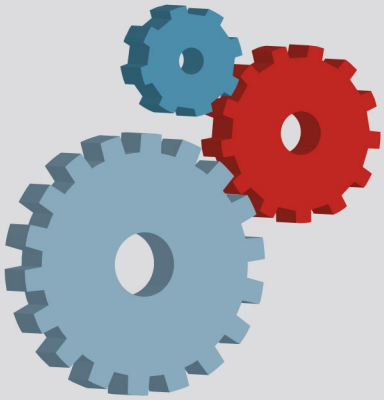
Bundesamt
für Sicherheit in der
Informationstechnik

Überblickspapier Consumerisation und BYOD



IT-Grundschutz aktuell

Was versteckt sich hinter Consumerisation und BYOD?

Zunehmend löst sich die Grenze zwischen beruflicher und privater IT-Nutzung auf. Viele Systeme, Programme und Dienste werden mittlerweile sowohl im beruflichen wie auch im privaten Umfeld genutzt. Diese Entwicklung wird als Consumerisation bezeichnet. Beispiele hierfür sind:

- Mitarbeiter wollen ihre privaten Smartphones und Tablets für dienstliche E-Mails, Termine und sonstige dienstliche Tätigkeiten nutzen.
- Mitarbeiter sind privat an Programme, wie z. B. das Grafikbearbeitungsprogramm GIMP, gewöhnt und möchten diese auch auf der Arbeit einsetzen.
- Mitarbeiter benutzen privat Internet-Dienste, wie z. B. Dropbox, zur Speicherung von Daten in der Cloud oder Werkzeuge, wie Doodle, um Termine abzustimmen und möchten diese Dienste auch beruflich nutzen.

Da sich für diese Entwicklung noch kein deutscher Begriff etabliert hat, wird in diesem Überblickspapier der englische Begriff Consumerisation benutzt. Unter dem Oberbegriff Consumerisation wird die Vermischung von privater und beruflicher Nutzung von Geräten, Programmen und Diensten diskutiert. In diesem Überblickspapier liegt der Fokus auf der Consumerisation von mobilen Endgeräten wie Smartphones und Tablets.

Eng mit Consumerisation der Endgeräte verwandt ist das unter der Abkürzung BYOD (Bring Your Own Device) bekannt gewordene Thema. Dabei handelt es sich um Strategien von Institutionen, ihre Mitarbeiter zur dienstlichen Nutzung ihrer privaten Geräte zu ermutigen oder sogar finanzielle Anreize hierfür zu schaffen. Die Besonderheit an BYOD ist, dass die Endgeräte zwar unter Umständen durch die Institution subventioniert werden aber Eigentum der Mitarbeiter sind. Consumerisation und BYOD sind also eng verwandte Themen. In diesem Überblickspapier wird der Fokus auf Consumerisation gelegt und am Ende ein Ausblick auf BYOD gegeben. Das Dokument richtet sich an IT-Grundschutz-Anwender mit dem Ziel zu sensibilisieren und Information zu einem aktuellen Thema bereitzustellen. Welche Lösungen in einer konkreten Institution umgesetzt werden können, kann nur vor Ort unter Abwägung aller Aspekte entschieden werden. Mit diesem Dokument soll die erforderliche Diskussion dazu angereichert werden.

Welche positiven Auswirkungen hat Consumerisation der Endgeräte für eine Institution?

Es gibt verschiedene Varianten, wie Consumer-Endgeräte in Institutionen eingesetzt werden. Beispielsweise nehmen einige Behörden und Unternehmen zunehmend Consumer-Endgeräte in die Produktpalette auf, aus der Mitarbeiter die für sie erforderlichen IT-Systeme auswählen können. Einige Unternehmen geben ihren Mitarbeitern jedes Jahr einen festen Betrag für Beschaffungen, lassen sie ihre Geräte frei auswählen und erlauben unter bestimmten Bedingungen die private Nutzung.

Vorteile der verschiedenen Varianten sind zum Beispiel:

- Die Zufriedenheit der Mitarbeiter steigt, wenn sie aktuelle Consumer-Endgeräte einsetzen können, beispielsweise weil sie benutzerfreundlicher sind oder als Statussymbole gesehen werden.
- Die Motivation der Mitarbeiter steigt, wenn sie bei der Auswahl der Endgeräte mitwirken können und ihre Vorlieben für bestimmte Produkte berücksichtigt werden.
- Die Mitarbeiter sind besser erreichbar, wenn sie beispielsweise ihr schönes und benutzerfreundliches dienstliches Consumer-Endgerät auch privat nutzen können.
- Mitarbeiter empfinden es als praktisch, anstatt mehrerer nur noch ein Smartphone für dienstliche und private Belange mit sich zu führen.

Einige Institutionen sehen einen Anreiz für Consumerisation auch darin, dass die IT-Anschaffungskosten auf den ersten Blick gesenkt werden, wenn die Endgeräte von den Mitarbeitern privat angeschafft werden und von der Institution subventioniert werden. Eine Wirtschaftlichkeitsbetrachtung muss aber auch die im Allgemeinen höheren Kosten für die zusätzlichen Administrations- und Sicherheitsmaßnahmen umfassen.

Herausforderungen für die Informationssicherheit

Der zunehmende Trend zur Consumerisation stellt das Informationssicherheitsmanagement in Unternehmen und Behörden vor große Herausforderungen, die sich auf unterschiedliche Bereiche zurückführen lassen.

