Mobile Security

White Paper

Siemens Enterprise Communications

May 2013

Siemens Enterprise Communications
www.siemens-enterprise.com

SIEMENS

Mobile Security

Contents

Mobile Security

Mobile change

Today's working world is changing, moving away from a sedentary 9 to 5 office day toward jobs where employees are constantly on the move, regardless of the size of the company or the sector. Fixed workplaces are giving way to hot desking solutions[1] and home offices. Desktop PCs are being replaced by notebooks, tablets and smartphones. Employees want to be able to employ a wide variety of devices to send and receive e-mails on the move, and to access the company intranet or internal services. Gone are the days when these mobile devices were regarded as gadgets for only a small group of employees – their use as key business tools is now widespread and increasing all the time. They are a natural part of everyday life for today's generation, the so-called digital natives[2].

Using communication devices on the move, however, exposes workers to potential security risks, including theft or loss outside of secure company premises. Notebooks can be left unattended in a car or conference room. And, left unsupervised, even a short period of time is sufficient to access any confidential data on a device.

Damage can be caused by:

- unauthorized viewing of data (loss of confidentiality),
- unauthorized modification of data (loss of integrity),
- impairment of functionality (loss of availability).[3]

These risks are further exacerbated as network and infrastructure boundaries become increasingly blurred. The upshot is that the data being transmitted has to be protected as well as the communication path itself.

All this leads to new questions regarding the security of your data:

- Should employees be allowed to have confidential documents on their mobile devices?
- What happens if this device is lost?
- What about employees' private devices? Should these be allowed in the corporate environment (Bring Your Own Device)?
- Which measures are needed to enforce security guidelines on mobile devices? (against malware etc.)
- Which services and corporate applications can be used with which devices?

[1]Flexible method of working where employees use any free desk and do not have a permanent workplace
[2]People who have grown up with digital technologies such as computers, the Internet, mobile phones and MP3 players
[3]European Network and Information Security Agency

Spanning company boundaries

From programs to apps

Originally, both programs and user data were stored on the actual device being used. Nowadays, these programs have been adapted for use on mobile devices as well, and the user data is stored centrally. These optimized programs are referred to as apps. Data is centrally stored using cloud technologies, with the advantages of it being constantly in sync and available from any location or device, while being highly secure.

Boundless communication

The desire to use the same apps on all devices applies particularly to communications applications, as outlined briefly below.

- Web conferencing: Collaboration in a virtual space with desktop sharing; in other words, shared display and processing of documents
- Social networks: Messaging, posts, blogging
- E-mail: Rapid delivery and access to all e-mails from different devices
- Telephony: Availability of contacts and user interfaces
- Video/teleconferences: Telephone calls with three or more participants, sometimes with video

Each of these types of communication requires suitable security measures to prevent eavesdropping on calls or interception of data. On January 17, 2012, the hacker group "Anonymous" was able to listen in on a conference between the FBI and Scotland Yard, and subsequently published it on YouTube.[4] All forms of communication are at risk, regardless of the technology used.

The cloud as a social entity

Applications are moving increasingly to the cloud with data storage consequently being placed in the hands of providers. However, this allows worldwide availability at the same time. Every data owner should pay special attention to data protection in this context as data is often stored outside of national boundaries and therefore not covered by local data protection laws.

Applications are being moving increasingly to the cloud and data storage outsourced to providers, permitting worldwide availability. Every data owner needs to pay special attention to data protection in this context - data is often stored internationally and therefore not covered by local data protection laws.

Social media platforms constitute a special domain of cloud services. Such platforms encompass a variety of networks such as Xing, LinkedIn, Facebook, Twitter, Yammer, YouTube, Wikipedia, Web Collaboration Portals, etc. They allow interaction between people at different locations and often also serve professional interests, such as finding business partners, employers and employees.[5] These platforms are also of interest for social engineering[6].

Mobile Devices

Nowadays, the vast number of applications that have become an integral part of everyday business life can be used on all sorts of different mobile devices. The most important of these include:

- Laptops: The laptop is the most "stationary" of mobile devices.
- Tablet: Operated by touching the screen with a stylus or a finger, tablets are much lighter than laptops and are therefore more suitable for mobile use.
- Smartphone: A hybrid of a mobile phone and PDA, smartphones are the optimal compromise between size, battery life, weight and functionality – a well-known device in this category is the iPhone from Apple.

