IT Requirements in The Real Estate Sector

Georg Rockel, Linard Barth

Abstract*: Digitalization has reached the German real estate market. IT requirements have to be defined and followed. The state, companies and private households must implement appropriate requirements and take measures to jointly guarantee data protection and data security to be armed against cybercrime, and thus promote digitalization. Suitable measures will be examined here. IT facilitates many things but is also an instrument that can be abused also exploited, as it is operated by people. To be able to implement constant and secure overall solutions and concepts, this paper examines individual aspects in more detail and provides appropriate recommendations.

***Keywords*: GDPR, data protection, data security, cybercrime, real estate, IT security, threats of the Internet.**

I. INTRODUCTION

The real estate industry is growing rapidly. More and more living space is being created. Thousands of residential units have to be taken into account as the trend of digitalization is influencing the German real estate market. Information technology (IT) provides help, but the necessary requirements have to be defined. What these requirements are will be examined here.

Definition of digitalization in the real estate sector

The word digitalization is not generally defined. In the literature, there are different meanings due to different industries and processes. „Digitalization can describe the mere transformation and representation of information and knowledge into digital numerical codes, but also the so-called digital transformation, which is referred to as the digital revolution or digital turning point [1] “.

„In general, digitalization means any change based on new technologies, digital devices, the internet and modern information- and telecommunication technologies. Other aspects are highly networked and intelligent systems. The multitude of aspects thus creates an extended definition of the term. Firstly, in the narrower sense, it’s about transformation from analog to digital data. Secondly, another aspect is the permanent and location-independent availability of data. Thirdly, in the extended sense, the Digital Revolution changes all spheres of society as shown in the following “Fig. 1”.

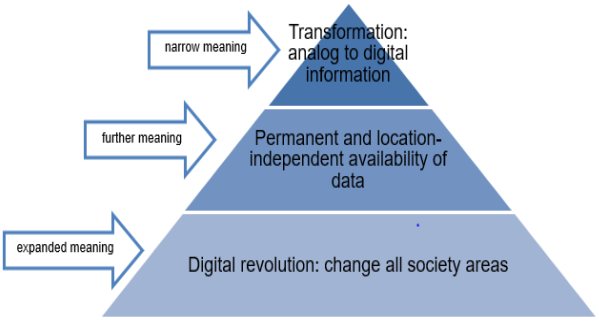

Fig. 1. Definition Digitalization [2]

A study from 2019 within 300 real estate investors shows, which megatrends will influence the real estate industry in Germany in the future. 53 percent agreed with the statement that digitalization will have the greatest impact on the German real estate market in the next 5 to 10 years. This can be seen in the following “Fig. 2”

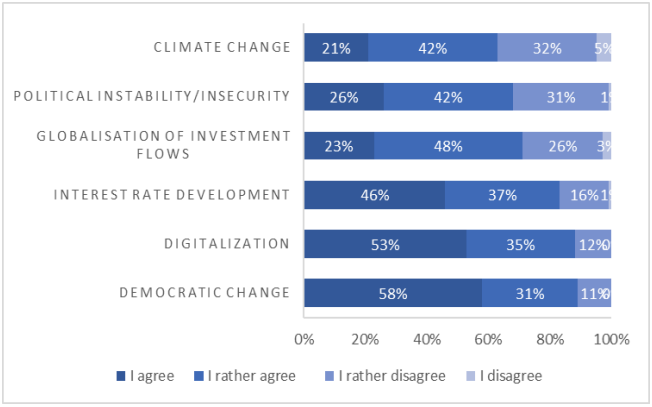

Fig. 2. Megatrends which will influence the real estate industry in Germany in the future [3]

This paper elaborates the topic of IT requirements in the real estate market, where digitalization was named as the second most important megatrend to influence the German real estate market in the next 5-10 years.

From this, the following definition can be derived for digitalization in the real estate sector. "Digitalization is the transformation of analog data into digital data, as well as of its permanent and location-independent availability.

According to this definition, data must be recorded analogously (e.g. on concluded contracts), fed into databases (e.g. Customer-Relationship-Management (CRM)-System) and then made available via mobile CRM applications, regardless of location (e.g. via apps).

For this reason, appropriate IT requirements in the real estate sector must be defined and followed.

Revised Manuscript Received on October 01, 2019.