- Mit Consumerisation wird die Grenze zwischen privater und dienstlicher Nutzung von IT-Systemen aufgehoben. Dadurch sind eine Reihe von Problemfeldern zu klären, beispielsweise durch wen und wie die Geräte gewartet, administriert und abgesichert werden, welche Kosten und Haftungsrisiken die Mitarbeiter und welche die Institution tragen und wer die Geräte wofür benutzen darf.
- Durch die Vermischung von privater und dienstlicher Nutzung ergeben sich spezifische Gefährdungen für die Informationssicherheit (siehe unten).
- Wenn Geräte sowohl privat und als auch dienstlich genutzt werden, ergeben sich dadurch verschiedene rechtliche Fragestellungen, die geklärt werden müssen. Hierzu gehört beispielsweise der Datenschutz. Da sich auf privat und dienstlich genutzten Endgeräten natürlich auch private personenbezogene Daten befinden, könnte eine zentrale Administration des Endgerätes durch die Institution datenschutzrechtlich problematisch sein. Ein anderer Bereich, der rechtlich geklärt werden muss, ist der der Software-Lizenzierung. Die Lizenzbedingungen von privat angeschaffter Software lässt eventuell keine dienstliche Nutzung zu und umgekehrt. Damit sind einige rechtliche Herausforderungen nur kurz angedeutet. Eine umfassende rechtliche Beurteilung muss in jedem Falle durch die Institution selbst vorgenommen werden.

Gefährdungen für die Informationssicherheit

Consumerisation bringt neben möglichen Vorteilen für die Institution auch verschiedene nicht zu vernachlässigende Gefährdungen für die Informationssicherheit mit sich.

- Ein Grundproblem mit vielen Consumer-Endgeräten ist, dass diese Geräte eher auf schönes Design und einfache Bedienung hin optimiert sind. Häufig entsprechen die Konfigurationsmöglichkeiten und die vorhandenen Sicherheitsfunktionen nicht dem Stand der Technik von anderen Endgeräten, die im professionellen Umfeld eingesetzt werden, wie z. B. Laptops. Oft lassen sich dadurch Sicherheitsvorgaben der Institution, wie Benutzertrennung und zentrale Administrierbarkeit, nicht oder nur teilweise umsetzen.

- Eine der größten Herausforderungen für die Informationssicherheit durch Consumer-Endgeräte besteht in der Durchlöcherung bzw. Auflösung der Grenzen des Informationsverbundes der Institution. Dies beginnt damit, dass schützenswerte Daten der Institution auf Endgeräten verarbeitet werden, die meistens nicht so gut abgesichert werden können wie Arbeitsplatzrechner. Zudem befinden sich mobile Endgeräte häufig außerhalb der geschützten Umgebung der Institution. Bei Consumer-Endgeräten lassen sich zwar Kommunikationsschnittstellen wie WLAN oder UMTS abschalten, wenn sie nicht genutzt werden. Allerdings kann in der Regel aber nicht ohne Weiteres erzwungen werden, dass nur gesicherte Netzverbindungen, also beispielsweise über einen verschlüsselten VPN-Tunnel, genutzt werden. Ferner werden Benutzer nicht immer darauf hingewiesen, wenn der VPN-Tunnel unwissentlich oder durch einen Angriff beendet und auf unverschlüsselte Datenverbindung umgeschaltet wird. VPN-Clients im Desktop-Bereich sind hingegen typischerweise so konfiguriert, dass in einem solchen Fall eine Warnmeldung ausgegeben und sogar der VPN-Tunnel wieder automatisch etabliert wird.
- Schwachstellen im Betriebssystem oder den installierten Anwendungen gefährden Consumer-Endgeräte im besonderen Maße, da Schwachstellen auf diesen Endgeräten unterschiedlich schnell oder manchmal sogar überhaupt nicht behoben werden. Dies hat mehrere Gründe: Zum einen muss ein Update in der Regel durch den Nutzer initiiert werden und geschieht nicht automatisch im Hintergrund. Zum anderen führt der deutlich kürzere Innovationszyklus der Endgeräte von derzeitig ungefähr einem halben Jahr dazu, dass der Fokus der Hersteller eher auf der Einführung von neuen Endgeräten als auf der langfristigen Unterstützung für ältere Geräte liegt. Zudem sind auf den eingesetzten Geräten unterschiedlicher Hersteller häufig verschiedene Varianten eines Betriebssystems installiert. Im Falle des bei Smartphones und Tablets weitverbreiteten Betriebssystems Android stellt beispielsweise jeder Gerätehersteller seine eigene Betriebssystemvariante für die jeweiligen Gerättypen her. Daher muss jeder Gerätehersteller einen entsprechend angepassten Patch für die jeweilige Betriebssystemvariante bereitstellen. Dies kann dazu führen, dass Endgeräte mit Betriebssystemen mit bekannten Schwachstellen längere Zeit ohne Patch verwendet werden. Wenn keine andere Sicherheitsmaßnahme greift, kann der hauseigene IT-Betrieb im Zweifelsfall solche Geräte nur noch aus dem internen Netz der Institution aussperren.
- Werden in einem Informationsverbund viele verschiedene Endgeräte mit unterschiedlichen Betriebssystemen eingesetzt, lassen sich in der Regel nicht alle Sicherheitsanforderungen, wie sie beispielsweise in der Sicherheitsleitlinie formuliert sind, auf allen Geräten in gleicher Weise umsetzen. Nicht alle Consumer-Endgeräte unterstützen beispielsweise eine vollständige Geräteverschlüsselung oder lassen differenzierte Rechtevergaben zu. Dadurch kann es zu unterschiedlichen Sicherheitsniveaus auf Geräten kommen, die eigentlich für vergleichbare Aufgaben benutzt werden sollen.

