

Fragen der Teilnehmer im Webcast Heise/Telekom

„Erfahrungen aus erster Hand: Die IT-Abteilung und eine Microsoft-365-Einführung“ am 30.1.2020

Hier sind die Antworten zu den in der Sendung unbeantwortet gebliebenen Fragen:

1) Erfolgt der klassische Internetzugriff von BestSecret über einen Proxy (OnPrem, Cloud)? Falls ja, wie erfolgt der Zugriff auf Office365? Wie erfolgt der Internet- und Office365 Zugriff der Remote User?

Antwort: Der Zugriff für Office 365 (Public Cloud) erfolgt direkt über das Internet. Es ist kein Proxy dazwischengeschaltet. Die Remote User bzw. Mobile Worker erfolgt direkt „vor Ort“ in die Public Cloud.

2) Was meint SignInLogs via PowerBI?

Antwort: Es sind die „Berichte zu Anmeldeaktivitäten im Azure Active Directory-Portal“ gemeint. Hier lassen sich u.a. Anmeldeaktivitäten erkennen, bei denen sich ein Benutzer „ungewöhnlich häufig“ manuell mit seinem Benutzernamen und Kennwort anmeldet.

<https://docs.microsoft.com/de-de/azure/active-directory/reports-monitoring/concept-sign-ins>

3) Wie kann man den O365-Login der Mitarbeiter auf Unternehmenshardware beschränken?

Antwort: Hier können Sie bspw. den bedingten Zugriff / Conditional Access verwenden. Der bedingte Zugriff ist eine Funktion, die von Azure Active Directory verwendet wird, um bspw. den Zugriff nur durch von der Organisation verwalteten Geräte zuzulassen.

<https://docs.microsoft.com/de-de/azure/active-directory/conditional-access/overview>

4) Wie stehen Sie zu der Frage, ein einheitliches Office-Design in allen Office-Produkten zur Verfügung zu stellen und die MS-Office-Designs zu entfernen?

Antwort: Die Frage können wir leider nicht beantworten.

5) Wie sieht es mit dem Datenschutz bei Patientendaten (z.B. Word-Arztbriefe) im Gesundheitswesen (Krankenhäuser & Co.) aus? In Bayern müssen meines Wissens die Daten ja noch nicht in der Cloud abgelegt werden.

Antwort: Die Fragen rund um den Datenschutz und die Anforderungen aus dem Bereich des Gesundheitswesens müssen immer individuell aus Sicht der jeweiligen Organisation betrachtet werden.

Hier möchten wir Sie an unseren T-Systems-KollegInnen verweisen: <https://www.t-systems.com/de/de/branchen/gesundheitswesen>

6) Hallo, gibt es Schnittstellen zwischen Exchange und Legacy bzw. On-Premise-Systemen? Konnten die problemlos migriert werden?

Antwort: Der Kunde hatte bspw. ein Raumbuchungssystem, auf denen der Name des Termins und Bucher des Raumes angezeigt wurden. Diese Integration war ursprünglich in Exchange OnPrem eingebunden und wurde im Rahmen der Migration auf Exchange Online auch hier integriert. Das ist jeweils aber eine Einzelfallbetrachtung.

7) Die Betrachtung, welcher Weg für welche Mitarbeitergruppen am besten taugt: Wie seid ihr da vorgegangen? Gibt's da eine Checkliste o.ä.?

Antwort: Beim Kunden haben wir verschiedene Mitarbeiterprofile gebildet, um diese auf ihrem jeweiligen Stand des Wissens abzuholen. Der Rollout wurde mit einer Pilotgruppe verprobt.

8) Guten Tag, gibt es aus eurer Sicht eine schlaue Lösung, wie die Teams (user based installation) Firewall Rule gesetzt wird, auch wenn mal ein neuer Mitarbeiter sich an einem Gerät anmeldet?

Antwort: Eine individuelle Zugriffsberechtigung kann bspw. mit dem bedingten Zugriff / Conditional Access gesetzt werden. Der bedingte Zugriff ist eine Funktion, die von Azure Active Directory verwendet wird, um bspw. den Zugriff nur durch von der Organisation verwalteten Geräte zuzulassen. Die Firewall-Regeln verteilen wir beim Kunden via Intune und ordnen die Nutzer via Benutzergruppen zu.

<https://docs.microsoft.com/de-de/azure/active-directory/conditional-access/overview>

9) Gibt es denn bezüglich kirchlicher Anforderungen schon Lösungen?

Antwort: Die Fragen rund um den Datenschutz und die Anforderungen aus dem kirchlichen Umfeld müssen immer individuell aus Sicht der jeweiligen Organisation betrachtet werden.

Hier möchten wir Sie an unseren T-Systems-KollegInnen verweisen: <https://www.t-systems.com/de/de/branchen/oefentlicher-sektor/telekommunikation-im-sozialen-bereich>

10) Guten Tag, mich würde interessieren, ob und welche unterschiedlichen Datensicherungskonzepte z.B. O365 (auch hinsichtlich DSGVO Einhaltung) verfolgt wurden und wie diese dann realisiert wurden.

Antwort: Das muss man sich individuell anschauen, da jeder Kunde bzgl. der DSGVO eigene Anforderungen hat. Ein Backup von Office 365 mit Hilfe eines 3rd-Party-Backup-Anbieters kann im Einzelfall durchaus sinnvoll sein.

11) Was waren Ihre kritischsten Punkte bei der Datenschutzfolgeabschätzung bei O365?

Antwort: Das können wir leider nicht mitteilen.

12) Guten Tag, wie wird der Mail-Empfang/-Versand während der Migrationsphase gewährleistet?

Antwort: Die Bereitstellung von Office 365 / Exchange Online erfolgt in einem Exchange-Hybrid-Konzept. Damit können sowohl die OnPrem-Postfächer als auch die Online-Postfächer Mails empfangen. Die Empfängerobjekte sind auf beiden Seiten bekannt. Das ist quasi die Standardvorgehensweise bei dem Weg in die Cloud.

13) Gibt es ein frei verfügbares Dokument zur Datenschutzkonformität zu Office365? Von einem externen, also nicht Microsoft.

Antwort: Microsoft gibt an, dass seine Dienste der DSGVO entsprechen. Inwiefern die Nutzung in einer Organisation möglich ist, wird eine Einzelfallbetrachtung sein. Deswegen kann hier keine generelle Aussage gemacht werden.

14) Was passiert im Falle eines Internetausfalls?

Antwort: Best Secret hat eine redundante Internetleitung, die wir auch jedem Kunden empfehlen, der große Workloads in der Public Cloud verwendet. Des Weiteren haben die Mitarbeiter selbst – bspw. im HomeOffice – eine direkte Verbindung ins Internet.

15) Welches Tool wurde hier verwendet?

Antwort: Die Migration von OnPrem in die Cloud wurde mit Hilfe der Microsoft-„Bordmittel“ vorgenommen.

16) Haben Sie einen Prozess zur Archivierung von Teams? Ablage der Daten etc.

Antwort: Mit den Aufbewahrungsrichtlinien von Office 365 können diese Inhalte archiviert werden.

17) Und vor allem das Restore!

Antwort: Archivierung ist nicht Backup. Wenn Sie ein klassisches Backup/Restore-Konzept umsetzen möchten, dann können Sie dies mit Hilfe von 3rd-Party-Anwendungen wie Veeam oder Skykick machen.

18) Gibt es eine Exit-Strategie aus Office365?

Antwort: Der Funktionsumfang von Office 365 kann OnPrem nicht nachgebildet werden. Natürlich können einfache Workloads wie E-Mail auch wieder aus der Cloud in Richtung OnPrem umgezogen werden.

19) Auf Postfach oder auf Nachrichtenebene ein Restore

Antwort: Wenn Sie ein klassisches Backup/Restore-Konzept umsetzen möchten, dann können Sie dies mit Hilfe von 3rd-Party-Anwendungen wie Veeam oder Skykick machen.

20) Wie groß dürfen Postfächer werden?

Antwort: Die Postfächer bei Exchange Online haben eine Größe von 50 bzw. 100 GB. OnTop zählt die Archivierung dazu. Diese ist bei E3/E5 unbegrenzt.

21) Backup: Soweit mir bekannt ist, werden richtigerweise Backups durch Microsoft gemacht. Sollte es doch zu Datenverlust kommen, sind die Haftungssummen extrem gering. Wie hat man das Risiko bewertet?

Antwort: Das können wir leider nicht mitteilen.

22) Anschluss-Bandbreite von 1GB in beide Richtungen für wie viele Mitarbeiter?

Antwort: Ja – BestSecret hat eine redundante, synchrone Leitung für die Azure-Dienste (auf Basis einer ExpressRoute). Office 365 wird direkt in das Telekom/Microsoft Backbone geleitet (ohne einen zentralen Breakout).