Detektion des Schadensereignisses und der anschließenden Alarmierung (siehe Abschnitt „Mehrstufiger Krisenstab und Meldeketten“) beginnt eine Reaktion der Hochschule, um die Kontrolle zurückzugewinnen und Maßnahmen zum Wiederanlauf einzuleiten, die einen definierten Notbetrieb herstellen. Verzögert, aber parallel beginnt die Wiederherstellung des Normalbetriebs.

Zeitpunkt des Vorfalls

Für eine angemessene Einordnung des Vorfalls ist der genaue Zeitpunkt im akademischen Jahr von Bedeutung. Hier sind drei Zeitbereiche zu unterscheiden:

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

Je nach Zeitpunkt sind unterschiedliche Schwerpunkte für die ersten Reaktionen zu legen und auch leicht unterschiedliche Personenkreise zu etablieren. Vor der Bewerbungsphase ist ein Schwerpunkt auf die Kommunikation und die Systeme zur Ermöglichung von Bewerbungen und Einschreibung zu setzen. Während der Prüfungsphase liegt ein zusätzlicher Schwerpunkt auf der sorgfältigen Kommunikation mit den Studierenden und der Bereitstellung entsprechender Systeme. Während des Semesters ist der Semesterbetrieb bestmöglich zu unterstützen.

Angriffe werden häufig erst durch bestimmte finale Aktionen der Akteure bemerkt, deren Ziel es ist, möglichst viel Druck auf die Angegriffenen aufzubauen. Solche Aktionen finden daher oft an Wochenenden, Feiertagen und Ferienzeiten statt. Sie orientieren sich zudem an der Situation der Angegriffenen – somit könnten diese Aktionen auch zu besonders kritischen Zeiten des Hochschuljahres stattfinden.

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

Weiterführend: BSI: 7.1.2 Festlegung der BIA-Parameter und betrachteten Zeithorizonte (Business Continuity Management, BSI-Standard 200-4)

Mehrstufiger Krisenstab und Meldeketten

(Leitung, Kommunikation, IT)

Im Laufe der Reaktion auf IT-Sicherheitsvorfälle müssen unterschiedliche Personengruppen informiert und für Entscheidungen einbezogen werden. Zusätzlich ist eine gesteuerte Kommunikation nach außen notwendig. Für diese Zwecke werden meist mehrere Krisenstäbe eingerichtet.

Das Hauptziel bei der Etablierung von Krisenstäben ist eine hohe Effizienz der Abstimmungsprozesse und die Freihaltung größtmöglicher Arbeitskapazität für diejenigen, die an der Wiederherstellung der IT-Dienste arbeiten.

Krisenstäbe müssen schwierige Entscheidungen zeitnah auf Basis unvollständiger Informationen innerhalb eines dynamischen Angriffsgeschehens treffen. Es ist während eines IT-Notfalls damit zu rechnen, dass die Angreifer kontinuierlich Maßnahmen ergreifen, um den Leidensdruck zum Erreichen ihrer Forderungen zu erhöhen.

Die Erfahrungen der Hochschulen zeigen, dass die Einrichtung von drei Krisenstäben empfehlenswert ist:

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

Die Teilnehmenden dieser Stäbe überlappen sich hierbei teilweise und werden mindestens durch die Teilnahme des IT-Sicherheitsbeauftragten/CISO und der IT-Leitung an allen Stäben koordiniert. Auch die Einbeziehung des Datenschutzes und möglichst aller Status-Gruppen, inkl. der Studierenden, sollte sichergestellt sein.

Die Teilnehmenden der Krisenstäbe müssen vorab bestimmt und auch für den Fall erreichbar sein, dass die IT-Infrastruktur der Hochschule nicht mehr in Betrieb ist. Hierfür sind Lösungen außerhalb der Hochschule zu organisieren, zu etablieren und einzuüben, wie z.B. externe Messenger-Gruppen (bspw. in Signal oder Threema) oder zumindest die Verteilung (und Aktualisierung) der benötigten Telefonnummern der Teilnehmenden der Krisenstäbe. Krisenstäbe müssen insbesondere auch außerhalb der regulären Arbeitszeiten tätig werden. Darauf müssen die Teilnehmenden vorbereitet sein.