Sicherheitsmaßnahmen

Sicherheitsmaßnahmen für Consumerisation lassen sich grob in die Aspekte Organisation, technische Maßnahmen am Gerät und Anbindung an das Institutionsnetz aufteilen.

Organisatorische Maßnahmen

Wie viel Consumerisation in einer Institution ermöglicht werden soll, ist eine strategische Entscheidung, die vom Sicherheitsmanagement begleitet werden muss, um die Risiken steuern zu können. Wichtige organisatorische Maßnahmen sind:

- Wenn Consumer-Endgeräte in den Informationsverbund einer Institution integriert werden sollen, setzt dies eine umfassende Strategie voraus. In dieser Strategie sind die folgenden Fragen zu beantworten:
  - Welche Gerätetypen sollen generell eingesetzt werden dürfen bzw. vom Einsatz ausgeschlossen werden?
  - Welche Betriebssysteme sollen bzw. welche sollen nicht zum Einsatz kommen?
  - Welche Mitarbeiter dürfen zu welchen Zwecken Consumer-Endgeräte einsetzen?
  - Welche Informationen mit welchem Schutzbedarf dürfen mit diesen Geräten verarbeitet werden? Welche dieser Informationen dürfen über welche Kanäle kommuniziert werden?

Anhand dieser strategischen Entscheidungen müssen Konzepte erstellt werden, die den sicheren Betrieb der Consumer-Endgeräte in der Institution gewährleisten. Wenn sich herausgestellt hat, dass der Schutzbedarf der zu verarbeiteten Informationen durch das erreichbare Sicherheitsniveau der eingesetzten Consumer-Endgeräte nicht abgesichert werden kann, muss der Einsatz von Consumer-Endgeräten eingeschränkt oder verboten werden.

- Es muss geregelt werden, wie Consumer-Endgeräte in der Institution administriert werden. Consumer-Endgeräte zeichnen sich durch hohe Mobilität und eine große Vielfalt der Geräte-Typen und Betriebssysteme aus. Die Geräte sollten möglichst zentral administriert werden. Es ist sinnvoll, dazu ein Programm für die zentrale Administration, also zum Mobile Device Management (MDM), einzusetzen, welches außerdem die privaten und dienstlichen Bereiche dieser Geräte voneinander trennen kann. Bei der Auswahl eines MDM-Systems muss geprüft werden, ob die genutzten Consumer-Endgeräte von den jeweiligen MDM-Systemen in angemessener Weise gesteuert und die vorgegebenen Sicherheitsrichtlinien damit durchgesetzt werden können. Ob das möglich ist, hängt dabei maßgeblich vom Endgerät und dem darauf verwendetem Betriebssystem ab. Bei iOS verwendet beispielsweise jedes MDM-System die sogenannte "Configuration Utility". Daher kann ein MDM-System nicht mehr Einstellungen vornehmen, als diese Schnittstelle bereitstellt. Bei Android wird eine App des MDM-Systems auf dem Endgerät installiert. Über die für diese App eingeräumten Rechte wird festgelegt, was durch das MDM für dieses Endgerät vorgegeben werden kann. Zusätzliche Sicherheit wird nicht durch das zentrale MDM-System selbst, sondern durch weitere Anwendungen ermöglicht, die mit dem MDM-System zusammenarbeiten. Viele MDM-Systeme bieten eine App, die einen verschlüsselten Container bereitstellt, in dem ein eigener Browser, das dienstliche Telefonbuch und ein eigener E-Mail-Client für dienstliche E-Mails integriert sind.

  Durch die Auswahl der Endgeräte und eines MDM-Systems wird festgelegt, welches Sicherheitsniveau mit den damit verwalteten Geräten erreicht werden kann. Theoretisch könnten zwar zusätzliche Maßnahmen direkt an den einzelnen Geräten ausgeführt werden, allerdings steigt dadurch der administrative Aufwand erheblich und es kann nicht ohne Weiteres sichergestellt werden, dass diese Einstellungen von den Benutzern nicht wieder abgeändert werden.

- Da mobile Endgeräte häufiger als stationäre Systeme verloren gehen, müssen sowohl präventive als auch reaktive organisatorische Vorkehrungen getroffen werden, wie Verluste und Diebstähle verhindert werden sollen bzw. wie im Falle eines Falles damit umgegangen werden soll. Hierzu müssen klare Richtlinien durch die Institution aufgestellt werden. Auf der präventiven Seite sind bereits im Überblickspapier Smartphones bzw. in den IT-Grundschutz Bausteinen 3.404 Mobiltelefon und 3.405 PDA typische Maßnahmen wie "vollständige Verschlüsselung" und "gute Passwortwahl" bzw. "Sperre bei Inaktivität" nach hinreichend kurzer Zeit genannt. Typische reaktive Maßnahmen sind Fernlöschung, Fernsperrung und Ortung eines verloren gegangenen Geräts. Diese Funktionen werden in der Regel durch Dritt-Anbieter-Anwendungen umgesetzt, die für gewöhnlich zusätzliche Sicherheitsfunktionalitäten bereithalten, wie z. B. Virenschutz, gesicherte Surfumgebung und Firewall. Bei der Planung dieser Maßnahmen ist darauf zu achten, dass diese Dienste in der Regel voraussetzen, dass das Endgerät eingeschaltet ist und die SIM-Karte nicht entfernt wurde. Sollte ein Dieb die SIM-Karte entfernt haben, so kann das Gerät nur noch mit speziellen Diensten über die International Mobile Equipment Identity-Nummer (IMEI-Nummer) geortet, aber nicht mehr gelöscht werden. Aus diesem Grund sollten gegen Diebstahl weitere technische Maßnahmen am Gerät (siehe unten) vorgenommen werden.

