Universität Bayern e.V.
Bayerische Universitätenkonferenz

HOCHSCHULE BAYERN

Gemeinsame Handreichung der IT-Leitungen

Einsatz von Windows 10 an Hochschulen

Johannes Nehlsen

Universität Würzburg
Rechenzentrum
Stabsstelle IT-Recht, Lizenzmanagement, E-Procurement
Am Hubland
97074 Würzburg

johannes.nehlsen@uni-wuerzburg.de

Stand: 25. Januar 2017

Zustimmung der CIO Hochschule Bayern e.V. am

Zustimmung der CIO Universität Bayern e.V. am

Inhalt

1. Zusammenfassung

Hintergrund

Das neueste Betriebssystem von Microsoft, Windows 10, ist aufgrund datenschutzrechtlicher Aspekte bezüglich seines Einsatzes in Hochschulen nicht unumstritten. Dennoch ist seine Einführung an Hochschulen nicht zu verhindern, da neue Hardware oftmals nur noch mit Windows 10 bestellt werden kann und viele Hersteller ab Herbst 2016 Geräte nur noch mit Windows 10 ausliefern. Eine nachträgliche Installation von Windows 7 auf neuer Hardware wird z.B. aufgrund fehlender Hardware-Treiber zunehmend schwierig. Alternative Betriebssysteme stellen für Hochschulen keinen vollwertigen Ersatz zu Windows dar.

Verantwortung der Leitung und Informationelle Selbstbestimmung

Die Leitungen der Hochschulen tragen in Bayern die Verantwortung für die Sicherheit ihrer IT-Systeme und haben im Rahmen ihrer Fürsorgepflicht als Arbeitgeber das informationelle Selbstbestimmungsrecht ihrer Beschäftigten zu schützen - Beschäftigte dürfen grundsätzlich davon ausgehen, dass bereitgestellte Betriebssysteme und Software datenschutzfreundlich konfiguriert sind. Vor diesen Hintergründen ist Windows 10 gegenüber vorherigen Windows-Versionen als ein informationssicherheitstechnisch wesentlich verbesserter Baustein für die Sicherheitskonzepte der nutzenden Hochschulen zu bewerten; dabei bietet insbesondere die zentrale Verwaltung von Windows 10 Systemen die Möglichkeit zur deutlichen Minimierung von Compliance-Risiken.

Versionswahl

Von den verschiedenen Versionen bieten Windows 10 Enterprise bzw. Education den besten Schutz und die umfangreichsten Einstellmöglichkeiten. Der Einsatz der Enterprise-Version – anders als der der Education-Version – gibt den Hochschulen die beste Planungssicherheit bzgl. der zur Verfügung stehenden Features und ermöglicht außerdem die Übernahme von „best practices“ für ihre IT aus der freien Wirtschaft.

Skype, OneDrive und Cortana

Die an private Endverbraucher gerichteten Dienste *Skype*, *OneDrive* und *Cortana* können derzeit nicht in rechtlich zulässiger Weise auf dienstlichen Geräten eingesetzt werden; weniger problematisch erscheint der Einsatz der Produkte *Skype for Business* und *OneDrive for Business*. Erforderlich ist jedoch der Abschluss eines Vertrages zur Auftragsdatenverarbeitung, den Microsoft unter Berücksichtigung der EU-Standardvertragsklauseln anbietet.

Azure Verzeichnisdienst

Die Nutzung der oben angesprochenen Businessdienste setzt einen Azure-Verzeichnisdienst voraus, für dessen Einführung der Abschluss eines Vertrages zur Auftragsdatenverarbeitung nach geltendem EU-Recht und die Dokumentation sowie die datenschutzrechtliche Freigabe des Verfahrens erforderlich sind. Darüber hinaus ist die Einführung mitbestimmungspflichtig.

Lizenzierung

Aus lizenzrechtlicher Sicht empfiehlt sich für die Hochschulen der Einkauf aller Nutzerendgeräte mit OEM-Windows-Lizenzen. So verfügen die Geräte über die notwendigen Basislizenzen, um dann z.B. mit einem auf Lizenzen aus Microsoft-Rahmenverträgen basierten Image bespielt zu werden.

Datenschutz

Betriebssysteme selbst sind nur mittelbar im Einsatz zur Verarbeitung personenbezogener Daten, somit muss der Einsatz von Windows 10 aus datenschutzrechtlicher Sicht nicht freigegeben werden.

Mitbestimmung

Windows 10 bietet keine Überwachungsmöglichkeit von Leistung oder Verhalten von Beschäftigten, daher ist der Einsatz nicht mitbestimmungspflichtig. Zu beachten ist allerdings die schon oben angesprochene Mitbestimmungspflicht beim Einsatz des Azure Verzeichnisdienstes oder der darauf aufsetzenden Kommunikationstools (z.B. Skype for Business).

