Current IT Security Situation in SME

Summary of representative survey results

Annette Hillebrand
Antonia Niederprüm
Saskja Schäfer
Sonja Thiele

wik Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste

IT-Sicherheit IN DER WIRTSCHAFT

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Foreword

IT security in SME: the right point in time is now, at the latest

Digitisation and network connections are making IT security increasingly important – just briefly consider the Internet of Things, Industry 4.0, smart cars or smart homes. In this connected world, small and medium-sized enterprises (SME) will still continue to play a significant role in the German economy. Although they are often very innovative, they usually have only limited resources to spend on IT security, unlike major companies.

This WIK study commissioned by the Federal Ministry for Economic Affairs and Energy (BMWi) within the scope of its initiative regarding IT security in businesses was based on our 2011/12 analysis with the aim of gaining up-to-date knowledge about the level of security in order to conclude recommendations on how IT security can be increased in SME.

The study shows: despite the increasing digitisation, there is still a lack of awareness when it comes to IT security. Even when the own risk level is considered high, SME do not ensure adequate protection. For example, two-thirds of the small SME state that IT security is extremely important to them, but only around twenty percent have carried out an IT security analysis.

Although there are many information and further training offers available, the sheer volume of offers and their disjointedness seem to lead to resignation. A regional approach with local contacts and a transparent range of offers that SME can grasp would be extremely helpful in this respect. Already ongoing programmes should be optimised further with a view to the long-term impact of these activities. A stronger awareness of "security by design" would be ideal for improving the IT security situation. IT security should not be addressed at the end of a process chain as an isolated issue but should be considered right from the start.

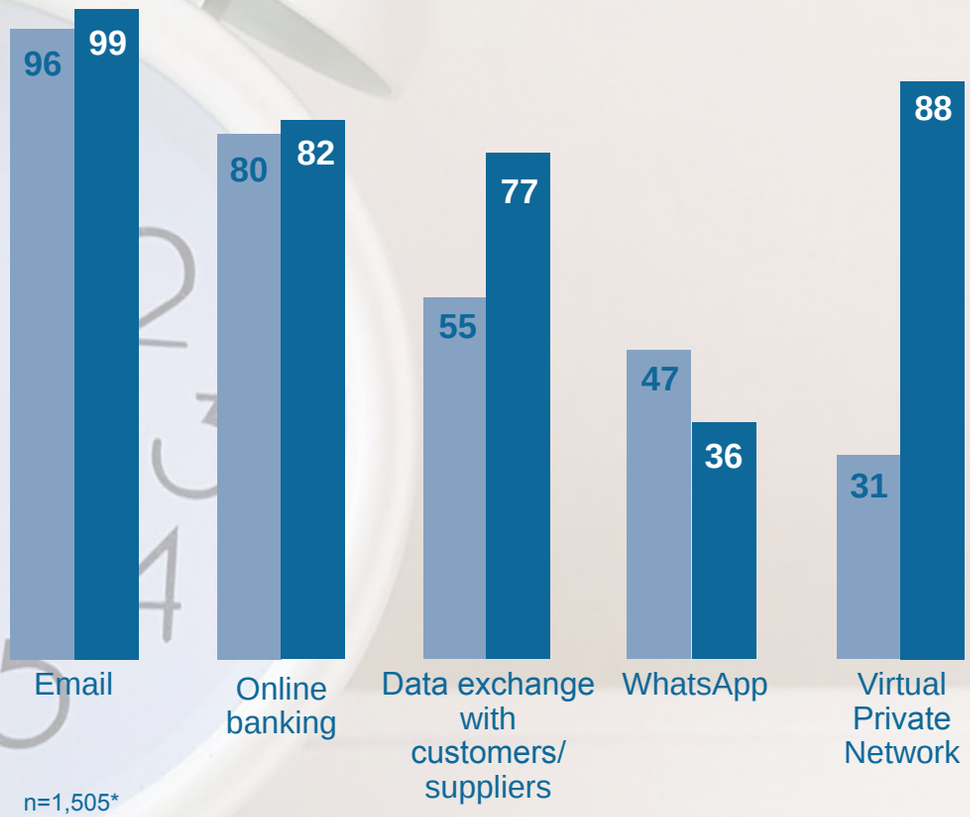
Compared to five years ago, the IT security situation in SME has not yet radically improved. In view of the considerably increased requirements, the challenge of helping the SME to at last prioritise the tackling of the current implementation deficits has therefore become even more pressing.

Dr Iris Henseler-Unger
General Manager and Director

Digitisation Calls for Increased IT Security

Wake-up call: time to wake up

Use of electronic communication in SME



Most SME in Germany routinely use emails and online banking.

More complex ICT solutions such as the exchange of data with customers or suppliers are used by more larger than smaller SME.

Especially small SME rely on WhatsApp as a means of communication.

Larger SME provide external access (e.g. via VPN) considerably more frequently than small companies.

small SME (<50 employees)

larger SME (50-499 employees)

*Representative survey of SME in Germany; n=1,508, n=1,505 of these companies that meet the "technical equipment" screening criterion (internet access, mobile devices etc.). All results in percent.

Gefördert durch:

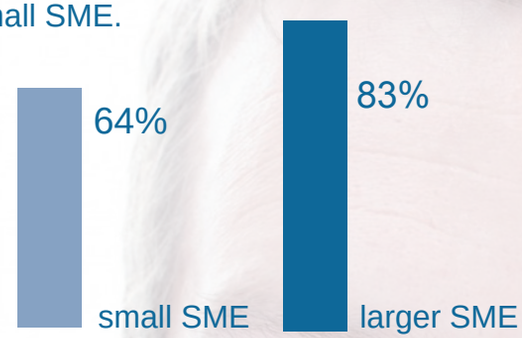
Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Importance of IT Security

Two-thirds of the SME consider **IT security to be "very" or "extremely" important**. Larger SME tend to consider IT security to be much more important than small SME.

How important is the issue of information and communication technology security in your company?



