Grundkonzept für Datensicherungs-Infrastruktur (DSI)

Die Hochschulen in NRW erarbeiten derzeit ein Konzept für eine hochschulübergreifende und arbeitsteilig erbrachte Datensicherung. Die Grundzüge dieser Zusammenarbeit sind bereits erarbeitet und stellen die Basis der vorliegenden Anträge dar.

Das Ziel der Antragsteller ist es, mit einer modernen, leistungsfähigen DSI die beteiligten Hochschulen in die Lage zu versetzen, immer wieder auftretende Ausfälle von IT-Systemen oder Angriffe auf diese zu überstehen und gravierende Auswirkungen auf Forschung, Lehre und Verwaltung zu vermeiden. Insofern wird mit diesem Grundkonzept ein wichtiger Baustein des IT-Grundschutz-Kompendiums[1] des BSI umgesetzt. Auf diese Weise kann wesentlich zum kontinuierlichen Ablauf der zahllosen IT-gestützten Prozesse beigetragen werden; ein Anspruch, der wesentlich über die klassische Fähigkeit zum Restore hinausgeht, indem er zusätzlich den Bereich der Business Continuity[2] adressiert. Die damit verbesserte Widerstandsfähigkeit der beteiligten Hochschulen gegen Schäden an der IT entspricht damit aktuellen Empfehlungen[3] auf nationaler Ebene, die das Ziel der Resilienz dem der Effizienz gleichrangig sehen und durch die Reduktion von Auswirkungen auf die Kernprozesse der Hochschulen selber einen signifikanten Beitrag zur Gesamteffizienz leisten.

In dieser Anlage sollen daher grundsätzliche Erwägungen und daraus folgende Anforderungen an die Konfiguration vorgestellt werden, die Einfluss auf die Entscheidungskriterien für geeignete Produkte in Hard- und Software haben. Hier finden auch die Empfehlung der Bitkom[4] Eingang, wonach eine Datensicherung sowohl einen logischen wie auch einen physischen Medienbruch realisieren und gesicherte Daten standortredundant speichern sollte.

Sicherungs- und Wiederherstellungs-Szenarien

Aus der Perspektive der Datensicherung können die folgenden Schaden-Typen auftreten, gegen die ein entsprechender Schutz realisiert werden muss:

Am Client[5], also am primären datenhaltenden System:

- **Ein Client kann Teile seiner Daten verlieren (z.B. durch versehentliches Löschen).** Wenn die Möglichkeit der lokalen Versionierung bzw. von Snapshots bereits ausgeschöpft (oder nicht gegeben) ist, muss die Datensicherungs-Infrastruktur die Möglichkeit bieten, im Selfservice auf Verzeichnis- oder Datei-Ebene Daten wiederherzustellen.

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2020.pdf
[2] https://www.datto.com/blog/the-difference-between-backup-and-business-continuity
[3] https://zenodo.org/record/4066319#.X4a7pe3gpaQ
[4] https://www.bitkom.org/Bitkom/Publikationen/Bitkom-Leitfaden-Backup-Restore.html
[5] „Client“ ist hier aus Perspektive der DSI jedes System, dessen Daten gesichert werden. Dies sind zu einem wesentlichen Anteil selbst Server-Systeme.

- **Ein Client kann alle seine Daten verlieren, sowohl durch Software- oder Nutzer-Fehler, gezielte Zerstörung oder physische Zerstörung beispielsweise durch einen Brand.**
  Für Clients mit einer moderaten Datenmenge muss die DSI in der Lage sein, den vollständigen Inhalt der Sicherung auf Ersatzgeräte zurückzuschreiben. Idealerweise besteht hier die Möglichkeit einer plattform-übergreifenden Wiederherstellung.
  Bei großen gesicherten Systemen im Bereich einiger 10 oder einiger 100 TB können die verlorenen Datenmengen eine adäquate Restore-Zeit unmöglich machen. Vor allem, wenn auch die Hardware betroffen ist und erst ersetzt werden muss.
  Für dieses Szenario muss die DSI die Möglichkeit des unmittelbaren Wiederanlaufs mit auf der DSI bereitgestellten virtuellen Ressourcen bieten. Dies ermöglichen geeignete Software-Lösungen im Zusammenspiel mit leistungsfähiger Hardware, indem beispielsweise unmittelbar auf dem Sicherungsdatenbestand virtuelle Maschinen gestartet werden. Einige Produkte erlauben, ganze Verbünde virtueller Maschinen auf diese Weise zu starten und behelfsmäßig zu betreiben, um die IT-basierte Handlungsfähigkeit der betroffenen Einrichtung wiederherzustellen.
  Für den Fall eines gezielten Angriffs beispielsweise durch Schadsoftware muss die DSI soweit wie möglich von allen Clients isoliert sein, um die Auswirkungen des Schädlings sowie ein Übergreifen auf die DSI selbst zu verhindern.