[4]BBC UK online (3.February 2012)
[5]fachartikel_cloud_virt_social_nis
[6]Interpersonal influences, which aim to elicit certain behavior in people, for example the disclosure of confidential information

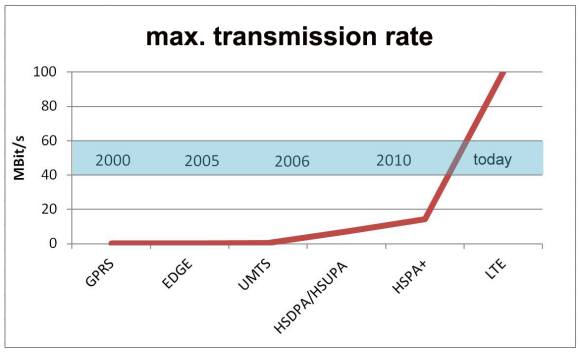
Networks galore

Users of mobile devices can now connect directly (VPN) or indirectly (Internet) to the corporate network and work productively anywhere and anytime.

Mobile radio

There are currently six methods of transferring data to mobile devices, and transmission rates have been significantly increased with each new standard.

More than 60 percent of the world's population will be able to access 4G (LTE) mobile broadband technology by 2015.[7] With faster connections and the additional opportunities this offers, mobile data traffic is increasing almost exponentially.



WLAN

WLAN design needs to cater for every user and all devices. Laptops, for example, differ significantly from smartphones in terms of their features.

The network has to allow simple inclusion of all mobile devices and be able to manage the increasing number of these devices.

LAN

Because they are generally connected to the corporate network using WLAN or a mobile phone network, the LAN has diminished in importance with the advance of mobile devices. Laptops are integrated directly with the corporate LAN via docking stations.

However, appropriate checks must be made before connection to the LAN as they could already be infected with malware as a result of their activities outside the internal company network or from private use (BYOD).

App-solutely secure?

The wealth of innovations, however, brings challenges to companies as well as benefits:

- Apps: Generally speaking, these are not designed for the levels of security required by companies
- Communication: Confidentiality and privacy are acutely at risk as professional and private boundaries at companies become blurred
- Cloud: Mobile data is adding a new dimension to data protection and security (Big Data)
- Social media: Everyone can speak to everyone - an enhanced sense of awareness is required here
- Devices: More options for everyone – also for hackers and spies
- Networks: One secure network (VPN) and many non-secure networks (WLAN, 3G/4G, UMTS possibly without VPN) – employees must use the "right" path

The existing security strategy has to be adapted to the new challenges.

Castles are outdated

Data security has focused traditionally on security measures that keep unwanted intruders out of the network. The new security strategy has to focus on protecting data and communication as well as ensuring network integrity. The question is not where a particular security measure should be implemented, but rather which security measures are relevant along the entire path.

[7]Forecast by ABI Research

"I picked up a little something on the way here"

"In many companies, it's the top managers with their newly acquired high-tech phones who are the first to create gaps in the protective IT security walls that have been built up around corporate systems[8]." Because they are used both within and outside corporate boundaries, these mobile devices are beyond the administrator's control. They consequently require protection of their own against viruses and attacks of all kinds.

Lost & found

Further risks are posed by the potential theft or loss of these devices, which often have sensitive data stored on them or allow access to such data.

Mobile Security V1.1

The challenge lies in integrating these various devices with the existing corporate infrastructure and being able to manage their operation securely, efficiently and with a minimum of administrative overhead.