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

Weiterführend: BSI: 13.3 Erstellung einer Jahresübungsplanung (Business Continuity Management, BSI-Standard 200-4)

1 Zielgruppen sind vielfältig, intern und extern, z.B. Mitarbeitende (in besonderen Positionen), Stellenbewerber:innen, Studierende, Studienbewerber:innen, Partner (Dienstleister, Kooperationen, Verbünde, Hochschule als Service-Provider), offizielle Stellen (Aufsichtsbehörden, Landesdatenschutz, Polizei, BSI) usw.

Externe IT-Ressourcen

Für den Fall der Fälle sollte unbelastete IT-Kapazität bereitstehen. Hierzu empfiehlt es sich, bereits vorab entsprechende längerfristige Kapazitäten auszuschreiben, um einzelne Dienste unabhängig von der kompromittierten eigenen Infrastruktur aufsetzen zu können. Auch ein Modell des Austauschs mit anderen Hochschulen kann in Betracht gezogen werden, wird jedoch von vielen Hochschulen aufgrund der möglichen Wechselwirkungen eher kritisch gesehen. Möglicherweise kann jedoch Fachpersonal temporär zur Verfügung gestellt werden, ohne selbst in die Schusslinie der Angreifer zu geraten.

TO DO: Beschaffen Sie rechtzeitig externe IT-Kapazitäten.

Website der Hochschule für den Notfall

Bei Informationssicherheitsvorfällen ist eine zeitnahe und umfassende Information unerlässlich. Die Notfallwebsite ist dabei das zentrale Kommunikationsmedium. Hierfür gilt es, Technologien, Design und Pflegemodelle vorab bereits abzustimmen und zu testen. Oftmals wird eine Notfallwebsite gezielt attackiert (z.B. Denial of Service), um den Leidensdruck zu erhöhen, sodass zusätzliche Absicherungen notwendig sind.

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

Vertrag mit Incident-Response-Dienstleister

Im Notfall benötigen Sie externe Unterstützung, um die Angriffe zu analysieren, Spuren zu sichern und die Schäden möglichst zu begrenzen. Hierfür gibt es eine Reihe von Dienstleistern, die „Incident Response"-Leistungen anbieten. Das BSI bietet hierfür eine Liste mit qualifizierten Dienstleistern an. Je mehr diese Dienstleister bereits vorab über Ihre Organisation wissen, desto effizienter können sie bei Notfällen Hilfe leisten. Deshalb sollte auch das Onboarding des Dienstleisters die notwendige Aufmerksamkeit bekommen. Je nach Komplexität der IT-Strukturen kann die Einführung auch größere Zeitanteile von mehreren Teams binden und sich über mehrere Monate erstrecken.

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

Weiterführend: BSI: Liste der qualifizierten APT-Response-Dienstleister

Trennung vom Internet

Eine komplette temporäre Trennung des Netzwerkes vom Internet ist zur Schadenseindämmung und -bewertung bei großen IT-Notfällen häufig geboten. Dabei soll jegliche Kommunikation von außen nach innen, aber auch von innen nach außen unterbunden werden. Diese Maßnahme muss insbesondere kommunikativ begleitet werden, denn sie erzeugt große Aufmerksamkeit bei allen Zielgruppen.

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

Isolation von Netzsegmenten

Bei Vorfällen, die nicht die gesamte IT-Struktur betreffen, werden einzelne Teile bzw. Segmente abgeschottet, z.B. eine Fakultät oder ein Netz für Geräte, um eine Ausbreitung über Netzgrenzen hinweg zu verhindern.

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

Weiterführend: BSI: Netzwerkarchitektur und -design (2023)

Wiederaufsetzplan für Rückkehr zum Normalbetrieb

Was kann vorbereitet werden, um die gesamte IT-Infrastruktur ggf. von Grund auf neu aufzubauen? Welche Kernkomponenten gibt es dafür zu berücksichtigen? Typischerweise wird neue Infrastruktur parallel zur bestehenden aufgebaut. Teile der alten Infrastruktur können nur übernommen werden, wenn das Risiko IT-forensisch, z.B. durch den Incident-Response-Dienstleister, geklärt wurde.