Proportion of companies that rate the need to protect their existing data as high or very high (2017 and 2011/12)

2017: n=1,505; 2011/12: n=922; all results in percent

Awareness = action?

All of the companies surveyed thought that the need to protect their existing data was significantly higher than five years ago. Recently reported incidents related to data leaks as well as attacks through malware such as ransomware, for example, have led to an increased risk awareness in the companies that is particularly marked with regard to customer, accounts and personnel details.

However, this does not mean that the companies act accordingly. **There is an implementation gap**. Only every fifth SME in Germany has already carried out an IT security analysis at least once, although in the larger companies, this figure after all increases to almost half.

Have you ever carried out a systematic IT security analysis in your company?

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Experiences with IT Security Problems and Causes

Experiences with IT security problems

Have you ever experienced the following IT security problems in your company?

Causes of IT security problems

What do you believe to be the main causes for potential problems and harmful incidents related to IT?

2017: n=1,505; 2011/12: n=952; all results in percent; *newly added in 2017

Most SME have already had to deal with the consequences of IT security problems at some stage. Key problem areas continue to be technology failure, virus attacks and (inadvertent) data loss or manipulation. However, considerably less SME currently state that their IT systems have failed. This indicates investments into more safeguards. Nevertheless, every fifth company was not aware of any IT security problems at all – which may be an important indicator of **prevention gaps**.

The main causes of harmful incidents are now considered to be mistakes made by their own staff, employee negligence or employee ignorance. Social engineering attacks therefore obviously continue to be a major risk, and raising their staff's awareness and the respective training is one of the main areas the SME must address. Technical problems tend to have decreased, by comparison. However, the SME believe that there are now considerable more harmful incidents due to sabotage and espionage. This calls for action, particularly on the part of the company management.

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Technical Measures

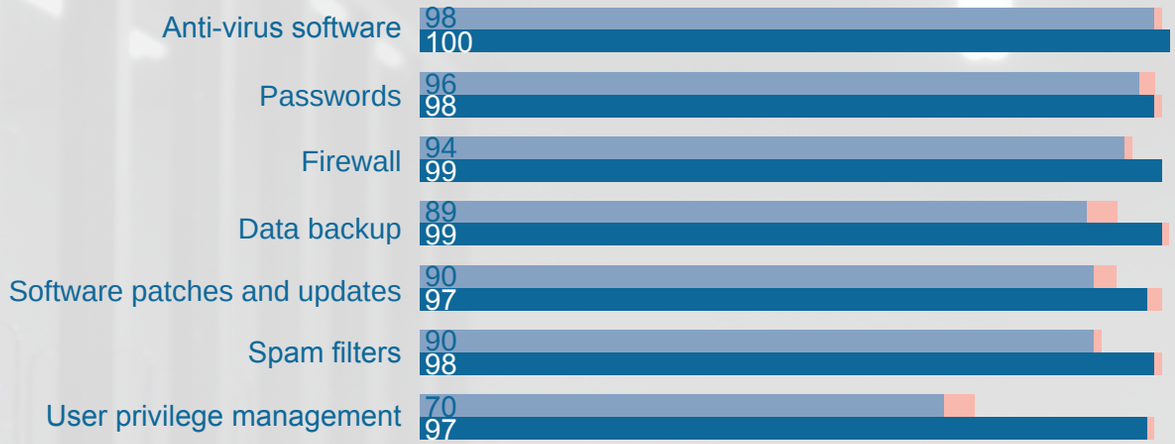
Basic technical measures such as anti-virus software, the use of passwords and setting up firewalls are generally in place in almost all smaller as well as larger SME. Small SME still have to catch up when it comes to making backup copies, applying software patches and installing updates, the use of spam filters or user privilege management.

The use of encryption programmes has significantly increased over the past few years. Thirty-five percent of SME now encrypt their emails, and 11% consider encryption important but have not implemented it yet. Compared to 2011/12, when only 17% of SME encrypted their data, this represents a considerable increase. However, small SME apparently still implement technical encryption measures considerably more rarely than larger SME.

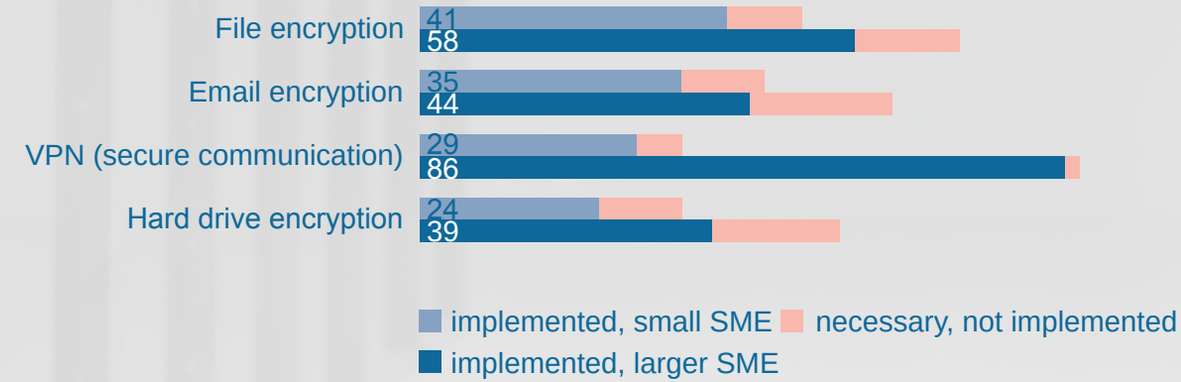
Larger SME are significantly ahead of smaller SME when it comes to the use of VPN connections, a solution for safe mobile access to company data. Eighty percent of the larger SME use VPN, whereas less than 30 percent of the smaller SME do.

Basic protection mostly in place – but small SME need to improve

Do you think these measures are necessary, and do you apply them?



Do you think these technical encryption measures are necessary, and do you apply them?

