Welches Tablet passt?

Zwischen dem Gerät mit nur einem Ein-/Ausschalter und einem voll qualifizierten Business-Rechner gibt es im Markt viele Lösungen – wo welche Lösung am besten eingesetzt wird, diskutiert dieser Artikel aus Sicht der IT-Sicherheit in Unternehmen.

*Von Dipl. Inform. Ramon Mörl, Geschäftsführer **itWatch** GmbH*

Der Siegszug der Tablets hat erst im zweiten Anlauf geklappt. Wie so oft war die richtige Bündelung von Funktionen (Browser, Video und Audio) zusammen mit den geeigneten Außenfaktoren (flächendeckende Breitbandversorgung über Funk) und einer innovativen Bedienung missionskritisch. Beim ersten Versuch Tablets als weitverbreiteten Standard durchzusetzen, waren diese Randbedingungen noch nicht gegeben.

Man möchte fast etwas lax sagen: Der Siegeszug der Tablets entstand durch die Idee, eine Kombination von Fernseher und Stereoanlagemobil in einem Top-Design mit innovativen Bedienoberflächen unterzubringen, zu der später noch ein Browser für die Internetnutzung und das einfache Laden von beliebigen Anwendungen als wesentliche Features dazu kamen. Kompakte Designs gehen dabei so weit, dass noch nicht einmal der Austausch des Akkus möglich ist. Zwischen dem Gerät mit nur einem Ein-/Ausschalter und einem voll qualifizierten Business-Rechner gibt es im Markt viele Lösungen – wo welche Lösung am besten eingesetzt wird, diskutiert dieser Artikel aus Sicht der IT-Sicherheit in Unternehmen.

Mehr Storage ist möglich – gewusst wie

Auf den Tablets ist der Speicherplatz im Vergleich zu gängigen Notebooks noch sehr begrenzt. Für die Aufhebung dieser Begrenzung gibt es verschiedene Lösungen. Zum einen sind natürlich die mobilen Speicher USB-Sticks oder –Platten, SD-Karten oder andere mobile Datenträger geeignet. Voraussetzung ist das Vorhandensein geeigneter Schnittstellen, die nicht jeder der „Flachmänner“ mit sich bringt. Zum anderen ist natürlich die Datenlagerung in der Cloud eine geeignete Alternative, die nur geeignete Bandbreite und – falls erforderlich – die Erfüllung der Vertraulichkeit, Compliance oder weiterer SLAs voraussetzt. Die Nutzung einer privaten Cloud hat dabei weniger Anforderungen an die Sicherheit als die Nutzung einer Public-Cloud, da die SLAs bezüglich der Vertraulichkeit und Integrität einfacher erfüllbar sind.

In jedem Fall kann durch eine lokale Verschlüsselung aller eingehenden und ausgehenden Daten die Vertraulichkeit auch bei der externen Lagerung der Daten zugesichert werden – wenn die Wahl der Verschlüsselung und das Management der Schlüssel adäquat umgesetzt werden. Sichere lokale Schlüssellagerung ist hierfür eine gute Voraussetzung. Für einige Tablets gibt es hierzu hardwarebasierte Zusätze, welche das sichere Schlüsselmaterial geeignet transportieren und lagern können. Kann das Schlüsselmaterial lokal nicht sicher gelagert werden, muss es online geladen werden, was weitere Anforderungen an Authentisierung und vertrauliche Kommunikation mit sich bringt – beide Themen sind in diesem Artikel separat diskutiert.

Sicher – nur bei richtiger Verwendung

Des Deutschen liebstes Kind ist noch das Auto und nicht das Tablet. Beim Auto ist Sicherheit Pflicht – unabhängig, ob günstig, Mittel- oder Oberklasse. Airbags, Sicherheitsgurt, Sicherheitsglas,

Intervallprüfungen durch den TÜV sind verpflichtend. Im Betrieb gibt es klare Vorschriften: Ein Airbag darf nach einem Unfall nicht weiter verwendet werden. Sicherheitsrelevante Bauteile unterliegen Qualitätskontrollen und zum Teil Herkunftsprüfungen. Fahrzeuge, die andere Teilnehmer gefährden könnten, werden nicht zugelassen.

Man fühlt sich also bei der ordnungsgemäßen Verwendung dieser „sicheren" Autos entsprechend gut geschützt. Trotzdem verwendet der Taucher, der Segelflieger oder der Schiffsbetreiber völlig andere Sicherheitsvorkehrungen und Schutzeinrichtungen.

