IT-DATENSICHERHEIT

vimotion is motion

DIE TECHNOLOGISCHE BASIS DES DIGITALEN WEITERBILDUNGSCAMPUS: IT-SICHERHEIT, DATENSICHERHEIT UND DATENSCHUTZ

Angesichts der stetig wachsenden Bedrohung durch Kriminalität im Internet wird die Sicherheit in der Informationstechnik zu einer immer wichtigeren Aufgabe für die Betreiber von IT-Systemen. Auch und gerade der Digitale Weiterbildungscampus muss sich wegen seiner Besonderheiten mit diesem Problem intensiv auseinandersetzen:

- Eine Besonderheit zeigt sich in der Struktur des Digitalen Weiterbildungscampus als integrierte Lehr- und Lernumgebung. Er ist eben nicht nur ein Lernmanagementsystem (LMS), eben nicht nur ein virtueller Konferenzraum, sondern ein System, das viele unterschiedlichste Applikationen und Tools unter einem Dach vereint. Den Nutzern – Weiterbildungseinrichtungen, Lehrende und Lernende – bietet sich damit der große Vorteil, für die unterschiedlichsten Szenarien die unterschiedlichsten Tools in einer einzigen Lernumgebung nutzen zu können, so als würde es sich um eine einzige Applikation in einer optisch individuell gestalteten Umgebung handeln.

- Eine weitere Besonderheit liegt darin, dass diese integrierte Lehr- und Lernumgebung als technische Infrastruktur für viele Weiterbildungseinrichtungen, sowohl für deren Kunden als auch deren Lehrende, ein Mittelpunkt ist. Das Vertrauen der Kunden in ihre Einrichtung ist ein wichtiges Gut, das die Einrichtungen durch die Nutzung des Campus teilweise an dessen Betreiber weitergeben. Mit diesem Gut gilt es höchst sorgfältig umzugehen. Unabdingbare Voraussetzung dafür sind die ITSicherheit, die Datensicherheit und der Datenschutz.

Dabei steht der Digitale Weiterbildungscampus vor drei wesentlichen Herausforderungen:

Vernetzung:
Die Informationstechnik (IT) des Digitalen Weiterbildungscampus zeichnet sich durch eine hohe Leistungsfähigkeit und Usability (Nutzerfreundlichkeit) für den Benutzer aus. Alle Aufgaben und technischen Dienste werden durch die IT erfasst und in das System integriert, was eine sichere Vernetzung aller Dienste voraussetzt.

Komplexität:
Durch eine Integration bestehender und neuer Funktionen wird der Wertschöpfungsprozess des Digitalen Weiterbildungscampus stetig erweitert. Dabei werden alle technisch vorhandenen Möglichkeiten genutzt und über nutzerfreundliche grafische Schnittstellen dem Nutzer zugänglich gemacht. Da diese Leistung vielen Nutzern gleichzeitig zur Verfügung stehen muss, ist eine sowohl vertikale als auch horizontale Skalierung notwendig.

Allgegenwärtigkeit:
Von virtuellen Lernumgebungen erwartet der Nutzer, dass er jeden Dienst praktisch zu jeder Zeit und von jedem Ort aus über das Internet erreichen kann, jeder auf der Welt das System von überallher in vollem Umfang nutzen kann, erhöht sich das Risiko, Angriffspunkt von Cyber-Kriminalität zu werden.

Aufgabe des Digitalen Weiterbildungscampus ist es somit, ein sicheres, stabiles und fehlerfreies

vimotion GmbH | Friedhofstrasse 26 | 71566 Althütte | Germany

System zu gewährleisten, das idealerweise dauerhaft und von jedem Ort der Welt erreichbar und nutzbar ist und stets erweiterungs- und veränderungsfähig bleibt.

Mit dem zunehmenden Funktionsausbau des Digitalen Weiterbildungscampus und dessen Vernetzung mit vielen Lebens- und Arbeitsbereichen ergibt sich eine erhöhte Gefährdungslage in Bezug auf die Cyber-Kriminalität. Die Ursachen von Cyber-Angriffen, die verwendeten Angriffsmethoden und die technischen Angriffsmittel entwickeln sich täglich weiter, hängen in vielfältiger Weise zusammen und beeinflussen sich gegenseitig.

URSACHEN DER CYBER-KRIMINALITÄT – DAS INTERNET ALS ANGRIFFSPLATTFORM

Kein Tag vergeht ohne Cyber-Angriffe auf Informationstechnologie, Server und private Nutzer. Viele davon verlaufen erfolgreich, weil die Angreifer zum einen immer professioneller werden und zum anderen die Rahmenbedingungen es zulassen.