  Bei jedem Verlust sollte die Lösch-, Sperr- und Ortungsfunktion von einer Service-Stelle der Institution eingeleitet werden, da hierfür in der Regel ein Computer mit Internetverbindung und Browser nötig ist, den die Mitarbeiter nicht unbedingt zur Verfügung haben. Es muss entschieden werden, zu welchen Zeiten diese Service-Stelle ihre Dienste anbieten soll (beispielsweise 24/7 oder 8/7) und es muss sichergestellt sein, dass alle Mitarbeiter mit mobilen Endgeräten die Kontaktdaten dieser Stelle kennen. Für die gegebenenfalls vorhandenen Zeiten, in denen keine zentrale Service-Stelle zur Verfügung steht, sollten Mitarbeiter die Möglichkeit haben, selbst angemessene Maßnahmen, z. B. über einen Web-Dienst einzuleiten. Überdies sollte der Zugang für verlorene oder gestohlene Geräte auf das Netz der Institution gesperrt werden. Ferner muss geregelt werden, wie mit wiedererlangten Endgeräten verfahren werden soll. Es wird empfohlen, mit speziellen Programmen alle Daten auf diesen Geräten zu löschen, danach auf den Werkszustand zurückzusetzen, gegebenenfalls vollständig neu zu installieren und dann neu zu konfigurieren. Mindestens sollten sie aber gründlich auf Schadsoftware untersucht werden. Gegebenenfalls sollten diese Geräte auch auf Manipulationen der Hardware hin untersucht werden.

- Mitarbeiter müssen für die Informationssicherheit bei Consumer-Endgeräten gesondert geschult und sensibilisiert werden, da sich die Gefährdungslage bei Consumer-Endgeräten wie z. B. Smartphones von der Gefährdungslage von Business-Endgeräten wie z. B. Laptops unterscheidet. Insbesondere müssen die Mitarbeiter verstehen, wieso die diversen Sicherheitsmaßnahmen nötig sind, damit diese von ihnen nicht umgangen werden, wenn sie als einschränkend empfunden werden. Die Mitarbeiter müssen auch wissen, welche Arten von Informationen mit diesen Geräten verarbeitet werden dürfen und welchen Schutzbedarf diese Informationen haben. Zudem müssen die Mitarbeiter wissen, wie sie sich bei Verlust oder Diebstahl von Geräten zu verhalten haben und wie die gegebenenfalls vorhandenen Dienste bedient werden, mit denen ein Gerät gesperrt, gelöscht und geortet werden kann.

Technische Maßnahmen am Gerät

Auf dem Endgerät müssen private und dienstliche Daten und Anwendungen strikt getrennt werden. Dienstliche Daten wie z. B. Telefonbücher oder Dateien dürfen nicht an privat genutzte Synchronisierungs- oder Cloudspeicher-Dienste weitergegeben werden. Auf der anderen Seite darf die Institution keine privaten Informationen, wie beispielsweise private Telefonbücher, E-Mails, Authentisierungsdaten zu Webdiensten oder Bilder der Kamera unerlaubt auslesen.

Anhand der gewählten Strategie und des Schutzbedarfs der mit dem Gerät zu verarbeitenden Daten muss ein geeignetes MDM-System (siehe auch die Veröffentlichung zur Cybersicherheit zum Thema MDM unter https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_downloads/empfehlungen/unternehmen/BSI-CS_052.pdf) und damit die geeignete Technik zur Trennung zwischen privaten und dienstlichen Bereichen ausgewählt werden. Es existieren verschiedene Möglichkeiten zur Trennung der privaten und dienstlichen Bereiche, die jeweils verschiedene Vor- und Nachteile aufweisen:

