itWatch Enterprise Security Suite

Which Tablet Suits Your Purpose?

There is a wide range of devices available, starting with those having only a On-/Off-switch up to fully qualified business computers. From an enterprise security standpoint the choice of the right solution should be contingent on the particular use case with its special requirements.

It took two attempts for tablets to make them a success. As in many other cases, a critical factor was the proper bundling of functions (browser, video and audio) in combination with suitable conditions (extensive supply of broad band communication) and innovative handling. Until recently these capabilities were not yet provided for.

Let's put it this way: The success for tablets was owed to the idea, to combine TV with a hi-fi system in a top design with innovative user interfaces, and later on the addition of a browser for the internet as well as for the loading of any application as key features.

There is a wide range of devices available: With some of the devices not even changing of battery is possible, whereas others can be seen as fully qualified business computers.

More Storage Available – If You Know How

Compared to notebooks the storage capacity of tablets is quite limited. However, there are several solutions available for this issue. One of them are mobile stores like USB sticks or disks, SD-cards and other mobile media. To be able to use them, the appropriate interfaces have to be in place, a requirement not met by all of these media. Another alternative, that is storing the data in the cloud, is only viable, if suitable bandwidth, privacy, compliance or further SLAs is taken care of.

Less security requirements are to be met, when using a private cloud instead of a public cloud, because here SLAs related to privacy and integrity are easier to be fulfilled. Privacy can be ensured via local encryption of all inbound and outbound data, even if the data storage is outsourced – assuming, of course, the company chooses the appropriate encryption and key management. Here a critical requirement is a secure local key handling. For some tablets there are hardware-based add-ons available for transporting and storing the secure key information. If a secure local storing of keys is not possible, it has to be loaded online – adding further requirements to the authentication and confidential communication.

Safe – Only at Proper Usage

Germans are well known for their passion for cars. Security is mandatory for any category of cars: e.g. air bag, shatterproof glass or checks by TÜV (German association for technical inspection) are imperative. In addition, explicit rules are regulating the operation of a car: After a car crash an air bag is not to be used any further, there has to be a quality control for security relevant components and so on. Cars, that could present a risk to other traffic participants, are not admitted. Drivers consider themselves well protected, when using these "secure" cars. However, a diver, glider pilot or sailer takes completely different security precautions. Everybody would agree, that under water a perfectly protected car will not provide any safeguarding.

Similarly, the abstract notion of security doesn't make any sense for IT either – the basis, on which appropriate protection measures can be defined, has to be the desired use case with real parameters for the environment and actual threats. Therefore companies need to determine first, where the data is stored, who the data's owners are, how it could be made sure, that, if required, information on third-party systems can be securely deleted. In addition it is key to check, what applications should be used by whom to retrieve what data, and where should the data be processed?

The critical questions for defining the strength of the deployed security mechanisms and security applications are: Where do they come from, who is operating them, who has build them and who guarantees the integrity of the security procedures? The integrity of the procedures also includes guaranteeing, that they cannot be accidentally or deliberately deactivated or modified.

For the operation of tablets all these scenarios have to be considered. But even more important is the question, whether a single unsecure tablet or the misconduct of a user is endangering other systems or enterprise processes. Critical issues could be an open network access point or infiltration of malware via a unsecure tablet.

The example of the much debated concept of „Bring Your Own Device“ (BYOD) demonstrates, that when using one’s own hardware for storing and handling enterprise data there are some facts to be considered.

1. hardware comes with its own operating system in a “unknown” version and patching state,
2. the user will bring his/her own potentially unknown applications being in a unidentified state, with
3. their own software distribution, update and patching mechanisms.
4. The use of a separate help desk with access to the applications and data, but also with a high probability of the enterprise help desk not being very familiar with the device in use and moreover not being able to access it.
5. Often the organization’s access to the data in case of a conflict is only possible, if there is evidence for the suspicion and a search warrant is obtained. By then the actual purpose already has been missed.

However, all issues can be solved, if they are actively included into the planning process and if higher costs for the operation of several different infrastructures and service lines are taken into consideration.
Therefore security also means setting up a granular control for the desired functions and for those, not being desired. Especially for the last ones it is required, that all the functions of a tablet have to be laid open, in order to be able to check their functionalities and the possible deactivation.

Security versus ease of use – the discussion is ongoing, this time with a slightly different view on the issue: On the one hand, users - not being much interested in security and not having IT-know-how – are happy with a device with few “options” (maybe only on/off). On the other hand, there are users much interested in security and IT, and those will not be happy, till they have been able to explore all the functionality and have personalized or deactivated all the critical functions.