Die offene Struktur, die technischen Möglichkeiten und die Anonymität sind die Ursachen, warum das Internet so massiv als Angriffsplattform missbraucht wird. Für erfolgreiche Cyber-Angriffe braucht man heute vielfach nicht mehr als einen Computer und einen Internetanschluss. Es existiert ein funktionierender globaler Markt, auf dem Angriffswerkzeuge und -methoden, Schwachstellen, Schadsoftware oder sogar Webseiten-Traffic einfach und kostengünstig eingekauft werden können („Malware-asa-Service“). Auch illegal beschaffte Daten wie Nutzeraccounts und Kreditkarteninformationen werden auf diesen kriminellen Online-Marktplätzen gehandelt. Sowohl gut organisierte Gruppen als auch Einzelpersonen bieten ihre Fähigkeiten und Dienstleistungen dort an. Diesen eher geringen Investitionen stehen die vielfältigen Möglichkeiten gegenüber, durch kriminelle Handlungen Geld zu verdienen, an vertrauliche Informationen zu gelangen oder Sabotageakte durchzuführen.

Die Attraktivität des Internets als Angriffsplattform zeigt sich in diesen Rahmenbedingungen, die die Angreifer für ihre Zwecke ausnutzen:

- Die zunehmende Vernetzung der IT ermöglicht es, Angriffe von nahezu jedem Standort weltweit und zu jeder Zeit durchzuführen. Ein Angreifer muss sich somit keinem unmittelbaren Risiko vor Ort aussetzen.

- Die zunehmende Komplexität der Technik und oftmals fehlendes Sicherheitsbewusstsein der Nutzer führen zu unzureichend abgesicherten Systemen und erhöhen damit die Erfolgsaussichten für Cyber-Angriffe.

- Der sorglose Informationsaustausch über das Internet und der „Always on“-Status mobiler Systeme erleichtern den Zugriff auf schützenswerte Informationen.

- Das dezentral und offen gestaltete Internet bietet Angreifern vielfältige Tarnungsmöglichkeiten, die das Risiko, entdeckt zu werden, minimieren.

- Unterschiede in nationalen Regularien erschweren Maßnahmen der Strafverfolgung.

Die Professionalisierung und Arbeitsteilung im Bereich der Cyber-Kriminalität nimmt weiter zu. Auf diese Weise kann ein Cyber-Angriff von verschiedenen Personen oder Gruppen, die sich auf einzelne Schwerpunkte spezialisiert haben, unabhängig voneinander realisiert werden. So gibt es beispielsweise:

vimotion GmbH | Friedhofstrasse 26 | 71566 Althütte | Germany

- Hacker, die neue Schwachstellen in weitverbreiteten Softwareprodukten suchen und diese zum Verkauf anbieten;
- Entwickler, die zu diesen Schwachstellen passende Schadsoftware oder Werkzeuge zur Generierung von Schadsoftware entwickeln und anpassen;
- Angreifer, die diese Schadsoftware einsetzen, um Informationen auszuspionieren;
- Kriminelle, die die gestohlenen Informationen kaufen, ausnutzen und einen monetären Gewinn daraus ziehen.

So kann selbst ein unerfahrener Angreifer ohne technisches Know-how professionelle Angriffe auf gewünschte Ziele durchführen oder durchführen lassen, ohne sich mit den technischen Details und der Ausführung befassen zu müssen.

Aufgrund der Medienberichte über die Snowden-Enthüllungen, über Cyber-Angriffe auf bekannte Wirtschaftsunternehmen und den damit verbundenen Abfluss von Kundendaten sowie über großflächigen Identitätsdiebstahl ist das Vertrauen vieler Anwender in die Informationstechnik erheblich erschüttert. Die Nutzer scheinen zunehmend für Themen der IT-Sicherheit sensibilisiert. So ermittelte eine Studie des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI), dass sich das Sicherheitsgefühl der Deutschen im Internet signifikant verschlechtert hat[1].

SCHWACHSTELLEN IN DER SOFTWAREENTWICKLUNG ALS NÄHRBODEN FÜR CYBER-KRIMINALITÄT

Schwachstellen in Softwareprodukten sind ein idealer Nährboden für die Entwicklung von Cyber-Angriffsmitteln und meist auch die Ursache für erfolgreiche Cyber-Angriffe. Wie schon in den Jahren zuvor war die Anzahl kritischer Schwachstellen in Standard-IT-Produkten in den Jahren 2014 und 2015 extrem hoch (vgl. Abb. 1). Allein in 13 Softwareprodukten, die weitverbreitet genutzt werden, traten im Jahr 2015 1.115 kritische Schwachstellen auf. Für 2016 rechnet das *Bundesamt für Sicherheit in der Informationstechnik* (BSI) mit mehr als 1.000 kritischen Schwachstellen[2].

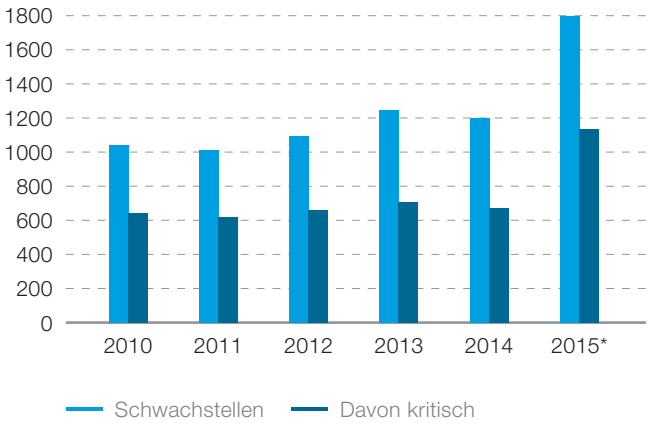

Abbildung 1: Schwachstellen von 13 weitverbreiteten Softwareprodukten in den Jahren 2010 bis 2015[3].

