

Executive Brief

IT-Security in Germany 2011

New Challenges through Cloud Computing, Mobility and Social Media

.....

Sponsored by Siemens Enterprise Communications

Introduction

IT security is a high priority in the IT departments of German companies, and for many years now protecting corporate information technology and the IT landscape against threats has topped the agendas of IT officers.

There is, however, no such thing as absolute security. IT security is constantly increasing in complexity and sophistication and regularly takes on new aspects. Corporate IT is becoming an increasingly open field where on one hand certain boundaries are clearly marked out and on the other where a constant stream of new loopholes emerges, shortcomings are revealed and applications for new solutions added. Cloud services, mobile end devices and Web 2.0 technologies are representative of this blurring of boundaries and continual change.

Every company has specific, individual security requirements. IT must meet these requirements and continuously analyse individual risk potential. Threat scenarios constantly change — they become more grainy and there are more of them — and all IT trends are "plumbed" for their damage potential.

Trends and Developments in Germany

Focus on IT Security

In June 2011 IDC conducted a survey of 202 companies with more than 100 employees to obtain a better understanding of companies' handling of IT security solutions and responses to threat scenarios, and to understand users' changing security issues.

This document summarises the key results of this survey for IT officers in companies.

IT Challenges for IT Security

A high level of IT security can only be achieved if you are well aware of the main challenges. Risks for companies can arise for a variety of reasons. Sources of risk tend to lie in programming, design and configuration errors, and in human error. In the case of programming errors, companies need assistance in detecting errors and patching shortcomings. Design and configuration errors are real dangers, and avoiding or minimising them demands a lot of specialised know-how.

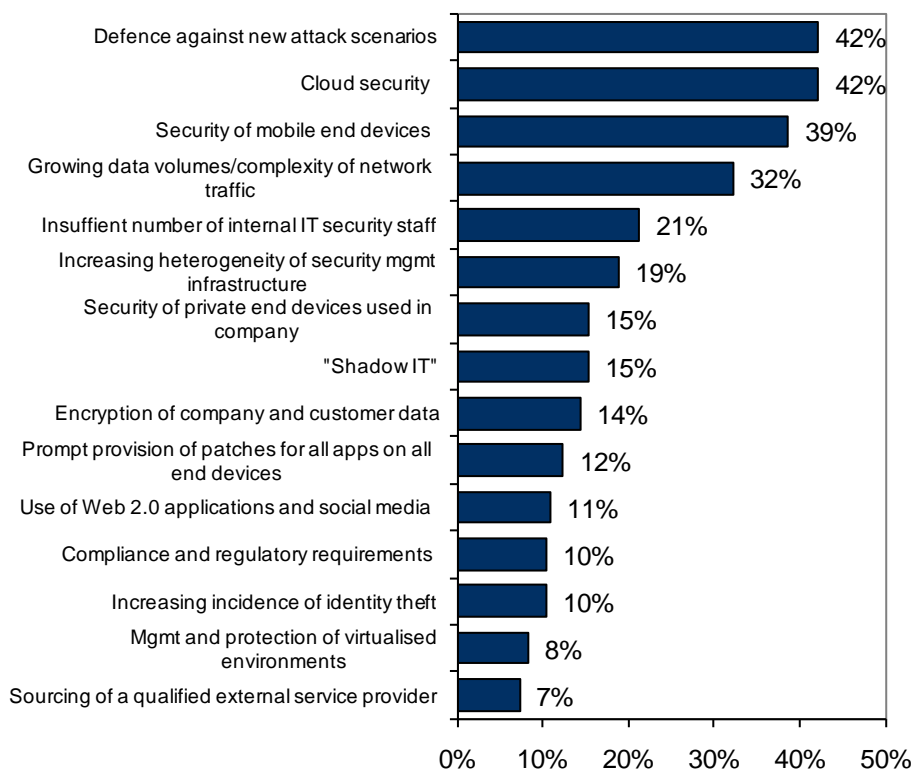
The survey identified a few key issues among the many challenges. 42% of companies interviewed said fending off new attack scenarios is the main challenge, which highlights the level of uncertainty among users. Although companies know that many applications contain hidden errors and loopholes, they have great difficulty in determining the risk to their own company.