2. Rechtliche Fragen im Detail

2.1. Private Microsoftbenutzerkonten

In den Benutzungsordnungen der Hochschulen werden die Beschäftigten zur Einhaltung von Mindestanforderungen z.B. bei der Wahl von Passwörtern angehalten[1]. Die Einhaltung derartiger Sicherheits- und Schutzmaßnahmen ist allerdings bei der Verwendung privater Microsoft-Benutzerkonten aufgrund fehlender Regelungskompetenz der Hochschulen nicht durchsetzbar, daher sollten private Microsoft-Benutzerkonten auf Dienstgeräten gesperrt werden[2].

Alternativ müssten bei der Gestattung der Nutzung privater Microsoftbenutzerkonten die durch den Datenschutz erforderlichen technischen und organisatorischen Maßnahmen überprüft werden, insbesondere Benutzerkontrolle, Zugriffskontrolle und Organisationskontrolle[3].

2.2. Windows Stores

Der Zugriff auf den Windows Store ist inzwischen auch nach einer Sperrung der privaten Microsoftbenutzerkonten möglich.[4] Aus lizenzrechtlichen Gründen ist eine Sperrung oder Kontrolle des Stores empfehlenswert, um zu verhindern, dass zu dienstlichen Zwecken über private Accounts beschaffte Apps nach Ausscheiden des Mitarbeiters für die Universität in Ermangelung der entsprechenden Lizenz nicht mehr zur Verfügung stehen; eine Übertragung von Nutzungsrechten ist in den Bedingungen des privaten Windows Stores nämlich nicht vorgesehen.[5] Noch schwerwiegender ist, dass in den Allgemeinen Nutzungsbedingungen, auch für die ohne Account erhältlichen Apps, die kommerzielle Nutzung von Apps ausgeschlossen wird, die aber bei der Installation einer App auf einem dienstlichen Endgerät im Regelfall vorliegen wird.[6] Verkompliziert wird dies nochmals dadurch, dass die jeweilige App wiederum eine gewerbliche Nutzung in zusätzlichen Lizenzbedingungen gestatten kann.[7] Bei der Verwendung des Stores mit Microsoft Businesskonten sind die oben genannten Lizenzschwierigkeiten wohl nicht zu erwarten. Über diese Kennungen wird auf den Windows Store für Unternehmen zugegriffen, der unter anderem den Erwerb von Volumenlizenzen, die Verteilung (auch eigener unternehmensinterner) Apps, sowie eine komplette App-Lizenzverwaltung ermöglicht.

2.3. Übermittlung von personenbezogen Daten

Grundsätzlich ist die Übermittlung von personenbezogenen Daten an Dritte und deren Verarbeitung durch diese nur nach Abschluss eines Vertrages über eine Auftragsdatenverarbeitung möglich[8]. Das heißt, dass auch die Nutzung des durch die Telekom treuhänderisch angebotenen Office 365 nicht den Abschluss dieses Vertrages erspart.[9]

Bei der Übertragung von Daten in Länder jenseits des europäischen Wirtschaftsraumes gelten darüber hinaus noch weitere Einschränkungen[10] zum Schutz der Privatsphäre sowie der Freiheiten und Grundrechte – für die USA wurden bis dato kein angemessenes Schutzniveau durch die zuständige EU-Kommission festgelegt. Um den Datentransfer zu einzelnen amerikanischen Unternehmen dennoch unbürokratisch zu ermöglichen, hatte die EU-Kommission die Entscheidung 2000/520 (Safe Harbour-Abkommen) getroffen, welche allerdings mit dem Urteil des EuGH für ungültig erklärt wurde[11]. Ab dem 1. August steht Unternehmen das Nachfolgeabkommen EU-US-Datenschutzschild zur Verfügung, wenn diese ihre Datenschutzmaßnahmen zertifizieren lassen.[12] Alternativ stehen für den Datentransfer auch die EU-Standardvertragsklauseln zur Verfügung[13].

Über die Gültigkeit dieser beiden Möglichkeiten entscheiden letztlich nicht die Datenschutzbehörden, sondern der Europäische Gerichtshof, dessen Rechtsprechung zu diesem Themenkomplex zu beobachten bleibt. Denn soweit Rechtsgrundlagen für den Datentransfer ungültig werden, müssen rechtlichen Grundlagen für den jeweiligen Auftragsdatenverarbeitungsvertrag durch andere gültige ersetzt werden oder der Vertrag ist zu beenden.

2.4. Cortana

Cortana ist der persönliche Assistenzdienst von Microsoft, ähnlich wie Siri von Apple oder Google Now von Google. Der Dienst benötigt folgende Daten: Gerätestandort, Daten aus dem Kalender, aus den Apps, die verwendet werden, Daten aus E-Mails und SMS-Nachrichten, Anrufinformationen, Kontakte und Geräteinteraktionen. Nach den Microsoft-Datenschutzbestimmungen[14] können zudem die erhoben Daten von Microsoft für Werbung und Business-Intelligenz eingesetzt werden. Nur für personalisiere Werbedaten verspricht Microsoft eine Löschung nach 13 Monaten.