1 Ipsos-CIGI-Umfrage: Deutschland – Land der Internetskeptiker?

2 https://www.bsi.bund.de/DE/Publikationen/Lageberichte/bsi-lageberichte.html

3 ebd.

vimotion GmbH | Friedhofstrasse 26 | 71566 Althütte | Germany

Schwachstellen sind heute ein immanenter Bestandteil von Softwareprodukten, denn die Entwicklung fehlerfreier Software ist faktisch nicht oder nur in sehr eingeschränkten Spezialbereichen möglich. Allein bei den 13 oben genannten Softwareprodukten muss mit einer Erkennung von durchschnittlich jeweils zwei bis drei kritischen Schwachstellen pro Tag gerechnet werden. Aufgrund der enormen Anzahl von Schwachstellen ist das Patch-Verhalten der Hersteller, also die Versorgung der Nutzer mit Updates, von besonderer Bedeutung. Diese sind zunehmend gezwungen, bei der Beseitigung von Fehlern Prioritäten zu setzen und sich auf kritische Schwachstellen zu konzentrieren.

Details zu Schwachstellen werden häufig erst nach Herausgabe eines Sicherheitsupdates (Patch) durch den Softwarehersteller bekannt. Daher ist eine rasche Einspielung dieser Softwareaktualisierungen zwingend erforderlich. Falls Details oder gar Exploits (eine systematische Möglichkeit, Schwachstellen auszunutzen), die eine bestimmte Schwachstelle ausnutzen, vor dem Patch des Softwareherstellers an die Öffentlichkeit gelangen (Zero-Day-Exploits), ist bei einem Einsatz der betroffenen Software höchste Vorsicht geboten. Im Jahr 2015 gab es bis Ende Juli sieben öffentlich bekannte Vorfälle dieser Art.

Für den Digitalen Weiterbildungscampus ist es daher unumgänglich, auf einen Mechanismus zurückzugreifen, mit dem Updates zeitnah eingepflegt und vollzogen werden können, ohne einen Ausfall des Systems wegen Inkompatibilität der Software zu riskieren. Bei Zero-Day-Exploits sollte dieser Mechanismus gewährleisten, dass der betreffende Dienst innerhalb von ein bis zwei Stunden nach Bekanntgabe entweder durch andere Funktionen ersetzt oder mit einem lauffähigen Update auf dem System gepatcht und somit auf den neuesten Stand gebracht wird.

Weiterhin benötigt der Digitale Weiterbildungscampus eine Sensorik, durch die mit verschiedensten Methoden auf Cyber-Angriffe reagiert werden kann. Alle Logfiles müssen konsequent auf Angriffe hin überwacht und ausgewertet werden.

TYPISCHE SICHERHEITSMÄNGEL

Das BSI führt regelmäßig Sicherheitsprüfungen wie Penetrationstests oder ISRevisionen (Informationssicherheitsrevision) bei Unternehmen und Behörden durch. Häufig werden dabei diese Sicherheitsmängel festgestellt:

- Die Aktualisierungen der Software sind nicht auf dem neuesten Stand, Applikationen veraltet und verfügbare Sicherheitsmechanismen deaktiviert.
- Passwörter sind – auch bei kritischen Anwendungen – leicht zu ermitteln. Nicht selten werden Standardpasswörter, schwache oder gar leere Passwörter verwendet.
- Maßnahmen zu Netzwerkmanagement und -überwachung existieren nicht oder lediglich als Insellösungen, Logdaten werden lediglich lokal auf den Komponenten selbst vorgehalten und nur anlassbezogen manuell ausgewertet.
- Eine Netzwerkzugangskontrolle (auch für Wartungszugänge und -verbindungen), die ausschließlich autorisierten dienstlichen Endgeräten den Zugang zum internen Netzwerk ermöglicht, wird oftmals nicht genutzt.
- Es existiert keine Schnittstellenkontrolle für mobile Datenträger und mobile Endgeräte werden nicht verschlüsselt.

vimotion GmbH | Friedhofstrasse 26 | 71566 Althütte | Germany

- Änderungen an Anwendungen und Betriebssystemen werden ohne angemessenes Änderungs- und Versionsmanagement in den Produktivbetrieb eingestellt und größtenteils nicht dokumentiert.

- Schulungen und Sensibilisierungsmaßnahmen finden insbesondere für die Zielgruppe der Anwender nicht oder nur in geringem Umfang statt.

- Die Verantwortlichkeit für Informationssicherheit durch die Unternehmens- oder Behördenleitung bzw. das Management ist oftmals nicht klar geregelt.

- Sicherheitskonzepte sind unvollständig und inkonsistent.

DENIAL OF SERVICE

Denial-of-Service-Angriffe (DoS = Verweigerung der Leistung) richten sich gegen die Verfügbarkeit von Diensten, Webseiten, einzelnen Systemen oder ganzen Netzen. Dabei wird versucht, die Ressourcen des betreibenden Systems zu erschöpfen, das heißt möglichst unendlich viele Webseiten aufzurufen und Inhalte abzufragen.