An der Datensicherungs-Infrastruktur im Backend:

Die DSI, mittels derer der Schutz der Datenbestände der Hochschule realisiert wird, kann auch selbst Schaden nehmen bzw. angegriffen werden. Geeignete Maßnahmen müssen sicherstellen, dass der Anspruch an Datensicherung nicht gefährdet wird. Folgende Fälle sind dabei zu berücksichtigen sind:

- **Physischer Verlust von Infrastruktur.** Diesem Fall ist durch Redundanz bzw. Replikation und hinreichende räumliche Trennung bzw. Verteilung zu begegnen. Dabei muss sichergestellt werden, dass neben den eigentlichen Sicherungsdaten auch die Katalogdaten und andere DSI-internen Metadaten in einer Weise repliziert werden, dass der Zugriff auf die gesicherten Daten auch bei längerfristigem Ausfall eines Standorts sichergestellt ist. Zusätzlich muss durch eine redundante (oder kurzfristig bereitgestellte) Konfiguration der Backup-Server sichergestellt sein, dass auf die gesicherten Daten auch zugegriffen werden kann. Genauso wichtig ist es, weiterhin Sicherungsdaten von Clients entgegennehmen zu können, da sonst diese neuen Daten gänzlich ungesichert blieben. Bis zum Wiederaufbau der Redundanz besteht hier zwar nur eine eingeschränkte Resilienz gegenüber weiteren Schäden. Trotzdem können Client-Daten weiterhin gesichert werden.
- **Eine gezielte Beschädigung der gesicherten Daten auf der Ebene der DSI.** Dieses Schad-Szenario kann durch einen böswilligen Insider oder durch einen Befall mit Schadsoftware (z. B. „Ransomware“) ausgelöst werden und setzt in beiden Fällen entsprechende privilegierte Zugriffe voraus. Moderne Speichersysteme als „letzte Verteidigungslinie“ bieten rollenbasierte Zugriffsmodelle und Betriebsmodi, so dass auch für – möglicherweise ausgespähte – Accounts von Administratoren gar kein oder ein streng beschränkter Zugriff auf gesicherte Daten besteht. In Kombination mit einer zwingenden Token-basierten 2-Faktor-Authentifizierung, die einen weiteren Schutz vor dem Missbrauch ausgespähter Zugangsdaten darstellt, ist ein Speichersystem mit einem solchen Zugriffs- und Rechtemodell geeignet, ein angemessen hohes Schutzniveau zu realisieren. Noch mehr Schutz gewähren

Speichersysteme, die eine Rücknahme einer einmal zugewiesenen Haltezeit grundsätzlich nicht zulassen. Beide Ansätze stellen nach Auffassung der Antragsteller einen hinreichenden Schutz vor böswilliger Zerstörung von Daten dar, wobei letzterer bei konsequenter Umsetzung auch einen Schutz gegen Innentäter realisiert.
Über diese Ansätze hinaus kann ein Schutz auch durch physische Isolation der gesicherten Daten erfolgen. Ein Weg hierzu ist die Verwendung von Tape als letzte Speicherschicht. Dabei stellt jedoch lediglich die inhärent hohe Latenz des Mediums eine Barriere für böswillige Manipulationen dar, eine erzwungene Sperre wird hierdurch nicht realisiert. Ein echtes Auslagern von Medien aus einem Tape-Roboter mit dem Ziel der physischen Unerreichbarkeit der darauf gespeicherten Daten stellt hingegen eine nur für dedizierte Datenbereiche sinnvoll durchführbare Option dar.
Die weitestmögliche Isolation der Speichersysteme auf Netzwerkebene ist Stand der Technik.

Sicherheitskonzept der DSI

Die DSI ist aus der Perspektive der Antragsteller eine besonders kritische Infrastruktur, die mit dazu beiträgt, Reputationsschäden und Wettbewerbsnachteile durch potentiellen Verlust, Diebstahl oder Verfälschungen von Daten zu verhindern.
Dazu soll sie im Falle eines Ausfalls oder eines Angriffs sicherstellen, dass die Auswirkungen auf die zu schützende Organisation minimiert werden, indem gesicherte Daten dem Zugriff eines Angreifers wirksam entzogen und damit gegen Zerstörung geschützt werden. Im nächsten Schritt soll die DSI in der Lage sein, einen möglichst sofortigen Wiederanlauf geschäftskritischer Systeme zu unterstützen.

