IDC MULTI-CLIENT PROJECT

IT-SECURITY IN GERMANY 2018

Challenges and Plans

IDC ANALYZE THE FUTURE

JULY 2018

SPONSORED BY BARAMUNDI

IT SECURITY NEEDS TO TACKLE DIVERSE CHALLENGES

IT security is set to remain a constant issue in IT departments and for employees across all other departments. This is due to the following reasons:

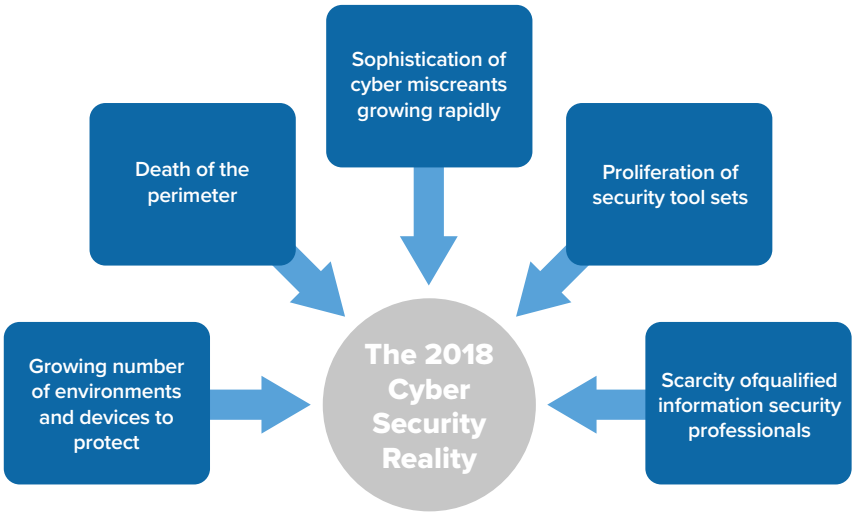
- A key factor is the digital transformation, which means all enterprises need to review and realign their IT security. Extensive process automation and interaction in ecosystems with partners, suppliers and customers – important aspects in the digitisation of business processes – go hand-in-hand with the widespread connectivity of IT and IP-based devices. Consequently, cloud computing, the Internet of Things (IoT), virtualization, open interfaces (APIs) and IT systems represent potential vulnerabilities that need to be protected.

- Statutory provisions, regulations, compliance requirements and the data security this entails – think of the EU GDPR, – not to mention protecting IT systems in critical infrastructures, also compel companies to make new investments.

- Furthermore, all enterprises and organizations need to repel two basic types of attack. To start with, common everyday attacks that hackers launch on the web indiscriminately. These attacks are aimed at employees in departments and our private accounts. As a rule of thumb, assume that 5 to 10 per cent of users click on the links in phishing mails. And, at the opposite end of the scale, sophisticated cyber attacks. They typically target specific individuals or information. The end justifies the considerable effort: these attacks come in multiple stages, over a longer period and employ diverse methods.

The frequency and quality of cyber attacks is set to rise further in the upcoming months. In practically all cases, it is about money: blackmail, competitive edges, defamation etc.

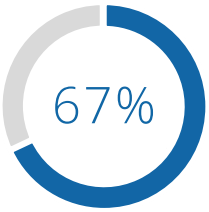
Figure 1: Five fundamental security trends



Source: IDC Market Analysis Perspective, Worldwide Security Products, September 2017

APPROACH SECURITY PROACTIVELY, REDEFINE YOUR SECURITY FOCUS

The survey shows the critical nature of the security situation in enterprises and organizations in Germany. 67 per cent of the enterprises interviewed admitted having had security incidents in recent months. Most commonly involved were PCs and notebooks (34 per cent), networks (31 per cent) and smartphones and tablets (30 per cent). This is critical in the sense that they are used to gain access to data centers. However, data centers (29 per cent) and servers (28 per cent) were also affected, and albeit to a lesser extent, printers, sensors and the IoT. Every IP address is a vulnerability that needs to be minimized, and every employee without exception a potential target. This applies to everyone, from the porter to the chairman of the board. So it is high time to take a proactive, strategic and holistic approach to IT security in your enterprise.



