

Your Business Partner In Mobile Solutions



www.smartphonesolutions.fi

Mobile Security With Smartphone Solutions Ltd

Jukka Talja, Chief Technical Officer, Smartphone Solutions Ltd

Smartphone Solutions has been security focused since the early days of the mobile revolution. This has allowed us to acquire both knowledge of mobile communication security issues and the trust of the company's partners and customers. Smartphone Solutions has implemented in tens of thousands of solutions globally, with the most popular being the service-based mobile office (push email, calendar and contacts).

As the market leader, Smartphone Solutions has visited hundreds of organisations where the hot topics currently seem to be mobile device management (DM) solutions and mobile security. Over the past year the most common mobile system development projects have been mobile device management as a service coupled with service provider selection and the integration of the mobile smartphone system into a client organisation's phone system, as well as smartphone standardisation. Security issues have also been a high priority, together with ways of extending existing IT systems (intranet, enterprise resource planning (ERP), customer relationship management (CRM) to mobile communications.

When your organisation is creating business critical applications, security is something that must be embedded during the implementation process and be maintained throughout the system lifecycle. It cannot be an afterthought. Security is the basis upon which Smartphone Solutions builds its relationships with partners and customers.

Can your customers and partners trust you?

Security risks have changed a lot during last the few years in which mobile devices have evolved from simple Wireless Application Protocol (WAP) browser-based mobile devices to becoming small



Jukka Talja

computers. At one time personal computers were for the most part electronic typewriters or spreadsheet analysers. Users were not able to install anything on those devices; they couldn't take them home, to a cafe, restaurant or bar, or on public transport. However, with the arrival of laptops, security and access control became a number one priority for companies.

Even if you have a non-disclosure agreement with your partners and customers, unless their communications systems are secure, you cannot entrust them with commercial secrets. Of course, your customers and partners can equally reasonably ask: can they trust you? Perhaps your laptops are secure, but how about all the new mobile devices? They accompany employees wherever they go in their business and personal life. Just imagine where a device allowing as much access to confidential data as a laptop could end up. No company can afford to be revealed in the media as negligent of its security responsibilities. Partners and customers do not want to read about major security leaks; they want to continue to communicate with confidence.

Do employees have admin rights to laptops?

It makes no sense to allow employees to have admin rights to mobile devices when you would not contemplate allowing them the same right with

respect to laptops. Yet mobiles nowadays can hold a lot more information than just phone numbers and names. Confidential emails, meetings, applications with access to company databases, documents, access to wireless local area networks and virtual private networks - or, perhaps, just simple text documents with user names and passwords, addresses, etc... The devices do not automatically have admin and user level access rights, automatic security control, application monitoring tools, policy management and all other security instruments that are must in modern up-to-date enterprise network. Modern device management is well adapted to enterprise markets because it replaces this security vulnerability with a rich list of easy-to-use features.

Intelligent rules based on automated security

With modern device management access control can be enforced. Company data is secure and unauthorised use is impossible. If an unauthorised SIM card is substituted for the authorised one, the memory can be completely wiped if the wrong code is typed in too many times. However, a SIM lock is a very good insurance against company data getting into wrong hands perhaps even before the device's owner has become aware that it has been lost. Naturally, if necessary, a full remote wipe can also be initiated by administrator at any time.

Do you know what and where your devices are?

Enterprise administrators have an exact inventory of all the company laptops and where their users are generally located. However, in most cases when asked, they will probably only have a limited knowledge of what kind of mobile devices are accessing the company network or how many of them there are. The modern device management solution includes a

detailed inventory showing devices, models, capabilities, installed software and other important information.

Full remote control for smartphones

There are many mobile applications that can be rated as viruses, Trojan horses or against company policy. A blacklist of these applications can be maintained and either prevent them from being initiated or even discreetly uninstall them. Bluetooth is also minor security risk if it is widely accessible and can be used by anyone. This and multitude of other settings can be changed and enforced.