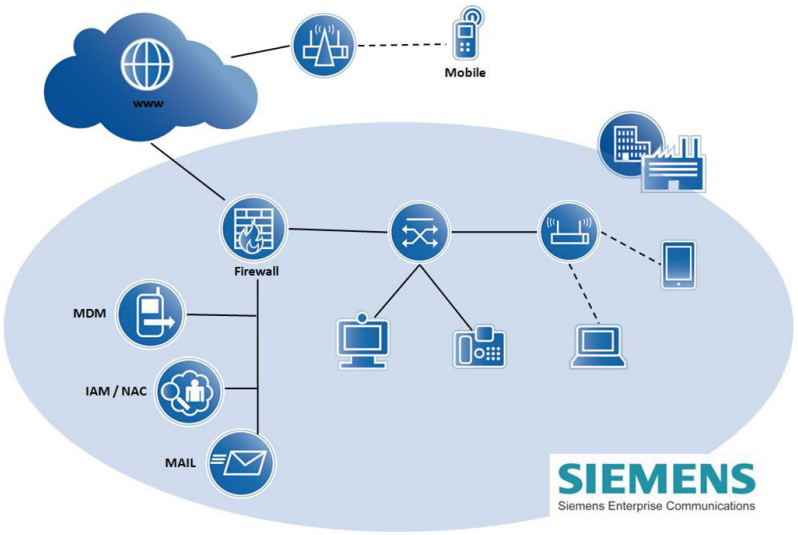
Conventional security concepts are based on the "castle" principle, i.e. building a strong perimeter defense against intruders. This involves powerful defense systems in the form of firewalls, anti-spam and anti-virus solutions, content filtering and reputation verification.

In addition to this, appropriate authentication solutions are often set up to regulate access to the company's most sensitive information and zones, which are located – to maintain the analogy – within the castle's "tower".

Authorized entry to the respective zone normally grants broad access to the relevant processes and information. The increasing use of mobile devices means that applications and identities are being used both inside and outside companies, leading to a blurring of professional and private boundaries. Employees keep in contact with customers using blogs, use social networks or twitter information on the move – the potential scenarios are many and varied and can scarcely be mastered using traditional security architectures.

There is a definite trend toward an interaction and information-based protection model. Although traditional security solutions, such as firewalls, will always remain in demand, additional new components are needed to alleviate the new security problems that are arising, and to keep the associated administrative overhead as low as possible.

Some promising elements of this extended security architecture are outlined briefly below.



[8]Financial Times Deutschland (2011)

Network Access Control

One of these components is already familiar - Network Access Control (NAC). NAC identifies devices and users and allows them to access network sections and services based on defined rules. NAC is now a must-have extension to the existing infrastructure, especially for companies with mobile devices.

But NAC is not relevant to mobile devices alone, it is pertinent to many different areas of networked companies. A vital aspect of NAC solutions are the guidelines used to control them. After all, access control is only as good as the guidelines on which it is based.

Modern NAC products can already detect the type of device accessing the network, and consequently have no difficulty assigning these to defined groups with the relevant security levels/guidelines.

Identity & Access Management (IAM)

Without effective rights management for every user, chaos is inevitable. However, in order to determine who actually has which rights to what, the users as well as the devices have to be identified. Professional IAM therefore precisely regulates which user can access which company applications and data using which devices.

Mobile Device Management (MDM)

"Mobile Device Management" (MDM) is used to efficiently implement and enforce the appropriate security guidelines. It's deployment becomes all the more crucial when confidential company data is stored on mobile devices.

An MDM solution enables:

- Central management of mobile devices
- Provision of updates and applications
- Blocking of non-trusted apps
- "Remote" deletion of data

Any overall solution that is worthy of the name should be able to support a large number of different mobile operating systems and manufacturers. Numerous MDM platforms, however, still lack adequate support for the wide range of operating systems in use.

What impact does this have? What should I look out for?

Strategic implications

CIOs and IT managers are faced with a dilemma: They see an acute need for action in almost all mobility areas, but only rarely is strategic planning used to address these needs. This not only opens up potential security risks and endangers the efficiency of mobile employees, it also means that companies fail to turn mobile devices and applications into innovative business technologies. To be able to systematically cope with the growth of the mobile sector and tackle its infrastructure consequences, CIOs need a viable mobility strategy.[9]

Faced with all of these new trends and opportunities, companies need to consider which strategy they want to follow in order to gain the maximum benefits.

Companies that do not have a long-term mobility strategy run the risk of their devices, platforms and applications proliferating to the extent that they become difficult to control and tough to integrate efficiently with the existing infrastructure.

[9] cio.de (23.04.2012)

The first step to consider is how to control the adoption of mobile devices within the company. Decisions need to be made about the types of devices that are to be supported, and about the feasibility and impact of a Bring-Your-Own-Device strategy at the company. The companies should also have a good idea of the services to be used and how these fit in with the corporate strategy. External aspects, such as customers, should also not be ignored. This means that corporate IT must adapt so that customers, partners and employees, together with their applications and intelligent products, are integrated in the most beneficial way possible.