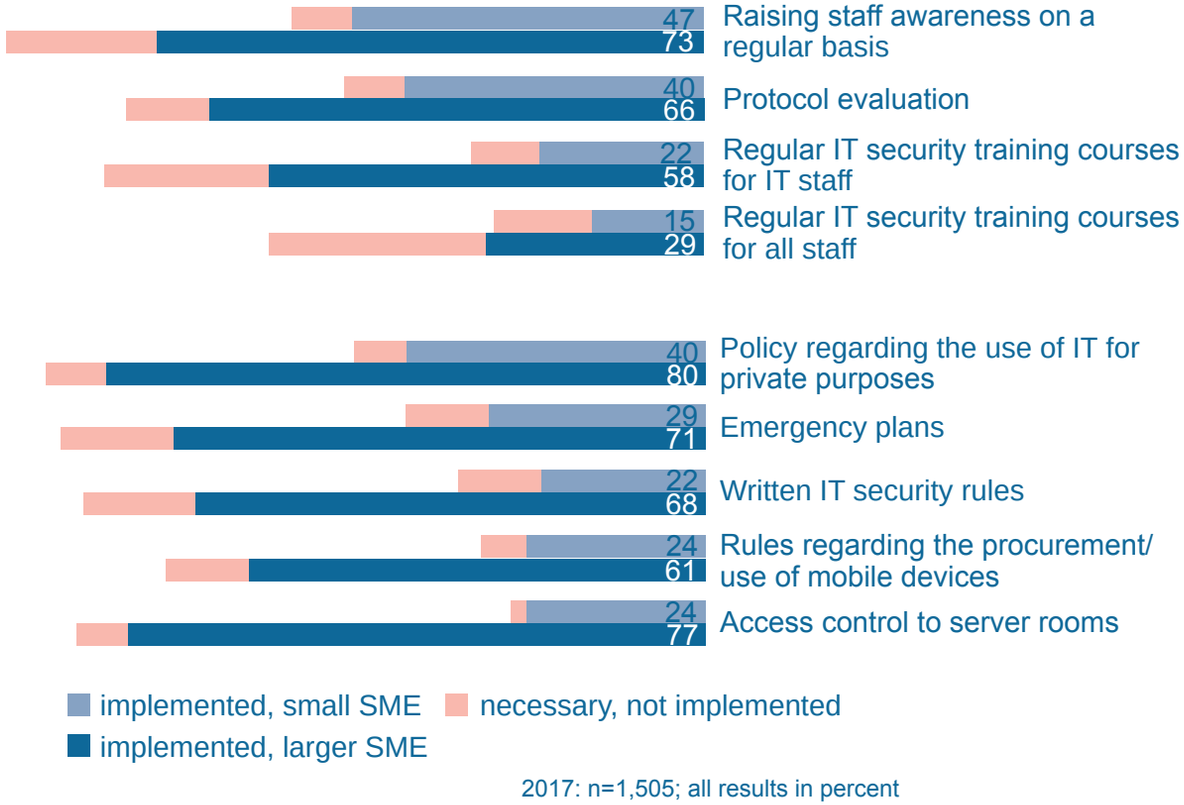


2017: n=1,505; all results in percent

Organisational Measures

Staff are increasingly working online – which means that they must become more aware of IT security

Please state which measures you consider essential in your company and which you have implemented.



2017: n=1,505; all results in percent

Most of the companies surveyed cited their own employees as the main cause of potential problems and harmful incidents. However, even simple organisational measures and rules such as registering and escorting all visitors to the company premises or the safe disposal of confidential printed matter are not being implemented to an adequate extent, according to IT security experts. **SME implement far fewer organisational than technical measures.**

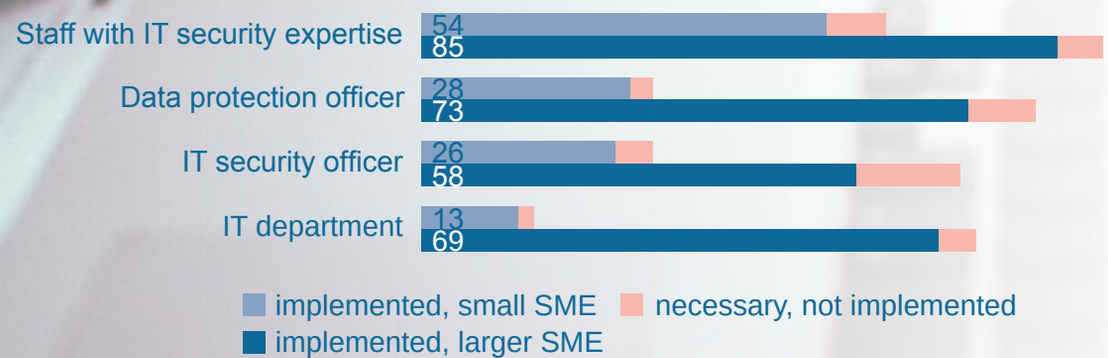
It is essential that measures such as **awareness raising, training courses and controls** are implemented regularly in order to equip employees with the necessary skills when it comes to IT security. It seems that **SME are lagging behind quite considerably where this is concerned**. Although information and training measures are considered essential, they are hardly ever implemented. Even specialised staff are not trained frequently enough.

The same applies to IT security related **rules and policies**: small SME are considerably less equipped. Should the worst happen, 71% of the small and 29% of the larger SME do not have an emergency plan in place.

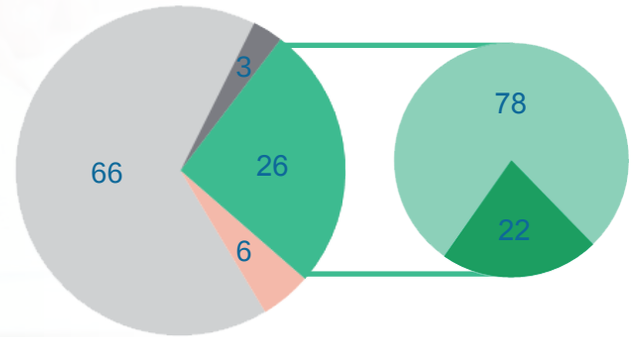
Personnel Measures

Slightly more than half of all SME in Germany employ staff with IT security expertise. The larger SME are ahead in this respect; 85% of these companies employ staff with IT security expertise. The lacking employment of IT specialists is also due to the high cost of suitably qualified personnel. Experts believe that SME rate the expense of employing an IT security specialist to be considerably higher than the cost of any (potential) harm due to gaps in their IT security.