Enforcing built-in auto lock security on devices is essential today, much as you would lock your front door, your car or boat. Yet while you may need a password to sign into a PC, far too often mobile devices will be left without any protection at all. This is quite incredible when you think about it, but hopefully it doesn't happen in your company? This, like all the other aspects of security, should be controlled by administrators. So often we discover when talking to customers that while company policy is that an auto lock code must be used, if it is not enforced end-users will very likely disable it.

Comprehensive device management is not only consists of the aspects already discussed, but includes a wide variety of settings, tasks, commands, reports, lists, scripts, live screen capture for helpdesk, ready made templates, etc. Whatever function may be considered desirable, it can be fully implemented.

Security action plan

To eliminate security threats and risks, IT management should be able to define a proper action plan in co-operation with the service provider. For example:

- Complement the information management strategy with a special mobile strategy
- Have an open discussion with the current service provider about the present and future threats and risks to the existing mobile systems
- Employ an information security consultant, as required
- Adapt the mobile policy to eliminate present and potential security threats and risks
- Evaluate the security of an existing push email solution

- Standardise the Smartphones used by each user group
- Implement a device management solution
- Maintain or increase the service level agreement of the mobile solutions now in use
- Instruct user groups on security issues
- Remind the users of the cost risks associated with data roaming
- Extend mobility to business applications, if possible
- Ensure that proper procedure is known and adhered to for reporting a lost device 24/7.

Based on Smartphone Solutions' experience, only a few organisations recognise the security threats and real risks that everyday mobility brings.

Save money with protect security

Administrators who have started to implement mobile device security will be aware that good mobile device management software not only increases the level of security, but also saves time and money. Software installations, policies and settings can be scripted and used not just for one type of device, but for a defined group of devices and their users. Group level policy management is a great asset for administrators when used correctly. It is easy to see that this all saves time for administrators and frees them for other tasks. Also, it should be remembered that when security is in place for devices they are better cared for and less likely to create daily problems, therefore saving time and money.

Needless to say, the possibility of restoring a damaged device remotely is also extremely valuable. Imagine a sales executive on a two-week business trip losing his mobile phone on day two. No more mobile email communication, no calendar, contacts lost, task list lost, documents lost... Creating an exact duplicate of the device and its contents remotely is time consuming for the administrator if it has to be done manually. Also, remember, the sales executive will have to spend time on the phone while the administrator tries to explain how to install the required software and set properties. This can waste hours if it has to be done manually; good device management software is

needed not just to give security, but also to save valuable time.

Case study: Deploying 200 new smartphones

At the beginning of 2009 Smartphone Solutions helped a customer to deploy 200 new Smartphones to personnel situated in various different locations all over the country. The end-users involved were not technically capable of installing software or understanding what settings needed to be in place. The plan was that a few people from the company's helpdesk would travel around and install the new devices and train the personnel how to use them and the software installed on them. As the end-users moved around a great deal in the course of their work, Smartphone Solutions suggested the mobile device management solution. Smartphone Solutions collaborated with customer over the setting up of the system, scripts and packages so that they were ready in less than a week to start a small-scale pilot with a few users. Everything went well from helpdesk, end-user and management perspectives. The helpdesk personnel did not need to travel and the end-users appreciated how easy it all was. Again, time and money were saved.

Country-based security bulletin

The device management solution does not comprise simply control and remote management. It can also be used as a company-wide bulletin/messaging system for mobile devices. Messages can be standard text messages or more sophisticated master data management messages with delivered-and-read receipts. Country-aware automated bulletins based on the smartphone's current country location is an valuable security addition to every enterprise. Travelling employees can be reached immediately when they enter the local network. Not only are your data and devices secure, but so too are your most valuable assets, your employees. ■

Contact information

Smartphone Solutions Ltd
Nilsjankatu 10-14

00510 Helsinki, Finland

Tel: +358 207 401 945

Email:

smart.info@smartphonesolutions.fi

Web: www.smartphonesolutions.fi