Wird ein solcher Angriff auf mehreren Systemen parallel durchgeführt, spricht man von einem verteilten DoS- oder DDoS-Angriff (DDoS = Distributed Denial of Service). DDoS-Angriffe erfolgen häufig von einer sehr großen Anzahl von Computern aus. Dabei kann es sich um zu einem sogenannten Botnetz zusammengeschlossene Systeme, bei denen Computer ohne Wissen des Besitzers übernommen werden, oder auch um wissentlich zusammengeschaltete Rechner von freiwillig Teilnehmenden handeln, beispielsweise bei politisch motivierten Angriffen. DDoS-Angriffe auf große Unternehmen und Regierungen sind oft eher politisch oder ideologisch motiviert, bei Angriffen auf E-Commerce-Anbieter geht es hingegen vermehrt um Wettbewerbsbeeinflussung oder Erpressung. DDoS-Angriffe erfolgen mit zunehmender Häufigkeit auch gegen kritische Infrastrukturen (z. B. von Banken, Transport- oder Medienunternehmen). Auch hier verfolgen die Täter bislang in erster Linie finanzielle Interessen, etwa durch Erpressungsversuche.

Eine Studie hat gezeigt, dass die meisten Angreifer bereits als Nutzer Zugang zum betreffenden System besitzen und ihnen damit schon ein gewisses Grundvertrauen vom System entgegengebracht wurde. Daher ist auch der Schutz vor Angriffen durch den Endnutzer nicht zu vernachlässigen[4].

Ein wichtiger Ansatzpunkt zur Abwehr von oS-Angriffen besteht darin, genügend Systemressourcen vorzuhalten, die einen Angriff fast unmöglich machen. Allerdings ist bei jedem noch so großen System die Kapazität irgendwann erschöpft. Deshalb ist hier ein Maßnahmenkonzept nötig, das bei einem eventuellen Angriff zum Einsatz kommt.

INHALTE UND AUFGABEN DER IT-SICHERHEIT

Die IT-Sicherheit beschäftigt sich hauptsächlich mit dem Schutz der Technik vor Fremdeinflüssen und technischem Ausfall. Die Verfügbarkeit des Systems im Jahresmittel spielt hier eine maßgebliche Rolle. Soll sie hoch sein, muss eine entsprechend aufwendige Technik zum Einsatz kommen, die meist für den Endnutzer unsichtbar bleibt. Selbst eine mini-

4 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html

vimotion GmbH | Friedhofstrasse 26 | 71566 Althütte | Germany

male Steigerung der Verfügbarkeit um nur ein Prozent (z. B. von 98 % auf 99 %) reduziert die Ausfallzeit erheblich (im Beispiel von 7,3 auf 3,65 Tage). Je höher die angestrebte Verfügbarkeit ist, desto schwieriger wird es, sie zu realisieren. Unter dem Aspekt der Wirtschaftlichkeit betrachtet ist ein Ausfall von zum Beispiel nur einer Sekunde im Jahresmittel fast unmöglich zu erreichen.

Dementsprechend müssen in diesem Bereich auch bewusst Risiken eingegangen werden. Damit diese kalkuliert werden können, müssen sie im System bekannt sein und in der Ausfallwahrscheinlichkeit berücksichtigt werden.

Das Produktivsystem des Digitalen Weiterbildungscampus besteht aus einer ausfallsicheren Serverlandschaft. Diese bietet eine Sicherheit und Verfügbarkeit, die bei isolierten Angeboten zu vertretbaren Kosten kaum erreicht werden kann. Jede Funktionalität wird durch einen eigens hierfür konzipierten virtuellen Server realisiert, der separat gewartet wird. Dieser modulare Aufbau reduziert die Komplexität der einzelnen Funktionseinheiten und erhöht die Wartbarkeit des Systems auf lange Sicht. Die Vielfalt an Möglichkeiten entsteht durch das Zusammenspiel dieser technischen Einheiten, die mindestens zweifach ausgelegt sind. Fällt eine Komponente aus, springt automatisch ihr entsprechendes Gegenstück ein.

Der Digitale Weiterbildungscampus ist durch verschiedene Mechanismen vor fehlerhafter Software geschützt, die ein Hacker ins System hochladen und über diese dann das System in Besitz nehmen könnte. Wenn eine nicht autorisierte Person bösartige Software auf einer Serverlandschaft installieren kann, hat sie die Möglichkeit, das Betriebssystem so umzubauen, dass es durch Standardtools nicht mehr entdeckt wird. Einem solchen nicht autorisierten Zugriff stehen diese Maßnahmen entgegen:

- Alle Dienste, die Einfallstore für Software bieten, sind auf separate virtuelle Server verteilt. Durch diese Architektur eines „Flickenteppich“ ist eine Übernahme des kompletten Produktivsystems durch Zero-Day-Exploits nahezu unmöglich.