Which personnel related measures in the area of IT security do you believe to be necessary in your company, and which have you already realised?



IT security officers in small SME



An IT security officer...

- is necessary, but has not actually been realised
- is not necessary
- no comment
- has been realised, in the form of a separate position or department
- has been realised, but also has other responsibilities

Two-thirds of the small SME believe that they do not need an IT security officer. In small SME, responsibilities such as the management of IT as such, IT security, data protection and administrative tasks are often just one element of someone's overall responsibilities and are therefore given only part-time consideration.

2017: n=1,505; all results in percent

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Information and Education: Further Training in SME

Information research has arrived in the digital age

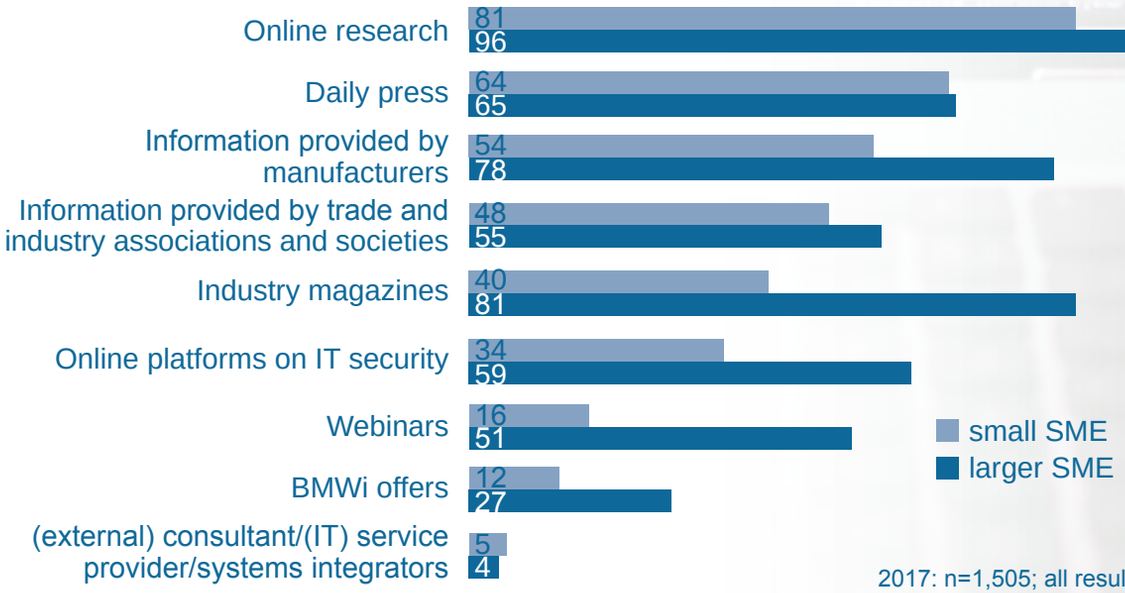
Information is mostly absorbed "in passing" via the mass media or online research. Small SME specifically research IT security less often. For most of the larger SME, the information provided by manufacturers and industry magazines are an important source of information.

External consultants play an extremely insignificant role for the companies.

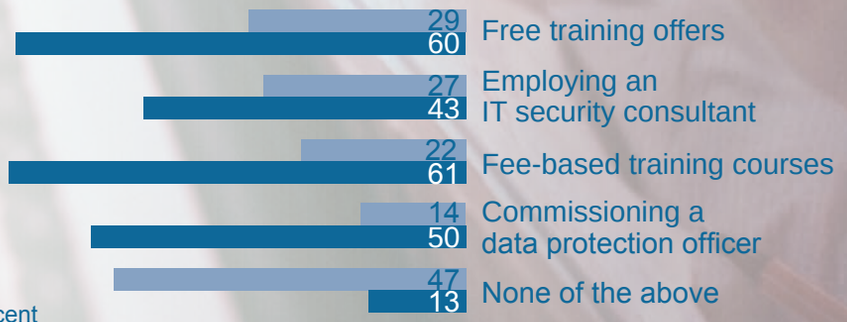
Free training courses are important in order to arouse awareness of IT security. According to experts, whether this will increase the subsequent attendance of specific training courses (subject to fees) depends largely on the size of the company.

Small SME are most likely to use free training courses. In the opinion of the experts, free offers often serve as an introduction to the issue of IT security. Specific questions are subsequently addressed in one-on-one consultations. Once their awareness has been raised, SME tend to be more willing to make the respective investments.

We obtain our information about IT security related matters from...



