Datensicherung.nrw - Maßnahmen zur Wiederherstellung nach einem Datenverlust

25.08.2023

Ein Kooperationsvorhaben der
DIGITALE HOCHSCHULE NRW

Gefördert durch
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

Ein Kooperationsvorhaben der
DIGITALE HOCHSCHULE NRW
Gefördert durch
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

1. Präambel

Der im Rahmen von Datensicherung.nrw aufgebaute Service erlaubt es den Hochschulen in Nordrhein-Westfalen (NRW), ihre Datenbestände geographisch und organisatorisch getrennt zu sichern und bei Bedarf wiederherzustellen.

Während das Backup von Systemen die notwendige Voraussetzung für die Wiederherstellung der Datenbestände ist, sind für die verlässliche Wiederaufnahme des Hochschulbetriebs nach einem IT-Notfall je nach Größe, Grad und Art des IT-Notfalls weitere Vorbereitungen notwendig.

Die Arbeitsgruppe „Restore and Disaster Recovery“ hat sich mit diesen vorzubereitenden Maßnahmen aus verschiedenen Perspektiven auseinandergesetzt und die vorliegende Handreichung zusammengestellt. Diese dient als Orientierungshilfe ohne Anspruch auf Vollständigkeit. Auszugestalten ist dieses Dokument jeweils individuell durch die Hochschulen, sowohl was die technischen und infrastrukturellen Voraussetzungen betrifft als auch die notwendigen organisatorischen Vorbereitungen.

1.1. Definition Notfallplan

In einem Notfallplan werden alle denkbaren Vorbereitungen zur Wiederherstellung des Betriebs nach einem IT-Notfall in einer Einrichtung festgehalten mit dem Ziel, die Ausfallzeiten nach einem IT-Notfall so gering wie möglich zu halten. Im Hochschulkontext bedeutet dies unter anderem aus den bisherigen Erfahrungen von anderen Hochschulen zu lernen und vorbereitet zu sein. Hinsichtlich der IT-Notfälle, die potenziell Hochschulen betreffen können, werden hier mögliche Schadfall-Szenarien exemplarisch unterschieden. Diese Unterscheidung ist für die konkrete Umsetzung der Wiederaufnahmemaßnahmen maßgeblich, um auf die unterschiedlichen Umstände adäquat eingehen zu können.

1.2. Definition und Arten von Schadfällen

Mit Blick auf die Verfügbarkeit von IT-Services unterscheiden sich die unterschiedlichen Schadfälle vor allem dadurch, ob im Anschluss an das eigentliche Schadensereignis die betroffene Infrastruktur vorhanden und zeitnah nutzbar ist oder nicht.

1.2.1. Physische Zerstörung

Um sich vor physischer Zerstörung im Kontext IT-Infrastruktur zu schützen, ist es notwendig die Gefahren durch physische Einwirkung auf die entsprechenden IT-Systeme zu identifizieren und möglichst abzuwehren. Dabei sind die Möglichkeiten zum Schutz vielfältig -von speziell geschützten Zugängen und Serverräumen bis hin zu standortredundant aufgestellten Systemen ist vieles möglich. Wichtig dabei ist es, die potenziellen Gefahren zu identifizieren und entsprechende Maßnahmen zu ergreifen. Da die Integrität der gesicherten Daten nicht verletzt wird, liegt der Fokus hier auf Wiederaufbau und Inbetriebnahme einer geeigneten Ersatz-Infrastruktur.

1.2.2. Stromausfall

Ein Stromausfall ist eine plötzliche Unterbrechung der Stromversorgung im Rechenzentrum oder einer IT-Infrastruktur. In solchen Fällen besteht die Gefahr eines Datenverlusts, einer Datenbeschädigung oder sogar einer Beschädigung der HW-Komponenten der IT-Infrastruktur. Darüber hinaus kann davon ausgegangen werden, dass nach der Wiederherstellung der Stromversorgung die IT- wie auch die Gebäudeinfrastruktur unversehrt zur Verfügung stehen. Hier nicht betrachtet wird eine geplante Stromabschaltung, da durch geeignete Vorbereitungen die Gefahr eines Datenverlustes sehr stark minimiert werden kann.