Der Dienst bietet unbestreitbar einen erheblichen Komfortgewinn für den Nutzer. Auf der anderen Seite wird ein Risiko geschaffen, dass vertrauliche Informationen und personenbezogene Daten Dritter ungewollt an Microsoft inklusive Tochterfirmen, Agenten und Lieferanten preisgebenden werden. Ferner fehlt es einer rechtlichen Grundlage für die Übermittlung personenbezogener Daten an Dritte. Zwar kann in die Erhebung und Verarbeitung *eigener* personenbezogener Daten (Standort, eigener Kalender, App-Verwendungen, Geräteinformationen) eingewilligt werden, nicht aber für die Erhebung und Verarbeitung personenbezogener Daten *Dritter* (E-Mails und SMS-Nachrichten, Anrufinformationen, Kontakte). Während die „Einwilligung für Dritte“ durch private Nutzer sich im rechtlichen Graubereich bewegt, ist die rechtliche Beurteilung desselben Vorgangs auf dienstlichen Geräten eindeutig. Bereits das Übermitteln der Daten ist eine Ordnungswidrigkeit des Users und bei fehlenden Kontrollmaßnahmen auch der Leitung nach dem BayDSG[15]. Ein zulässiger Einsatz von Cortana ist unter den derzeitigen Nutzungsbedingungen von Microsoft **nur für rein private Zwecke auf privaten Geräten ohne dienstliche Daten** möglich.

Die Cortana Intelligence Suite als Lösung zu Big Data, Machine Learning, Datenvisualisierung und Business Intelligenz von Microsoft ist für diese Handreichung rechtlich zu komplex und bedarf einer gesonderten Begutachtung.

2.5. Azure Active Directory und Business-Microsoftbenutzerkonten

Mit Azure bietet Microsoft eine zentrale Plattform für diverse Dienste sowie für Cloudcomputing an. Als Basis für deren Nutzung dient das Azure Active Directory (AD). Dieses ermöglicht es Einrichtungen, für Beschäftigte Business-Microsoftbenutzerkonten bereit zu stellen. Über diese Konten können dann die Beschäftigten z.B. den Windows Store, Skype for Business, OneDrive for Business usw. verwenden.

Unter dem Vorbehalt einer vorhandenen rechtsverbindlichen Auftragsdatenvereinbarung mit Microsoft stehen dem Einsatz dieser Lösungen derzeit keine rechtlichen Bedenken entgegen. Microsoft bietet für die Nutzung von Azure AD den dafür notwenigen Vertrag mit EU-Standardvertragsklauseln an[16].

Die umfangreichen administrativen Kontrollmöglichkeiten für die genutzten Anwendungen[17] ermöglichen teilweise eine Überwachung von Beschäftigten, daher bedarf es zwingend der Mitwirkung der Personalräte bei der geplanten Einführung[18].

Selbstverständlich erfordert die Einführung eines neuen Verzeichnisdienstes aufgrund der darin enthaltenen umfangreichen personenbezogenen Daten eine datenschutzrechtliche Freigabe[19].

Studierenden und Beschäftigten können im Rahmen von Lizenzverträgen z.B. über einen Webshop Azure Instanzen oder Entwicklungsumgebungen „on demand“ zur Verfügung gestellt werden. Dieses ist ohne die Übermittlung personenbezogener Daten möglich und bedarf daher keines Vertrages über eine Auftragsdatenverarbeitung. Zu beachten ist allerdings, dass die interne Bereitstellung im Webshop datenschutzrechtlich relevante Prozesse beinhalten kann.

2.6. Office 365

Unter dem Vorbehalt einer vorhandenen rechtsverbindlichen Auftragsdatenvereinbarung mit Microsoft stehen dem Einsatz dieser Lösungen derzeit keine rechtlichen Bedenken entgegen. Microsoft bietet für Office 365 den dafür notwenigen Vertrag nach EU-Standardvertragsklauseln an.

2.6.1. Office

Die Microsoft Office Desktopanwendungen wie z.B. Word, PowerPoint, Excel oder Outlook stehen auch im Rahmen von Office 365 zur Verfügung. Studierenden und Beschäftigten kann im Rahmen von Lizenzverträgen z.B. über einen Webshop Office zum Download zur Verfügung gestellt werden[20]. Soweit hierbei keine personenbezogen Daten an Microsoft übermittelt werden, bedarf es hier keines Vertrages über eine Auftragsdatenverarbeitung.