- Im einfachsten Fall wird auf den Geräten eine Applikation installiert, die einen Datencontainer mit allen dienstlichen Daten und Zugängen verwaltet. Diese Applikation muss für sämtliche dienstlichen Tätigkeiten ausgelegt sein. Das heißt, sie muss dienstliche Groupware (E-Mail, Termine, Kontakte, Aufgaben) und einen eigenen Browser beinhalten und selbsttätig eine verschlüsselte Verbindung zur Institution aufbauen. Die Trennung zwischen den verschiedenen Applikationen erfolgt allerdings ausschließlich durch das Betriebssystem. Daher ist die Wirksamkeit dieser Trennung vom eingesetzten Betriebssystem und dessen Zugriffskontrollmöglichkeiten (Mandatory Access Control, MAC) abhängig und somit von System zu System unterschiedlich. Für diese Variante muss in der Regel nicht in das Betriebssystem selbst eingegriffen werden und sie ist für verschiedene Betriebssysteme erhältlich. Unabhängig davon, von welchem Hersteller eine Applikation für die Trennung zwischen privaten und dienstlichen Daten eingesetzt wird, sollte die Applikation die dienstlichen Daten im Container verschlüsseln und so bei privater Nutzung des Endgerätes den Zugriff auf die Daten durch andere, gegebenenfalls bösartige Applikationen verhindern. Es kann sinnvoll sein, dass der IT-Betrieb zusammen mit dem Sicherheitsmanagement eine Ausschlussliste (Blacklist) von den Anwendungen erstellt, die Funktionen oder Rechte besitzen, durch die die Informationssicherheit der dienstlichen Anwendungen gefährdet werden könnte. Ein Einstieg kann sein, in diese Ausschlussliste alle Anwendungen aufzunehmen, die bestimmte Rechte verlangen, die vom Sicherheitsmanagement als kritisch eingestuft werden. Zusätzlich sollten sich Benutzer vor einem Zugriff auf den Container erfolgreich authentisieren müssen. Verbindungen zum Netz der Institution müssen kryptografisch abgesichert werden. Lösungen, die dies nicht unterstützen, bieten keinen hinreichenden Schutz und sollten daher nicht eingesetzt werden.
- Eine andere Möglichkeit, die Informationen der Institution zu schützen, ist, diese Informationen auch bei der Verarbeitung auf den Servern der Institution zu belassen. In diesem Fall wird auf dem Client lediglich eine Oberfläche bereitgestellt, die über eine abgesicherte Netzverbindung die Anwendung zur Bearbeitung der Information auf einem Server der Institution bedient. Das entsprechende Programm auf dem Endgerät muss dabei so konfiguriert werden, dass die Daten nicht lokal gespeichert werden können. Solche Thin-Clients oder serverbasierten Lösungen sind auch im Desktop-Bereich seit Längerem im Einsatz. Damit eine serverbasierte Lösung funktionieren kann, muss jedoch zu jedem Nutzungszeitpunkt eine ausreichend dimensionierte Internetverbindung verfügbar sein. Ferner muss der Dienst auf die Randbedingungen eines Smartphones oder Tablets (berührungsempfindlicher Touch-Screen statt Maus und Tastatur) angepasst sein. Reine Groupware-Anwendungen können auch ohne eigene Thin-Client-Anwendung durch einen Web-Service für den Browser im Smartphone oder Tablet bereitgestellt gestellt werden, der über VPN nur vom internen Netz aus erreichbar ist.

- Eine weitere Möglichkeit, private und dienstliche Bereiche auf Endgeräten zu trennen, besteht darin, diese Bereiche als unterschiedliche virtuelle Maschinen auf einem Gerät zu betreiben. Im Unterschied zur ersten Lösungsmöglichkeit wird bei der Virtualisierung der private und dienstliche Bereich nicht auf Anwendungsebene, sondern auf Betriebssystemebene getrennt. Die Schnittstellen, die sonst zwischen Anwendungen durch das Betriebssystem mit seinen vorhandenen Zugriffskontroll-Mechanismen bereitgestellt werden, werden hierdurch entfernt. Ein Datenaustausch zwischen beiden virtuellen Maschinen ist nur über die tiefer liegende Virtualisierungsschicht in Form des Hypervisors (auch Virtual Machine Monitor, VMM genannt) möglich. Zudem können in den einzelnen virtuellen Bereichen jeweils eigene Anwendungen installiert und getrennt voneinander betrieben werden. So kann auch dem Bedürfnis der Benutzer Rechnung getragen werden, eigene Apps zu installieren und zu benutzen. Eine Ausschlussliste für Anwendungen ist in diesem Fall in der Regel nicht nötig, da die Anwendungen nur in einer virtuellen Maschine arbeiten und somit Anwendungen in dem privaten Bereich nicht auf die Daten und Anwendungen im dienstlichen Bereich zugreifen können.

Welche der dargestellten Sicherheitslösungen als angemessen bewertet wird, hängt vom konkreten Anwendungsfall ab. Generell lässt sich zu den vorgestellten Lösungen aber Folgendes sagen:

- Eine Virtualisierungslösung bietet – bei entsprechender Qualität des Hypervisors – ein höheres Maß an Sicherheit als eine Container-Lösung. Andererseits haben Virtualisierungslösungen folgende Nachteile:
  - Es muss sehr tief in das Betriebssystem eingegriffen oder es muss sogar ausgetauscht werden. Dies wird von vielen Geräteherstellern verboten oder durch technische Maßnahmen unterbunden. Bei allen Geräteherstellern erlischt in der Regel mit einem solchen Eingriff in das Betriebssystem die Garantie auf das Endgerät.
  - Eine Virtualisierungslösung erhöht in der Regel den Stromverbrauch deutlich, sodass der Akku im Vergleich zu einem Gerät ohne Virtualisierung deutlich schneller entlädt.
  - Eine Virtualisierungslösung ist nicht auf allen Endgeräten realisierbar, da einige Gerätetreiber nicht zur Verfügung stehen.
- Eine Container-Lösung bietet zwar ein geringeres Maß an Sicherheit als die Virtualisierungslösung, aber im Gegenzug wird nicht so tief in das Betriebssystem eingegriffen, so dass die Gewährleistung für das Endgerät in der Regel nicht erlischt.
- Sowohl bei der Container- als auch bei der Virtualisierungslösung können eventuell unbeabsichtigt bei Datensicherungen durch die Institution private Daten mit einbezogen werden. Bei der Virtualisierungslösung ist dies deutlich unwahrscheinlicher als bei der Container-Lösung, da bei Ersterer die Trennung zwischen privaten und dienstlichen Bereich strikter umgesetzt ist. Bei der Thin-Client-Lösung ist dies hingegen ausgeschlossen, da keine dienstlichen Daten auf dem Endgerät gespeichert werden und damit auch nicht gesichert werden müssen.
- Eine Thin-Client-Lösung setzt eine durchgehend verfügbare und ausreichend dimensionierte Internetverbindung voraus. Dies ist nicht flächendeckend in Deutschland gewährleistet und im Ausland entstehen durch Daten-Roaming in der Regel hohe Kosten. Kurzzeitige Verbindungsausfälle können die Anwendungen auf dem Server stören und gegebenenfalls werden sogar Daten zerstört. Zudem steigt durch die dauerhafte Datenverbindung der Stromverbrauch erheblich an, wodurch die Betriebsdauer bis zum nächsten Aufladen verkürzt wird.