Georg Rockel, Economics and Management, Mendel University Brno, Czech Republic.

Linard Barth, Economics and Management, Mendel University Brno, Czech Republic.

II. STATUTATORY REQUIREMENTS

Traffic security duty

According to the German law, every company is obliged to ensure “safety” of others while pursuing their business, i.e. they must take the risks to others into account when making decisions. In the real estate sector, this obligation extends to all risks that can emanate either from the property itself or from the house built on it. In the event of disregard, the injured party must be compensated for the resulting damage following § 823 (1) Bürgerliches Gesetzbuch (BGB) / in English: civil code of Germany.

This means that property owners must take protective measures, the nature and extent of which must be determined case-by-case based on the specific hazard. Although there is a possibility of outsourcing, the organizational, selection and supervisory duties cannot be outsourced from a company.

In this case, IT offers the possibility of a digital representation of monitoring obligations, which can be represented in detail for each building. The duties can then be assigned individually to appointed employees. Reporting lists can be created to facilitate on-site monitoring. The logging of all data safety measures then provides proof of compliance with duties in the event of a legal dispute.

Data protection

The collection of personal data entails the danger of the "transparent person also called mass surveillance", which is why the Data Protection Act was enacted [4].

Chapter 1, Article 1, matter and objectives, paragraphs 1 to 3 of the General Data Protection Regulation (GDPR) contains necessary rules relating to the protection of natural persons regarding the processing of personal data and rules relating to the free movement of personal data. It protects the fundamental rights and freedoms of natural persons and particularly their right of protection of personal data. It also regulates the free movement of personal data within Germany based on the protection of individuals regarding the processing of personal data, without restricting or prohibiting it. This definition makes it clear that the handling, the duty to provide information when collecting personal data from the data subject (Chapter 3 Article 13 GDPR), the right to restriction of processing (Chapter 3 Article 18 GDPR) and General principle for transfers (Chapter 5 Article 44 GDPR), of personal data is only permitted in special cases [5].

The new GDPR has handed over the complete responsibility to the enterprises and has given them the duty to comply with the data protection regulations. The companies still have difficulties in realizing these goals. 606 enterprises were examined regarding GDPR conformity by industry. The result was that most German industries are only in the status of the processing of realization of these goals. Even the software industry, which should be a leading example, has reached just 21% of GDPR requirements, 64% of requirements are in progress and 14% have not yet started. At the worst, the pharmaceutical industry with 48% of the requirements in processing and 48% of the requirements with not yet begun. This can be seen in the following “Fig. 3”.

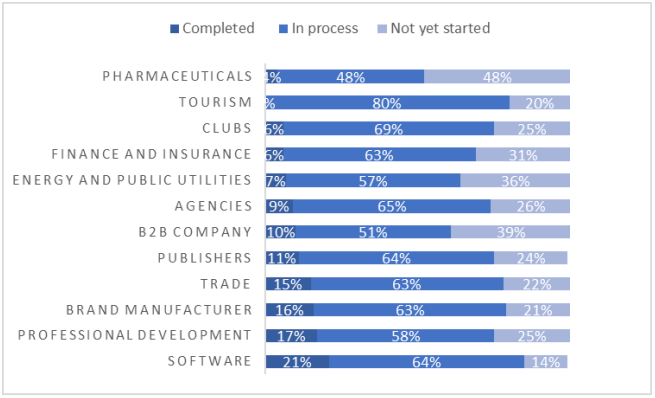

Fig. 3. GDPR - Conformity of the investigated companies according to industry [6]

The EU data protection regulation, which came into effect on 25 May 2018, has not only caused great uncertainty among many companies, organizations, and private individuals but has also brought additional work to recruiters in many places. The obligation to appoint a data protection officer following Chapter 4 Article 37 GDPR has led to an almost double increase in the demand for data protection officers from 2017 to 2018. Their tasks are defined in Chapter 4 Article 39 of the GDPR [7].

The data protection has become an important topic with the introduction of the GDPR in 2018, companies have considerably more expenditure around the GDPR guidelines to keep. 78% of the surveyed companies associate the compliance with the guidelines as additional effort, 502 companies with 20 employees or more were surveyed. This can be seen in the following “Fig. 4”.

