ING DiBa uses HEAT Software to centrally control all of its USB ports

ING DiBa, headquartered in Frankfurt, Germany, has 3 main locations serving over 7.5 million customers in its core business areas of savings accounts, mortgages, securities, consumer loans and current accounts for private clients.

ING DiBa

COMPANY

Name: ING DiBa
Industry: Finance

SOLUTION

HEAT® Endpoint Management & Security Suite (HEAT EMSS)

USB ports and Plug & Play: it really can be that simple! Just plug in a device and you can start using it straightaway. But it's actually this function which is often a problem in companies. We only need to mention viruses sneaking in, intentional or unintentional data loss and private use. After all, Plug & Play is very convenient for users, allowing them to install external devices in seconds. This includes not just removable media, but also devices that, because of their design, contain large amounts of memory. For instance, devices like iPods, digital cameras and PDAs are used to innocently copy every kind of data.

For many companies therefore, the migration to Windows XP was very much linked to a change in attitude to security issues and to the use of these new opportunities. The finance group ING DiBa recognized the need for this in early 2005. After extensive testing, Detlef Ebert at the IT Operations Center in Nuremberg decided against the option of total denial and chose to provide specific authorization to users and devices using Device Control from HEAT Software.

> "This means that security policies for individual departments can be implemented centrally, as well as the fact that the latest hardware can be quickly integrated, when required,"
>
> Detlef Ebert, ING DiBa

Direct banks are enjoying a boom thanks to the availability of high-speed Internet connections, as favorable terms can be achieved by providing advice via the Internet, telephone or correspondence.

ING DiBa has 40 years direct bank experience, even if it has only had its present name since 2004 (or maybe: even before it's names change in 2004). In 1965 BSV - Bank für Sparanlagen und Vermögensbildung AG - was first founded in Frankfurt am Main. After a stronger strategic shift to products such as direct banking, the company changed its name to "Allgemeine Deutsche Direktbank". In 2002 DiBa was aquired by the Dutch finance company ING, which is responsible for the bank's current strong position, with well over four million customers.

This figure has also been rising thanks to the highly effective publicity campaign run by Dirk Nowitzki and sponsoring various basketball clubs. For instance, since June 2005, ING DiBa has been supporting wheelchair basketball through the German Wheelchair Sports Association.

WHERE LESS MEANS MORE

Returning to the issue of IT, apart from having software and hardware policies implemented centrally at head office, local IT managers are also able to implement individual projects that are required. As a result of the total migration to Windows XP, a new solution for managing USB ports was needed in the German market. The IT Operations Center decided, in consultation with the Munich-based IT consultancy firm TRYPTIS, to opt for the HEAT Device Control solution from HEAT Software. Implementation only took a few days, which meant that the project could go live in March. "The estimated timeframe of a few days for implementation actually turned out to be far too long, as our colleagues from TRYPTIS only needed a few hours to do the job," adds Detlef Ebert from ING DiBa's IT Operations Center. "So the simple implementation structure was definitely not just marketing hype, as we were able to actually see it put into practice too." But in this instance, the relevant department managers decided on the devices they would use in the future.

CREATING A WHITE LIST

ING DiBa has a total of 2,600 licenses for Device Control covering all the workstations installed in the bank's German branches in Frankfurt, Hanover and Nuremberg. The software operates according to the White List principle. This means that all external devices are blocked and can only be used after central authorization is given to the relevant client. This applies to all connections for disk drives, CD-ROMs, DVDs, serial, parallel and USB ports. At ING DiBa, the decision was made to allow access only to USB ports after authorization is given. In order to do this, an Access Control List (ACL) is created for each device. Only the administrator can connect the users or user groups to the devices by way of authorizing access. "Our decision to opt for HEAT Software's solution was based on the numerous control options it offers, along with the device-related authorization facility for all employees," continues Detlef Ebert. "This even allows us, for instance, to authorize access to a special device just for one user group." The functionality for it is based on the encryption option. "At the moment, there are about 20 different devices being used, such as BlackBerry devices, Palms or iPacks," adds Detlef Ebert.

> "The biggest challenge in this project, therefore, was not the actual process of going live, but the evaluation carried out beforehand."

GIVING CREDIT WHERE CREDIT'S DUE

Windows XP is now the standard operating system used at ING DiBa and access to external devices is centrally administered. Fortunately, it is not possible to measure exactly the level of success from using HEAT Device Control, as damage could only be identified in the event of a serious incident. But one indication of this comes from ING DiBa's annual security report, where the use of this software is setting a very high standard, which is maintained over a long time. In addition, an audit is carried out twice a year to verify that all the legal policies relating to IT security are being observed. A positive outcome from this is no faults are identified. Last but not least, its success can also be measured on help-desk activity, which, at the moment, has few problems to deal with. A very rapid response can be given to requests to use new devices, as once the sector manager has given authorization; the signature is entered in the list of permitted devices.

So, where do we go from here with endpoint security? Based on the good feedback from using HEAT Software's White List principle, devices will continue to be authorized on a specific user basis in the future. The software is being updated regularly with the help of TRIPTYS. This means that the company is able to control exactly who is using what when. And this is where it is important for a bank dealing with sensitive customer data that this information does not, under any circumstances, get into the wrong hands. This can be guaranteed both now and in the future.

HEAT Software USA Inc.
490 N. McCarthy Blvd. Milpitas, CA 95035 USA
P. +1 800.776.7889 or +1 408.601.2800