of enterprises were affected by security incidents in the past 24 months

Many organizations have so far failed to get the security risk posed by users under control. Misconduct or a lack of awareness on the part of users, such as responding to phishing mails, downloading insecure apps or lost devices has again left company data vulnerable to external access in recent months. So it comes as no surprise that misconduct on the part of users (37 per cent) and inadequately protected endpoints (34 per cent) are the two most oft-cited security risks, even ahead of the activities of cyber criminals.

Figure 2: The major security risks in enterprises

1. Incorrect use, lack of user awareness
2. Insecure or inadequately protected endpoints
3. Malware, phishing, social engineering and DoS attacks
4. Willful user misconduct
5. Connectivity of devices and applications

N = 230 enterprises

In June 2018 IDC conducted a primary market survey to gain insights into the plans, challenges and success factors of German enterprises in the comprehensive protection of IT systems and business processes. Based on a structured questionnaire 230 organizations in key industries in Germany with more than 20 employees were interviewed. This Executive Brief provides best practice, suggestions and recommendations to strengthen cyber security for your organization.

FIVE RECOMMENDATIONS FOR INCREASING IT SECURITY

The five recommendations below are suggestions and ideas on how you can improve your IT protection and maintain operational processes.

Recommendation 1: Conduct a realistic inventory of your company's protective, resistive and recovery capabilities

Repeatedly, in very many enterprises we deal with, IT security landscapes have evolved over time. It is not uncommon for them to be spread over 50 to 80 different security solutions, either as on-premises software solutions, appliance, Security-as-a-Service or managed security service. Transparency is often lacking with regard to all these solutions, most of which are in the form of traditional security silo endpoint, messaging, network and web security. So transparency is the first major step towards improving IT security.

At the same time, you should be asking yourself whether and how well your cyber security risk management covers the five NIST aspects: identify – protect – detect – respond – recover. They will help you to follow up your inventory with a reassessment of your IT security. The survey shows that so far less than half the interviewed enterprises have moved on from the reassessment step of the hitherto prevalent "prevent and protect", i.e. a security landscape which tends to focus on a reactive approach, towards "detect and respond" aimed at continuous monitoring in real time and appropriate measures as a reaction to system irregularities.

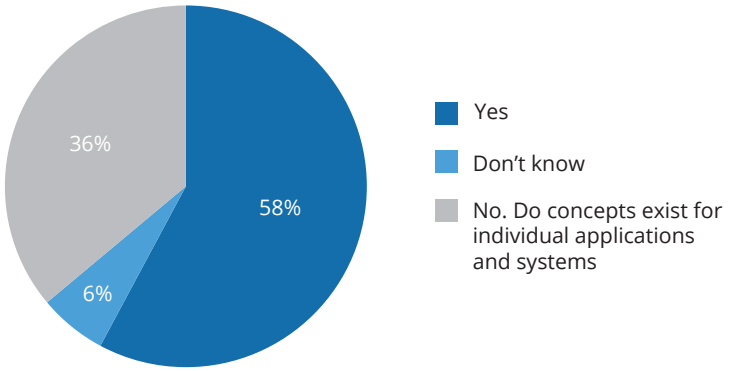
Do not confine your inventory to the central IT organization. Include the other departments as well. Departments and business units generally procure their own software and hardware and use cloud services. Compliance is often breached in the process, either due to unawareness or outright disregard of the relevant regulations. Even if the term 'shadow IT' is no longer quite so prominent, it has lost none of its relevance in describing IT resources managed outside the central IT organization.