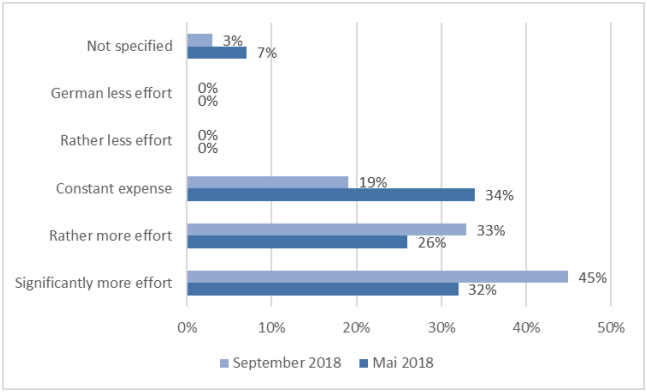

Fig. 4. GDPR - Effort during operation [8]

What about data protection on the Internet in private households? Despite the new GDPR. According to a survey on data protection on the Internet in Germany, 50% of those surveyed voted that they take security precautions, 14% of those surveyed are not worried, as it is only a question of the behavior of the masses on the Internet and not of individual users. 33% said that they would like to protect their data better but don't know how. 39% have nothing to hide and 40% said that it is not possible to protect their data on the Internet. This can be seen in the following “Fig. 5”:

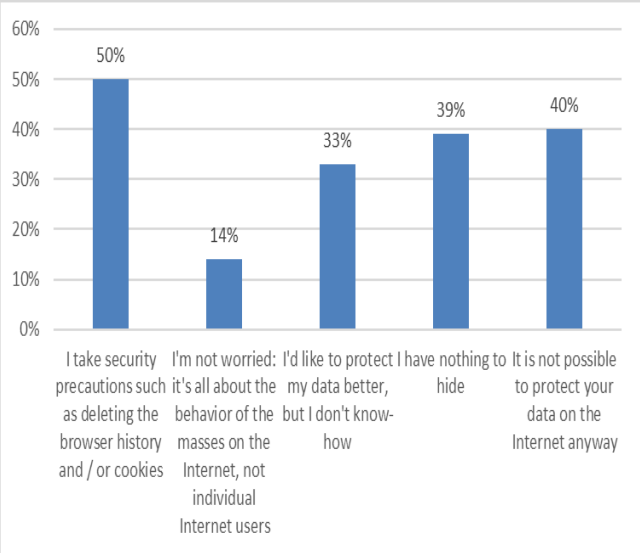

Fig. 5. Survey on data protection on the Internet in Germany in 2018 [9]

According to the survey on responsibility for data protection, in which 1007 people aged 16 and over were surveyed in January 2019, 74% of respondents believe that the user himself has the responsibility to protect his data on the Internet. Just 22% think that the state is responsible and just 3% think that the Internet providers or manufacturers of hardware and software need to take more care of data protection. This can be seen in the following "Fig. 6".

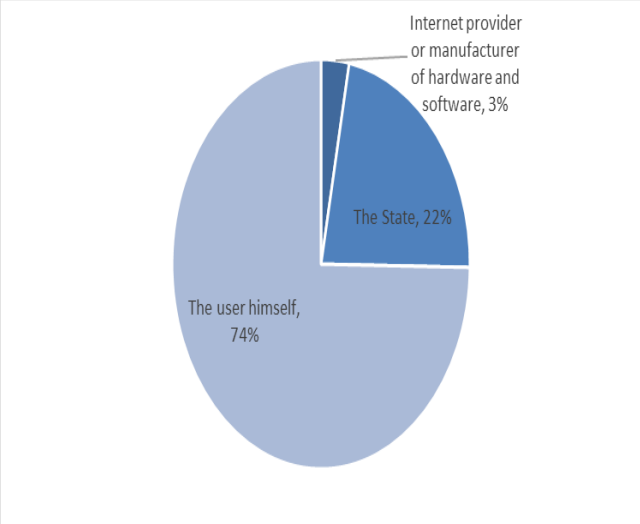

Fig. 6. Survey on data protection on the Internet in Germany in 2018 [10]

Especially young Internet users aged between 14 and 24 years consider the protection of their data on the Internet in 2018 with 43% as very important, 47% say that it is important to them, just 11% estimate this as not so important or not important at all.