2.6.2. Skype

Im Gegensatz zu *Skype for Business* (s.u.) wird *Skype* nur **Privatverbrauchern** zur Verfügung gestellt; es werden umfangreiche Zugriffsrechte auf gespeicherte Nachrichten, Videos und Dateien gewährt. Diese Zugriffsrechte können insbesondere auch zahlreiche in- und ausländische Behörden nutzen[21]. Die erhobenen Daten werden zudem für Marketingzwecke genutzt, für die zum Teil die „privacy policy“

des Online-Werbeunternehmens Conversant gilt[22]. Darüber hinaus liegt abseits einer in ihrer Wirksamkeit höchst zweifelhaften Einwilligung der User keine rechtlich tragbare Grundlage für den Datentransfer vor[23].

Die von Microsoft beworbene Selbstzertifizierung für Skype nach EU-US-Privacy Shield stellt alleine keine gütige Rechtsgrundlage für den Datentransfer dar, denn es fehlt an einem Vertrag über Auftragsdatenverarbeitung für „Skype".

Alleine diese ausschnittsweise Betrachtung der Nutzungsbedingungen zeigt, dass der Einsatz von Skype auf dienstlichen Geräten rechtlich nicht befürwortet werden kann. Auch mit Blick auf Alternativen wie Skype for Business, DFNVC[24] und andere VoIP-Lösungen **ist die Skype-Nutzung auf dienstlichen Geräten nicht zulässig**.

2.6.3. „Skype for Business"

Skype for Business ermöglicht Online-Besprechungen, Chats und Bildschirmübertragungen. Die Anwendung wurde für den Einsatz im Unternehmen entwickelt. Daten werden nur weisungsgebunden im Rahmen der erforderlichen Auftragsdatenverarbeitung von Microsoft verarbeitet. Beschäftigte die bisher Skype einsetzen, ist ein Umstieg auf die datenschutzfreundliche Businesslösung zu empfehlen. Microsoft bietet ferner kostenpflichtig über Partner Skype for Business Server an[25].

2.6.4. „OneDrive for Business"

Mit OneDrive for Business bietet Microsoft eine Cloudspeicher-Lösung für Unternehmen an, welche u.a. auch im Zusammenspiel mit einer lokal an der Hochschule betriebenen Sharepoint-Installation betrieben werden kann. Microsoft gibt an, dass in OneDrive gespeicherte Dateien verschlüsselt werden, es bleibt allerdings unklar, ob dabei auch die Dateinamen verschlüsselt werden. Eine Nutzung von OneDrive wäre somit nur bei Einsatz weiterer Lösungen[26] sinnvoll.

2.6.5. Nutzung der OneNote-App

OneNote ist ein umfassendes Notiz- und Merkzetteltool, welches zur Speicherung der darin enthaltenen Dateien OneDrive nutzt. Die Nutzung des OneNote-App sieht anders als die Desktopvariante zwingend den Einsatz eines Microsoftbenutzerkontos vor. Insoweit kann auf die vorherigen Ausführungen verwiesen werden, denn je nach eingesetztem Microsoftbenutzerkonto dient entweder OneDrive for Business, Sharepointserver oder das private OneDrive zur Notizablage.

2.7. Lizenzierung

Neben der mittlerweile üblichen Auditierung von Unternehmen werden in jüngster Vergangenheit auch zunehmend Hochschulen von Softwareherstellern auf die Einhaltung der Lizenzbestimmungen überprüft. Rechtlich tragen die Leitungen der Hochschulen die Verantwortung für eine ordnungsgemäße Lizenzierung, bei Überschreitung von Toleranzwerten drohen neben der Kostentragung für das Audit teure Nachlizenzierungen, Schadensersatzpflichten oder der Entzug der Lizenznutzungsrechte.

Für ein handhabbares Lizenzmanagement sollten nur Endgeräte mit einer Windowsbasislizenz angeschafft werden[27]. In der Regel ist dies die wirtschaftlichste Möglichkeit des Lizenzerwerbes, eine (auch nachträgliche) Softwareinventarisierung ist leicht über die auf den Geräten angebrachten Aufkleber möglich und der rechtmäßige Lizenzerwerb kann zusätzlich durch Vorlage der Rechnung nachgewiesen werden.

In Kombination mit der o.g. Basislizenzierung schaffen Lizenzen aus zusätzlichen Microsoft Rahmenverträgen[28] die rechtliche Voraussetzung, baugleiche Geräte mit hochschulspezifischen Images zu bespielen. Die Kombination aus Basislizenz und Rahmenvertragslizenzen schafft damit gute Voraussetzungen für eine einfache Verwaltung clientseitiger Windowslizenzen.

Abschließend ist zu bemerken, dass eine ordnungsgemäße Lizenzierung neben dem Erwerb auch die Zuweisung der Lizenz zu Geräten oder Nutzern erfordert. Wegen der Komplexität, die durch Zusatz-, Server- und Zugriffslizenzen entsteht, empfiehlt sich dazu der Einsatz eines zentralen Lizenzmanagements.