- Backups, also Sicherungskopien, werden nicht vom Produktivsystem erzeugt, sondern vom Backup-System explizit geholt. Beim Backup-System handelt es sich um eine virtuelle Serverlandschaft, die verantwortlich ist für die Überwachung von Backups und Updates des Produktivsystems. Es ist nur im VPN-Netzwerk der Administration erreichbar. Logfiles und andere Daten werden somit nicht auf den Arbeitsmaschinen gespeichert und überwacht, sondern ausschließlich im Backupsystem. Damit folgt der Digitale Weiterbildungscampus den Empfehlungen des BSI.

- Zwischen den Servern existieren mehrere eigene Netzwerke, die für ihre Aufgaben spezialisiert sind, was dem Trennungsgebot des BSI entspricht.

Bildet man alle technischen Empfehlungen des BSI ab, so gelangt man am Ende zu einem System, das nahezu reibungslos betrieben werden kann. Aus dem täglichen Umgang mit Logfiles und deren Auswertung können weitere Erkenntnisse über Angriffe gewonnen werden. Derzeit erfolgen pro Nacht ca. 100.000 Versuche, das System zu durchlöchern, wobei viele der Angriffe nicht ernst zu nehmen sind und auch von einer Standardinstallation ohne Mühe abgewehrt werden können.

Die Gewährleistung der IT-Sicherheit bindet meist mehr Ressourcen als der Funktionsumfang der Serverlandschaft. Dies wird in aktuellen Systemen oft unterschätzt.

4 https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html

TECHNISCHE INFRASTRUKTUR DES DIGITALEN WEITERBILDUNGSCAMPUS

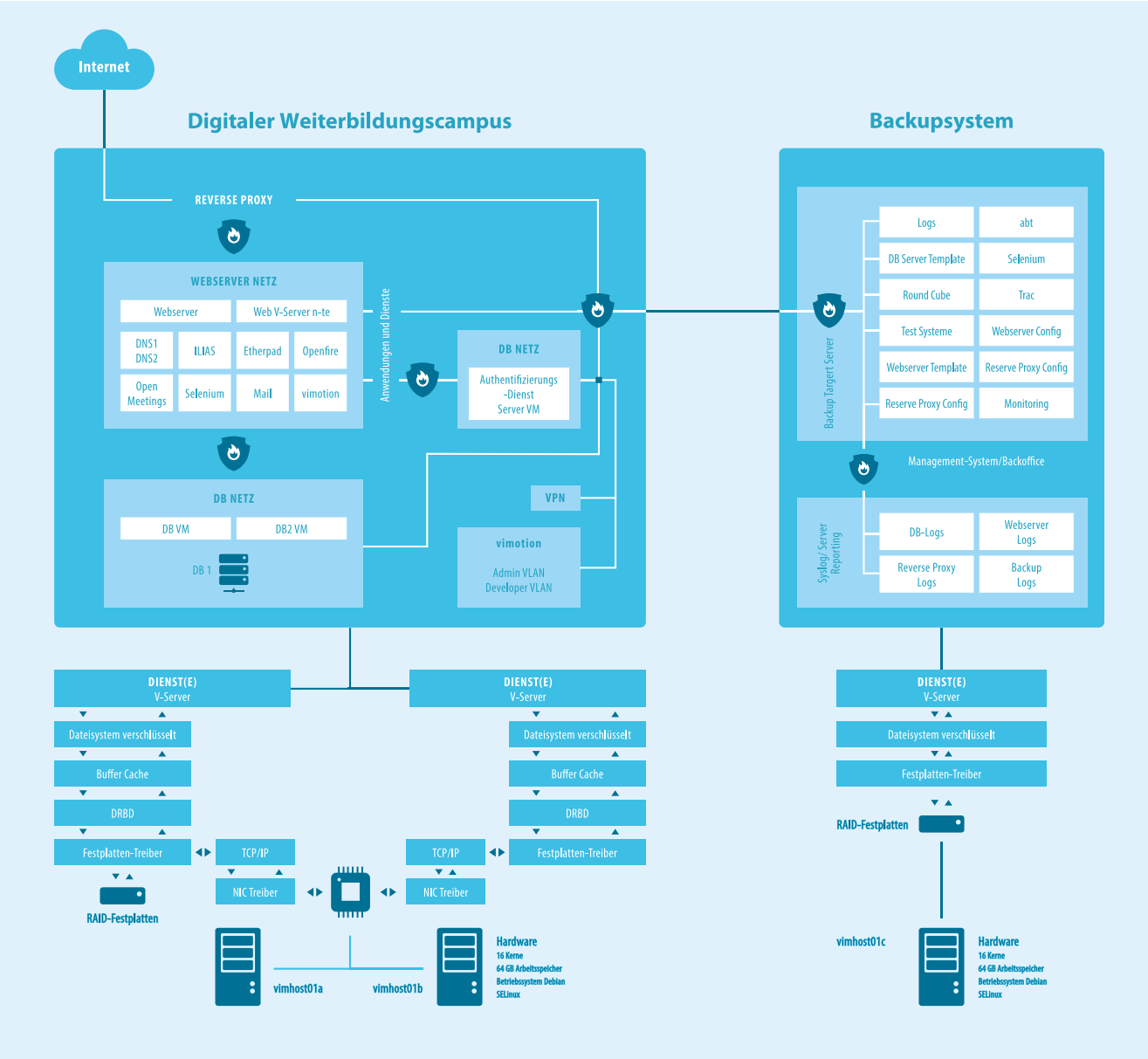

Abbildung 2 veranschaulicht die technische Infrastruktur des Digitalen Weiterbildungscampus. (Quelle: vimotion)