Use of training and advice offers



2017: n=1,505; all results in percent

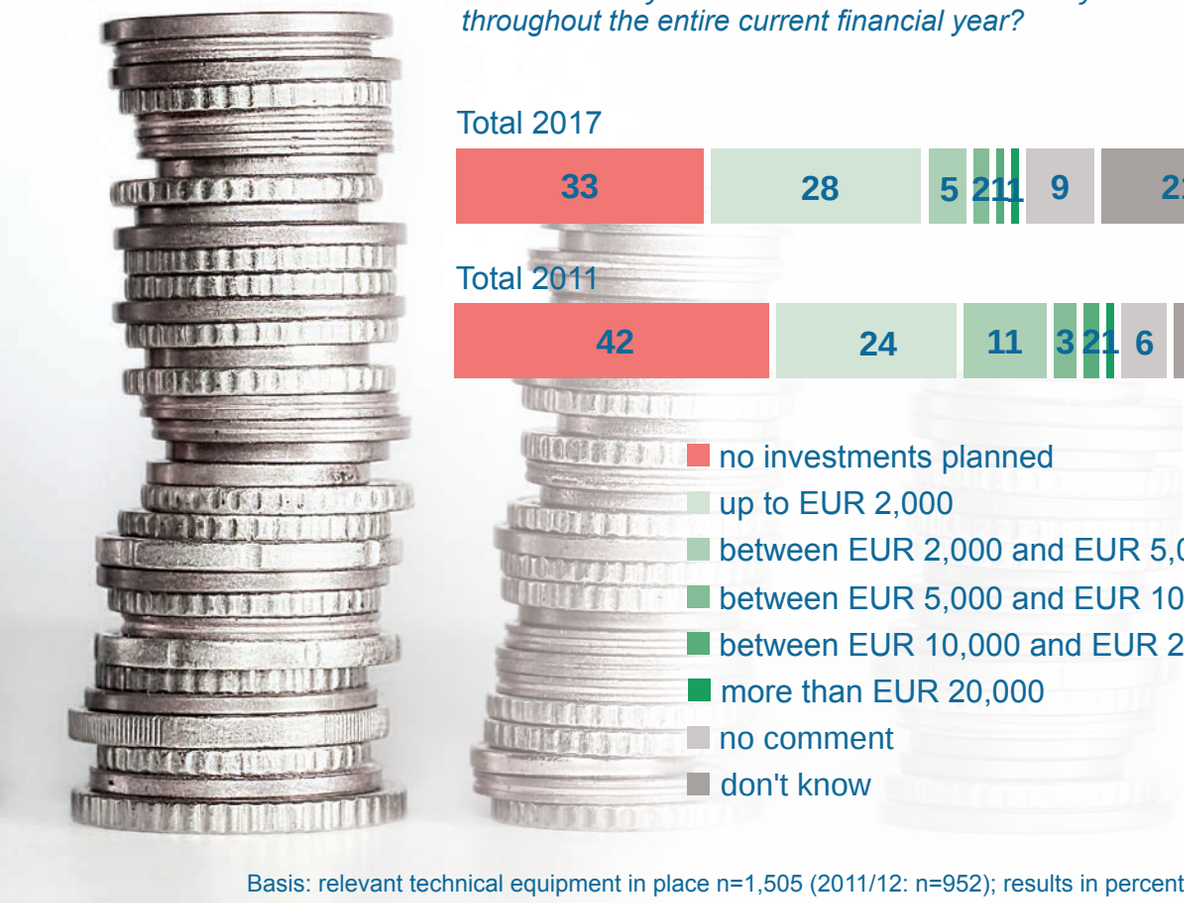
Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Investments into IT Security

A third of the SME had no plans to invest into IT security in 2017



How much do you intend to invest into IT security throughout the entire current financial year?

Basis: relevant technical equipment in place n=1,505 (2011/12: n=952); results in percent

The survey results show a **wide spectrum when it comes to the investments into IT security planned for 2017**. It ranges from less than 100 euros to a maximum of several hundreds of thousands of euros. On average, SME now invest considerable more into IT security, and more frequently than before. Small companies often do not invest into IT security at all, which leaves them exposed to considerable risks, in view of the level of their digitisation.

According to experts, many SME are not aware of how much adequate protection might cost. Other companies could be used as examples to allow them to make some initial cost-benefit considerations.

Companies often do not provide specific details of their investments. Where this point is concerned, the survey results must therefore be evaluated with some caution. Across the entire financial year 2017, the companies planned to invest an average of 2,600 euros each into IT security. In 2011, this figure amounted to only 1,800 euros.

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Barriers: Why so few IT Security Measures?

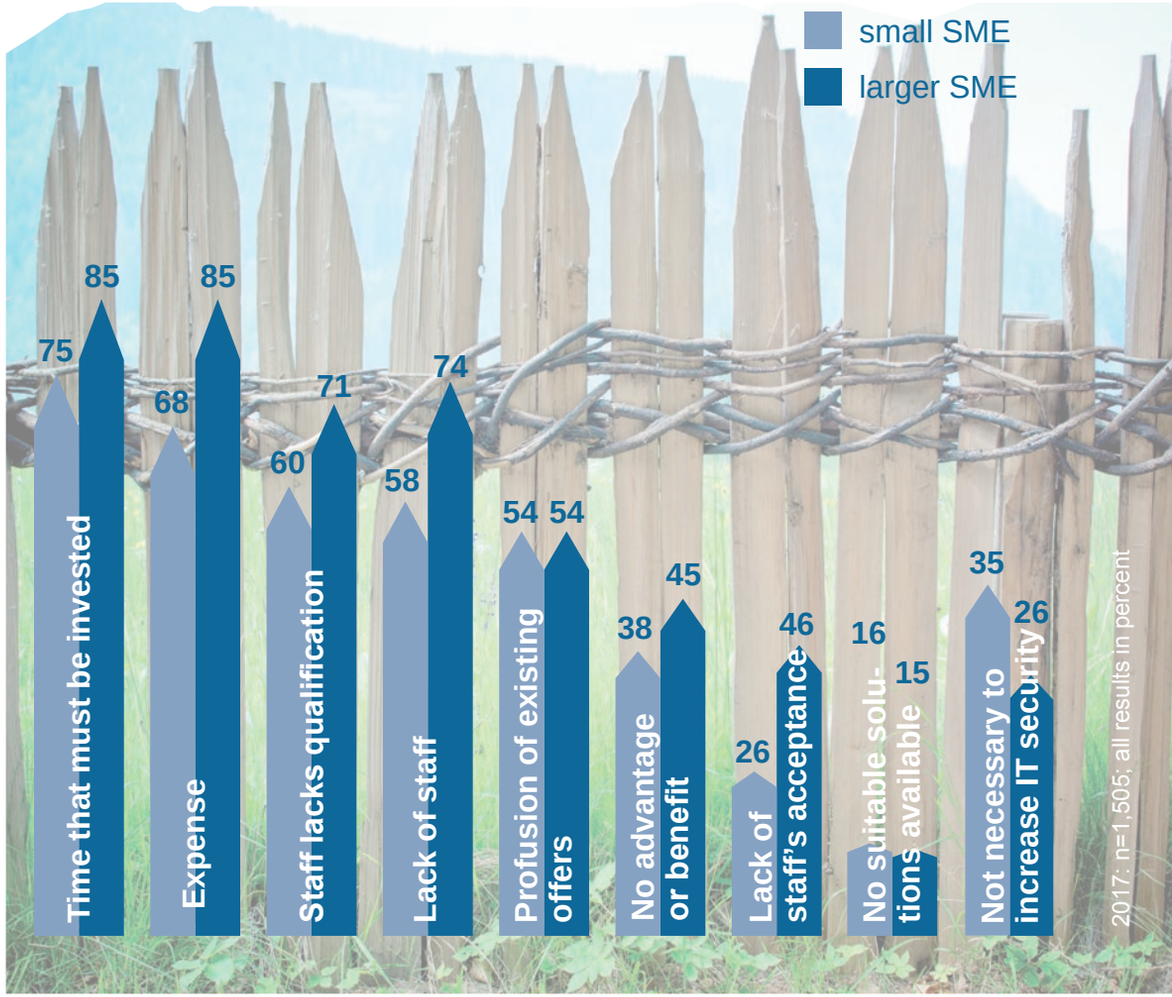
According to the survey, one main factor for both larger as well as small SME is the time that needs to be invested.

