Case Study

TNS Infratest protects sensitive data in specialised areas

Anyone who works with sensitive information and personal data is subject to very strict laws and internal security guidelines. TNS Infratest generates annually untold millions of bytes of this sort of data and has been one of the few ISO 27001 certified companies in Germany since 2013. In order to be able to guarantee its global customers even more security, the Munich-based market and innovation researchers depend on the encryption tool HiCrypt.

With TNS Infratest, everything started with radio listener research and developed in the course of the last 60 years into one of the best-known and most respected institutes for scientific and economic market and opinion research. Annually more than 4 million interviews on widely varied topics are collected in different forms. The Munich-based company therefore generates a massive volume of data that influence political and social insights as well as the ongoing development of products and services. Numerous ministries, authorities as well as national and global companies rely on the expertise of TNS Infratest.

Along with general data, TNS Infratest works primarily with sensitive infromation, both on the customer-side and on the participant-side. For that reason data security is a very important topic. At the end of 2013 TNS Infratest received the ISO 27001 Certification from TÜV Süd for its exceptionally good information security management. But some customers demand the application of additional measures. The worry that there might be unauthorised access to data. Most of all it is companies that work in areas of innovation, such as energy optimisation or development in the automotive industry that fear unauthorised access to or unwanted loss of their confidential data.

This became particularly clear in fall of 2013: TNS had to meet security requirements that far exceeded those very high requirements already in place in its work for a major automotive client. The security experts at TNS Infratest ultimately found their solution in HiCrypt, a network drive encryption technology by digitronic computersysteme gmbh of Chemnitz.

The evaluation decides independently of the IT-Department

Prior to the decision to use HiCrypt, TNS Infratest thoroughly tested the market for encryption solutions. The complexity of the application and the costs of licenses were two of the deciding factors but the decisive criterion for the offers from the major international manufacturers proved to have a feature that is rarely noticed: a security solution that can be operated largely independently of the IT-department.

"Starting at a certain degree of confidentiality, customers do not just demand sophisticated security measures against external threats, but the potential data access must also remain restricted internally to the authorised persons who are responsible for the project," commented Dirk Wocke, externally assigned Information Security Officer with TNS Infratest. "For that reason it was decisive that HiCrypt made it possible for the department to use the software independently," Wocke also declared.

Owing to the focus on the essential functions, the encryption tool does not need any specialised IT-infrastructure, so that the roll-out can be realised

rapidly and easily in the corresponding department at TNS Infratest.

"We were able to carry out the implementation completely on our own and without additional help from digitronic or third parties. This saved us enormous costs. We didn't even need to customise it. It functioned almost out-of-the-box", said security expert Wocke. The implementation of the encryption system took about five man-days. Added to that were about two days for training all of the users. "The basic version of HiCrypt should just encrypt the network drives. And it should do this very reliably and nearly without the possibility of operator error. We find it instructive that the research experts at TNS Infratest were able to integrate HiCrypt in to their accustomed work so quickly," said Matthias Kirchhoff, Managing Director der digitronic computersysteme gmbh.

Extensive test phase and added features

After the brief training period, a three-week test immediately started at TNS Infratest. "Since we have an existing backup-concept, the encryption software absolutely has to be compatible with it. HiCrypt went beyond our expectations in that aspect", Wocke noted. In this phase the restoration of data archives was extensively tested. The plus for HiCrypt: The tool only encrypts contents. Folder structures and file names are preserved. Incremental and differential data security measures are therefore completely supported.

Currently 20 TNS Infratest employees from the central office in Munich are using this tool developed in Chemnitz. The user group consists mainly of clients from the automotive market. Dirk Wocke explains: "Since HiCrypt has integrated user management, the department can take care of the access management independently so that only a few employees who are directly involved in the project remain integrated. This keeps the processes lean and secure."

2-factor-authentication was solved by the market introduction of HiCrypt 2.0 and USB Smartcard Token support. "The most important expansion of HiCrypt-use for us is the introduction of 2-factor-authentication. This makes it possible for use to replace a rather clumsy work-around and consolidate everything in to a single solution," the Information Security Officer at TNS reports.

Security is not a matter for hype

By expanding with the 2-factor-authentication and the easy operation, HiCrypt integrated itself into the daily work with TNS Infratest.
So that the user experience continues to be as positive as it has been, the opinion researchers in Munich have concluded a software maintenance contract for HiCrypt. This will continue to provide them with important updates and expansions and they will profit from the support of the developer in Chemnitz when emergencies arise.

"We are very satisfied with HiCrypt and are planning to expand our collaboration in area of high-security projects. The need will likely increase in the future," says Wocke.

HiCrypt™-Functions

Encryption of network drives

HiCrypt™ makes the encryption of network drives possible. The encryption and decryption is all done at the client's location so that a secure data exchange between the client and the

server is assured. The following algorithms are used for encryption: AES (256 Bit), Blowfish (448 Bit) and IDEA (128 Bit).

Sole Key-Holder-Guarantee

HiCrypt™ guarantees its users the sole control of the encryption information for the encrypted data. Using the Zero Knowledge-Principle, the manufacturer guarantees that it will not have any sort of access to the data.

Working together

Compared to conventional container-encryptions, HiCrypt offers the option of providing joint access and is therefore suitable for secure teamwork.

Central user management

HiCrypt™ has integrated user management that can be configured separately from the IT-department. User management can be applied independently of the local domain user accounts.

Access to Cloud-storage

Along with standard Windows releases, HiCrypt™ supports online harddrives that can be integrated as network drives. This makes it possible to use Cloud-services in order to exchange encrypted files. Additionally, HiCrypt supports terminal server-environments and is therefore suitable for many variants of desktop as-a-service applications.

Disaster Recovery

HiCrypt™ offers different options for recovering encrypted data after a catastrophic loss.

Support of SmartCards

HiCrypt™ currently supports all SmartCard- or USB-SmartCard-tokens taht are used by SafeSign Identity Client. Additionally it is possible to represent companies' password guidelines using HiCrypt.

Support of roll-out strategies

Thanks to its easy installation, HiCrypt™ can be integrated into any roll-out strategy without any difficulty. No additional IT-infrastructure is needed.

Support of Microsoft operating systems

HiCrypt™ supports the desktop and server variants from Microsoft in the 32- and 64-Bit versions.

Apps for mobile encryption

HiCrypt™ offers an App for iOS and Android Smartphones and Pads. This allows encrypted data to be decrypted while you travel as well.

Contact

TNS Infratest
Dirk Wocke
Exterally assigned Information Security Officer
Telephone: +49 (0) 89 5600-0
E-Mail: dirk.wocke@supplier.tns-infratest.com

digitronic computersysteme gmbh
Peter Liebing
Oberfrohnaer Straße 62
09117 Chemnitz
Telephone: +49 (0) 371 81539-0
Telefax: +49 (0) 371 81539-900
E-Mail: marketing@digitronic.net
Internet: www.digitronic.net,
www.hicrypt.com