Despite the decreasing prioritization of data security of young people between 2015 and 2018, the issue of data security is considered to be predominantly important. This can be seen in the following "Fig. 7".

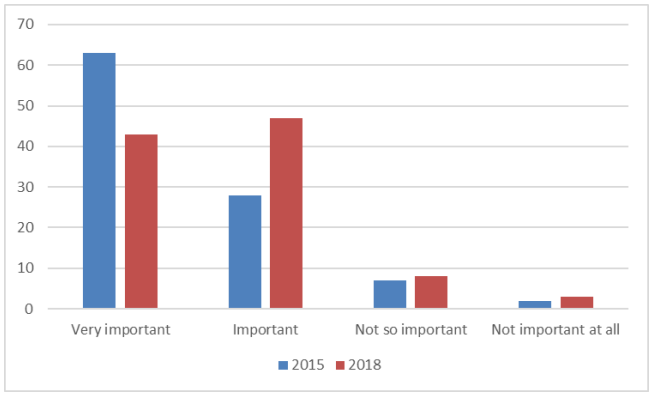

Fig. 7. Results of the survey on the protection of personal data of young people online in Germany 2018 [11]

A survey of young people aged 14-19 has been dedicated to the issue of data protection. 998 young people in Germany were asked how they try to protect their data on the Internet. 58% of the interviewees said that their profiles in social networks are set to private. 51% repeatedly delete their browser history, 45% deactivate the location function on all devices, 30% repeatedly delete the cookies in their browsers, 24% deactivate the geo stamp on photos, 3% protect the data in a different way, 6% do not protect their data, 1% did not know that they can protect your data and 5% did not provide any information or no information at all in response. This can be seen in the following "Fig. 8".

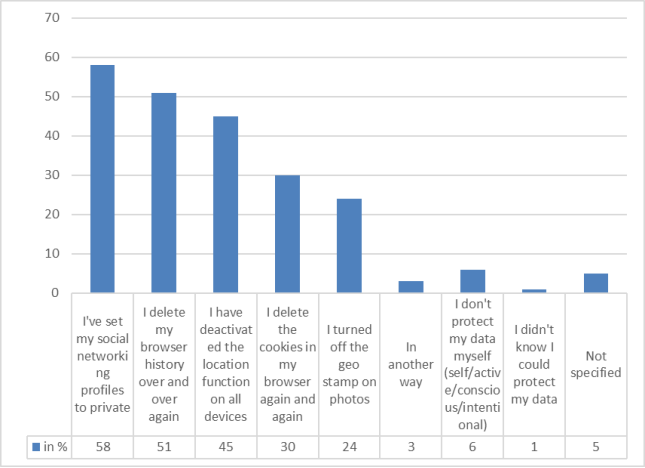

Fig. 8. Results of the survey on data protection behavior of young people in Germany 2018 [12]

The topic data protection is a topic for itself, for the realization the state takes the enterprises with the new GDPR on the responsibility for data protection. But the enterprises have their difficulties to implement these topics as seen in "Fig. 4: GDPR - Effort during operation" and nevertheless, the confidence of the private persons in the data protection is to be classified as low see also Figure 9: Assessment of data security on the Internet in Germany by 2018. The conclusion is that both state, enterprises, providers, manufacturers and private households must work together to realize data protection. From this follows:

1) The state sets the minimum requirements for data protection

2) The private households must take care to whom they make which data available.

3) Internet providers or manufacturers of hardware and software must supply secure networks and secure hardware to counteract unauthorized access.

4) Companies need to take security precautions How to handle customer data. Points 2), 3) and 4) give rise to the subject of data security.

Data security

The term data protection is used practically exclusively in connection with personal data. The term data security is concerned with the general protection of data, regardless of whether or not they relate to individuals [13].

Data security is more important today than ever. As a user of the Internet, you have to leave your data everywhere, be it to obtain information, to order goods or to chat with friends on Facebook. The people are already suspicious and then this feeling is also confirmed by the press reports about data theft and data misuse.

According to Chapter 5 Article 47 Section 2d) GDPR, data protection should take place through the security of data, especially when using technical devices, companies must take all technical and organizational measures necessary to prevent data theft and misuse.

All collected data may only be used for the purpose for which it was originally collected. In comparison to the data protection, which refers to personal data, the data security covers all kinds of information [14].