Jedem ist sofort klar, dass ein perfekt geschütztes Auto unter Wasser keinen Schutz bietet. In der IT macht Sicherheit als abstrakter Begriff wenig Sinn, wenn nicht aus den gewünschten Anwendungsszenarien die konkreten Bedrohungen und geeignete Schutzmaßnahmen abgeleitet werden. (Bild: bigfoto.com)

Jedem ist sofort klar, dass ein perfekt geschütztes Auto unter Wasser keinen Schutz bietet. In der IT ist analog das Verständnis essenziell, dass Sicherheit als abstrakter Begriff wenig Sinn macht, wenn nicht aus den gewünschten Anwendungsszenarien (Use-Cases), den Einsatz-/Umgebungsparametern, die konkreten Bedrohungen und dadurch geeignete Schutzmaßnahmen abgeleitet werden. Dafür gilt es zu untersuchen, wo die Daten liegen, wem die Daten gehören, wie sichergestellt werden kann, dass Daten auf „fremden" Systemen auch sicher gelöscht werden können, wenn es die Situation erfordert.

Mit welchen Anwendungen soll wer welche Daten von wo abrufen und wo verarbeiten? Die Gretchenfrage für die Mechanismusstärke der eingesetzten Schutzmaßnahmen und Sicherheitsanwendungen ist oft: woher kommen diese, wer betreibt sie, wer hat sie gebaut und wer sichert die Integrität der Verfahren zu? Zur Integrität der Schutzverfahren gehört natürlich auch die Zusicherung, dass das Verfahren an sich nicht zufällig oder absichtlich unberechtigt abgeschaltet oder modifiziert werden kann. Diese Szenarien sind für den individuellen Tablet-Betrieb zu berücksichtigen. Viel schwerer wiegt die Betrachtung, ob ein einzelnes unsicheres oder unsicher betriebenes Tablet oder das individuelle Fehlverhalten eines Anwenders eine Gefährdung von anderen Systemen oder der Unternehmensprozesse darstellt. Hier ist natürlich ein offener Netzzugang oder das Infiltrieren von Schadcode über ein Tablet, dessen Schutzgrad nicht dem Firmenstandard entspricht, ein kritisches Potenzial. Auch dieses Potenzial lässt sich weiter in handhabbare Einheiten zerlegen. Allein das Beispiel des vieldiskutierten „Bring Your Own Device" (BYOD), also die Verwendung von nicht betriebseigenen Endgeräten zeigt hier, dass auch einige Eigenschaften, besprochen werden müssen, die nicht sofort aufscheinen. Das Mitbringen eigener Hardware und die Verwendung der Unternehmensdaten auf dieser Hardware ist gekoppelt an:

1. Das Mitbringen eines eigenen Betriebssystems in einem unbekannten „Zustand" bezüglich Version und Patchstand.
2. Das Mitbringen eigener potenziell unbekannter Anwendungen in unbekanntem Zustand.
3. Eigene Softwareverteil-, Update- und Patchverfahren.
4. Das Verwenden eines eigenen Helpdesks mit Zugriff auf die Anwendungen und Daten, jedoch auch der hohen Wahrscheinlichkeit, dass der unternehmenseigene Help-Desk das eingesetzte Endgerät nicht gut kennt und sich insbesondere dort nicht aufschalten kann.
5. Die Zugriffe auf die Daten können im Streitfall durch das Unternehmen häufig nur noch über einen bewiesenen Tatverdacht und einen richterlichen Durchsuchungsbeschluss erwirkt werden – in diesem Fall ist zumindest durch den Zeitverzug schon das eigentliche Ziel verfehlt.

Alle Herausforderungen sind keine unlösbaren Probleme, wenn man sie in die Planung richtig und aktiv mit einbezieht und die erhöhten Kosten für den Betrieb mehrerer nicht baugleicher Infrastrukturen und Servicelinien berücksichtigt. Sicherheit heißt also auch granulare Steuerung der Funktionen, die gewünscht sind, und der Funktionen, die nicht gewünscht sind. Gerade der zweite Punkt setzt voraus, dass alle Funktionen eines Tablets offen

gelegt sind, denn sonst lässt sich deren Funktionsweise und gegebenenfalls deren Abschaltung nicht prüfen. Apple hatte sich in der Vergangenheit hier einen Lapsus mit gespeicherten Geo-Daten geleistet. An dieser Stelle trifft man wieder auf die Diskussion zur Sicherheit versus der einfachen Verwendung – aber aus einer etwas neuen Betrachtungsweise. Freut sich der „Anwender ohne große Sicherheitsinteressen oder ohne IT-Kenntnisse/Interessen“ über ein Endgerät mit wenigen „Optionen“ – im einfachsten Fall nur An und Aus -, so wird der sicherheits- oder IT-affine Anwender erst zufrieden sein, wenn er selbst oder Gruppen seines Vertrauens alle Funktionen erkundet haben und die subjektiv als kritisch empfundenen Funktionen individualisiert oder abgeschaltet sind.