Das Herzstück des Produktivsystems bilden zwei Server, die zueinander wie eineiige Zwillinge aufgebaut sind (Cluster). Daneben gibt es mehrere virtuelle Server (den bereits erwähnten „Flickenteppich“) sowie das Backupsystem, das die Einheit aktualisiert, überwacht, Backups und ihre Aktivitäten mitlogt.

vimotion GmbH | Friedhofstrasse 26 | 71566 Althütte | Germany

Die Daten werden in jeder Einheit so verschlüsselt, dass die Nachbareinheit gerade noch ihren Dienst damit verrichten kann. Eine besondere Herausforderung ist es, durch die Menge an Einschränkungen und Trennungen der Server die Softwareeinheiten einer bestehenden Software dennoch funktionsfähig zu machen und zu halten. Dies erfordert meist massive Anpassungen bis hin zur Entwicklung eigener Software, denn im Gegensatz zur einfachen Installation als Standardlösung wird der volle Funktionsumfang des Digitalen Weiterbildungscampus nur erreicht, wenn alle Softwarepakete in die bestehende IT-Landschaft integriert werden.

Um ein wartbares und störungsfreies System zu schaffen, wurde ein erhöhter Aufwand für die Installation, den Betrieb und die Behebung von Störfällen in Kauf genommen. Die sehr guten Ausfallzahlen aus den Jahren 2014 (99,991 %) und 2015 (99,994 %) belegen, dass diese Entscheidung richtig war. Wird dagegen beim Aufbau des Systems nur die reine Funktion betrachtet, sind Störungsfälle jeglicher Art nicht ausgeschlossen.

Abbildung 3 zeigt, wie IT-Sicherheit, Datensicherheit und Datenschutz zusammenhängen. Aus der IT-Sicherheit folgt die Datensicherheit – erst dann ist Datenschutz überhaupt möglich.

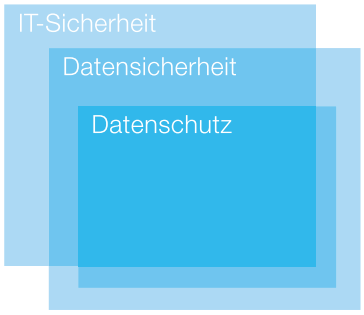

Abbildung 3: Zusammenhang von IT-Sicherheit, Datensicherheit und Datenschutz

FAZIT

Störungsfälle in großen Organisationen, wie zum Beispiel der Hackerangriff auf Sony im Jahr 2014/15, der eine hohe mediale Aufmerksamkeit erlangte, sind oft auf eine verminderte Bereitschaft zurückzuführen, Kapital bzw. Know-how in IT-Sicherheit zu investieren. Vom Endnutzer wird dies an den zur Verfügung gestellten Funktionen zwar nicht bemerkt, jedoch kann anhand der Ausfallzahlen auf eine fehlerhafte ITSicherheit geschlossen werden, die meist auch die Bereiche Datensicherheit und Datenschutz berührt.

Der Digitale Weiterbildungscampus hat einen Raum geschaffen, in dem IT-Sicherheit, Datensicherheit und Datenschutz stets ein maßgebliches Anliegen sind. Hierfür verbürgen sich die Betreiber.

RECHTLICHE ASPEKTE DES DIGITALEN WEITERBILDUNGSCAMPUS

(DSB, vimotion GmbH)

DATENSCHUTZ, NUTZUNGSBEDINGUNGEN, DATENSICHERHEIT

Neben seiner inhaltlichen Zweckbestimmung hat der Digitale Weiterbildungscampus auch den Betrieb eines stabilen, sicheren und fehlerfreien Systems zu gewährleisten, das alle Auflagen des Bundesdatenschutzgesetzes (BDSG) vollständig erfüllt. Dieses Gesetz soll den Schutz der persönlichen Daten und das Recht auf informationelle Selbstbestimmung gewährleisten. Anders ausgedrückt: Jeder Mensch soll grundsätzlich selbst und frei darüber entscheiden, wann wem welche seiner persönlichen Daten zugänglich gemacht werden dürfen.

vimotion GmbH | Friedhofstrasse 26 | 71566 Althütte | Germany

Datenschutz umfasst verschiedene Komponenten:

- Schutz vor missbräuchlicher Datenverarbeitung;
- Schutz des Rechts auf informationelle Selbstbestimmung;
- Schutz des Persönlichkeitsrechts bei der Datenverarbeitung;
- Schutz der Privatsphäre.