The Bundesamt für Sicherheit in der Informationstechnik (BSI) in English: Federal Office for Information Security developed several basic IT protection catalogs with security standards for information security, especially when using information technology systems. Three basic values were developed for data security. This can be seen in the following "Fig. 9".

Confidentiality	The data may only be read, changed, stored or deleted by automated users.
Availability	The data may only be accessed within a certain period time.
Integrity	The data must be complete and unchanged, and if a change is made, then all changes must be traceable.

Fig. 9. Basic values of data security according to BSI [15]

According to the study by Bitkom Research in the survey period 2014 to 2018 within 1027 Internet users (2018) aged 14 and over, the confidence of Internet users in data protection increased from 13% in 2014 to 23% in 2018. However, most Internet users with 75% in 2018 still classify data protection as rather insecure to completely insecure. This can be seen in the following "Fig. 10".

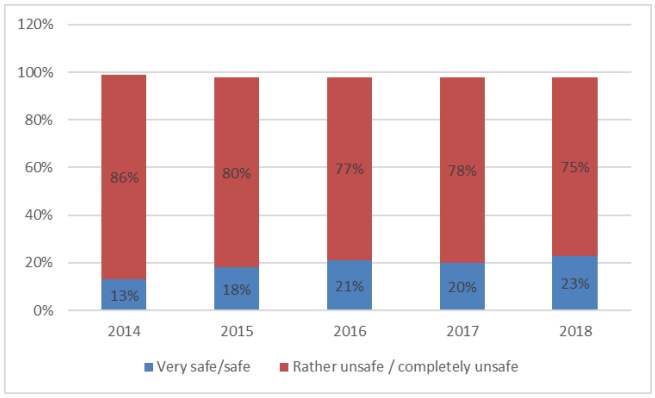

Fig. 10. Assessment of data security on the Internet in Germany by 2018 [16]

For comparison: The survey on the security assessment of personal data on the Internet in Germany in 2019 among approximately 2000 consumers aged 16 and over showed that 6.5% of respondents stated that their data on the Internet are very secure, 21.3% stated that their data are secure, 38.5% stated that they are rather secure, 25.7% less secure and 7.9% stated that their data were unsafe. This can be seen in the "Fig. 11".

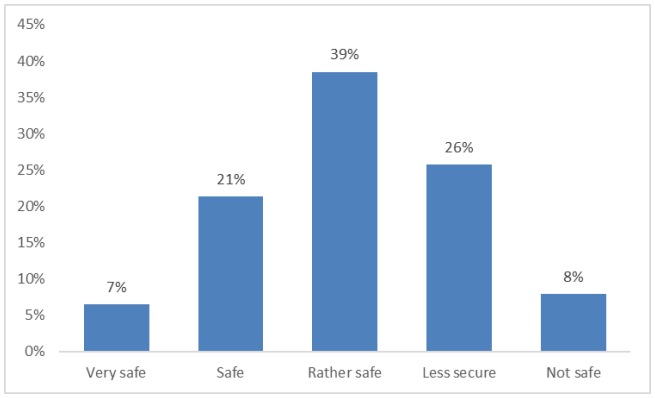

Fig. 11. Assessment of the security of personal data on the Internet in Germany 2019 [17]

It's recognizable, that the opinions between the Internet users and consumers fall apart. Internet users rated data security at 75% in 2018 as rather insecure as seen in Figure 10. On the other hand, consumers rated their data at 67% as secure to rather secure as seen in Figure 11. Here speculations can be derived which statistics are more representative. However, not all consumers are Internet users. According to the German Civil Code (Bürgerliches Gesetzbuch BGB) § 13 Consumer Definition: A consumer is any natural person who concludes a legal transaction for purposes which are predominantly neither commercial nor self-employed [18]. From the definition it can be inferred that a consumer is "any natural person", but this does not mean that he or she also uses the Internet. For this reason, the meaningfulness of the survey may be distorted. That is why we take the survey from Figure 10: Assessment of data security on the Internet in Germany by 2018 as an approach, since it comes from direct Internet users. It states that the Internet is perceived as rather insecure with a 75% share stating that data security is not given.

This raises the question of how IT and data security can be implemented from the defined points of data protection:

For point 1) The state sets the minimum requirements for data protection.