Inventories must necessarily include printers because they are increasingly becoming a chink in an enterprise's armor. Although end devices are equipped with basic protection in most enterprises, a comprehensive approach to protection across the life cycle of PCs, printers and multifunction devices is frequently lacking. Why? Many enterprises identify only a low risk of data loss or attacks on the company IT, or they have outsourced print management to managed print service providers.
So, as you see, inventorying covers many different areas and tasks. Tempting though it may be, avoid half measures. Activities to improve IT security should always follow hot on the heels of inventorying.

Recommendation 2: Take a holistic view of IT security and plan strategically

IT security solutions, technologies and services only unlock their full potential as part of holistic concepts. Only 58 per cent of enterprises possess a central concept for information security that covers all systems and devices. That is not enough. We always recommend a centrally focused approach. Otherwise, you run a high risk of not covering all vulnerabilities and potential weak points. This is an essential aspect to always bear in mind.

Figure 3: Does your enterprise have a central concept for information security?



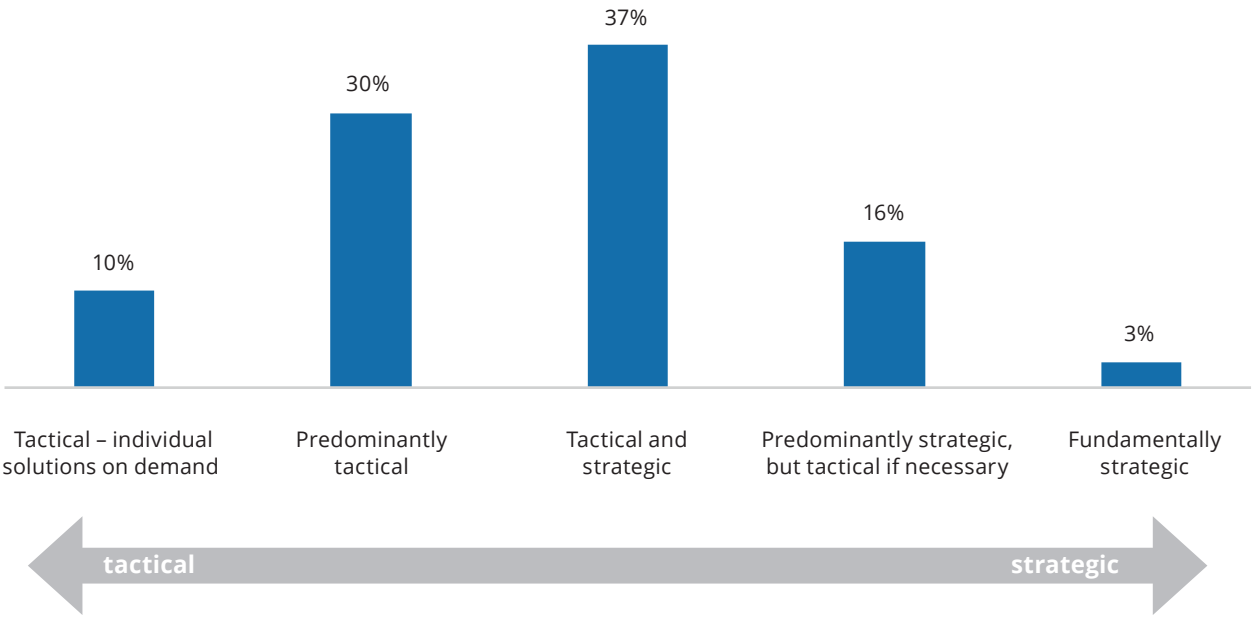
N = 230 enterprises

When devising holistic concepts, use common best practice and security frameworks from NIST, ENISA or BSI as a reference. After all, 82 per cent of your colleagues adhere to IT security best practices and deem them to be an effective means of improving security processes. Try to deploy these frameworks in as many security domains as possible. Admittedly, this is not an easy task, and it often involves major expense.

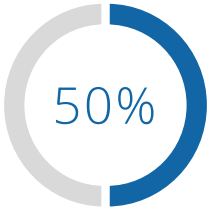
Many IT security officers conduct a risk classification when they launch new solutions or initiatives. However, in many cases, it remains static and is not changed or modified across the life cycle. We therefore urgently recommend you to conduct IT risk assessment and rating annually.