Ein Kooperationsvorhaben der
DIGITALE HOCHSCHULE NRW

Gefördert durch
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

1.2.3. Cyber-Angriff

Bei einem Cyber-Angriff versucht der Angreifer, Zugriff auf Datenbestände der angegriffenen Organisation zu erlangen. Die Schäden, die durch Ausspähung von Daten entstehen, sind nicht Gegenstand dieser Handreichung. Das derzeit verbreitete Angriffsmuster besteht in der Verschlüsselung von Datenbeständen und damit der Blockade aller betroffenen IT-Services, was wiederum weite Bereiche aller Geschäftsbereiche einer Hochschule betrifft. Das Ziel der Angreifer ist es, für die Herausgabe des Schlüssels ein Lösegeld zu erpressen. Die Folgen eines solchen Angriffs werden wesentlich abgemildert, sofern die Sicherungsdaten nicht selbst verschlüsselt werden konnten.

1.3. Einsatz von Notfallplänen

Notfallpläne erstellen und aktualisieren

Der Einsatz eines Notfallplans kann nur dann effektiv und effizient sein, wenn er vor dem Ernstfall erstellt wird. Dazu gehört, dass im Idealfall alle möglichen Szenarien abgedeckt werden. Aus diesem Grund sind die oben aufgeführten Schadfälle angeführt worden. Dazu gehören auch eine Liste aller betriebskritischer Systeme und Anwendungen sowie organisatorische Prozesse, Zuständigkeiten und Kontakte der Mitarbeitenden, die im Notfall involviert sein werden. Eine solche Liste muss regelmäßig aktualisiert werden.

Um im Ernstfall schnell und angemessen auf eine Krise reagieren zu können, ist ein im Vorfeld gut ausgearbeiteter Notfallplan nützlich, um den betrieblichen Schaden einzudämmen. Die Entwicklung eines Notfallplans ist eine gute Gelegenheit, Entscheidungen zu treffen und diese mit den Stakeholdern entsprechend abzustimmen, um sich im Ernstfall auf die Wiederherstellung der Betriebsbereitschaft fokussieren zu können.

Folgende Aspekte sollte der Notfallplan enthalten:

- Das Notfallteam:
  Eine Gruppe aus Mitarbeitenden, Entscheidungstragenden, die im Ernstfall kooperieren und die verantwortlich für das Notfallmanagement sind.

- Gefährdungsanalyse:
  Antizipieren und identifizieren Sie die potenziellen Bedrohungen und die damit verbundenen Risiken für Ihren Betrieb. Bewerten Sie dabei nach Möglichkeit die potenziellen Auswirkungen der Schadenereignisse auf Ihre Einrichtung.

- Maßnahmenkatalog:
  Der vorliegende Leitfaden dient der Erstellung eines Maßnahmenkatalogs, aus dem die notwendigen Maßnahmen hervorgehen, um im Ernstfall systematisch, effizient und effektiv agieren zu können. Wichtig ist, dass absehbar notwendige Maßnahmen im Vorfeld festgelegt werden und turnusmäßig iteriert werden.

- Kommunikationsplan:
  In Kapitel zwei werden im Bereich der Organisation die Verantwortlichkeiten, Kommunikationssysteme, Handlungsbereiche, uvm. festgelegt. Wichtig ist, dass sich die Beteiligten auf Kommunikationskanäle und -Teams im Vorfeld festlegen, sodass bekannt ist, welche Mittel im Ernstfall genutzt werden.

- Datenwiederherstellung:

Ein Kooperationsvorhaben der
DIGITALE HOCHSCHULE NRW

Gefördert durch
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

Wesentlicher Bestandteil der Wiederaufnahme des Betriebs ist die Wiederherstellung kompromittierter oder verlorener Daten. Hier wird auf die Datensicherung zurückgegriffen. In Kapitel drei werden Abläufe, technische Voraussetzungen und Aktivierungen definiert. Darunter ist das Vorgehen zur Überprüfung der Datenintegrität ebenfalls festzulegen und ein wichtiger Schritt in der Wiederaufnahme der Betriebsfähigkeit.