When it comes to restructuring, one of the most important points to look at first is the existing strategy. Can any existing components of this strategy be retained and savings made by doing so? Is the existing strategy actually compatible with planned business development? Answering these questions involves examining the existing security paradigm, determining the new risks, and reviewing the possible solutions from an economic perspective.

Organizational implications

Once the economic factors have been examined and the strategy for a mobile infrastructure has been defined, some of the most critical aspects come into play, involving areas such as mobility management, organizational security and risk management.

A necessary first step is to set up internal guidelines for the use of these devices and modify existing guidelines to take account of any new aspects. In addition, all changes need be clarified with the relevant company bodies, such as the works council. It is also important to ensure that there is a clear assignment of tasks and responsibilities for any connected implementation or administration tasks.

Another critical aspect is employee awareness. The system can never be protected against its own users. Security achieved through implementing technical measures stands or falls with user awareness about security. It is important that users are made particularly aware of the need for greater personal responsibility and a more conscientious approach. "Only when users come to realize that security measures are meaningful and necessary are they prepared to accept them more readily, even when they entail some restrictions in terms of use."[10]

Technical implications

Additional software, such as a VPN client, is generally needed in order to be able to access company resources. This software must run on a wide variety of devices and be easy to install.

Today's security requirements demand extensive measures on both the personnel and technical levels. A basic level of protection for the traditional IT infrastructure can be largely ensured through purely technical measures, through a firewall or proxy systems with the appropriate policies, for example.

Over and above this, the use of mobile devices requires a rethink of existing security mechanisms. Switching from endpoint to access-based security solutions is absolutely essential. Endpoint security is based on the principle that a device is responsible for its own protection. Should a device actually be compromised, this means that the attacker has direct access to the company's data.

Access-based solutions give the attacker no direct access to company data in the event of a device being compromised. This approach is based on multi-stage protection. On the one hand, the device is protected against unauthorized access by third parties using a PIN or a similar mechanism. On the other hand, access to company data is controlled by means of user authentication. A positive side-effect of such a portal or proxy system is that external devices have no direct data connections to the company's internal network. The proxy system "brokers" the data and presents an additional hurdle for potential attackers. Appropriate authorization policies ensure that users are only granted access to the data that is relevant for them. Implementing a mobile solution also requires a modern NAC[11] and IAM[12] solution that takes account of the specific mobile security risks.

[10]Vgl. Horster 2006, Page 10
[11]Network Access Control
[12]Identity & Access Management

And now?

Mobility is good for productivity but also represents a serious risk to information security. The key to comprehensive end-to-end security lies in a combination of device, network and data security. Measures that go beyond basic data protection and include user authentication, access control and policy enforcement are absolutely indispensable.

The right technology partner can provide comprehensive support at all levels. This includes security solutions, optimization and managed system administration and recovery that guarantee comprehensive security, compliance and integrity for the entire mobile infrastructure.

The following points are of vital importance to the use of mobile devices within a company:

- The creation of guidelines for using and handling mobile devices and company data is essential
- The IT infrastructure has to be adapted to the new challenges and risks, taking account of both the existing infrastructure and the planned future development of the company
- A mature cross-platform Mobile Device Management solution offers distinct advantages for managing different devices
- Clear responsibilities must exist for the respective topics, with clearly defined scopes for company and employee
- Employees must be made aware of how the devices are to be treated
- Any known weaknesses or security risks, such as unregulated app downloads on devices, must be kept in check
- Support tools are required to enforce compliance with guidelines

Siemens Enterprise Communications is a leading global provider of unified communications (UC) solutions and network infrastructure for enterprises of all sizes. Leveraging 160 years of experience, we deliver innovation and quality to the world's most successful companies, backed by a world-class services portfolio which includes international multi-vendor managed and outsourcing capabilities.

Our OpenScape communications solutions provide a seamless and efficient collaboration experience – on any device – which amplifies collective effort and dramatically improves business performance.

Together, our global team of UC experts and service professionals set the standards for a rich communications experience that empowers teams to deliver better results.

Siemens Enterprise Communications is a joint venture of The Gores Group and Siemens AG, and includes Enterasys Networks, a provider of network infrastructure and security solutions, creating a complementary and complete enterprise communications solutions portfolio.

For more information, please visit:

www.siemens-enterprise.com or www.enterasys.com

Follow us 

Hofmannstr. 51 D-80200 Munich, 05/2013