Neben diesen oben genannten Lösungen zur Trennung von privaten und dienstlichen Daten werden aktuell auch noch weitere Konzepte diskutiert. So könnte auf das Endgerät ein komplett neues Betriebssystem installiert werden, das mit einem besonders gehärteten Betriebssystemkern ausgestattet ist und die Trennung zwischen privaten und dienstlichen Daten durch restriktivere und stärkere Zugriffskontrollmechanismen realisiert. Des weiteren wird eine Dual-Boot-Lösung diskutiert, bei der ein zweites, speziell abgesichertes Betriebssystem von einer separaten Speicherkarte bei Bedarf gestartet wird. Wie gut die tatsächliche Sicherheit dieser genannten Konzepte ist, lässt sich im vorhinein jedoch nicht abschätzen und hängt neben der vielversprechenden Idee von der konkreten Umsetzung ab.

Abgesehen von diesen technischen Maßnahmen, um die Consumer-Endgeräte im Informationsverbund einer Institution sicher zu steuern und den privaten und dienstlichen Bereich zu trennen, gibt es noch eine ganze Reihe weiterer technischer Maßnahmen, die bereits im IT-Grundschutz Überblickspapier zu Smartphones aufgeführt worden sind und umgesetzt werden sollten. Je nach Höhe des Sicherheitsbedürfnisses oder sonstigen Anforderungen der Behörde oder des Unternehmens kann es sein, dass trotz der ergriffenen Maßnahmen ein zu hohes Risiko für die Informationssicherheit bestehen bleibt. In diesem Fall muss der Einsatz von Consumer-Endgeräten im Informationsverbund der Institution hinreichend eingeschränkt oder verboten werden.

Maßnahmen zur sicheren Anbindung an das Institutionsnetz

Um den Gefährdungen für die Informationssicherheit durch die Anbindung von Consumer-Endgeräten über unsichere Netze an das Netz der Institution zu begegnen, sollten folgende Maßnahmen ergriffen werden:

- Die Verbindung zwischen Endgerät und Institution muss verschlüsselt werden, z. B. über einen verschlüsselten VPN-Tunnel. Nur so kann verhindert werden, dass die Informationen aus der Datenverbindung abgehört werden können.
- Die Consumer-Endgeräte sollten in einem eigenen Netzsegment untergebracht werden, das von den Netzsegmenten der übrigen Arbeitsplatzrechner getrennt ist. Diese Trennung sollte so ausgestaltet sein, dass die Consumer-Endgeräte nur mit den notwendigen Komponenten im Netz (beispielsweise dem Groupware-Server) kommunizieren können. Nur so kann verhindert werden, dass prinzipiell unsicherere Consumer-Endgeräte die übrigen Arbeitsplatzrechner kompromittieren.
- Alle Serverdienste, die durch die Consumer-Endgeräte in den Informationsverbund der Institution aufgenommen werden müssen, sollten soweit möglich ebenfalls in einem eigenen Netzsegment untergebracht sein. Die Datenübertragung zu anderen Servern und Clients im Informationsverbund und zum Internet sollte auf ein notwendiges Maß eingeschränkt und soweit wie datenschutzrechtlich möglich überwacht werden, damit schützenswerte Informationen nicht an unbefugte Stellen abfließen können.
- Es sollten sich nur dafür zugelassene Endgeräte mit dem Netz der Institution verbinden dürfen. Nur so kann sichergestellt werden, dass nur freigegebene Geräte Zugang zum Netz der Institution haben und der Zugang für verloren gegangene oder gestohlene Endgeräte verwehrt werden.
- Es sollte nachvollziehbar sein, welche Endgeräte wann mit dem Netz der Institution verbunden waren.
- Auch Consumer-Endgeräte müssen die Geräte einen aktuellen Virenschutz (Dies ist derzeit bei iOS nicht möglich.) und die freigegebenen Betriebssystem-Updates enthalten. Es muss überprüfbar sein, ob die Geräte diese und alle sonstigen Sicherheitsvorgaben der Institution erfüllen. Geräte, die diese Vorgaben nicht erfüllen, dürfen keinen Zugriff auf das Netz der Institution erhalten oder müssen in einem getrennten Quarantäne-Netz untergebracht werden.