Other top challenges include cloud security (42%) and security of mobile end devices (39%), both of which are relatively new IT security issues. While cloud services are only relevant at the moment for some companies, a growing number of the latter must address the security of mobile end devices and mobile business processes. CIOs still face considerable cost pressure, so reducing IT costs (cited by 52% of respondents) remains the most important challenge for German companies, as shown in Figure 1. Company management is also making huge cuts to IT, as operating the IT environment accounts for 70%–80% of the personnel and financial resources available to IT directors.

Operating a heterogeneous IT environment is complex, and leaves IT organisations with little scope for innovation and optimisation. This, however, is exactly what heads of department and management are increasingly expecting.

FIGURE 1

Top Challenges for IT Security



Multiple answers possible

n = 202

Source: IDC, 2011

Companies find themselves faced with a growing volume of data traffic and various data sources. Increasing heterogeneity applies not only to the data per se but also to the manner in which it is saved, administered, processed and forwarded. In some companies, for instance, so-called "shadow IT" systems have developed. These, which run outside the responsibility of the central IT organisation, must also be considered when it comes to IT aspects relevant to security. In the worst case, the central IT departments are unaware of such systems or changes to systems, which is a huge potential source of danger for the company as a whole.

The Employee as a Risk Factor

Half of the companies interviewed identified employees as the weakest link in their IT security chain, followed by smartphones, laptops and PC workplaces.

In many companies IT security is still not taken seriously enough. Topping the list of potential internal threats and risks was lack of security awareness among employees, including ignorance of security issues and an inability to identify risks. Deliberate misconduct, however, is also considered a source of risk. IT and security officers frequently have difficulty in spelling out the risks and therefore the consequences for decision makers. Security is all too often regarded as a bothersome IT matter. Companies must do more educating in this area and also point out the operational and strategic risks related to IT security risks. Secure the support of the management and responsible specialists to strengthen IT security in your company.

The Question Is Not Whether, But When, Your Computer Will Come Under Attack

Attacks or compromising attempts are either targeted or accidental. The question nowadays is not whether a company has been attacked but when it was attacked and whether the attack was successful. 21% of companies interviewed admitted they had already been victims of successful attacks. 7% were unable to say so with certainty and 72% believe they have escaped attacks in the past. It may, however, be assumed that the majority of companies have at least been attacked or that they have unknowingly been victims of attacks.

Hackers have different motives, and their choice of technical media varies. Spyware, malware and unauthorised access to the IT system are top of the list of attack types. These attacks are either directed at the company as a whole or individual business units like sales (with its customer data) or the financial sector (with financial data).

More Than 20% of Companies Feel Completely Secure

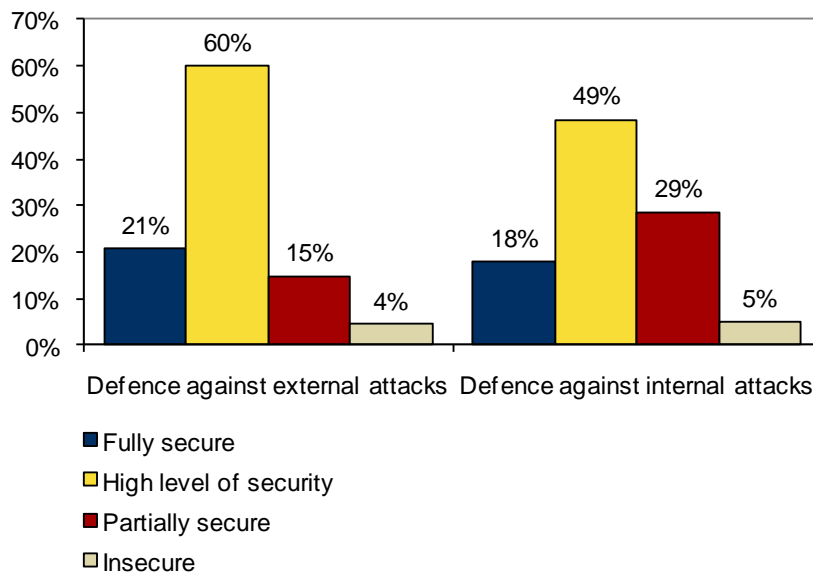
Nevertheless, the companies interviewed all confessed to having complete faith in the quality of their security precautions and mechanisms.

21% of companies interviewed rated their security against external attacks as fully secure and 60% as highly secure. 15% of companies professed some degree of security and 4% rated their security against external attack as unreliable. Defence against internal attacks — from within the company — was rated more critically by interviewees. In this case, 18% of interviewees cited fully secure security and 49% a high degree of security. 29% assume some security and 5% believed the situation as unsafe. Where do you see your company today? Where will it be tomorrow? Many security officers are aware that maintaining high security standards makes permanent demands on resources.