Among the greatest challenges in this connection is budget availability. Following large-scale attacks prompted by the likes of WannaCry or Petya, enterprises tend to burst into frenzied activism and provide budgets at short notice. They could take such attacks in their stride if they had thought about the issue sooner and made targeted purchases, for instance of back-up and recovery solutions. In our view, willingness to invest strategically is still too scant and underdeveloped. In this case, we recommend sitting down together with the management and departments to work out a solution.

Figure 4: In your enterprise, do you tend to invest tactically (single solutions on demand) or strategically (based on a well-defined plan) in IT security solutions?



N = 230, Mehrfachnennungen



Less than 50 per cent of enterprises have largely automated their security processes

Recommendation 3: Integrate your tools and automate your processes

Modern IT security consists of a clear concept that covers as many aspects as possible, a willingness to invest; a solution mix of established and new solutions that takes into account all the above challenges, and process automation.

Practically all enterprises have basic protective measures like anti-malware, spam defense and firewalls. However, as single solutions they no longer suffice by a long chalk. The majority of enterprises interviewed, two-thirds of them to be precise – regard integration as necessary for improved protection and defense capabilities, and have meanwhile realized that an integrative approach offers better protection than the sum of all security solutions. Integrative approaches can be realized in various ways, including integrating solutions from one or different providers, orchestrating various solutions, synchronization based on a communication layer or the correlation of various solution components. Get your providers to show you which forms of integration they currently support and what they are planning on the subject of APIs and connectors, for instance over the next one to two years. In IDC's view, integrating, synchronizing, orchestrating and correlating diverse solution components, is a step that end-to-end security architects cannot afford not to take.

Aside from integration, automation is among the key items on the security agenda. Although offering huge potential for freeing up resources, it has not made much headway in enterprises so far. Although the survey reveals that 80 per cent of enterprises have started to automate their IT security processes, in many cases only randomly so. Automation is primarily aimed at unburdening employees. Many IT security managers are keen to reduce manual activities like patching systems, installing servers and configuring firewalls to spend more time and resources on other activities. The danger of solution misconfiguration is also very high when manual activity is involved.

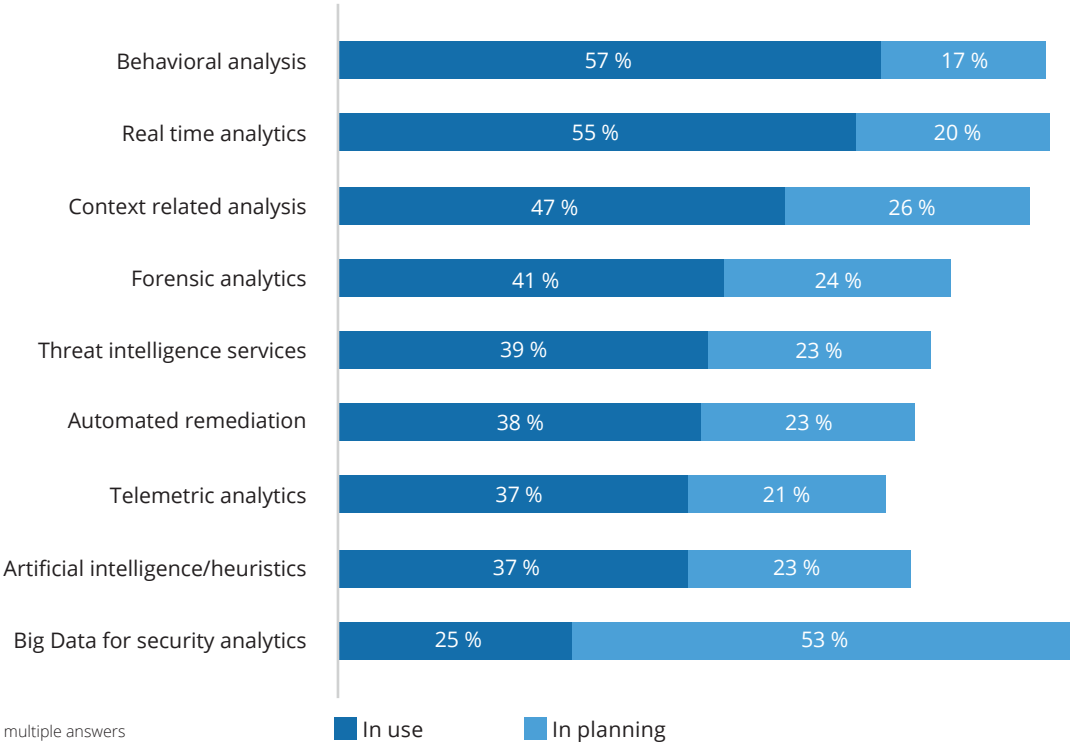
Analytics and machine learning improve protective mechanisms from the outset, as unknown activities can be detected, analysed and averted faster using self-learning systems

