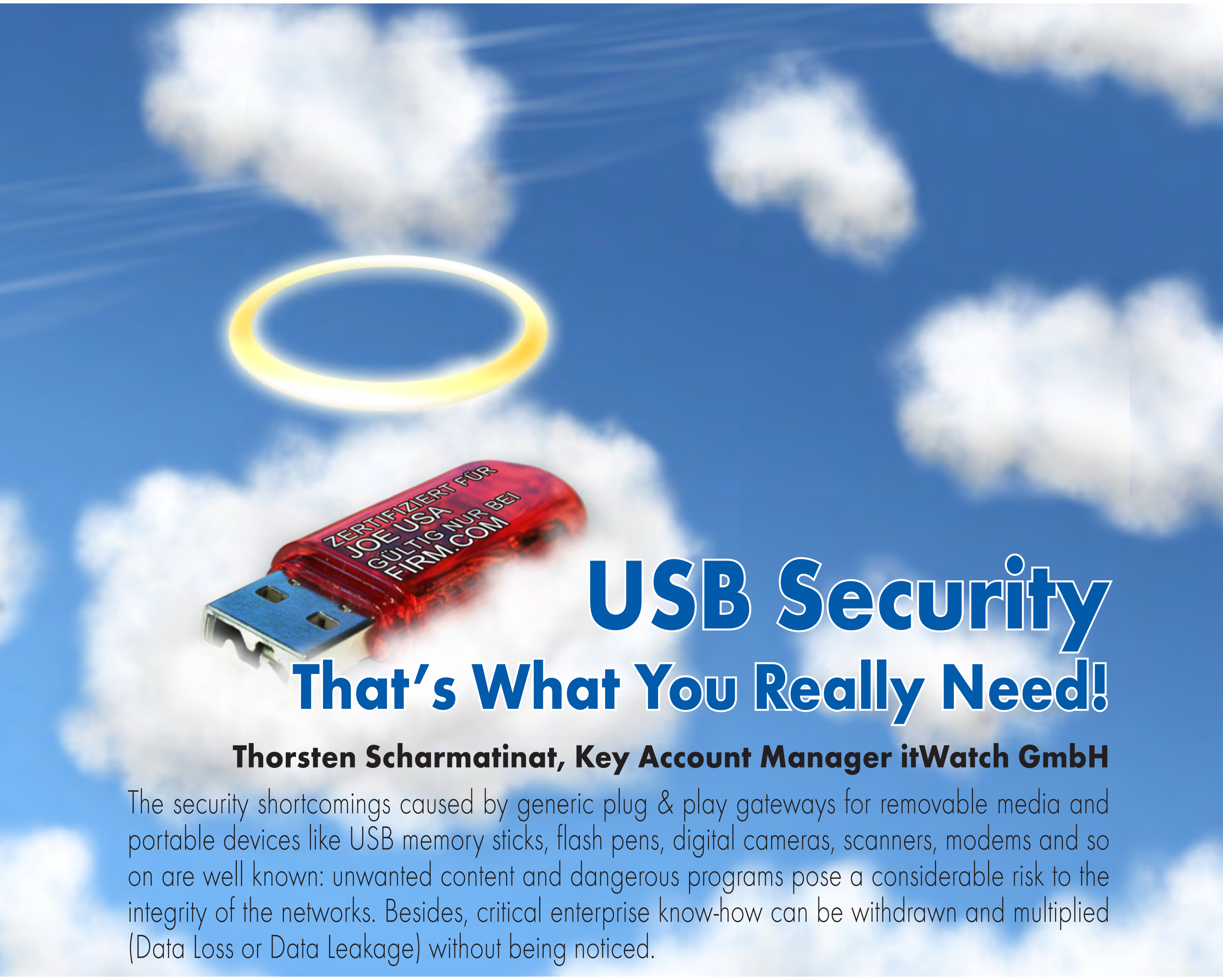

USB Security

That's What You Really Need!

Thorsten Scharmatinat, Key Account Manager itWatch GmbH

The security shortcomings caused by generic plug & play gateways for removable media and portable devices like USB memory sticks, flash pens, digital cameras, scanners, modems and so on are well known: unwanted content and dangerous programs pose a considerable risk to the integrity of the networks. Besides, critical enterprise know-how can be withdrawn and multiplied (Data Loss or Data Leakage) without being noticed.

The companies IT departments cannot get a handle on the problem by their own without help. There are a lot of solutions available, but unfortunately in many cases they cover only parts of the issues in question. What is more, organizations have got requirements regarding efficiency and cost reduction as well as the need to support users in complex scenarios with the required real time information.

Hence, the topic of endpoint security turns out to have much broader aspects than just putting in place efficient access control for all the device interfaces, be they USV, firewire, bluetooth, PCMCIA, infrared or others. The following gives an overview on the capabilities, an up to date solution should offer for the endpoint security in certain usage scenarios, in order to cover not only the immediate need but also the requirements in further project phases.

Device- and Port-Control

There are questions to be answered: Who is entitled to use which device (peripheral or fixed hardware)? When, where and in what situation can he/she do so? In addition, no update by the security vendor should be necessary for a new class of devices or interfaces. The usage of WLAN or UMTS is not tied to specific users but to the available networks (friendly net detection), as well as to the communication costs and to the rule: “Only one active network card at a certain point in time”.