More than half of the SME cite the expense, lacking qualifications on the part of the staff or the shortage of respectively qualified professionals as reasons for the currently inadequate IT security situation of SME in Germany. Although there are offers such as information brochures or free training courses, there is often uncertainty about what is right for their own company and who provides these offers, maybe even for free. SME are deterred by the profusion and the complex technical language.

In the opinion of many experts, there is above all still a lack of awareness with regard to the security of the IT in their own companies in all SME, regardless of their size and despite all of their digitisation and online activities.

Many experts believe that SME do not carry out a sound cost-benefit analysis and that there is a lack of awareness when it comes to the potential expenses as well as the assets that are worth protecting. Even a simply IT security analysis with the support of a consultant with only a few well-chosen questions can change this and does not cost too much in terms of money or time. **Regional IT service providers, trade associations and societies as well as institutions that offer objective advice play an important role in this respect.**

What are the general obstacles SME are facing, in your opinion, when it comes to the improvement of IT security?

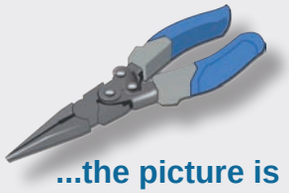


Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Focus **Trades**



Communication has long since become digitised

37% access company data via smartphones.

55% use WhatsApp.

60% exchange data with customers/suppliers.

...the picture is similar in the manufacturing industry

Skilled trades businesses are in the possession of sensitive customer, supplier and employee data – and are therefore a worthwhile target for attackers.

The Internet of Things has arrived in the workshop: many skilled trades businesses use machines that are connected to networks but do not protect them adequately against attacks.

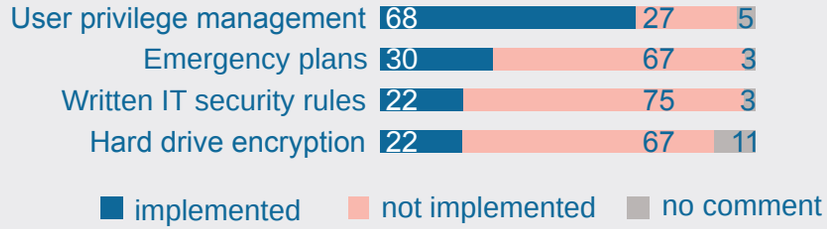
IT security weak points in skilled trades businesses

Lack of comprehensive IT security concepts:

79% of the skilled trades businesses had not carried out an IT security analysis.

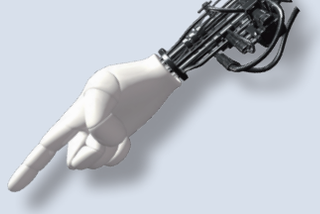
60% employ no staff with IT security expertise.

Technical and organisational measures in skilled trades businesses



Basis: 354 skilled trades businesses

Focus **Industry 4.0**



Industry 4.0 companies: increased digitalisation calls for increased IT security

Industry 4.0 companies are better equipped with IT technology than the average SME, use more mobile devices, use digital channels more often and exchange data with customers and suppliers electronically. In short: they are **more digitised and therefore more vulnerable.**

However, these SME seem to be aware of the **increased security requirements**. Compared to the average across all sectors, they consider the protection of their existing data to be of high or very high importance.

Due to the close digital links between partners in the value chain, for example suppliers and manufacturers, stricter IT security requirements apply to these companies. In the best case scenario, major companies put pressure on partners to implement IT security measures. However, even in this kind of set-up, there are evidently implementation gaps between the required and the existing level of protection.

Personnel and organisational measures in Industry 4.0 SME

High and very high importance of protection of existing data

Basis: 77 companies that are active in the Industry 4.0 area

All results in percent

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

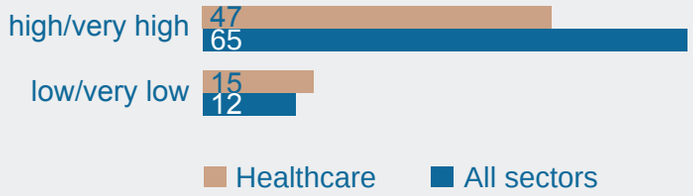
aufgrund eines Beschlusses des Deutschen Bundestages

Focus **Healthcare**

The disparity between the necessity of IT security and the reality in surgeries and health institutions could hardly be greater. Above all, the risk awareness of companies in the health and social services sector is alarmingly low. On average, these companies, which handle highly sensitive personal data, believe IT security to be less important than companies in other sectors do. The healthcare sector also lags far behind when it comes to the proportion of companies that have carried out a systematic **IT security analysis**: only 15% have systematically analysed their IT security.

