Always one step ahead of data thieves

The State Office of Criminal Investigation of the federal state of Saarland leverages device management to ensure control over mobile devices

Data have become mobile and transportable – in the full sense of the word. Even large databases can meanwhile be stored on a chip of the size of a thumbnail; due to the universal availability of storage devices such as mobile phones, digital cameras or MP3 players these devices can be used as tools for large-scale data thefts. USB interfaces and the higher USB 2.0 data transfer rates have facilitated the fast and easy transfer of data to multiple devices. As a matter of course, this development is very useful and beneficial for many fields of application, but it also bears significant risks, including data theft and the uncontrolled transmission of malicious code such as Trojans or viruses. This article describes how the State Office of Criminal Investigation (Landeskriminalamt, LKA) of the federal state of Saarland has gained control over these risks through an intelligent device management solution.
LKA Saarland, which celebrated its 50th anniversary in 2007, is the most important operational unit in the fight against crime and also acts as central agency for the federal state of Saarland, as defined by the BKA Law, the "Law on the Bundeskriminalamt (BKA, German Federal Office of Criminal Investigation) and the Cooperation between Federal and State Authorities in Criminal Police Matters". Areas of responsibility include searches, investigations, the preservation of evidence and also prevention and victim protection. In 2007, the police force of Saarland worked on 73,813 registered criminal acts, with a clear-up rate of more than 52 percent.

Information as the basis of the fight against crime

Today as in the past, information is at the core of any police work. Without verified and up-to-date information, the fight against crime cannot be successful. Key for success are the police force's fast responses to social and technical changes and the ever-changing criminality. The LKA, as the central IT service provider for the state police (Landespolizeidirektion, LPD) and the LKA itself, must also allow and ensure access to sensitive data and has joined the general trend to use mobile devices and storage devices in their daily work. While such devices allow the police force to fight crime more efficiently, they also constitute a weak spot and raise certain security issues. Since March 2007, the EgoSecure endpoint device management solution has been in use at the LKA to ensure that only authorized persons with authorized mobile devices have access to data.

Mobile devices are changing the threat potential

The police force of the federal state of Saarland uses common security measures such as firewall, antivirus software and regular software updates to ensure protection against external threats. Networks, too, are subject to the highest security standards, as defined by the German Federal Office for Security and Information Technology (Bundesamt für Sicherheit und Informationstechnik, BSI). "Until 2007, mobile devices had constituted no major threat for the police force, since the operating systems in use did not provide USB support", says Michael Kraemer, chief inspector and head of the division LKA 2 - Information and Communications at LKA Saarland. In early 2007, the broad rollout of the Windows XP operating system and migration of hardware and software changed the situation completely – now, it was possible to access USB interfaces from anywhere.

While each update increased the performance of interfaces such as USB, Firewire or Bluetooth devices, the large security vendors had been somewhat negligent in their efforts to provide optimum control of such interfaces. As numerous studies and reports have revealed, unmanaged mobile storage media can be used to store large amounts of data very quickly, and these data might end up in the wrong hands. For instance, the popular iPod can store data volumes of up to 160 GB (not only music files), which is sufficient for most customer and product databases. As a consequence, more and more data are stolen through these interfaces and undesired software and code is also imported much more often.

„To prevent such problems from the very beginning, we have considered the implementation of a professional device management solution very early in the process ", says Patrick Stift, system administrator in the LKA's operating system and database administration team. Together with his colleagues, he is in charge of the overall IT administration. "The police are a security organization, and as such, we want to and must use leading-edge security technology and get prepared against data theft; after all, more than 3,000 users can use more than 1,200 PCs to access sensitive data."

Good device management needs not be expensive

The LKA was looking for a solution that would allow them to control connectable devices and define who is allowed to connect which mobile device when and where and to which PC. A white list, which defined authorized mobile devices for each employee, PC and its interfaces, based on the vendor or serial ID, was to be used for access authorization purposes. Since the LKA uses Microsoft's Active Directory as directory service for user administration, the solution also had to support this platform and use audit-proof protocols. Other requirements included comprehensive functionality, easy implementation, an intuitive user interface with minimal training, comprehensive control through a management console and real-time modifications.

Patrick Stift relied on the Internet when he searched for a suitable product and performed an evaluation of relevant products based on their scope of functionality. In February 2007, three short-listed products were tested intensively. The device management solutions of EgoSecure gained the highest scores, in particular for criteria such as management capabilities, functionality and extensibility. Patrick Stift's decision to suggest EgoSecure to the management board was based on the many strengths of the product: "Key criteria included the functional scope and the product's ease of use, as well as granular permissions assignment, which is indispensable if you have to administrate more than 3,000 users."

Ease of implementation and use

Within few weeks a final decision was made, and in early March 2007 the LKA started with the implementation, which is very easy: After purchasing the product, it can be downloaded, is installed on one server only and scans all required information via the network from Active Directory. The client components were distributed via LKA's existing software distribution solution. The EgoSecure solution performs any updates such as version updates automatically, causing no network overloads or user interruptions. "Within one afternoon we installed the product and activated key functionality", Patrick Stift confirms the easy handling of the solution.

An existing Microsoft SQL database could be used without any additional costs; no other software is required. The administrator manages the product via the management console with its intuitive handling, which ensures that practically any administrator can use the product immediately, without any training. In a first step, the solution captured all devices, including interfaces. Based on this inventory, policies were set up to determine who is allowed to communicate when, where and with

which device. Since not all devices were known and the LKA has to comply with highest security standards, all employees must submit a request for each of their devices – quite some work for the employees, which is, however, worth the effort, since this inventory-taking does not only ensure the security of devices, but also provided an up-to-date overview of existing devices. New devices can be entered within one minute and any changes made in the central management console are available in the network without any delays in real time.

One step ahead of data thieves – today and in the future

Meanwhile, the EgoSecure solution has been included in an LKA policy and is installed on all clients. “We have achieved our goal to ensure that only authorized users may use explicitly approved devices”, says a happy Patrick Stift. “LKA employees can now connect their authorized mobile devices all over the country to their PCs, under compliance with highest security standards.” Another strength of the EgoSecure product is its exception handling feature. For instance, the operating system often provides wrong identifications of external devices – PDAs are identified as hard disks or automatic detection is not possible due to the multiple assignment of serial numbers. “The upcoming new version of the EgoSecure product even allows administrators to correct these wrong assignments and define their own device classes “, explains Patrick Stift.

In the future, device management shall be decentralized to reduce the workload of the central administrators. Technical prerequisites for such decentralization are already implemented, for the EgoSecure solution includes the required role and authorization model to define each administrator’s scope of control. LKA also can imagine to use additional features of EgoSecure for encryption purposes in the future. Switching to this solution would allow the LKA to control their device management as well as file encryption through one central management console.

„From the very beginning, EgoSecure Data Protection has helped us to control and manage mobile devices“, Michael Kraemer sums up the situation. “Vendor EgoSecure did not only provide comprehensive functionality, but has also worked closely with us in a way that exceeded normal support services by far. Our experience will contribute to future software versions, which gives us the good feeling that we will remain one step ahead of data thieves also in the future.”

EgoSecure GmbH
Pforzheimer Str. 128a
76275 Ettlingen
Germany

Phone: +49-7243-354 95-0
Fax: +49-7243-354 95-10
Web: www.egosecure.com
Mail: contact@egosecure.com