Offene Ports – Leid und Lösung

Auf den Windows-basierten Tablets sind offene Ports und Schnittstellen mit Bordmitteln abschaltbar und mit einigen Einschränkungen auch zu verwalten. Über schon seit vielen Jahren etablierte Zusatzprodukte lassen sich die Ports und die daran angeschlossenen Geräte bezüglich der verwendeten Protokolle, Funktionen und ausgetauschten Inhalte sowie die verwendeten Anwendungen detailliert steuern. Hier gilt es, die Robustheit der angewendeten Sicherheitsverfahren entsprechend der Sensibilität der verwendeten Daten und der Einsatzszenarien zu verfolgen. Nicht nur bei den einfachen Device-Control-Lösungen findet der interessierte Kunde erst nach intensiver Recherche heraus, dass das Herzstück, der Treiber, der Verschlüsselungsalgorithmus oder der Sicherheitskern aus fremder, zum Beispiel russischer Produktion stammt oder gar keine Herkunftsnachweise geführt werden können. Der Kunde oder Nutzer kann sich jedoch auf langjährige Expertise verschiedener Prüfstellen, allen voran das Bundesamt für Sicherheit in der Informationstechnik (BSI), verlassen. Bei kabelgebundenen Schnittstellen kann der Anwender „physikalisch“ kontrollieren, dass keine unberechtigten Dritten die Daten abhören oder manipulieren. Funkschnittstellen lassen sich durch den Anwender in dieser Art nicht kontrollieren. Insofern ist es notwendig sicherzustellen, dass keine sensiblen Daten, zum Beispiel Anwendername und Passwort, über ungeschützte – also unverschlüsselte – Funkverbindungen gehen. Bluetooth-Verbindungen können mit einfachen und relativ günstigen Hardwarekomponenten von jedem mitgehört werden. Da auf Tablets meist die remote liegenden Systeme über eine Authentisierung mit Name und Passwort angesprochen werden und Anwender häufig zu kabellos angebundenen Tastaturen übergegangen sind, wenn es mehr Inhalt zu tippen gibt, ist hier besondere Vorsicht geboten.

Des einen Leid ist des anderen Freud. Ports sind Einfallstore für Schadcode, diese gilt es abzusichern.

Auf nicht-Windows Tablet-Betriebssystemen lassen sich diese Ein- und Ausfallstore der Daten nicht so granular steuern. Gleichzeitig bieten die Ports – allen voran natürlich USB – die

Möglichkeit, besondere Sicherheitsfunktionen einfach und flächendeckend zu nutzen. Insbesondere SmartCards, selbst verschlüsselnde Datenträger, externe Schlüsselspeicher, USB-Token, Finger-Print-Leser oder Netzwerkverschlüsselungskarten sind aus heutigen Sicherheitsarchitekturen nicht mehr wegzudenken. Will man auf deren Funktion nicht verzichten, so benötigt man Tablets mit geeigneten Schnittstellen und eine Steuerungsfunktion, sodass schädliche Geräte oder Funktionen die Systeme nicht gefährden können. Bieten die Tablets keine kabelgebundenen Schnittstellen für das Anbinden der firmeneigenen Sicherheitsinfrastruktur, kann man versuchen auf Funkverbindungen auszuweichen, wird aber dadurch die Mechanismusstärke des Verfahrens deutlich senken, da eine gute Abhörsicherheit und Vertraulichkeit dieser Funkkommunikation auf Tablets kaum zu erzielen ist.

Michele Quaid, CTO von Google [1], empfahl auf der Nato-Tagung NNEC den Einsatz von Google Earth für militärische Zwecke – der Spontankommentar aus dem Publikum, den der Autor, da anwesend, mitnotieren konnte: „… dann muss Google aber auch aufhören die abgerufenen Contents je Nutzer zu Profilen zusammenzustellen und diese Profile zu speichern …“. Gerade für Nutzer von Tablets ist die Profilspeicherung der abgerufenen Contents häufig ein zu deutlicher Blick in ihre aktuelle Geschäftsplanung und die aktuellen und zukünftigen Vorhaben.