Content Control

The reading of Word or PDF documents from CD/DVD may be permitted, but you have to make sure, that these files don’t contain embedded malware (embedded executables). At the beginning of last year for instance the automated detection of Java script in PDF documents would have been of great help in avoiding considerable damage. Of course, the content analysis has to be performed with the same mechanisms on archives (zip etc) and on encrypted documents or archives.

Logging and Alerting

Merely blocking and permitting does not suffice, beyond that logging is also indispensable, when it comes to critical applications. Nowadays in many environments provability of different critical actions concerning safety has become a integral part of compliance. To narrow down the flood of data, there is the need for a sophisticated filtering mechanism with simple administration. Certain events require a reaction in real time, such as alerting of a predefined distribution list by e-mail or text messages. Safety critical actions can be:

- Moving sensitive data,
- Using critical devices or applications,
- Applications accessing sensitive files,
- Separating safety critical information (e.g. assignment of e new key) from system management information (e.g. non usability of a USB device on account of a too low power supply),
- Permissions via challenge response processes or by self-granted permission
- Printing sensitive information, and
- Network contacts with certain attributes.

All these actions have to be assessed by their particular usage context such as time, day of the week etc., in support of a correct evaluation in real time.

Benchmarking The Risk

The loggings provide the correct information on the present risk situation and allow for the forwarding of the risks directly to the risk management, anonymously or pseudonymously with respect to quality and quantity. This way organizations can always act on a basis of the real situation.

Encrypting Sensitive Information

The incidents during the first quarter 2010 have clearly demonstrated the weaknesses of many self encrypting memory sticks. The often used partition encryption has got major drawbacks, because a single key in charge of opening irrevocably large data sectors, so that the data for so called USB dumper is completely laid open. Increasingly the level of privacy is defined by the file content and its sensitivity. That is, why today’s systems provide enterprise keys and private keys, which are employed for an optional or mandatory encryption of the content with the appropriate keys, depending on the user’s privileges and the sensitivity of the data. The compulsory encryption with a company key can lower the risk of data loss down to zero percent.

Controlling The Applications

Organizations are delivered a permanent overview by monitoring all the applications, having been tried to start with their genuine properties and with further attributes. The differentiation between permitted and not permitted applications requires -- on practical reasons -- the use of whitelists AND blacklists, that is per user, PC or network. This way you can for instance prohibit the use of skype in a home network but make it available in a hotel via WLAN.

Controlling the Used Networks

Systems are connected to potentially risky networks via UMTS cards, WLAN devices or other access possibilities to networks like modems in PDAs. By differentiating between permitted and not permitted networks the IT department can control these contacts. For each identified network, the appropriate security policy is applied in real time (home office, headquarter, production site, training etc.).

Correspondingly, the PC can enforce the appropriate security configuration. By doing so, permissions don't have to be assigned to the user anymore.

Safeguarding Against Spyware

Attackers exploit vulnerabilities in programs to infiltrate malware into the organization, without being noticed by the user. The malicious code executes in the background with the permissions of the infected user and sends the encrypted sensitive data to the internet without being noticed. With an integrity check of the application and the checking of the application's access rights these attacks can be effectively avoided.

Local Double Door System Function

Decryption and decompression are done in local quarantine. Only after this procedure the content can be verified in plain text, and depending on the outcome be released. forwar-

ded for checking or otherwise blocked and deleted. As a result, the system cannot be infected by malware – and no additional hardware or further trouble are incurred.

Personalization Of Data Media

Low cost devices don't have properties like their own serial number. However, for compliance reasons the use of media in critical areas like executive level, acquisition etc., essential data actions have to be stored in a provable manner. Therefore personalization of media for users or project groups is a prerequisite. The best way to build an "enterprise medium" consists in the personalization on the group of domain users. This way neither a complicated process of administration of serial numbers is required nor is there a need for investment in expensive hardware.

Event-Based Reaction

A simple integration with the established mechanisms already in place, like intrusion detection or help desk, is of the same importance as is the possibility to configure real time reactions to critical events. Such a reaction could be for example to instantaneously get in contact with an untrained user and to put security awareness in real time into a provable practice.

Security Awareness In Real Time

Often, end users don't easily understand all the aspects of data privacy and the locally applicable laws nor some industry specific restrictions. Also, the effect of trainings vanishes too soon, because users are overwhelmed with too much content, they don't have to put into practice on a daily basis. Besides, e-learning systems are not used properly. The best way is to combine all the advantages and link the learning content or certain electronic statements of intent (e.g. consent to logging for compliance reasons) directly to the critical action as well as embed the timeframe for the iteration of the user dialog into the security policy in order to avoid too many loops.

Reports And Management Information

Provable compliance at hand saves time for checking, saves money and allows for a spontaneous and precise answer to the core question: "How secure are we?". Revision, auditing, risk management and the executive board of an enterprise get additional value, because they are provided historical and real time information on all the events, sorted by sites, department or other criteria in support of a purposeful and responsible business leadership.

The Endpoint Security Suite by itWatch offers the solution to these and many further challenges on many million PCs daily with approval for NATO-restricted, confidential matter NfD and SECRET. Not only is the suite technical scalable for any company size but also for any budget.

For further information or questions concerning DLP and endpoint security please contact us:

itWatch
GmbH

Tel.: +49 (0) 89 620 30 100
Email: Info@itWatch.de
www.itWatch.info