IDC is confident that automation and integration will gain dramatically in importance in the upcoming years to complete process chains, eliminate security silos, fast track processes and increase transparency.

Recommendation 4: Use different solutions and provisioning models

In recent years, the solution base and technological approaches related to security have developed extensively. These technologies rely strongly on proactive monitoring. Analytical approaches already integrated into security solutions for some years now are touted by providers as big data security, artificial intelligence and machine learning. Modern analytical technologies are sufficiently mature and a must in your toolset. Target your investment in analytics as the technology is developing at a rapid pace, offering better and better protection. Combine traditional solution approaches with active analytical monitoring and detection tools to identify irregularities in real time and react promptly. This lets you ruggedize your IT landscape against attacks from inside and out, and thus improve data protection and security.

Figure 5: Which analytical security approaches do you use or plan to use?



N = 230 enterprises, multiple answers

When evaluating current approaches, you should always consider cloud-based security as an option. Two thirds of the enterprises rely on security from the cloud, most commonly for firewall/IDS/IPS, email protection, web filtering and client management. Security from the cloud is also very good for protecting mobile workplaces. In IDC's opinion, cloud-based security services will continue to grow in the upcoming years as without them, real-time protection is nigh impossible.

Security solutions from the cloud are used by two thirds of the interviewed enterprises

Recommendation 5: Develop a security culture in your enterprise

IT security has an unenviable status in many enterprises, where it is either taken for granted, deemed an obstruction to daily business, or as a necessary evil and bothersome duty. This is an unsatisfactory state of affairs. Merely drafting guidelines or no-gos doesn't go far enough, nor do they go down well with users. Explore new, more creative paths to raise employee awareness about the secure use of mobile end devices, apps and data. Ideas are plentiful. Live hacks, faked phishing mails, penetration tests and incentives for particularly security-conscious employees are all promising possibilities.

Cooperate with the management and heads of department to raise employee awareness of the role played by IT security in securing business operations in the digital age. Ultimately, only a high level of information security can protect your data, intellectual capital, image and reputation built up by your company.

CONCLUSION

The current survey – like last year's before it – clearly shows that many organizations are still inadequately protected. While all organizations have some form of basic protection and standard security solutions, this alone is not enough to fend off large-scale, relentless daily standard attacks. Against the background of the digital transformation, comprehensive protection of IT systems remains one of the greatest challenges for German IT organizations. Yet only a few of the interviewed enterprises maintain more or less watertight security chains.

Many enterprises tweak individual levers, but fail to address the issue holistically. It is however clear that security does not hinge on technology alone. A holistic solution approach to information security is a basic prerequisite for covering all components, solutions and processes as a basis for defining necessary guidelines. Focus your security concepts on reducing complexity. Breaking down classic IT security silos and focusing more on the integration and automation of security processes is a must in the medium term.