2.8. Datenschutz

2.8.1. Datenschutzrechtliche Freigabe

Betriebssysteme, wie auch auf diesen eingesetzte Anwendungssoftware, werden nur mittelbar zur Verarbeitung von personenbezogenen Daten durch Beschäftigte eingesetzt. [29] Auch ist der Zweck der Verarbeitung der Daten schon zuvor festgelegt worden, beispielsweise für Personaladministrations- und Informationssysteme oder Arbeitszeiterfassung;[30] daher ist für den Umstieg auf Windows 10 keine datenschutzrechtliche Freigabe erforderlich.

Die Verfahrensverzeichnisse sind jedoch dann anzupassen, wenn in diesen Client-Betriebssysteme aufgeführt sind. In der Regel lassen sich die meisten Verfahrensverzeichnisse jedoch auch abstrakt für einen Zugriff von Client auf Server / Datenbanken beschreiben mit Begriffen wie: Webanwendung oder Remotezugriffsanwendung.[31]

2.8.2. Schutz der Informationellen Selbstbestimmung der Beschäftigten

Die Leitungen der Hochschulen tragen in Bayern die Verantwortung für die Sicherheit ihrer IT-Systeme und haben im Rahmen ihrer Fürsorgepflicht[32] als Arbeitgeber das informationelle Selbstbestimmungsrecht ihrer Beschäftigten zu schützen – Beschäftigte dürfen grundsätzlich davon ausgehen, dass bereitgestellte Betriebssysteme und Software so konfiguriert sind, dass personenbezogene Daten nicht in unnötiger Weise leichtfertig preisgeben werden[33].

Entsprechende Schutzmaßnahmen müssen eingerichtet werden, sofern dieses unter wirtschaftlich zumutbaren Bedingungen möglich ist. Dabei müssen effektive Möglichkeiten wie z.B. der Einsatz von zentralen Administrationsmöglichkeiten (Gruppenrichtlinien) berücksichtigt werden. Unwirtschaftliche Maßnahmen und solche, die die IT-Sicherheit gefährden, können nicht verlangt werden, denn die Hochschulen bleiben in allen ihren Maßnahmen auch an Haushaltsrecht und die Grundsätze ordnungsgemäßer Verwaltung gebunden. Für die durch den Endanwender für Dienste freigegebenen **eigenen Daten**[34] sowie für die für den Betrieb von Systemen erforderlichen Datenübertragungen sind keine weiteren Schutzmaßnahmen vorzusehen.

Eine reine Information von Benutzern über datenschutzfreundliche Einstellungen von Windows 10 bietet oftmals nur einen sehr eingeschränkten und temporären Schutz; wirksamer geschützt werden können die Beschäftigten insbesondere durch zentral verwaltete Gruppenrichtlinien, welche die Umsetzung von Empfehlungen und Leitfäden wie z.B. die des Arbeitskreises Informationssicherheit der deutschen Forschungseinrichtungen (AKIF) ermöglichen[35]. Entsprechend der Bedürfnisse einzelner Anwendergruppen können individuelle oder generelle Anpassungen erfolgen. Zudem kann über Gruppenrichtlinien die Nutzung der privaten Microsoftbenutzerkennung unterbunden werden. Den besten Schutz und maximale Einstellmöglichkeiten ermöglichen die Versionen Windows 10 Enterprise bzw. Education, denn nur diese Versionen ermöglichen es, das Übersenden von Telemetrie-Daten an Microsoft nahezu vollumfänglich zu unterbinden.[36] Auch für die Microsoft Office Produkte sind ähnliche datenschutzfreundliche Voreinstellungen und ein Abschalten der Telemetrie möglich.

Empfehlenswert ist es zusätzlich, die Geräte über einen lokalen WSUS-Dienst mit Updates zu versorgen. Auf diese Weise können die Updates vor ihrem Rollout auf Probleme getestet werden, zugleich wird der einzelne Updateprozess nicht von Microsoftservern erfasst.