Not even **one** in **five** healthcare sector SME has carried out a security analysis.

The importance of IT security in our company is



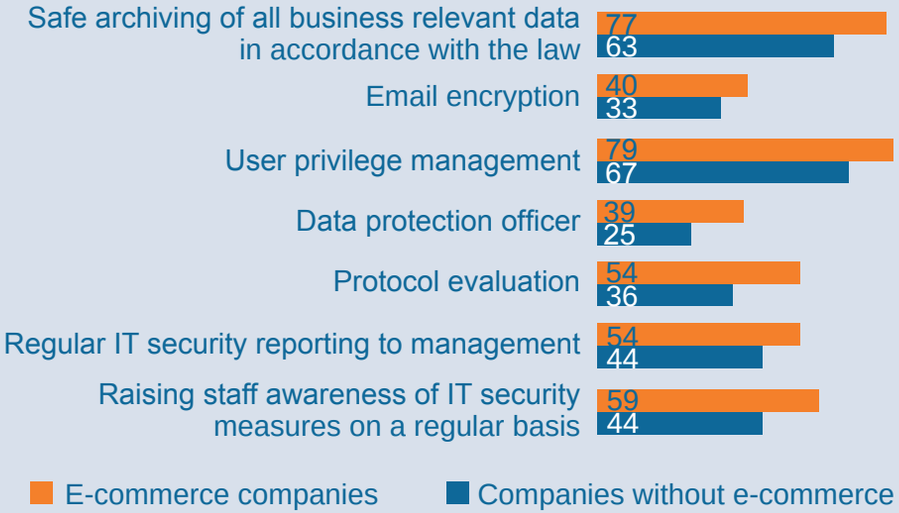
Basis: 98 healthcare sector companies

Focus **E-commerce**

Due to their digital business models, e-commerce companies are extremely well equipped with ICT. They also use innovative wearables such as data glasses, for example, and digital channels more frequently than the average. Particularly the utilisation of social networks for sales and marketing activities is widespread. Every second e-commerce company is active in this area.

The majority of the SME in Germany believes the importance of IT security to be high or very high – but does not act accordingly. The reverse is true for e-commerce companies: they tend to rate the importance of IT security lower than the average, but use more technical, organisational and personnel IT security measures.

Use of technical, personnel and organisational measures by e-commerce companies



All results in percent

Basis: 428 companies that are involved in e-commerce

Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages

IT Security in SME 2011/12 and Today

Digitisation means even stricter IT security requirements

The use of ICT in SME has steadily increased since 2011/12. Significantly more companies outsource IT applications and Cloud computing.

IT security can no longer be a marginal topic these days but should become an integral element of the corporate strategy.

In the past five years, the efforts with regard to IT security have hardly increased, bar in the technical area. Basic solutions exist throughout, and at least there is some positive news with regard to the use of encryption solutions. Personnel and organisational measures, on the other hand, continue to lag even behind the companies' own risk assessment and the objective protection requirements.

What is striking is that companies that are already extremely digitised, meaning companies that are involved in Industry 4.0 projects or active in e-commerce, use more comprehensive IT security measures. However, in the large majority of SME, the increased IT security requirements are met with inadequate protection measures.

More than ever before, it is therefore essential that the issue is addressed as a matter of urgency.

Step by Step

Small steps can already make a decisive difference when it comes to improving a company's IT security.

The starting point is a simple IT security analysis, carried out internally, on the basis of existing checklists.

- Record existing IT and data handling policies in writing and constantly remind everyone of them.
- Use free offers by objective regional providers to obtain some initial information.
- Managers must lead by example: establish security culture in the company.
- Develop emergency plan for worst case scenario.
- Carry out an IT security analysis: what existing data in the company should be protected?

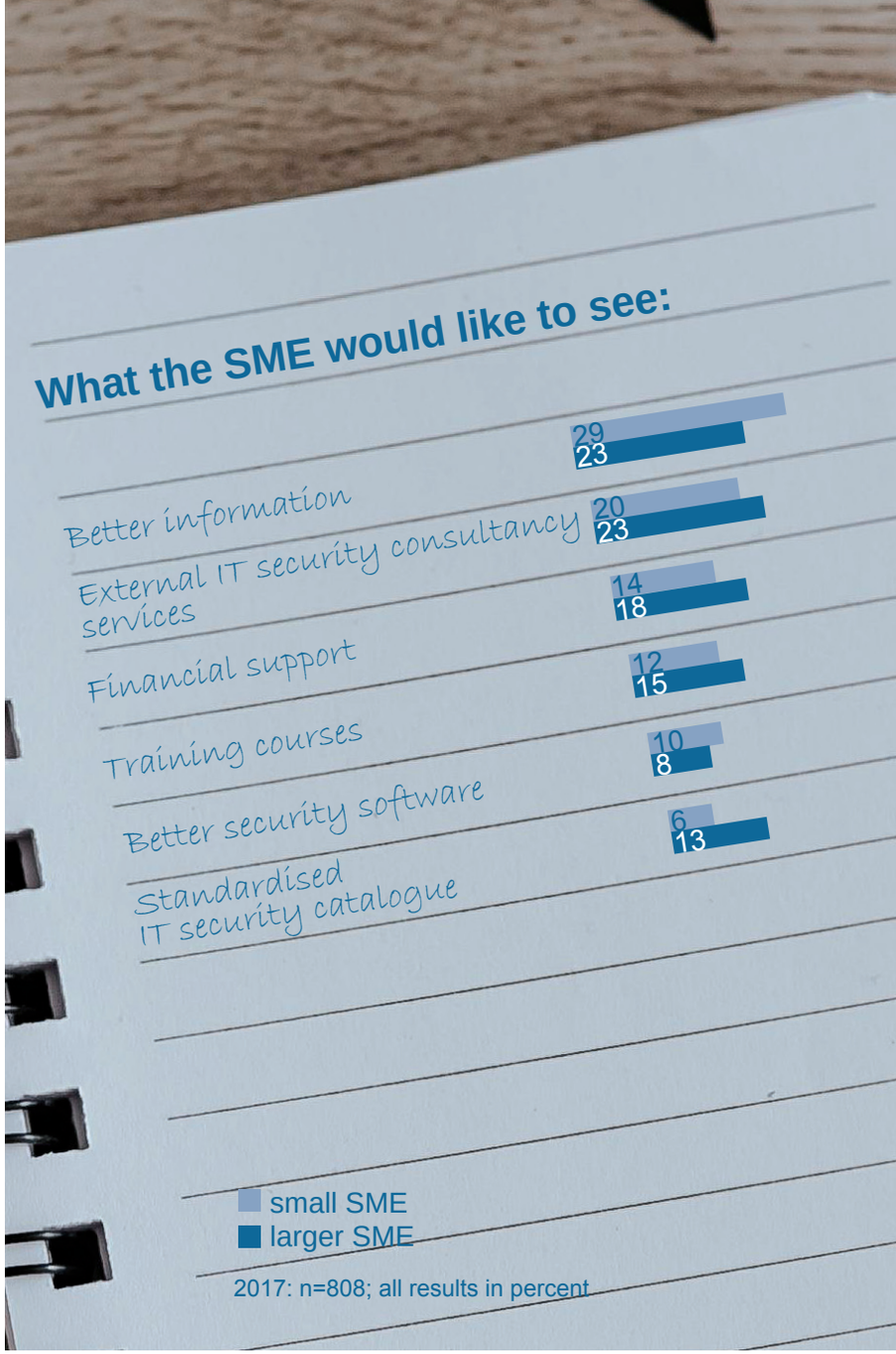
What Can Be Done to Help SME on their Way to Increased IT Security?