New IT security challenges and changes are already emerging that also need to be addressed. IDC predicts a stronger focus on the increasing autonomy of departments, new use cases beyond business IT and Internet of Things scenarios. So it won't be any easier in the future for IT decision-makers trying to reconcile business enablement with secure IT operations.


ONLINE STATISTIC
PROFILE-15N-432
PROFILE-64M-330
PROFILE-251-543
PROFILE-170-853
PRODUCT
$820.51
$678.06
$697.98
$507.74
$455.59
$316.40
$284.48
$240.26
$197.22
$192.19
$116.63

USER RECOMMENDATIONS FOR USERS

Interviewees were asked to pass on their best practices within the context of IT security. Here are some of the unedited answers we received. We intentionally refrained from any editing to preserve their authenticity.

"Implementing the GDPR prompted us to adopt extensive measures."

"Technologies and solutions need to be kept up-to-date."

"We ruggedized our servers."

"We rolled out managed endpoint protection across the enterprise, and it has paid off."

"IoT increases the danger of outside interference. Plan it meticulously."

"Digitization and cyber security demand that new concepts to be devised and deployed. Getting in-depth advice is useful because you can't cover all the bases on your own."

"The automation of security systems and automated monitoring is advisable in any case."

"Security aspects and employee requirements need to be harmonized without compromising the enterprise's operability."

"The increase in external sensor systems puts us at greater risk from external threats. We have to counteract this risk."

"Increasing complexity also makes the human factor an increasing source of errors."

"Coordinated IT security platforms and standards are important."

"(Most) employees now appreciate the risks."

"We shifted our data to the cloud in the hope that they will be safer there than with us."

METHODS

The aim of the survey of IT and security managers was to gain an insight into the plans, challenges and success factors of enterprises in their deployment of IoT initiatives.

Against this background, IDC interviewed 230 managers from enterprises in various sectors in Germany with more than 20 employees. 58 per cent of the enterprises have between 20 and 1,000 employees and 42 per cent have more than 1,000 employees.

The following information was provided by Baramundi. IDC accepts no responsibility for this content.

IDC
ANALYZE THE FUTURE

BARAMUNDI

Case study: GRAWE

baramundi

WWW.BARAMUNDI.COM

"A new module from baramundi has always been, and still is, of interest to us. Ongoing optimization of client management is an important issue for us."

ANDREAS LAMPEL, SYSTEM ADMINISTRATOR AT GRAWE-IT

CUSTOMER INFORMATION

Grazer Wechselseitige Versicherung AG (GRAWE), headquartered in Graz, employs more than 1,500 people at its head office, ten regional offices, and over 100 customer centers in Austria. In addition, the GRAWE Group has fifteen subsidiaries in Southern and Eastern Europe. With the philosophy of individual customer advice, and a tailor-made and demand-focused product portfolio, GRAWE can serve its customers in the best possible way.

CUSTOMER REQUIREMENTS

Long-term success by chance

Due to the large number of Microsoft patches, patch management at GRAWE could only be handled with very high personnel costs. Therefore, it made sense to search for an automated solution.

"Ultimately it was by chance that we came across baramundi," says Andreas Lampel, System Administrator at GRAWE-IT. He and a company representative of baramundi software AG first met at an information event. After presenting the current problems Lampel and his team were facing at the time, baramundi was able to answer all questions more than satisfactorily. "I had my doubts as to whether there was even a company that could solve our problems comprehensively, but baramundi proved it to us," Lampel sums up. The Austrian insurer is now relying on software solutions made in Germany for endpoint management.

PRESENTATION OF THE SOLUTION

Increase security through patch management and managed software

"With baramundi Patch Management, we have found this solution, and can now set when the necessary patches are distributed to clients. We do not need to unnecessarily allocate line capacities, and as a result do not impact users in their work," says Lampel. The integrated vulnerability scan checks all clients in the company network for vulnerabilities. "We can define which patches are to be installed automatically, and which ones after manual approval, thereby avoiding possible incompatibilities. We consider this significant added value," explains Lampel.