Das Recht aller Beteiligten auf Datenschutz zu wahren und zu respektieren, ist ein zentrales Anliegen des Digitalen Weiterbildungscampus. Die Serversysteme des Digitalen Weiterbildungscampus weisen eine hohe Verfügbarkeit mit einer geringen Fehler- und Ausfallquote auf und bilden die Basis für umfassenden Datenschutz. Sie werden in einem deutschen Rechenzentrum betrieben und garantieren einen reibungslosen Ablauf der Prozesse und des Datenaustauschs zwischen Nutzer, Anbieter und Betreiber.
Die Nutzung und der Austausch von Daten zwischen den Beteiligten sind rechtlich eindeutig geregelt, der Ablauf ist genau definiert und vertraglich abgesichert (siehe Abb. 4).

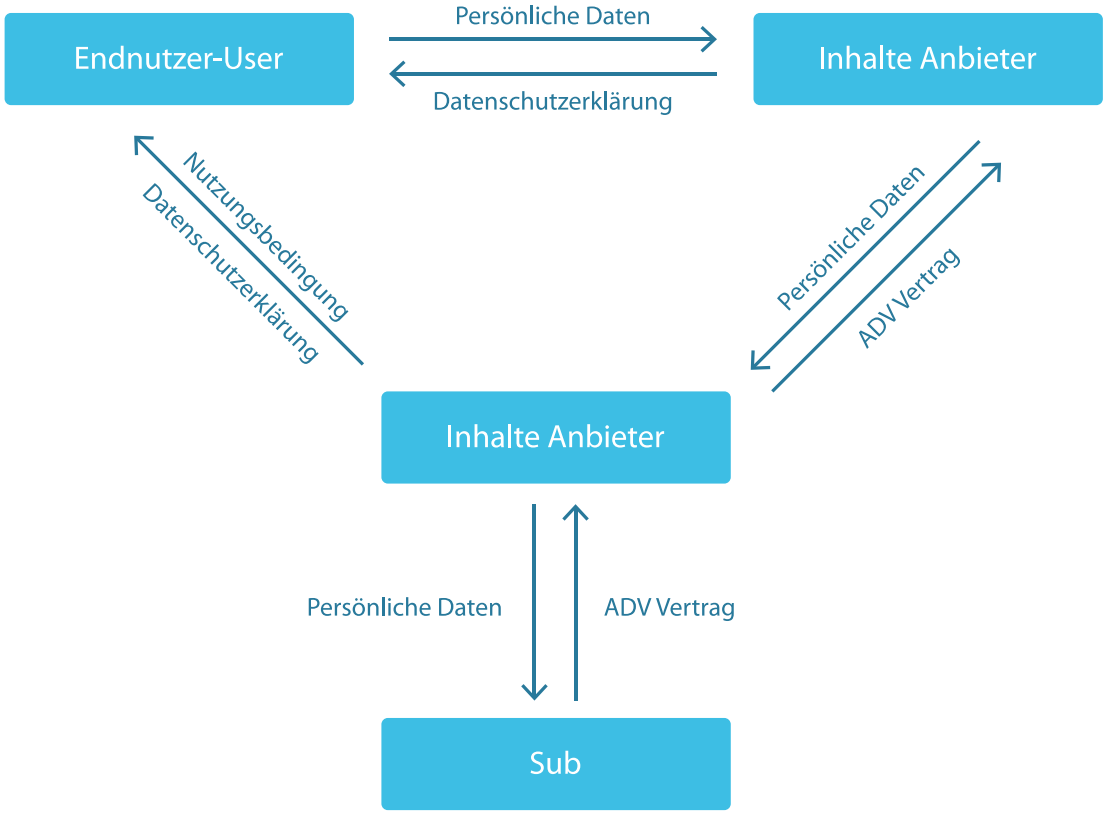

Abbildung 4: Datenfluss und Rechtsgrundlagen im Digitalen Weiterbildungscampus

vimotion GmbH | Friedhofstrasse 26 | 71566 Althütte | Germany

Wenn sich ein Interessent für einen E-Learing-Kurs eines Anbieters auf dem Digitalen Weiterbildungscampus entscheidet, stellt er diesem seine Nutzerdaten zur Verfügung. Im Gegenzug erhält er eine Datenschutzerklärung mit der Information, wie mit seinen Daten verfahren wird. Sie enthält detaillierte Angaben über die Erhebung, Verwendung, Weitergabe und Speicherdauer der Nutzerdaten, über das Nutzerkonto, die Einwilligung des Nutzers zur Verarbeitung seiner Daten, Widerrufsmöglichkeiten sowie über die Pflicht des Anbieters, dem Nutzer jederzeit Auskunft über die gespeicherten Daten zu geben.

Der Anbieter gibt die Daten des Nutzers an den Betreiber weiter, der im Vorfeld einen Auftragsdatenverarbeitungsvertrag (ADV-Vertrag, vgl. Abb. 1) mit dem Anbieter abgeschlossen hat. Dieser Vertrag berechtigt den Betreiber, die personenbezogenen Nutzerdaten im Auftrag des Anbieters zu verarbeiten. Außerdem beschreibt er organisatorische und technische Maßnahmen gegen den Missbrauch von Daten und gibt vor, welche Kategorien von Kontroll- und Schutzmaßnahmen sichergestellt sein müssen. Dabei handelt es sich im Einzelnen um:

Zutrittskontrolle:
Unbefugte dürfen keinen Zutritt zu Datenverarbeitungsanlagen erhalten, mit denen personenbezogene Daten verarbeitet werden. Schutzmaßnahmen in diesem Bereich sind zum Beispiel die Gebäudesicherung mit Videoüberwachung und die Sicherung von Räumen durch Sicherheitsschlösser.