Viele Firmen investieren bereits in Strategien, wie die neuen Tablets in ihre Business-IT optimal integriert werden und alle Daten und Anwendungen auch auf Tablets mit verschiedenen Betriebssystemen verwendet werden können. Hersteller bauen Lösungen, um die Business daten möglichst einfach auch von den Tablets aller „Geschmacksrichtungen“ einzusehen. Es empfiehlt sich für die Unternehmen, vor dem Einsatz die Vor- und Nachteile sowie die Integrationsmöglichkeiten zu prüfen. Viele Unternehmen verlassen sich in ihren Businessprozessen unterwegs auf verschiedene Hardwarekomponenten: zum Beispiel SmartCards, USB-Token, USBSticks, Drucker. Dabei geht es nicht nur um Hardware, die vom Unternehmen selbst ausgegeben wurde, sondern häufig auch um Hardware für den spontanen Datenaustausch mit Partnern oder Kunden. Die Einbindung in die bestehende Sicherheitsarchitektur und die Verwendung aller Standardanwendungen haben verschiedene Auswirkungen. Die erreichte Compliance der Prozesse und der Verwendung der Daten zum Beispiel nach BDSG, GOBS, FAIT darf natürlich durch neue Endgeräte nicht gefährdet werden. So geht es im BDSG nicht nur um die Speicherung von personenbezogenen Daten, sondern auch um deren Verarbeitung. Bei Personaldaten verbietet sich sowohl das Ansehen / Verarbeiten als auch das Speichern, wenn keine geeigneten Schutzmaßnahmen getroffen worden sind oder getroffen werden können.

Zu den notwendigen Schutzmaßnahmen gehört sicher auch eine geeignete Authentisierung. Kann diese nicht technisch mit Besitz und Wissen oder sogar mit lokalen, fest integrierten Hardware-Elementen unterstützt werden, muss davon ausgegangen werden, dass die Authentisierung über Name Passwort einfach ausgespäht werden kann – insbesondere, wenn Funkverbindungen prinzipiell verwendet werden können. Diesem Risiko sollte mit einer Einschränkung der Rechte der Kennung begegnet werden.

Für die Vertraulichkeit der gespeicherten Daten und der übermittelten Daten benötigt man Schlüssel. Diese müssen, wenn sie längerfristige Gültigkeit haben, gut geschützt am richtigen Platz liegen. Der richtige Platz verdient hier eine besondere Erwähnung. Remote Virtualisierungen werden häufig für die Nutzung auf Tablets eingesetzt. In diesem Fall liegt der Schlüssel auch remote, hilft also nicht für die Vertraulichkeit bei der Kommunikation oder lokal auf dem Tablet.

Fazit

Jeder kann das passende Tablet für alle seine Anwendungen und die Nutzung all seiner Daten aus der großen Auswahl im Markt finden. Für Windows-basierte Systeme ist sogar ein Einsatz bis zu Verschlusssache NfD über geeignete zugelassene Zusatzprodukte darstellbar. Die Möglichkeiten, die firmeneigene Sicherheitsarchitektur abzubilden, hängt von vielen Parametern ab und ist für iOS und Android-Systeme nicht immer gegeben. Tablet-Systeme unter Windows 7 fehlt noch der Reifegrad. Mit Windows 8 ist eine überzeugende Produktreife gegeben.

Potenziell unsichere Tablets können in einem virtuellen Netzsegment eingebettet werden, um andere Teilnehmer nicht zu gefährden. Ähnlich wie in NAC-Lösungen für „Fremdrechner“ im Haus, denen auch Netzwerk, Internet und einige genau abgegrenzte Fachinformationen zur Verfügung gestellt werden. Der Zugriff erfolgt dann zumeist über Standardverfahren zum Beispiel im Browser, Spezialanwendungen werden virtualisiert und über Remoteverbindungen dargestellt Wichtig ist auch, die Daten in diesen Netzen zu segmentieren, sodass die „Kronjuwelen“ des Unternehmens nicht durch unsichere Tablets gefährdet werden.

Quellen

[1] www.alcatel-lucent.com/wps/DocumentStreamerSevlet?LMSG_CABINET=Docs_and_Resource Ctr&LMSG_CONTENT_FILE=Other/2012-NNEC-Conference-Agenda. (Stand: 14.05.2012)