Furthermore, the short times between updates for third-party software were a considerable time challenge for the GRAWE IT team. With "baramundi Managed Software", IT staff are able to distribute the essential and latest updates for standard software to over 3,800 clients. Andreas Lampel and his colleagues use the software packages provided for the first-time installation of software, as well as for updates or uninstallations. And: this solution provides IT staff with detailed information about necessary updates and their relevance to security. In addition, information relevant for a rollout is also provided.

As with Patch Management, the "baramundi Managed Software" module allows updates to be distributed to individual clients as a test. "The test option gives us a first impression of what the updates mean. Only when everything is working properly will the updates be distributed across the company to the relevant clients," says Lampel.

The beginning of a long partnership

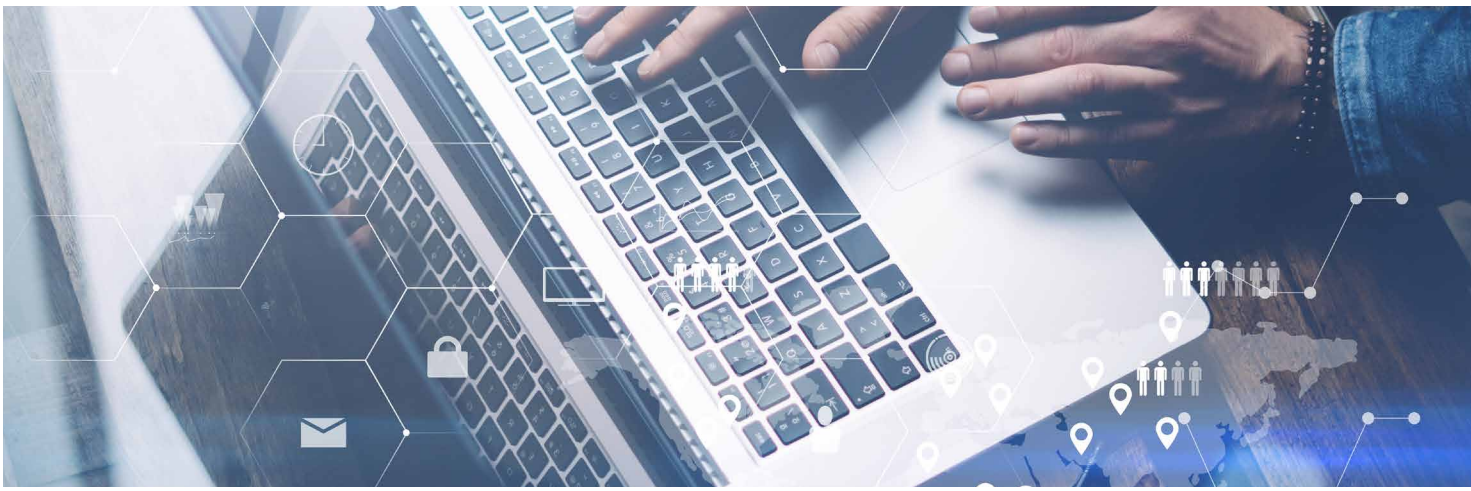
Since 2003, baramundi software AG from Augsburg has been a reliable partner at GRAWE's side with its baramundi Management Suite (bMS). Over 3,800 clients, 40% of which are laptops, and the remaining 60% desktop PCs, are securely managed and continuously kept up to date with bMS. Convinced of the quality, GRAWE has constantly added new modules over time.

"We as a company place high demands on ourselves and have to prove our quality anew in daily customer contact, which is why we expect a very high level of professionalism from an IT service provider."

DR. GERNOT REITER, DEPUTY GENERAL MANAGER AND HEAD OF IT AT GRAWE

"baramundi has been with us for more than ten years now, and has proven to be the right choice in every respect – especially in terms of products, but also in terms of cooperation based on partnership. Short communication paths and an ear for new suggestions characterize our cooperation. baramundi gives us the feeling that they focus on customer satisfaction in addition to business benefits."

ANDREAS LAMPEL, SYSTEM ADMINISTRATOR AT GRAWE-IT



Interview with Dr. Lars Lippert, CEO of baramundi

IT-SECURITY IN GERMANY 2018

At the presentation of the "IT Security in Germany 2018" survey findings IDC spoke to Dr. Lars Lippert, CEO of baramundi.

IDC: What are the major IT security challenges currently facing enterprises?

Dr. Lars Lippert: One of the biggest challenges is the generally significant increase in pace: more and more vulnerabilities are becoming public at ever shorter intervals. In order to avoid any gaps in IT security, IT's responsiveness must increase at the same rate.

This is exacerbated by continuing professionalization in the cyber crime sector: the lone hacker in a dark room has largely been replaced by organized structures that conduct their attacks like a business – from botnets and industrial espionage to crypto-trojans with their own support hotline, and an annually increasing number of attacks and attempted attacks. It is no longer individuals, but entire companies that are in the attackers' crosshairs. More than ever, this calls for IT that is capable of action.

IDC: Many organizations see IT security primarily as an IT issue. What do you think of this?

Dr. Lippert: Basically, IT security concerns everyone! End users contribute to the security of the corporate network as much as administrators. Technical solutions must therefore always be accompanied by organizational measures supported by company management. After all, the economic risks of cyber attacks also affect all employees.
IT security also always touches on data protection. IT solutions can help achieve compliance, but implementation must also be across the entire company.

IDC: What are the three most important factors that IT decision-makers must take into account when securing their IT environment?

Dr. Lippert: According to the motto 'Prevent, Detect, Respond' the following aspects should be considered when securing the IT environment: Transparency and traceability on a technical and organizational level are the basic prerequisite for any measure. A realistic risk assessment is only possible if there is an exact inventory of all end devices, software products and processes present in the network. This is followed by continuously checking for vulnerabilities and security gaps using the associated patch management. Last but not least, solutions must also be implemented that offer active protection in an emergency, such as enterprise mobility management, which is used for example to delete unwanted applications, or to render lost mobile devices harmless via a remote wipe.

IDC: Providers from various sectors are engaged in the IT security market. Why does your firm's background make it the right choice for security managers?

Dr. Lippert: baramundi software AG can look back on more than 18 years of experience in the IT business. Numerous companies and decision-makers in critical infrastructures such as energy utility companies have relied on our Unified Endpoint Management for many years. The comprehensive baramundi product portfolio helps to reduce IT spending through automation, and at the same time improve IT response times, provides an overview of all endpoints in the company, and ensures fast and reliable patching of vulnerabilities. Our software is also completely made in Germany,

as is our support. Our customers are also supported by access to our well-connected baramundi community of users and partners, so that help is never more than a few clicks away.

IDC: What about the future? What should enterprises look out for in the long run to avoid unnecessary risks?

Dr. Lippert: IT security must not be seen as a project to be completed, but as an ongoing process. This requires a strategic approach with continuous investment in IT security: employees must be sensitized to handle IT correctly. Companies should also rely on an integrated IT solution. This ensures all relevant security aspects are covered equally, and they do not risk open gaps or blind spots in IT security by using individual solutions. It is crucial to realize that IT security can no longer be limited to desktop PCs, but must cover the entire spectrum, from PCs, servers and mobile devices to network devices and IoT at the production level.

Dr. Lars Lippert
CEO, baramundi

For more details of this publication please contact:
Katja Schmalen, Marketing Director, +49 69 90502-115 oder kschmalen@idc.com.

IDC CENTRAL EUROPE GMBH

Hanauer Landstr. 182 D
60314 Frankfurt • Germany
T: +49 69 90502-0
F: +49 69 90502-100
E: info_ce@idc.com
www.idc.de

IDC
ANALYZE THE FUTURE