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

Weiterführend: BSI: Wiederanlaufparameter bestimmen

Wiederanlauf in den Notbetrieb

Der Wiederanlauf beschreibt alle Maßnahmen, um strukturiert in einen vorab geregelten Notbetrieb wechseln zu können. Er beschreibt nicht die Wiederherstellung eines Normalbetriebs. Hierfür muss ein Notbetriebsniveau für IT-Dienste definiert werden, die als grundlegend für einen Notbetrieb gesehen werden, wie z.B. die Betriebsfähigkeit des Netzwerkes, von Telefonen oder E-Mails.

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

Vergabe neuer Passwörter

Ab einem bestimmten Grad der Kompromittierung ist die Vergabe neuer Passwörter an alle rechtmäßigen Account-Inhaber:innen notwendig. Alle kompromittierten Accounts sind somit zu sperren. Die initiale Vergabe neuer Passwörter, deren Ausgabe und Versand danach stellen in vielerlei Hinsicht eine große Herausforderung dar, insbesondere auch aufgrund der ggf. hohen Anzahl von Personen. Es empfiehlt sich deshalb, Rahmenbedingungen und die konkrete Ausführung eines solchen Prozesses bereits vorab zu klären und konkrete Verfahren bzw. auch Dienstleister auszuwählen.

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

Prioritäten für die IT-Dienste

Das Wiederaufsetzen einer komplexen IT-Struktur, wie sie Hochschulen üblicherweise betreiben, benötigt Zeit und Ressourcen. Deshalb sollte bereits vorab klar sein, in welcher Reihenfolge bzw. mit welchen Prioritäten einzelne Dienste oder Kategorien von Diensten versehen werden. Die Festlegung einer solchen Prioritätenliste geschieht in enger Abstimmung zwischen IT-Zentrum und Hochschulleitung.

Nicht jeder Dienst benötigt einen Notbetrieb: Eine Reduzierung auf das Wesentliche ermöglicht schnelleres Handeln mit den begrenzten Ressourcen. Neben den Prioritäten für den Wiederanlauf in den Notbetrieb sollten gleichzeitig Prioritäten für die Wiederherstellung des Normalbetriebs definiert werden.

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.

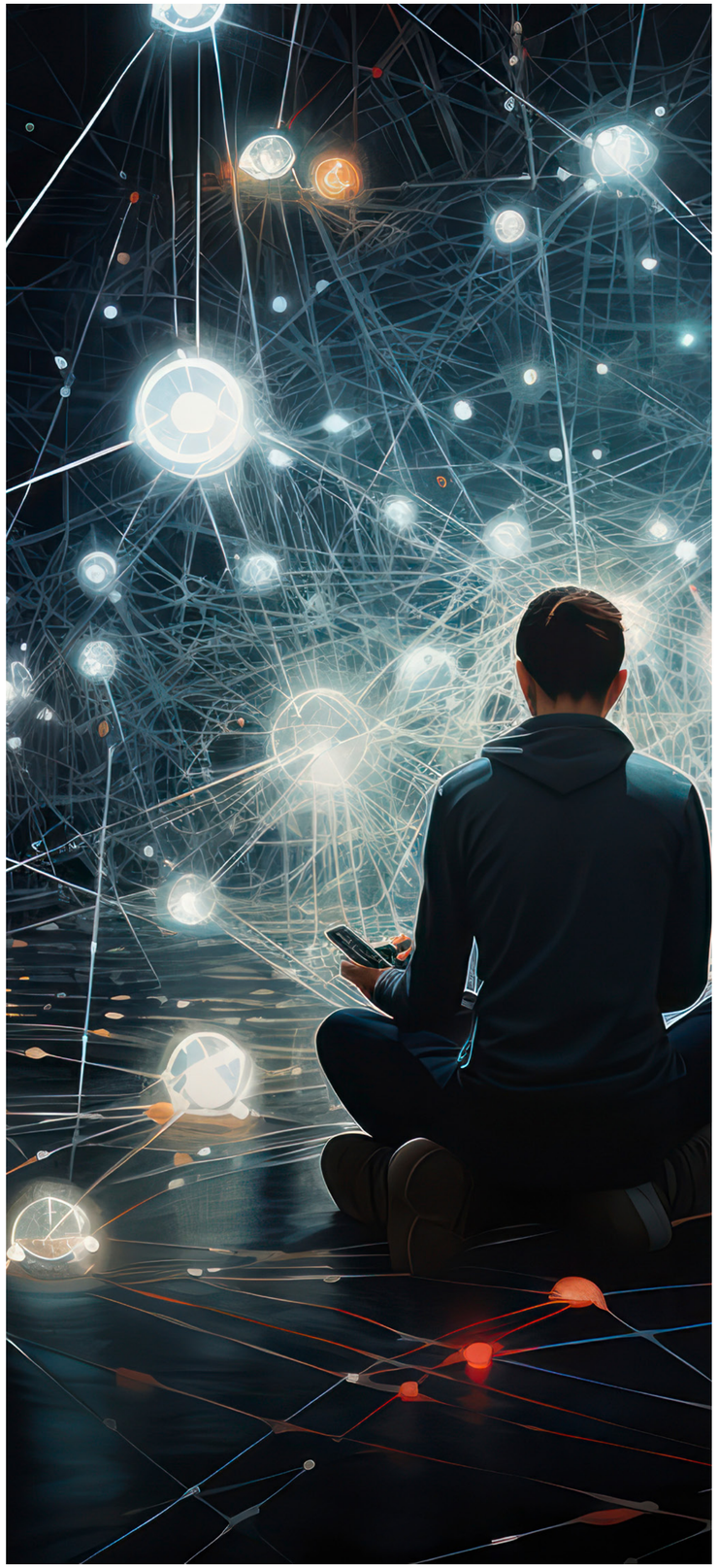
Weiterführend: BSI: Geschäftsprozesse priorisieren