Nach der Erstellung und finalen Iteration des Notfallplans sollten Mitarbeitende aller Abteilungen über die entsprechenden Maßnahmen und Regelungen informiert und geschult werden. Die Empfehlungen des BSI stellen einen guten Ansatz für einen solchen Notfallplan dar.

2. Vorbereitungen

2.1. Organisation

2.1.1. Verantwortlichkeiten

Definition derjenigen Personen, die für das Notfallmanagement die Verantwortung und Steuerung innehaben. Definieren Sie auf den unterschiedlichen Ebenen die entsprechenden Verantwortlichkeiten (bspw. Entscheidungstragende, Fachleute für die Wiederaufnahme des Betriebs, Kommunikation mit Externen, Kommunikation intern, uvm.).

2.1.2. Handlungsbereiche

Stecken Sie die Handlungs- und Verfügungsbereiche der Beteiligten ab. Gehen Sie dabei abteilungs-, dezernats- oder fakultätsweise vor. Wählen Sie zielgruppenorientiert oder nach Expertise die entsprechenden Handlungsbereiche der Beteiligten aus, sodass Personen in den jeweils definierten Handlungsbereichen eigenständig Entscheidungen im Ernstfall treffen können, um möglichst effizient zu agieren.

2.1.3. Akquise externer Dienstleister

Bestimmen Sie Personen, die mit der Akquise externer Dienstleister betraut werden. Diese externen Dienstleister sind in der Regel darauf spezialisiert Forensik und Wiederanlauf von Systemen, vor allem nach Cyberattacken wie Ransomware-Angriffen, so gesichert wie möglich durchzuführen. Die aus dem Notfallteam bestimmten Personen dienen vor, während und nach dem Ernstfall als dedizierte Ansprechpartner*innen für die externen Dienstleister.

2.2. Kommunikation

2.2.1. Kommunikationssysteme

Bestimmen Sie dedizierte Kommunikationskanäle und achten Sie bei der Wahl darauf, dass es sich um Kanäle handelt, die nicht an das Identitymanagement, Verzeichnisdienste oder ähnliche Systeme angebunden sind, da diese womöglich ebenfalls betroffen sein können. Es ist empfehlenswert, für diesen Zweck mit dem Einverständnis der Beteiligten des Notfallteams Rufnummern oder weitere Kontaktdaten außerhalb der eigenen IT-Infrastruktur zu verwenden. Definieren Sie diese Systeme unbedingt vor dem Ernstfall, um sicherzustellen, dass alle Beteiligten einander erreichen können.

2.2.2. Kommunikationsgruppen

Legen Sie fest, ob innerhalb des Notfallteams spezielle Kommunikationsgruppen notwendig sind. Entscheiden Sie, ob eine Unterscheidung zwischen externer und interner Kommunikation notwendig ist und wer für die Vermittlung verantwortlich ist und ggf. Entscheidungen treffen kann, um einen effizienten Informationsfluss zu gewährleisten.

Ein Kooperationsvorhaben der
DIGITALE HOCHSCHULE NRW

Gefördert durch
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

2.2.3. Prioritätenliste Kommunikation

Legen Sie nach Möglichkeit fest, welche Instanzen bzw. Stakeholder mit Priorität informiert werden. Es kann sinnvoll sein, je nach Verantwortlichkeit und Handlungsbereich die Kommunikationspartner aufzuteilen bzw. Ansprechpersonen zuzuordnen. Beachten Sie jedoch auch bei dieser Zuordnung auf Vertretungsregelungen und die Pflege bei Personalfluktuation, um sicherzustellen, dass der Kommunikationsfluss im Zweifel aufrecht erhalten bleibt.

2.3. Priorisierung

Für eine möglichst schnelle Wiederaufnahme des Dienstbetriebs ist es notwendig, eine Priorisierung vorzunehmen, die systematisch abgearbeitet werden kann.