What else is important:

1. **Raise awareness:** Initiate and support awareness campaigns; utilise topics such as digitisation or the EU General Data Protection Regulation (GDPR) to make SME more aware of IT security
2. **Cite examples:** Publicise best-practice and case studies that show how comparable companies are addressing IT security
3. **Educate sensibly:** Promote the didactic design of the offers to ensure that SME can understand the contents
4. **Stronger regional presence:** Make institutions that offer objective advice available as SME prefer local offers
5. **Help with cost-benefit considerations:** Offer information and training courses that introduce the topic and help with the initial IT analysis
6. **Provide guidance:** Help SME to find objective IT consultants and IT products
7. **Information:** Report objectively about the latest security incidents, the gateways that were used and the potential harm and costs

Particularly important today, compared to 2011, in view of the digitisation:

8. **Ensure long-term availability and use of offers:** constantly changing SME need regular IT security information and training courses
9. **Support school-based, vocational and professional training** and adapt it to the constantly changing digitisation and IT security challenges
10. **Security by design:** Consider user-friendly safety features right from the start and integrate them into company processes



Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

About this publication

Within the scope of its "IT-Sicherheit in der Wirtschaft" initiative on IT security in businesses, the Federal Ministry for Economic Affairs and Energy (BMWi) promotes projects that focus on increasing IT security, especially in small and medium-sized companies. WIK – Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste – realised the BMWi-funded project "Current IT Security Situation in SME" within the scope of this initiative. The results are not only based on an extensive evaluation of the respective literature but also on a representative survey (CATI) of 1,508 SME in Germany and 30 in-depth expert interviews. The long version of the study can be downloaded from *www.wik.org*. The starting point for the current study was a study on the level of IT security in small and medium-sized enterprises conducted by WIK on behalf of the BMWi in September 2012, with two representative surveys in 2011 and 2012.

About the BMWi's IT security in businesses initiative

The Federal Ministry for Economic Affairs and Energy "IT-Sicherheit in der Wirtschaft" IT security initiative intends to help above all small and medium-sized companies to use ICT systems safely. With the assistance of researchers, business and government IT security experts, the ministry intends to establish a basis for increasingly raising the awareness of IT security in German SME involved in the digital economy. Practical support measures are designed to enable companies to improve their IT security. See *www.it-sicherheit-in-der-wirtschaft.de* for more information about the initiative and its purpose (in German).

About WIK – Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste

The scientific institute for infrastructure and communications services "Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste" (WIK) in Bad Honnef has been advising its worldwide public and private clients on telecommunication, the internet, mail and energy for over 30 years. It focuses primarily on the respective policies, regulations, competition and strategy. For more information, see: *www.wik.org*.

Legal notes

WIK Wissenschaftliches Institut für
Infrastruktur und Kommunikationsdienste GmbH
Rhöndorfer Str. 68
53604 Bad Honnef, Germany
Phone: +49 2224 9225-0
Fax: +49 2224 9225-63
Email: info@wik.org
www.wik.org

VAT identification no.: DE 123 383 795
Authorised representatives and signatories
General Manager and director: Dr Iris Henseler-Unger
Director and Head of Department
Postal Services and Logistics: Alex Kalevi Dieke
Director and Head of Department
Networks and Costs: Dr Thomas Plückebaum
Director and Head of Department
Regulation and Competition: Dr Bernd Sörries
Head of Administration: Karl-Hubert Strüver

Chairperson of the Supervisory Board: Dr Daniela Brönstrup
Companies register: Registered at Amtsgericht Siegburg district court; company number HRB 7225
Tax no.: 222/5751/0722

December 2017
(translated November 2019)

Image credits: P. 1, 16: Unsplash.com–Jason Blackeye; p. 3, 4, 6, 7, 8, 9, 10, 11, 12, 13, 14: Pixabay.com; p. 15: Kaboompics.com

wik Wissenschaftliches Institut für Infrastruktur und Kommunikationsdienste

IT-Sicherheit IN DER WIRTSCHAFT

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages