Das Mobilfunkkonzept - Logistik, Support und MDM

Warum wurde das Projekt Mobilfunk - Logistik, Support und MDM gestartet?

Der stationäre Arbeitsplatz verliert so langsam an Bedeutung und es werden immer mehr mobile Geräte eingesetzt. Betrachten wir beispielsweise die Nutzung der Web-Seiten von Verlagen, wird auch dort sichtbar, dass mittlerweile weit mehr als die Hälfte aller Zugriffe von mobilen Geräten kommen. Um diese Geräte sicher betreiben zu können wurden Mobil-Device-Management (MDM) Systeme entwickelt. Heute nennt man diese Systeme auch Enterprise Mobility Management (EMM) System. Die Nutzung von Smartphones und Tablets durch Mitarbeiter kann mithilfe eines MDM bzw. EMM Systems sicher gestaltet werden. Die Strategie des Projektes befasst sich nicht nur mit Sicherheitsfragen, sondern unterstützt vor allem die Mitarbeiter dabei, die wichtigen Apps und Einstellungen auf das mobile Gerät zu bringen. Last-but-not-least werden mit diesen Mitteln die Anforderungen, die durch die DSGVO neu auf Unternehmen zugekommen sind, umgesetzt.

Was genau bedeutet das nun für den einzelnen Nutzer (für mich)?

Wird ein neues mobiles Gerät, egal ob Smartphone oder Tablet, in Betrieb genommen, so ist das bisher durch den Mitarbeiter selbst geschehen und war, je nach Gerät, mehr oder weniger aufwendig und kompliziert. Mit dem MDM System wird dieses nun deutlich einfacher. Die wichtigsten Einstellungen werden direkt mit der Inbetriebnahme auf das Gerät gebracht und die wichtigsten Unternehmens-Apps werden automatisch installiert. Schnell ist das neue Gerät einsatzbereit, nur die persönlichen Passwörter müssen noch eingegeben werden und es kann losgehen.

Sucht man im Netz nach MDM Systemen, so findet man auch Aussagen wie "Der Arbeitgeber kann dann alles auf meinem Smartphone sehen". Das mag von anderen Arbeitgebern durchaus so umgesetzt sein. In dem von MSP betriebenen System ist das jedoch so nicht vorgesehen und auch nicht eingerichtet. Es wird weder ein Geo-Tracking noch die Überwachung der mobilen Geräte durchgeführt. Das hat aber auch zur Folge, dass es kein Backup der mobilen Geräte gibt. Daten, die nur auf dem Gerät vorhanden sind, müssen vorm Mitarbeiter selbst gesichert werden. Das war vor der Einführung dieses Systems so und hat sich auch nicht verändert. Apps, die vom System installiert werden, halten ihre Daten aber auf zentralen Unternehmensservern und müssen nicht gesichert werden.

Vom MDM System werden keine PIN bzw. Kennwörter von Apps bzw. für den Zugang zu Diensten gespeichert. Aus diesem Grund muss bei der Einrichtung auch an einigen Stellen das Kennwort eingetragen werden.

Apps, die nicht zentral bereitgestellt werden, kann und muss jeder Anwender für sich selbst installieren. Genau wie vor der Einführung des MDM Systems, muss sich jeder selbst um die Sicherung der Daten und den rechtlich zulässigen Einsatz dieser Apps kümmern. Apps aus den üblichen Stores, z.B. Apple iTunes und Google Playstore, sind als zulässige Quellen eingestuft und können selbst installiert werden.

Dennoch gibt es ein paar Einschränkungen, die wir umsetzen mussten.

Die DSGVO fordert von Unternehmen die Einhaltung von einigen Vorschriften. Dazu zählt hauptsächlich der Schutz personenbezogener Daten. Gerade auf diesen Geräten gibt es eine Menge dieser Daten. Jeder hat eine umfangreiche Adress- bzw. Kontaktliste auf seinem mobilen Gerät gespeichert und auch in jeder E-Mail sind personenbezogene Daten, wie die Signaturen. Diese dürfen nur auf Servern innerhalb der Europäischen Union (EU) verarbeitet werden.

Nun gibt es Apps, die ihre Daten sofort auf Server außerhalb der EU speichern, wie z.B. WhatsApp und Facebook. Aber auch andere Apps tun dieses und das zum Teil sogar ohne den Anwender nach einer Erlaubnis zu fragen. Dennoch ist es durch die Einführung des MDM Systems jetzt möglich, auch diese Apps gesetzeskonform einzusetzen. Dazu wurde jedoch eine Einschränkung auf den mobilen Geräten notwendig. Es ist daher nicht möglich von nicht freigeschalteten Apps, wie z.B. die erwähnten Apps, auf die Exchange Adressbücher und Daten zuzugreifen. Daher müssen für diese Apps zusätzliche Adresslisten verwaltet werden. Dies kann z.B. das lokale Adressbuch sein, oder auch ein anderer Cloud-Dienst. Hierbei ist darauf zu achten, dass die gesetzlichen Vorschriften eingehalten werden.

Die zweite Einschränkung greift erst zum Jahreswechsel 2020/2021. Da Unternehmensdaten nicht auf privaten Endgeräten verarbeitet werden müssen, ist der Zugriff auf diese Daten (z.B. Mail- bzw. Exchange-Server) ab 2021 nur noch von Endgeräten möglich, die durch das MDM System verwaltet werden. Ist mein Gerät noch nicht im MDM registriert, wird ab 2021 der Zugriff auf mein Postfach und meine weiteren Daten auf dem Exchange-System verweigert. Die Dokumentation, wie das persönliche Endgerät im MDM registriert werden kann, steht auf diesem Confluence Bereich zur Verfügung.

Nach der Registrierung des Gerätes im MDM System werden Sie aufgefordert eine PIN zu setzen, die mindestens 6-stellig ist. Das dient Ihrer eigenen Sicherheit. Diese PIN wird nicht auf dem MDM System gespeichert, sondern nur auf dem Endgerät. Der Support hat keinen Zugriff auf diese PIN. Sollte die PIN verloren gehen, kann Ihnen dennoch geholfen werden, nur ist das Verfahren aus Sicherheitsgründen ein Einzelfall und wird hier nicht weiter beschrieben.

Hotline und Support

Mit der Einführung des neuen Systems wurde ich eine zentrale 7x 24h Hotline für Fragen rund um das mobile Endgerät eingeführt. Die Kontaktdaten dieser Hotline sind hier zu finden. Was leistet diese Hotline? Es werden Fragen rund um das eingesetzte Endgerät, das Betriebssystem auf diesem und zum Mobilfunkvertrag bearbeitet, sofern das Gerät im MDM registriert ist und der Mobilfunkvertrag bereits in das neue System migriert wurde. Nicht bearbeitet werden Fragen zu Apps, das kann kein Dienstleister zusagen, dass die Apps von sehr unterschiedlichen Herstellern kommen. Für Apps, die von Ihrem Unternehmen oder von MSP kommen, kann ein eingeschränkter Support gegeben werden. Es kann aber auch dazu kommen, dass Ihre Anfrage zunächst weitergegeben wird und erst am nächsten Arbeitstag während der Bürozeiten bearbeitet bzw. beantwortet werden kann. In diesem Fall werden Sie darauf vom Mitarbeiter der Hotline hingewiesen.

Ihr MSP Servicedesk Team