2.3.1. Wiederherzustellende Services

Eine Betrachtung der Geschäftsprozesse ist notwendig, um zu identifizieren, auf welchen Systemen die IT-Services beruhen. Hierbei müssen auch Abhängigkeiten zwischen und zu anderen Services berücksichtigt werden.

2.3.2. Wiederherzustellende Systeme

3. Die zuvor identifizierten Services und die für den Betrieb dieser Services verantwortlichen Systeme sind mitsamt der notwendigen Datenbestände und Sicherungskopien zu benennen.

3.1. Technische Vorbereitungen

Der Dienstnehmer hat die technischen Vorbereitungen getroffen, um im Schadensfall (siehe Kapitel 1.2.) einen Wiederherstellungsprozess zu beginnen und die wiederhergestellten Daten in Betrieb zu nehmen.

3.1.1. Systembackup

Neben Anwendungsdaten enthalten viele Serversysteme auch spezifische Einstellungen für den Betrieb der Anwendungen. Für eine schnelle Wiederherstellung ist eine regelmäßige Sicherung dieser Daten sinnvoll.

3.1.2. Notfallserver

Der Dienstnehmer verfügt über ein vom Schadensereignis unberührtes System oder Endgerät, von dem er den Wiederherstellungsprozess starten kann. Alle notwendigen Zugriffe (Ports, Netzanschluss, Accounts, Passwörter) sind hier vorhanden oder können dem System zugeführt werden.

3.1.3. Zielsysteme

Im Fall der Wiederherstellung ist definiert, auf welche Systeme welches Backup wiederhergestellt werden darf und kann. Die Forensik, Feuerwehr, Polizei und weitere externe Dienstleister haben die Systeme als Zielsysteme einer Wiederherstellung freigeben. Die technischen Voraussetzungen sind gegeben, um auf dem Zielsystemen das Backup vom Dienstleister einspielen zu können.

3.1.4. Infrastruktur

Der Dienstnehmer hat im Schadensfall eine von dem Ereignis unberührte Infrastruktur, auf der Backupdaten wiederhergestellt werden können. Dies kann eine Infrastruktur eines entfernten Standorts (vgl. Stromausfall oder physische Zerstörung), Infrastruktur eines externen Dienstleisters oder einer Partnerhochschule sein. Im Fall eines externen Dienstleisters oder einer Partnerhochschule liegt der Vorteil in einer organisatorischen-, räumlichen- und netzwerktechnischen Trennung.

Ein Kooperationsvorhaben der
DIGITALE HOCHSCHULE NRW

Gefördert durch
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

Diese macht den gleichzeitigen Eintritt des Schadensfalls bei beiden Organisationen sehr unwahrscheinlich.
Sollte es zu einem Stromausfall kommen, wird empfohlen, dass der Dienstleister für seine wichtigsten Dienste (vgl. Kapitel 2.3.) eine unterbrechungsfreie Stromversorgung (USV) angeschlossen hat. Die USV dient dem batteriebetriebenem Notbetrieb. Des Weiteren sollte die Stromversorgung der USV über eine Netzersatzanlage (NEA) gewährleistet sein.

4. Datenwiederherstellung

4.1. Organisatorische Voraussetzungen

- Notfall-Zugänge für den Fall, dass der IDP ausgefallen ist, müssen vorhanden sein. Diese sollten mit lokaler 2-Faktor-Authentifizierung abgesichert sein.
- Die Prozessbeschreibung für die Wiederherstellungs-Abläufe muss nutzbar vorliegen. Bereits vor Eintritt des Schadensereignisses muss die Definition eines Prozesses (Antrag auf Wiederherstellung, Genehmigungsverfahren, Priorisierung, Prioritätenliste, usw.) zur Datenwiederherstellung erfolgt sein, da in der Regel kein Ticket- oder Management-System mehr zur Verfügung steht, mit dem Anfragen analog zum Regelbetrieb abgearbeitet werden können.
- Verträge mit externen Dienstleistern müssen vor Eintritt des Schad-Ereignisses geschlossen werden. Diese Dienstleister müssen bei Eintritt des Schad-Ereignisses zeitnah aktiviert werden.
- Den Dienstleistern (externe Firmen ebenso wie den Dienstleister-Partnern im Rahmen von Datensicherung.nrw) sollten regelmäßig die zur Einleitung spezifischer Maßnahmen berechtigten Personen benannt werden. Hierzu gehört auch das Vorhalten geeigneter Authentifizierungsmittel für den Fall, dass Verzeichnisdienste und signierte Emails nicht zur Verfügung stehen. Dies ist essenziell für die Auslösung einer Datenwiederherstellung.
- Notwendige Geheimnisse müssen in einer von der IT unabhängigen Form vorliegen. Dies betrifft neben Passwörtern auch Informationen zur Wiederherstellung verschlüsselt gespeicherter bzw. gesicherter Daten.

4.2. Technische Voraussetzungen zur Wiederherstellung

- Schnellstmögliche Wiederherstellung der Netzwerkanbindung zwischen Kunden und Dienstleister.
- Eine nutzbare Sandbox Umgebung muss bereitstehen, ein Malware-Scanverfahren muss etabliert sein.

4.3. Ablauf

- Beantragung des Restores von Systemen durch Kunden
- Genehmigung des Restores durch Krisenstab o. ä.
- Restore in Sandbox-Umgebung
- Scan der Daten
- Bereitstellung der Daten an die Kunden (Netzwerk-Share oder bei zu schwacher Netzanbindung transportable Festplatten)

4.4. Sandbox-Umgebung und Datenscan der zu restaurierenden Daten

Wenn Daten wiederhergestellt werden, muss sichergestellt sein, dass diese nicht kompromittiert sind und zu weiteren Sicherheitsvorfällen führen. Die wiederherzustellenden

Ein Kooperationsvorhaben der
DIGITALE HOCHSCHULE NRW
Gefördert durch
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

Daten und Systeme sollten daher zunächst in eine abgeschottete Sandbox-Umgebung zurückgesichert werden, in der sie dann mit Hilfe eines Offline-Virenscanners wie z. B. Desinfec't überprüft werden.
Hierfür kann z. B. eine isolierte VM verwendet werden, die ausschließlich den Backup- und Restore-Client installiert hat und so abgeschottet ist, dass sie nur über den Restore-Port auf die Restore-Umgebung zugreifen kann.

4.5. Restore-Lösungen

4.5.1. Fast Recovery Area

Hier werden Backups der wichtigsten Systeme als startbare VMs vorgehalten. Ist dieser Bereich noch intakt, können diese Systeme schnell wieder verfügbar gemacht werden.

4.5.2. Lokale-Sicherungen und Notfall-Infrastruktur

Sofern lokale Datensicherungen verfügbar sind, muss für einen Restore zunächst eine Notfall-Infrastruktur lokal oder bei einem Dienstleister errichtet werden (z. B. lokaler Virtualisierungs-Cluster oder VMs bei einem Dienstleister). Die Daten können dann aus den lokalen Sicherungen wie oben beschrieben wiederhergestellt werden.

4.5.3. Offsite-Sicherungen und Notfall-Infrastruktur

Falls lokale Backups nicht mehr verfügbar sind, muss für einen Restore zunächst ebenfalls eine Notfall-Infrastruktur lokal oder bei einem Dienstleister errichtet werden. In diesem Fall müssen evtl. bei zu geringer Netzwerk-Performance Datenträger vom Dienstleister zum Kunden transportiert werden. Beim Kunden muss ein System vorhanden sein, welches den Zugriff auf die Backupdaten auf diesem Datenträger ermöglicht (z. B. lokaler Media-Agent).