The main and most important task of IT security remains real and active defence against attacks on IT and the protection of users and data. In IDC's view, however, it is becoming more important to take preventive steps towards identifying threats at an early stage. Do you merely react to critical events or are you a step ahead of your "opponent"? If, like many companies, you belong to the first group, then change your strategy from reactive to proactive.

FIGURE 2

Security Level — Self Assessment



n = 202

Source: IDC, 2011

Companies Invest in Data Leakage/Loss Prevention, PKI and Intrusion Detection/Intrusion Prevention

In past years, companies have invested heavily in security products and solutions. The interviewed companies are highly equipped with IT security solutions and products. Basic tools like firewalls, antivirus protection and spam filters are widely used or planned.

IDC assumes that the requirements of endpoint security will continue to increase to protect company information and data from unauthorised access. Endpoint security solutions are far from becoming a commodity due to the constantly changing nature of threats. In future, companies and organisations must give more thought to their security and specifically address their own security risks. This offers IT security providers a good starting point.

The following were the most commonly cited topics when interviewed companies discussed their plans for various solutions — data leakage/loss prevention (48%), PKI (43%), intrusion detection/intrusion prevention (41%), biometrical processes (41%) and weakness management (41%).

In view of the variety of security solutions implemented, companies need to view their IT security holistically. They should ensure, for example, that all IT security tools implemented are optimally adjusted to one another and do not have a reciprocally adverse effect. Point solutions should be avoided as far as possible, and spending always committed to an over-arching security strategy.

IT Security Budgets on the Rise

IT security budgets are set to grow among the majority of German companies over the next few years. Many companies have realised they must continually invest in IT security and spend more on improving their IT security. More than two-thirds of interviewees plan to spend more on IT security over the next two years, with 35% of interviewees aiming to spend 10% more in this area. Around 18% plan to invest the same amount and only 3% expect to spend less. You therefore have a good line of reasoning for obtaining higher IT security budgets for your company, too.

IT Security for New Topics and Technologies

Cloud Services: Opportunities for Higher IT Security

Cloud computing offers various openings for bringing up the subject of IT security with users. IDC differentiates between cloud security in the form of security as a service and the secure use of cloud services.

Security as a service as a committed form of external cloud-based IT security services is an interesting option for around a third of companies. IDC believes medium-sized companies should consider the value of security as a service for their enterprises. From a company point of view, fast reaction times to change requests (signatures, files, update and code fixes), low commitment and usage costs and central administration support the need for security as a service. Security-as-a-service and cloud-based managed security services — such as denial-of-service defence, network security, messaging and Web security — are increasingly offered by some providers.

Cloud services in Germany are enjoying growing popularity and the market is maturing gradually. This results in new requirements for IT security, whether public, private or hybrid cloud scenarios are concerned. Companies must tread very cautiously when addressing cloud services, and make IT security a top priority. Preliminary steps are necessary in order to avoid or limit risks and achieve a higher level of data security when using cloud services. For instance, 54% of interviewed companies optimised their internal IT security first, and 41% conducted IT security assessments of their internal IT. Check up on the security standards offered by your provider. Cloud service providers should at least implement a security management system based on current standards (basic IT security, ISO 2700x, etc.)

The Many Facets of Mobile Security

Mobile security is becoming increasingly important for companies, given that in recent years the number of mobile platforms and applications has risen steadily and most business processes feature at least one mobile component. Discounting the notebook/laptop category, it can be assumed that the actual number of potential threats in the mobile environment is currently lower than in IT in general. By linking into companywide networks, however, threat levels could rise, and IDC expects this to become an increasingly important issue for organisations.

Are you aware of the potential risks of mobile solutions? Most frequently cited (2.6 in each case) in the survey was the use of unauthorised or unlicensed programmes, data loss and the use of apps. Other risks cited were gateways for malicious codes (2.7), use of social media (2.7), identity theft (2.7), low loss thresholds (2.8) and reputation damage (3.0). The risks are indeed high.

Malicious codes can be smuggled in through unauthorised programmes, as these tend to be supplied by questionable sources. This also represents a breach of software suppliers' terms of usage. Attacks are often initiated via social networking Web sites. The hackers then also exploit any weaknesses in end devices.