Belastungen für die Beschäftigten

Notfälle der hier beschriebenen Größenordnung sind eine ungewöhnlich hohe Belastung für die beteiligten Mitarbeitenden. Diese Belastungen dauern meist mehrere Monate nach Eintreten des Schadensereignisses an. Sie entstehen z.B. durch den hohen Zeitdruck oder auch wenn Beschäftigte das Gefühl haben, an dem erfolgreichen Angriff eine Mitschuld zu tragen. Mitarbeitende sind nicht selten eng verbunden mit bspw. den durch sie betreuten IT-Diensten und finden sich somit in einer zusätzlich belastenden Stresssituation wieder.

Aufgrund der Fürsorgepflicht des Arbeitgebers gegenüber seinen Mitarbeitenden sollte in solch einer Notfallsituation eine besondere Aufmerksamkeit auf der Anerkennung und dem Erhalt der Arbeitskraft liegen. Hierbei können bereits einfache Maßnahmen höchst wirkungsvoll sein, wie bspw. regelmäßiges Essen anzubieten, auf Pausenzeiten zu achten und wertschätzend zu agieren. Möglicherweise klingt dies ungewöhnlich in einer Notsituation – tatsächlich ist es aber von großer Bedeutung: Eines der größten Risiken im Notfall ist der Ausfall von Schlüsselpersonal.

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



Weitere Quellen

- **BSI: Ersthilfe/Linksammlung**
  https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Unternehmen/unternehmen.html?nn=133680&cms_pos=1

- **BSI: Erste Hilfe bei einem schweren IT-Sicherheitsvorfall**
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware_Erste-Hilfe-IT-Sicherheitsvorfall.pdf?__blob=publicationFile&v=3

- **BSI: Qualifizierte APT-Response-Dienstleister**
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.pdf?__blob=publicationFile&v=16

- **BSI-Standard 200-4 Business Continuity Management (BCM)**
  https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-200-4-Business-Continuity-Management/bsi-standard-200-4_Business_Continuity_Management_node.html

- **BSI: Qualifizierte DDoS-Mitigation-Dienstleister**
  https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister-DDos-Mitigation-Liste.pdf?__blob=publicationFile&v=5

- **DFN.Security (im Aufbau): Mehr als DoS-Basisschutz und DFN-CERT**
  https://www.dfn.de/dfn-security-ein-dach-fuer-it-sicherheit/