In der Regel verfügen Institutionen bereits über Möglichkeiten, eine Verbindung zum institutionseigenen Netz über VPN aufzubauen, die unter Beachtung der Netzsegmentierung auch auf die neu anzubindenden Consumer-Systeme ausgeweitet werden kann. Besondere Sicherheitshinweise sind im Baustein 4.4 VPN der IT-Grundschutz-Kataloge enthalten. In der Regel sind heutige Consumer-Endgeräte VPN-fähig und gestatten meistens sogar eine zertifikatsgestützte Authentisierung für eine Netzzugangskontrolle.

Die Übrigen der oben genannten Empfehlungen können durch eine Netzzugangskontrolle und das gewählte MDM-System umgesetzt werden. Eine Netzzugangskontrolle besteht neben dem Authentikator und Authentisierungsserver in der Regel aus einem weiteren Serverdienst, der überprüft, ob das Endgerät die Sicherheitsvorgaben erfüllt. Außerdem kann dieser Serverdienst auf Verstöße reagieren und z. B. ein ungepatchtes Endgerät in ein besonderes Quarantäne-Netzsegment einsperren und so die Gefahr für andere Endgeräte im Netz der Institution gering halten. Um zu überprüfen, ob ein Endgerät die Sicherheitsvorgaben der Institution erfüllt, muss entweder das Endgerät von außen gescannt werden oder mit einem sogenannten Agenten ausgestattet werden, der das Gerät lokal überprüft und die Informationen dem Server zur Verfügung stellt. Dieser Agent ist entweder ein Bestandteil des MDM-Systems oder Teil des Betriebssystems und kann bei Abweichungen das Endgerät so konfigurieren, dass es wieder alle Sicherheitsvorgaben erfüllt.

Nähere Details zum Thema Netzzugangskontrolle sind im gleichnamigen IT-Grundschutz-Überblickspapier zu finden.

Bring your own Device (BYOD)

Mit Bring your own Device werden Strategien bezeichnet, bei denen Mitarbeiter ihre eigenen IT-Geräte in die Institution mitbringen und einsetzen dürfen. Im Gegensatz zu Consumerisation werden durch BYOD also Consumer-Endgeräte im Informationsverbund der Institution zugelassen, die ***nicht der Institution gehören***. Alle hier vorgestellten Gefährdungen für die Informationssicherheit sind im Wesentlichen auch dann relevant, wenn in der Institution eine BYOD-Strategie umgesetzt wird, da sowohl bei Consumerisation als auch BYOD IT-Geräte aus dem privaten Endkunden-Bereich im beruflichen Umfeld eingesetzt werden.

Allerdings sind die Sicherheitsmaßnahmen bei BYOD deutlich schwieriger umzusetzen, da viele Benutzer erfahrungsgemäß nicht bereit sind, für ihre eigenen Geräte Einschränkungen hinzunehmen oder Zugriffe auf das Gerät durch den Arbeitgeber zu erlauben. Vor allem Sicherheitsmaßnahmen, bei denen Eingriffe erforderlich sind, so dass die Garantie für das Gerät erlischt, werden sich in der Regel nicht umsetzen lassen. Zusätzlich steigt die Heterogenität des Endgeräte-Parks, wenn eine BYOD-Strategie umgesetzt wird.

Daher muss bei BYOD-Überlegungen als Erstes geklärt werden,

- ob eine solche Strategie mit den Sicherheitsanforderungen der Institution vereinbar ist und
- welche Rahmenbedingungen dabei eingehalten werden müssten und ob unter diesen Rahmenbedingungen BYOD für die Mitarbeiter überhaupt noch akzeptabel ist.

Wenn eine BYOD-Strategie nicht mit den Sicherheitsanforderungen des Unternehmens oder der Behörde vereinbar ist, beziehungsweise die nötigen Randbedingungen für die Mitarbeiter inakzeptabel sind, kann in dieser Institution in der Regel kein BYOD umgesetzt werden. Aus Sicherheitssicht kann BYOD zudem auch nicht bedeuten, dass beliebige Endgeräte uneingeschränkt eingesetzt werden dürfen. Typische und meist tragbare Lösungen sind:

- Beschränkung auf ausgewählte Endgeräte-Typen: Die wenigsten Institutionen werden in der Lage sein, eine unbeschränkte Menge von verschiedenen Endgeräte-Typen, Betriebssystemen und Applikationen zu administrieren und deren Sicherheit im Blick zu behalten. Daher sollte auch bei einer BYOD-Strategie die Art der zugelassenen Endgeräte beschränkt werden, abhängig von den Ressourcen des IT-Betriebs.
- Benutzertypen identifizieren: Ebenso sollten die verschiedenen Benutzertypen identifiziert werden. Nicht jeder Mitarbeiter möchte unbedingt eigene Geräte einsetzen und auch die Motivation, dies tun zu wollen, kann sehr unterschiedlich sein. Daher kann es sinnvoll sein, für die verschiedenen Personengruppen jeweils angepasste Spielregeln zu erstellen. IT-affine Personen können z. B. auch Sicherheitsmaßnahmen umsetzen, die erklärungsbedürftig sind und bei denen sie selbst aktiv werden müssen. Viele Mitarbeiter wollen meistens nur unterwegs Termine einsehen oder im Internet arbeiten können. Hierfür lassen sich meist einfach sicherheitskonforme Lösungen finden. Wünsche, administrative Zugriffe aus der Ferne von einem Smartphone aus durchführen zu können, sind aus Sicherheitssicht wesentlich schwieriger zu lösen.