Zugangskontrolle:
Datenverarbeitungsanlagen dürfen nicht von Unbefugten benutzt werden. Beispielsweise ist ein Rechnerzugang nur mit Benutzerkennung und Passwort möglich.

Zugriffskontrolle:
Die Nutzer der Datenverarbeitungsanlagen dürfen ausschließlich auf die Inhalte zugreifen, für die sie berechtigt sind. Personenbezogene Daten dürfen bei der Verarbeitung und Nutzung sowie nach dem Speichern nicht unbefugt kopiert, verändert oder gelöscht werden. Dies wird zum Beispiel durch getrennte Systeme gewährleistet.

Weitergabekontrolle:
Personenbezogene Daten dürfen bei der elektronischen Übertragung, beim Transport oder bei der Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden. Außerdem muss festgestellt werden können, an welchen Stellen eine Übermittlung solcher Daten im Datenverarbeitungssystem vorgesehen ist. Geeignete Maßnahmen der Sicherung sind zum Beispiel die Verschlüsselung der Daten beim Transport und Protokollierungsmaßnahmen bei der Datenübermittlung durch ein verschlüsseltes Netzwerk (VPN für Virtuelles privates Netzwerk) handelt es sich um ein geschlossenes logisches Netzwerk.)

Eingabekontrolle:
Es muss nachträglich überprüft werden können, ob und von wem personenbezogene Daten eingegeben, verändert oder gelöscht wurden. Dieserfolgt zum Beispiel durch das Protokolieren der Aktivitäten des Benutzers.

Auftragskontrolle:
Die Verarbeitung personenbezogener Daten im Auftrag Dritter darf nur gemäß den Weisungen des Auftraggebers erfolgen. Maßnahmen zur Sicherstellung sind zum Beispiel ein Datenschutzvertrag für Mitarbeiter und ein ADV-Vertrag für Subunternehmer gemäß § 11 BDSG sowie eine Stichprobenprüfung (Audit).

vimotion GmbH | Friedhofstrasse 26 | 71566 Althütte | Germany

Verfügbarkeitskontrolle:
Personenbezogene Daten müssen gegen zufällige Zerstörung oder Verlust geschützt werden, zum Beispiel durch Brandschutzmaßnahmen oder ein konsequent umgesetztes Backup-Konzept.

Trennungsgebot:
Personenbezogene Daten, die zu unterschiedlichen Zwecken erhoben wurden, müssen auch getrennt voneinander verarbeitet werden. Dies wird zum Beispiel durch getrennte Ordnerstrukturen (bei der Auftragsdatenverarbeitung) und getrennte Netze realisiert.

Die Beziehung zwischen Nutzer und Betreiber wird durch die Nutzungsbedingungen geregelt (siehe Abb. 1). Sie betreffen das Verhalten des (End-)Nutzers auf der Plattform und den Schutz seiner Daten im Sinne des BDSG.

Alle Mitarbeiter des Anbieters und des Betreibers, die Zugriff auf personenbezogene Daten haben, müssen über eine Datenschutzerklärung zur Wahrung des Datenschutzes verpflichtet werden. Dementsprechend ist es notwendig, dass auch eventuelle Subunternehmer des Betreibers und/oder des Anbieters einen ADV-Vertrag unterzeichnen.

Datenschutzmaßnahmen können auf zwei Arten umgesetzt werden:

durch organisatorische Maßnahmen:
Diese umfassen Arbeitsanweisungen an die betreffenden Mitarbeiter, welche die Anweisung durchführen. Die Umsetzung erfolgt mitarbeiterindividuell und ist kostengünstig, enthält aber einen menschlichen Faktor als Fehlerquelle.

durch technische Maßnahmen:
Die technische Umsetzung sorgt dafür, dass der Datenschutz grundsätzlich immer konstant und elementar eingehalten wird, ist aber finanziell aufwendig. Dennoch wird beim Digitalen Weiterbildungscampus die technische Lösung bevorzugt, da der menschliche Faktor damit ausgeschlossen werden kann.

FAZIT

Aufgabe des Datenschutzes ist, den Missbrauch von personenbezogenen Daten zu unterbinden und damit Tendenzen zum „gläsernen Menschen“ sowie zu Datenmonopolen von Privatunternehmen entgegenzuwirken. Diese Aufgabe wird in der Zukunft immer wichtiger werden. Der Digitale Weiterbildungscampus spiet hier eine Vorreiterrolle, indem er dem Datenschutz eine sehr hohe Priorität beimisst und die aktuellen Erkenntnisse des Bundesamts für Sicherheit in der Informationstechnik (BSI) zeitnah technisch umsetzt.

vimotion GmbH | Friedhofstrasse 26 | 71566 Althütte | Germany