Business and connection data stored on mobile devices is becoming increasingly interesting to hackers, resulting in a growing number of viruses, malware and exploits. IDC expects that by 2015 mobile threat management solutions (antimalware, firewalls, IDS, antispam) will account for the lion's share of the mobile security solutions market.

The interviewed companies use mobile security software for different implementation scenarios. Most frequently cited was the use of mobile secure content management and threat management (MSCTN). MSCTN heads the list of citation frequencies (47%), followed by mobile VPN with 43%. Mobile IPC accounts for 28% of the citations. IDC believes users should attach importance to the easy implementation and installation of mobile security software. The most convenient option is via the mobile telephony connection itself. Aside from the purely technical aspects, the convergence of telecommunications and IT, compliance or social networks can trigger the introduction of mobile security software.

Social Media and Web 2.0 Call for Security Concepts

Social media applications and Web 2.0 tools have become a permanent feature in many companies. Facebook, Twitter, LinkedIn and similar tools offer excellent communication options. Using them, however, is not without risks. In social media applications false identities are also used and malware propagated. Does your company only use the company's own accounts and tools, or do users also use private accounts for professional purposes? Do you have all the activities in this environment under control? Do you have clear guidelines about who can use the different tools? Have the responsibilities been clearly assigned between IT and specialist departments? Are users aware of the potential dangers?

According to the survey, 34% of companies have drafted guidelines on the secure use of the company's own Facebook accounts. Despite this, IDC believes many companies still need to take action, not only when it comes to Facebook use but also in other areas. IDC advises that IT departments deal with these subjects proactively.

IDC Recommendations

Being responsible for IT security, it is up to you to protect your company as best you can. IDC believes the following should be taken into consideration as the basis for a high level of security:

- Do you always keep signatures and patches up to date and implement the recommended engines and applications?
- Do you use standards and best practices in the design of your security architecture and concepts, and do you check your concepts on a regular basis?
- Do you educate management and employees in your company on security issues?

Based on the survey results, IDC offers the following recommendations for user companies.

Adopt a Holistic Security Approach

Every company has its own specific security requirements, and these must be implemented in such a way to prevent potential attacks on IT. In particular, the company's individual risk potential should be taken into account. Hackers' motives can also be varied and implemented through different methods and technologies.

Pursue a holistic concept. Acquire a fully rounded picture of the threats facing your company and align security measures and components within a holistic approach. You should also set up an efficient process to ensure IT security. It must be noted that IT security is an open-ended project.

Enhance Employee Awareness

Companies see users as the weak link in the security chain, and many security risks are indeed caused by in-house users.

IT security is frequently perceived only as a time-consuming duty that hampers efficient operations. This, in turn, leads to carelessness, which can be a very real danger for companies. Security measures can only be effective if security concepts are actively experienced by every single employee.

So increase awareness on the part of users, particularly at management level, about potential threats, and foster understanding of changes in the danger situation and new solution approaches. At this point, you should highlight the business and legal consequences, while avoiding exaggerated horror scenarios.

Establishing security guidelines and sensitising employees are essential to defend the company.

Promoting Security in Cloud Computing

Cloud computing is a key IT trend. Many companies use cloud services in a wide variety of sectors, and IDC believes the market will grow considerably in the coming years.

Assess whether cloud-based managed security services such as denial-of-service defence, network, messaging or Web security are a good alternative for your company in comparison with conventional security solution models.

Cloud services make high demands on IT security concepts and their realisation. Take great care, particularly with network security, identity and access management, and endpoint security.

Protecting and Integrating Mobile Solutions

The number of mobile users and mobile business scenarios is increasing rapidly. Securing mobile end devices must be part of your overall security solution and should be incorporated into security concepts.

Take into consideration the growing complexity of security solutions in the mobility sector and make investment security a priority.

Mobile end-device users should be able to understand the security concepts behind mobile solutions. User acceptance increases or is only generated at all when users understand why certain security measures are taken.

Using Social Media and Web 2.0 Securely

Many companies already use social media and Web 2.0, and are now increasingly addressing security related matters. Inform your colleagues of the risks and potential dangers of social media and Web 2.0. These include:

- Identity theft, faking identities
- Circulating prohibited/compromising information through users
- Hackers smuggling in malicious codes

Conduct awareness campaigns and implement security concepts that are specifically designed for social media and Web 2.0. IDC believes identity and access management should also be taken into account for social media. Also check how the IT security of social media and Web 2.0 can be integrated into companywide IT security concepts.