In diesem Zusammenhang ist auch darauf hinzuweisen, dass das von Microsoft angekündigte „Microsoft privacy dashboard“, das mit dem „Creators Update“ erscheinen soll, wohl nur für Privatanwender unter Nutzung eines Microsoftbenutzerkontos zur Kontrolle über die von Microsoft gesammelten Daten eingesetzt werden kann.[37] Gleichzeitig hat Microsoft angekündigt die Sammlung von Diagnose- und Telemetriedaten zu reduzieren. Für Organisation bleibt es jedoch die Aufgabe der Administratoren der Endgeräte und der IT-Infrastruktur eine datenschutzfreundlichen Voreinstellungen umzusetzen.[38] Soweit Microsoft technische Spezifikationen über die Auswertung von Telemetrie-Daten veröffentlicht hat, bedarf es darüber hinaus keiner weiteren Zusicherungen seitens Microsoft.[39]

2.9. Technische und Organisatorische Datenschutzmaßnahmen

Um den gesetzlichen Anforderungen[40] an den technischen Datenschutz zu genügen, sollte der Einsatz von Windows 10 ausschließlich in „Active Directories“ mit den entsprechenden Gruppenrichtlinien erfolgen.[41] Hierbei sollten Berichte und Empfehlungen der Fachpresse aufmerksam verfolgt werden und bei Bedarf umgesetzt werden.[42]

Ist ein Betrieb außerhalb eines „Active Directories“ jedoch organisatorisch unabwendbar, sollte Windows 10 nur zurückhaltend eingesetzt werden. Die betroffenen Mitarbeiter sind entsprechend über die Einhaltung des Datenschutzes und die Gefahren unbefugter Datenübermittlungen zu informieren.[43] Außerdem sollten auf solchen Geräten verpflichtend alternative technische Lösungen eingesetzt werden, die eine Datenübermittlung an Microsoft auf ein Minimum reduzieren.[44]

2.10. Versionswahl

Bereits wegen der nur in den Versionen *Enterprise* und *Education* vorhandenen umfangreichen Datenschutzeinstellungen (s.o.) sind diese Versionen den anderen vorzuziehen. In Test hat sich die LTSB als noch datensparsamer herausgestellt, bedingt jedoch einen Verzicht auf zahlreiche Funktionen.[45] Es kann zwar auch die LTSB-Version für den Einsatz auf Produktivsystemen gewählt werden, aber Microsoft gibt Brüche in der IT-Sicherheitsarchitektur der Einrichtungen zu bedenken.[46] Auf Grundlage einiger Informationen von Microsoft[47] sowie auf Basis der Features erscheint die Education-Version auf Schulen ausgerichtet und stellt gegenüber der Enterprise-Version die schlechtere Alternative für Hochschulen dar. Es ist weiterhin davon auszugehen, dass aufgrund der hohen Verbreitung der Enterprise-Version auf umfangreichste Informationen und „Best Practices“ zu allen Aspekten des Systembetriebs zurückgegriffen werden kann.

2.11. Sicherheit

Windows 10 ist gegenüber vorherigen Windows-Versionen als ein informationssicherheitstechnisch wesentlich verbesserter Baustein für die Sicherheitskonzepte der nutzenden Hochschulen zu bewerten[48]; dabei bietet insbesondere die zentrale Verwaltung von Windows 10 Systemen die Möglichkeit zur deutlichen Minimierung von Compliance-Risiken.

Microsoft hat für Windows 10 das sogenannte „Bounty Programm“ eingerichtet, welches die Zahlung von hohen Prämien für identifizierte und an Microsoft berichtete Sicherheitslücken vorsieht[49]; es ist davon auszugehen, dass dadurch auf Windows 10 gerichtete Cyberangriffe weniger wahrscheinlich als bei Vorgängerversionen von Windows sind. Darüber hinaus garantiert Microsoft Sicherheitsupdates im Extended Support bis 14. Oktober 2025, was den Hochschulen sehr gute Planungssicherheit bietet.

Das Bayerische E-Government-Gesetzt fordert zum 01.01.2018[50] die Erstellung von Informationssicherheitskonzepten[51]; in Hinblick darauf wird den Hochschulen empfohlen, kurz- bis mittelfristig Migrationspläne von Vorgängerversionen auf Windows 10 zu erarbeiten, auch, weil der Extended Support für Windows 7 am 14.01.2020[52] ausläuft und danach keine Herstellersicherheitsupdates mehr zur Verfügung stehen werden.

2.12. Beteiligung des Personalrats

Windows 10 bietet keine potentielle Überwachungsmöglichkeit von Leistung oder Verhalten der Beschäftigten, daher ist der Einsatz nicht mitbestimmungspflichtig. Zu beachten ist allerdings die schon oben angesprochene Mitbestimmungspflicht[53] beim Einsatz des Azure Verzeichnisdienstes oder der darauf aufsetzenden Kommunikationstools (z.B. Skype for Business).

---

1 Siehe z.B. § 5 Abs. 4 der Benutzungsordnung für Informationsverarbeitungssysteme der Universität Würzburg; § 4 Abs. 3 Benutzungsrichtlinien für Informationsverarbeitungssysteme des Leibniz-Rechenzentrums der Bayerischen Akademie der Wissenschaften - Appendix Nr. 1,2.

2 Die Einschätzung trifft im gleichen Maße auch auf private Apple-IDs oder private Google Konten zu. Eine technische Kontrolle über den Einsatz privater Accounts ist unter Windows 10 sowie unter MacOS leicht möglich, für das Management mobile Geräte bedürfte es eines Mobile-Device-Managements.