Mit einer BYOD-Strategie wird den Mitarbeitern eine sehr große Verantwortung nicht nur für die Sicherheit der Endgeräte, sondern auch für die Gesamtsicherheit der Institution übertragen. Diesem Kontrollverlust muss ein valides Vertrauen der Institution in das Verantwortungsbewusstsein der Mitarbeiter gegenüberstehen. Auf der Basis dieses Vertrauens müssen klare Regelungen zwischen Mitarbeitern und Institution vereinbart werden. Die Mitarbeiter müssen dabei zusichern, dass auf den Endgeräten

- aktuelle Virenschutz-Programme (soweit verfügbar) eingesetzt werden,
- alle Sicherheitspatches zeitnah eingespielt werden,
- jedes Endgerät ausschließlich durch den jeweiligen Mitarbeiter genutzt wird,
- der Zugriff auf die Endgeräte angemessen geschützt ist, z. B. durch starke Passwörter, und
- alle lokal gespeicherten Daten verschlüsselt werden.

Weitere Punkte aus dieser Vereinbarung sollten sein:

- Die Mitarbeiter müssen sofort melden, wenn Endgeräte, die auch für berufliche Belange genutzt wurden, verloren gegangen sind. Eine solche Meldung sollte auch gemacht werden, wenn ein Endgerät nur für eine gewisse Zeitspanne nicht auffindbar ist. Die Institution sollte prüfen, ob Mitarbeiter durch einen institutionseigenen bereitgestellten Dienst zur Löschung, Sperrung und Lokalisation der Endgeräte motiviert werden können, Verluste besonders schnell zu melden.

- Es sollte geklärt sein, welche Anwendungen auf dem Endgerät ausgeführt werden dürfen und welche explizit ausgeschlossen werden. Hierzu könnte es beispielsweise eine Liste im Intranet geben. Viele MDM-Lösungen bieten Funktionen an, um spezielle Anwendungen zu erlauben bzw. auszuschließen. Ferner sollte es einen Prozess geben, Anwendungen in diese Listen aufzunehmen bzw. wieder entfernen zu lassen.
- Es ist für die Anwender explizit zu verbieten, die Endgeräte zu rooten, einen Jailbreak oder sonstige tiefer gehende Eingriffe in das Endgerät durchzuführen.
- Es ist zu regeln, welche Daten die Mitarbeiter mit anderen Endgeräten oder Diensten im Internet synchronisieren dürfen. Eine strikte Trennung von privaten und dienstlichen Daten muss dabei sichergestellt sein.
- Die Institution sollte die Erlaubnis einholen, automatisierte Scans der Endgeräte im Rahmen von Netzzugangskontrollen durchzuführen, um überprüfen zu können, dass die Endgeräte die Sicherheitsvorgaben einhalten.
- Es muss geregelt werden, wie mit dienstlichen Daten auf den Endgeräten verfahren wird, wenn diese nicht mehr dienstlich genutzt werden oder ein Mitarbeiter die Institution dauerhaft verlässt.

Außerdem muss die Institution in einer solchen Vereinbarung festlegen, dass sie die Mitarbeiter regelmäßig über aktuelle Gefährdungen durch mobile Endgeräte und notwendige Sicherheitsmaßnahmen informiert.

Fazit

Die zunehmende berufliche Nutzung von Endgeräten aus dem privaten Umfeld durch Consumerisation und BYOD führt zu großen Herausforderungen für die Informationssicherheit, aber auch für den Datenschutz. Dies muss als strategische Herausforderung angesehen und von der Leitungsebene einer jeden Institution sinnvoll gestaltet werden. Wie in diesem Überblickspapier beschrieben, reichen technische Maßnahmen alleine nicht aus, sondern diese müssen durch organisatorische Maßnahmen flankiert werden, die im Einklang mit der Gesamtstrategie der Institution stehen. Dabei muss in dieser Gesamtstrategie der durch Consumerisation erhöhten Verantwortung für die Informationssicherheit für den Mitarbeiter angemessen Rechnung getragen werden. Es sollte immer im Blick behalten werden, ob die Geschäftsprozesse und deren Schutzbedarf es zulassen, dass sich die zugehörigen Informationen mit Consumer-Endgeräten sicher, rechtskonform, wirtschaftlich und einfach handhabbar verarbeiten lassen. Je nach den vorhandenen Rahmenbedingungen kann dies kann auch bedeuten, dass in der Institution Consumer-Endgeräte nicht oder nur eingeschränkt im Informationsverbund der Institution eingesetzt werden können.

Weitere Veröffentlichungen des IT-Grundschutzes zum Thema

- Überblickspapier zu Smartphones
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_Smartphone_pdf.pdf?__blob=publicationFile

- Überblickspapier zu Netzzugangskontrolle
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_Netzzugangskontrolle.pdf?__blob=publicationFile

An das BSI werden häufig Wünsche für IT-Grundschutz-Bausteine herangetragen, die aus verschiedenen Gründen nicht zeitnah realisierbar sind. Meist werden zu aktuellen neuen Vorgehensweisen, Technologien oder Anwendungen spezifische Sicherheitsempfehlungen benötigt, mit denen auf IT-Grundschutz basierende Sicherheitskonzepte schnell und flexibel erweitert werden können. Mit den Überblickspapieren sollen zeitnah zu aktuellen Themen Lösungsansätze präsentiert werden. Kommentare und Hinweise richten Sie bitte an: grundschutz@bsi.bund.de