Andererseits stellt die DSI den Kumulationspunkt aller Daten einer Organisation dar und muss damit unter Integritäts- und Vertraulichkeitsaspekten genauso geschützt werden wie die wichtigsten zu sichernden Systeme. Für die Datensicherung kommen daher nur Lösungen mit einer hohen Reputation hinsichtlich Software-Qualität und Update-Policy in Frage.

Für den Schutz gesicherter Daten gegenüber einem Angreifer oder vor einem Ausfall gibt es unterschiedliche Ansätze. Beispielsweise erlauben moderne Object Storage-Systeme, das Löschen oder Ändern gespeicherter Daten vor Ablauf einer einmal gesetzten Fälligkeit gänzlich zu unterbinden oder einen Zugriff nach dem Vier-Augen-Prinzip zu erzwingen. Neben dem Schutz der Informationen wird hierdurch auch ein Schutz der Mitarbeitenden hergestellt.

Ausschlaggebend für die Integrität der DSI sind die administrativen Prozesse. Über diese Prozesse erfolgt die Zuordnung sowohl der Nutzenden und ihrer Rollen sowie zu Clients und deren Datenbereichen.
Daher müssen die Pflegeprozesse und Transportwege der Metadaten

- Identitäten,
- Credentials bzw. sichere Authentifizierung,
- Rollen,
- Kontexte und
- Zuordnung der Configuration Items zu Kontexten und Identitäten

so gestaltet und dokumentiert werden, dass diese Informationen zweifelsfrei und authentisch vorliegen, sodass deren Integrität sichergestellt ist. Idealerweise kann hier die DSI hochschulübergreifend an etablierte Pflegeprozesse andocken. Darüber hinaus muss dokumentiert werden, welche Prozessschritte bzw. welche Formen von Zugriffen durch wen und von wo aus erfolgen (sollen). Diese Dokumentation ermöglicht es beispielsweise, die Durchführung kritischer Schritte am Kern der DSI nur von vorab benannten Arbeitsplätzen aus durchzuführen. Gleichzeitig wird für die Endnutzenden durch z. B. weltweite Erreichbarkeit für Sicherung und Wiederherstellung mobiler Systeme ein Höchstmaß an Gebrauchswert realisiert.

Für das Erreichen dieser Ziele haben die Betreiber-Rechenzentren einen auf dem BSI-Grundschutz oder anderen allgemein anerkannten Sicherheitsstandards basierenden Sicherheitsprozess eingeführt oder werden diesen einführen. Die dazu erforderlichen organisatorischen und technischen Maßnahmen werden ebenso wie die Dienstgütezusagen des Datensicherungs-Service kontinuierlich an die sich verändernde Bedrohungslage, sich verändernde Technologien und Anforderungen angepasst, ohne dabei die Wirtschaftlichkeit und „Usability“ aus den Augen zu verlieren.

Auf technischer Ebene muss die Netzwerk-Architektur der Betreiber-Rechenzentren die IT Sicherheit durch eine starke Segmentierung der Netze und insbesondere einer größtmöglichen Isolation der DSI unterstützen. Alle aus dem Internet erreichbaren Server und System-Komponenten werden regelmäßig auf Schwachstellen hin überprüft.

Zusammenfassung

Die Anforderungen an die DSI sind in den letzten Jahren qualitativ und quantitativ massiv gestiegen. Gleichzeitig können zeitgemäße Lösung einen wesentlichen Beitrag zur Kontinuität aller Bereiche der Hochschulen. Dem entsprechend orientiert sich die Auslegung von Hard- und Software an den Kapazitätsanforderungen und ganz maßgeblich an den Schutz- und Wiederherstellungszielen. Dies geht damit wesentlich über bisherige Konfigurationen, die sich lediglich an der Fähigkeit zum Restore orientiert haben, hinaus. Für die Umsetzung der hier ausgeführten Ziele soll im Zuge der beiden vorliegenden Anträge der Hardware-Teil der DSI aus einer leistungsfähigen, räumlich verteilten Konfiguration aus Servern und Speicher bestehen. Das BMS muss diese Funktionen vollumfänglich unterstützen und gleichzeitig geeignet sein, in die komplexe Struktur und die Prozesse kooperierender Hochschulen als Dienstleister und Dienstnehmer integriert zu werden.