3 Art. 7 BayDSG.

4 https://heise.de/-3518211 - Appendix 2.1

5 https://www.microsoftstore.com/store/msde/de_DE/DisplayTermsOfUseAndSalePage/ Sofern nichts anderes angegeben ist, sind der Microsoft Store und die Dienste für Ihre persönliche und nichtgewerbliche Nutzung vorgesehen.

6 Wie vor – Appendix Nr. 3.

7 Z.B die VLC-App https://www.microsoft.com/de-de/store/p/vlc/9nblggh4vvnh . Weitere Beispiele im Appendix Nr. 3.1.

[8] Art. 6 BayDSG, Art. 11 BDSG.
[9] https://cloud.telekom.de/software/office-365/ - Appendix Nr. 4
[10] Art. 21 BayDSG.
[11] Urteil vom 6. Oktober 2015 - EuGH C-362/14 – Appendix Nr. 5.
[12] Entscheidung EU-Kommission 2016/4176 – Appendix Nr. 6.
[13] BeckOK DatenSR/Schantz BDSG § 4c Rn. 42-46, beck-online – Appendix Nr. 7.
[14] https://privacy.microsoft.com/de-de/privacystatement - Appendix Nr. 8.
[15] Art. 37 Abs. 1 BayDSG.
[16] Diese Verträge müssen individuell von jeder Hochschule abgeschlossen werden.
[17] https://products.office.com/de-de/business/office-365-trust-center-security - Appendix Nr. 9.
[18] Art. 75a Abs. 1 BayVG, PdK Bayern Bayerisches Personalvertretungsgesetz (BayPVG) BayPVG Art. 75a Mitbestimmung bei technischen Einrichtungen und automatisierten Verfahren 2. Mitbestimmung nach Absatz 1 Nrn. 1 und 2, beck-online – Appendix Nr. 10.
[19] Art. 26 Abs. 1 S. 1 BayDSG.
[20] Dieses wird z.B. bei „Studisoft“ bereits so praktiziert.
[21] Auszug aus den Datenschutzbestimmungen von Microsoft:
Gründe, warum Wir persönliche Daten teilen […] Schließlich greifen wir auf persönliche Daten inklusive Ihrer privaten Inhalte (wie die Inhalte Ihrer E-Mails in Outlook.com oder Dateien in privaten Ordnern auf OneDrive) zu, legen sie offen und bewahren sie auf, wenn wir in gutem Glauben annehmen, dass dies notwendig ist, um: 1. geltende Gesetze einzuhalten oder auf gerichtliche Verfahren zu antworten, einschließlich denen von Strafverfolgungsbehörden oder anderen staatlichen Stellen […] – Appendix Nr. 8.
[22] http://www.conversantmedia.com/legal/privacy– Appendix Nr. 11.
[23] Die Nutzungsbedingungen von Conversant, sind auf Englisch, während Skype in deutscher Sprache beworben wird. Englische Nutzungsbedingen sind in diesem Fall unwirksam: KG, Urteil vom 08.04.2016 - 5 U 156/14 zu WhatsApp; MüKoBGB/Wurmnest BGB § 307 Rn. 246, beck-online. – Appendix Nr. 12.
[24] https://www.vc.dfn.de/ - Appendix Nr. 13
[25] https://products.office.com/de-de/skype-for-business/server-hybrid - Appendix Nr. 14
[26] Appendix Nr. 15 und 16 - https://www.boxcryptor.com/de/firmenpaket, Kommerzieller Anbieter; https://cryptomator.org/de/, Open Source Software; derzeit nur für iOS verfügbar.
[27] Dieses wird auch für den Fall empfohlen, dass das Gerät zunächst z.B. mit Linux betrieben werden soll, da sich Einsatzszenarien von Hardware häufig während deren Lebenszyklus ändern können.
[28] Dies ist eine übliche Klausel in Microsoft Volumen Lizenzverträgen.
[29] Nicht einzelne Softwareprodukte sind nicht Gegenstand von Verfahren, sondern die dahinter stehenden Dienste oder Systemverbünde. Sibylle Gierschmann | Markus Saeugling in: Gierschmann/Thoma/Säugling, Systematischer Praxiskommentar Datenschutzrecht, 1. Aufl. 2014, § 4d Meldepflicht, Rn. 11 – Appendix Nr. 17
[30] v. d. Bussche in: Plath, BDSG, 4d BDSG, Rn. 6 - Appendix Nr. 18
[31] Diese Methode wird auch ausdrücklich vom der zentralen Datenschutzstelle der baden-württembergischen Universitäten gebilligt - Appendix Nr. 18.1.
[32] Der Begriff wurde dem rechtsdogmatisch richtigeren Begriff „Nebenpflicht“ wegen der besseren Verständlichkeit vorgezogen, vgl. ErfK/Preis BGB § 611 Rn. 615-616, beck-online. – Appendix Nr. 19. Für das Bestehen der Schutzpflicht allgemein: BeckOK ArbR/Joussen BGB § 611 Rn. 240ff – Appendix Nr. 20.
[33] Dies entspricht auch der Empfehlung des Community Draft des BSI-Grundschutzes zu Windows 10; SYS.2.2.3.A2 – Appendix Nr. 21
Für die Schutzpflicht ausgeprägt durch z.B. besonderen Browserkonfiguration siehe Ernst: Social Networks und Arbeitnehmer-Datenschutz(NJOZ 2011, 953, 957) – Appendix Nr. 22
[34] Der Schutz personenbezogener Daten Dritter besteht weiterhin fort; vgl. Ausführungen zu „Cortana“.
[35] Appendix Nr. 23: abrufbar unter: https://www.it-sicherheit.mpg.de/Orientierungshilfe_Windows10.pdf .
Der Leitfaden (Mai 2016) des Landesbeauftragten für den Datenschutz in Baden-Württemberg,unter: http://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2016/04/2016-04_leitfaden_win10.pdf abrufbar, berücksichtigt noch nicht die Änderungen des neuen Windows 10 Build 1607 von August 2016.
[36] https://technet.microsoft.com/en-us/itpro/windows/manage/configure-windows-telemetry-in-your-organization - Appendix - Nr. 24

[37] So heißt es in einem Blog von Microsoft dazu: “When you are signed in with your Microsoft account, you can go to account.microsoft.com/privacy to review and clear data such as browsing history, search history, location activity, and Cortana’s Notebook – all in one place.” Abrufbar unter https://blogs.windows.com/windowsexperience/2017/01/10/continuing-commitment-privacy-windows-10/#F3DAOAv3q1bE81Wc.97 .

[38] Auf diesen Umstand weist Microsoft explizit hin „Learn more about what we’re doing to help IT pros manage telemetry and privacy within their organizations here.” (wie vor) – Der Link verweist auf den in Fußnote 37 erwähnten – Appendix 24.

[39] Hier kann die rechtliche Wertung aus dem Vergaberecht übertragen werden, dass Erklärungen als ausreichend anzusehen sind, die sich aus Herstellerspezifikationen beziehen.

[40] Art. 7 Abs. 1 S. 1 BayDSG.

[41] Diese Pflicht wurde auch nochmals sehr deutlich in der Empfehlung des DFN-Vereins zu dem Thema „Datenschutzrechtliche Probleme bei der Einführung neuer Betriebssysteme – Eine Untersuchung am Beispiel von Windows 10“ hervorgehoben – Appendix 24.1.

[42] Hier sei auf den Beitrag in der iX 11/2016 S. 68 ff – Appendix 24.2. verwiesen.

[43] Siehe dazu Empfehlung Appendix 24.3.

[44] Eine empfehlenswerte kostenfreie Lösung ist z.B. O&O ShutUp10 von der O&O Software GmbH – Appendix 24.4. IT-Dienstleister können für diese Lösung auch fertige Profile anbieten.

[45] Siehe Appendix 24.5. https://technet.microsoft.com/itpro/windows/manage/introduction-to-windows-10-servicing

[46] Quelle: wie vor: “IT administrators can also install universal apps on devices when apps are compatible with the feature upgrades running on the device. They should do so with care, however, as servicing updates targeted for devices running Windows 10 Enterprise LTSB will not include security or non-security fixes for universal apps.”

[47] https://blogs.technet.microsoft.com/microsoft_presse/windows-10-anniversary-update-bietet-spannende-extra-features-fuer-lehrer-und-schueler/ - Appendix Nr 25.

[48] Vgl. nur Jan-Henrik Damaschke, Windows 10 - das Ende von Malware?, abrufbar unter http://www.golem.de/news/sicherheit-windows-10-und-das-ende-von-malware-1512-117849.html ; ct 2015 S. 87 – Appendix Nr. 26

[49] https://technet.microsoft.com/en-us/library/dn425036.aspx – Appendix Nr. 27.

[50] Art. 10 Abs. 2 S. 2 Nr. 3 BayEGovG.

[51] Art. 8 Abs. 1 BayEGovG.

[52] https://support.microsoft.com/de-de/lifecycle/search?sort=PN&alpha=Windows%207%20Enterprise&Filter=FilterNO – Appendix Nr. 28

[53] Art. 75a Abs. 1 BayVG, PdK Bayern Bayerisches Personalvertretungsgesetz (BayPVG) BayPVG Art. 75a Mitbestimmung bei technischen Einrichtungen und automatisierten Verfahren 2. Mitbestimmung nach Absatz 1 Nrn. 1 und 2, beck-online.