4.6. Aktivierung externer Dienstleistungen

- Die Kontaktdaten der externen Dienstleister müssen im Notfallplan hinterlegt sein.
- Es muss festgelegt sein, wer den Auftrag zum Start der Dienstleistungen erteilen darf.
- In folgenden Bereichen hat sich eine externe Unterstützung als hilfreich erwiesen:
    - Unterstützung des Krisenstabes durch Sicherheits-Dienstleister
    - Betriebsunterstützung bei der Wiederherstellung
    - Inbetriebnahme der Notfall-Infrastruktur

4.7. Überprüfung der Datenintegrität

Um sicherzustellen, dass die wiederhergestellten Daten korrekt und unverändert sind, ist die Überprüfung der Datenintegrität durch die verschiedenen Techniken (Hashes, regelmäßiges Testen, Abgleich z.B. mit Referenz-Datensätzen aus unveränderbaren Backup-Datensätzen) entscheidend. Zur Automatisierung des Validierungsprozesses können Skripte verwendet werden, die eine Hash-Berechnung durchführen und einen Bericht erstellen.

5. Übergang aus dem K-Fall in den Regelbetrieb

5.1. Überprüfung IT-Betriebsbereitschaft

Mit der Überprüfung der IT-Bereitschaft wird das Ziel verfolgt, den Regelbetrieb der IT-Services (und damit der Hochschule) wiederherzustellen. Es muss gewährleistet werden, dass alle durch den K-Fall betroffenen IT-Services nach der Wiederherstellung keine Beeinträchtigungen aufweisen. Es gilt daher, jegliche erneute potentielle Auswirkung des K-Falls für den IT-Betrieb auszuschließen. Die jeweilige Überprüfung der IT-Services liegt in der Verantwortung der Fachabteilungen.

Ein Kooperationsvorhaben der
DIGITALE HOCHSCHULE NRW

Gefördert durch
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen

Während der Arbeiten zur Wiederherstellung sollte der aktuelle Status der einzelnen Wiederherstellungen an die betroffenen Nutzer*innen kommuniziert werden, z.B. per Status-Website.

5.2. Lessons-Learned

Im Rahmen des sogenannten "Lessons learned" soll das Ziel verfolgt werden, die Erfahrungen während des Prozesses zur Wiederherstellung des IT-Betriebs nach dem K-Fall zu dokumentieren. Es ist zu empfehlen, dieses Ziel zeitnah an alle Mitarbeitenden zu kommunizieren, die am Wiederherstellungsprozess beteiligt sind. Das Sammeln und Aufbereiten der Informationen kann in Workshops bzw. Meetings erfolgen, indem die Erfahrungen der Mitarbeitenden zusammengetragen und verschriftlicht werden. Die Ergebnisse können u.a. auch für die K-Fall-Dokumentation und die Aktualisierung der Pläne verwendet werden. Wie bereits angesprochen hat es sich als hilfreich erwiesen, diese Dokumentation auf einer einheitlichen Plattform zu sammeln und intern bereitzustellen.

5.3. K-Fall-Dokumentation

Die Dokumentation des K-Falls sollte während der gesamten Krisensituation erfolgen. Hierzu empfiehlt es sich im genutzten Wissensmanagementsystem oder einer nicht kompromittierten Cloud-Lösung die Dokumentation anzulegen und prozessbegleitend zu pflegen. Für NRW-Hochschulen eignet sich, sofern verfügbar, die sciebo-Campus Cloud als Lösung oder entsprechende Lösungen in der freien Wirtschaft. Wichtig ist, dass alle Beteiligten des Teams Notfallmanagement über Zugriff und Schreibrechte verfügen, um eine lückenlose Dokumentation zu gewährleisten. Die Dokumentation dient nicht nur der effizienten Ablage und Kommunikation von krisenrelevanten Informationen, sondern auch der Berichterstattung gegenüber Stakeholdern. Für die Entwicklung der "Lessons learned" sowie der Ableitung der Best Practices ist die Dokumentation ebenfalls unerlässlich. Diese finalen Evaluationen sollten nach erfolgter Krisenbewältigung keineswegs übersprungen werden, sondern zugunsten nachhaltiger Personal- und Ressourcenentlastung umgesetzt werden.

Ein Kooperationsvorhaben der
DIGITALE HOCHSCHULE NRW

Gefördert durch
Ministerium für Kultur und Wissenschaft des Landes Nordrhein-Westfalen