Open Ports – Harm and Cure

On Windows-based tablets open ports and interfaces can be deactivated and, with a few restrictions, also managed via the existing mechanisms. For many years now well established products have been available with capabilities for a detailed control of the ports and connected devices concerning used protocols, functions as well as the applications in use and the exchanged content.

Security procedures should be defined according to the criticality of the data and the respective use cases. Often customers after an intensive search find out, that core components like driver, encryption algorithm or the security kernel are being produced in a foreign country, like Russia, and that a proof of origin is impossible. However, users and customers can rely on the expertise of different inspecting authorities, especially the Bundesamt für Sicherheit in der Informationstechnik (BSI).

In case of tethered interfaces, users can “physically” check, that no unauthorized third-party is spying on or manipulating the data. Radio interfaces on the other hand cannot be controlled in this way. Therefore it is key to make sure, that no sensitive data like user name and password, is sent over unsecure, that is unencrypted, radio connections.

With the help of convenient hardware components Bluetooth-connections can be easily intercepted by anyone. Therefore tablets mostly using remote systems, with users authenticating themselves by user name and password and having wireless keyboards, have to be secured with due care.

On tablets with other than Windows operating systems the data’s entry and exit points cannot be controlled with the proper granularity. At the same time ports, especially USBs, offer the possibility of simply using special security functions, like smartcards, self-encrypting data media, external key stores, USB tokens, finger print scanner or network encryption cards.

However, if an organization wants to use such functions, the tablets require appropriate interfaces and a monitoring function, to make sure, that malicious devices or functions don't put the systems on risk. In case of untethered tablets users can try using wireless connections for the enterprise security infrastructure, but they have to be aware of the fact, that strength of security mechanisms is diminished.

Michele Quaid, CTO at Google [1], at the NATO-conference NNEC recommended the use of Google Earth for military purposes. There were comments from the audience, like "but then Google must stop to assemble and store user profiles out of the searched contents …". Especially for tablet users storing such profiles allows for unwanted insight into current business planning or future business activities.

Many companies are investing in strategies for integrating new tablets into their business-IT, thus being able to use all data and applications on tablets with different operating systems as well. Also, there are solutions available for easily viewing business data on all kinds of tablets. It is good advice though to thoroughly assess the integration possibilities as well as the benefits and drawbacks beforehand.

Many organizations when being mobile rely on different hardware components for their business processes, like smartcards, USB tokens or sticks. There are not only company-owned components in use but often it is hardware for the data exchange on the fly with partners or customers.

The components' integration into the existing security architecture and use of all the standard applications has different implications. For instance when considering the use of new devices an organization should never risk compliance to BDSG, GOBS, FAIT concerning processes and data use. The BDSG doesn't only regulate storage of personal information but also its processing. For personal data viewing, processing and storing is prohibited, unless appropriate protection measures are in place or could be taken.

Certainly, the appropriate authentication is one of the mandatory protection measures. If the authentication is not supported by ownership, knowledge or even by locally integrated hardware elements, username and password is likely to be spied out – especially if connections over air are allowed to be used.
Restricting the identification permissions can considerably reduce the associated risk. For ensuring confidentiality of the stored and transmitted data keys are required. If the keys need to be long-term valid, they should be stored in a secure place. The choice of an appropriate store is important, because tablets are often used in connection with remote virtualization. Here in many cases the key is also stored remotely, and thus doesn't support the confidentiality at communication time or locally on the tablet.

Conclusions

There is a large variety from which anyone can choose the suitable tablet for all the applications in use and for all the needed data. For Windows-based systems even the usage of data up to "confidential" or "restricted" is possible, when approved additional security products are in place. The possibilities of mapping the enterprise security infrastructure depend on many parameters – for iOS and Android-systems this is not always possible. Tablets with Windows 7 and 8 lack the required maturity. Potentially unsecure tablets can be embedded in a virtual network segment, so that other users are not put at risk, similar to NAC solutions for third-party systems in an enterprise network, having made available a network, internet as well as exactly defined information.

Access is provided mostly via standard procedures, like browsers, whereas special applications are virtualized and can be used with remote connections. In such networks data should be segmented, so that the most critical enterprise information is not endangered by unsecure tablets.

by Dipl. Inform. Ramon Mörl, CEO itWatch GmbH

First released in kes Special Mobile Security · June 2012 © SecuMedia Verlags-GmbH

Literature
[1] www.alcatel-lucent.com/wps/DocumentStreamerSevlet?LMSG_CABINET=Docs_and_ResourceCtr&LMSG_CONTENT_FILE=Other/2012-NNEC-Conference-Agenda