Recommendations by Users for Users

In survey IDC asked companies to list the three most dangerous attack scenarios. As expected, answers varied and some were very specific to the particular company.

Below are some areas highlighted by interviewees:

- External hacker attacks, internal data theft, internal manipulation
- Hacking, Trojan horses, worms and viruses, data loss
- Industrial espionage, data loss by employees, attacks on cloud services
- Failure of the overall system, loss of customer data, attacks on product development
- DoS, targeted virus attacks, network sabotage
- External attacks on smartphones, external attacks on tablets, a new threat dimension through malware
- Damage to reputation caused by employees' embarrassing social media comments
- Server attacks, identity theft, viruses

Methodology

This document is extracted from the multiclient survey *IT Security in Germany 2011 — New Challenges From Cloud Computing, Mobility and Social Media*, which was sponsored by Siemens Enterprise Communications, among others.

IDC carried out the survey in June 2011, interviewing 202 companies with more than 10 employees. The survey focused on specialist and managerial staff responsible for IT security.

The following company profile is based on information supplied by Siemens Enterprise Communications GmbH & Co. KG. IDC accepts no responsibility for this content.

Siemens Enterprise Communications Case Study

Customer Information

Sportcast GmbH is one of the world's largest producers of live sport in HD, and, as a subsidiary of the DFL Deutsche Fußball Liga GmbH, host broadcaster of the German premier and second division. Sportcast also produces all DFB cup matches and advises other associations and divisions.

Sportcast is a TV media service provider and competence centre for the production and staging of TV sports events. It analyses production scopes, defines the ideal interaction of all involved and supports efficient implementation. Systematic quality management is of primary importance, ensuring production continuity and an outstanding final product.

Client Requirements

A high-availability secure IT infrastructure is essential to meet the constantly growing demands of production continuity. With the eSieNet solution for VPN and mail gateways and the computer centre premises reaching their capacity and performance limits, Siemens Enterprise Communications (SEN) was assigned the job of developing and implementing a coherent overall concept for the network and security infrastructure, virtualisation of the server landscape and process-supporting Web applications for collaboration with partners.

Solution Description

The multilayer, multivendor security design by SEN Professional Services integrated IronPort appliances for Web and content security, CheckPoint appliances to protect network areas with high data volumes, a virtualisation concept with VMWare and central storage server with NetApp, a SharePoint portal as central information hub and Enterasys network components to create a holistic overall concept.

The targeted state-of-the-art security solutions customised to Sportcast's needs, the innovative virtualisation concept, high-performance network infrastructure and central backup concept guaranteed production continuity and high availability for the production and staging of TV sports events and ensured that customers and partners of Sportcast GmbH enjoy a high-quality final product.

A central, outsourced managed-services-hosted, SharePoint Web portal optimised processes and improved information flow to partners and customers. Considerable savings were also made in the process: virtualisation precluded the need for a new computer centre, and energy consumption has been permanently reduced.

Project Highlights

- High availability and security based on an innovative network infrastructure combined with state-of-the-art security solutions
- Reduced costs through virtualisation of the server farm
- Process optimisation through a central SharePoint portal as an information hub for all connected Web portals
- Guaranteed production continuity and an outstanding final product for customers and partners of Sportcast GmbH

Customer Quotes

"Siemens Enterprise Communications knew how to turn our requirements — top quality, reliability and targeted innovation — into reality with a holistic security concept customised to our needs."

Dirk Fußwinkel, IT Manager, Sportcast GmbH

Copyright Hinweis

Die externe Veröffentlichung von IDC Information und Daten – dies umfasst alle IDC Daten und Aussagen, die für Werbezwecke, Presseerklärungen oder anderweitige Publikation verwendet werden, setzt eine schriftliche Genehmigung des zuständigen IDC Vice Presidents oder des jeweiligen Country-Managers bzw. Geschäftsführers voraus. Ein Entwurf des zu veröffentlichenden Textes muss der Anfrage beigelegt werden. IDC behält sich das Recht vor, eine externe Veröffentlichung der Daten abzulehnen.

Für weitere Informationen bezüglich dieser Veröffentlichung kontaktieren Sie bitte: Katja Schmalen, Marketing Manager, +49 (0)69/905020 oder kschmalen@idc.com.

Urheberrecht: IDC, 2011. Die Vervielfältigung dieses Dokuments ist ohne schriftliche Erlaubnis strengstens untersagt.