The state defined the data protection with the GDPR, however, this deposits the responsibility of the data security indirectly to the enterprises. It is not defined how the data security must be realized. However, the duty to guarantee this was given to the private enterprises.

2) The private households must take care to whom they make which data available.

3) Internet providers or manufacturers of hardware and software must supply secure networks and secure hardware to counteract unauthorized access.

4) Companies need to take security precautions. How to handle customer data

First of all, point 2) The private households must take care to whom they make which data available.

How do private households counter data misuse? An online survey conducted in 2017 with 1037 respondents over 18 years of age indicated the following measures (multiple answers were possible).

66% stated that they do not open e-mails from unknown senders or delete them immediately, 62% use virus protection programs or virus scanners, 59% have a firewall, 49% use spam filters, 47% regularly delete cookies and the browser history, 43% use complicated passwords, 43% do not store passwords, PINs or TAN lists on the hard drive, 38% use anti-spyware, 36% use pop-up blockers or advertising blockers, 36% change passwords, 35% disable cookies in the Internet browser, 33% pay attention to quality seals when shopping online, 31% do not use external PCs, 23% use separate e-mail addresses for example for public games or competitions, 17% are anonymous or give false information or fake user names for example for social networks, 9% use software for anonymous surfing, 9% use encryption programs for e-mails, 7% deliberately use the Internet very seldom, 4% use special search engines, such as ixquick (metasearch engine, which voluntarily committed not to collect or store private data of users [19].), 4% did not specify anything. This can be seen in the following “Fig. 12”.

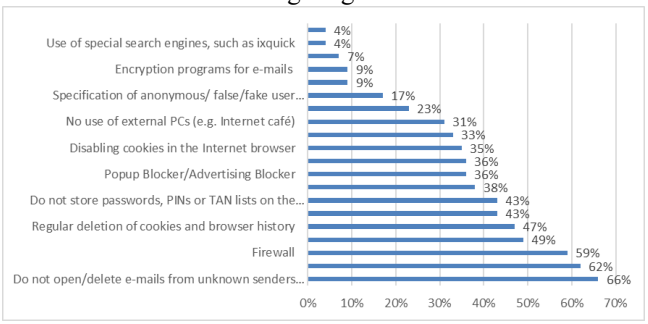

Fig. 12. Use of measures to protect against data misuse on the Internet 2017 [20]

It can be seen, that private households are already taking precautions for data security themselves. How these are implemented, however, differs from individual to individual.

What about Internet providers and manufacturers of hardware and software, what contribution do they make?

3) Internet providers or manufacturers of hardware and software must provide secure networks and secure hardware to counteract unauthorized access.

Both Internet providers and manufacturers of hardware and software are companies in the narrower sense. Also, they work with customer data and must meet the GDPR standards and take measures to ensure data protection and security. Some points are to be distinguished here.

I) Manufacturers of hardware and software: According to the Product Liability Act § 4 Manufacturer of the Federal Republic of Germany: a manufacturer is the entity who has manufactured the end-product, a basic material or a partial product. Anyone who claims to be a manufacturer by affixing his name, trademark or any other distinctive sign shall also be deemed to be a manufacturer [21].

According to the product liability law of the Federal Republic of Germany § 2 product: a product in the sense of this law is any movable thing, even if it forms part of another movable thing or an immovable thing, as well as electricity [22].

A manufacturer can be a manufacturer of an end-product or also produce partial products, called original equipment manufacturer (OEM). An original equipment manufacturer (OEM) is a company that produces parts and equipment that may be marketed by another manufacturer [23].

An example from the production of a router: A router is a telecommunications device that forwards data packets between computer networks [24].

The router itself is an end-product, but it consists of components that, when combined, enable its end function. However, in the times of globalization, individual components usually come from other suppliers who have specialized in having these components delivered from OEM according to their ideas and ultimately assemble these different components themselves to obtain end-product.

Here it must be considered that the individual components communicate with each other, already here the first programming takes place so that software is already necessary for hardware recognition. The more complex the technology, the more suppliers are integrated into the manufacturing process. Here there is already the risk of manipulation based on the integrated sub-products for the end-product, which means that there is already a risk in the manufacturing process of installing infected sub-products from third-party suppliers with harmful programs without being aware of it. In times of globalization, there is a large number of suppliers, but how do you distinguish between trustworthy suppliers and untrustworthy ones?

ISO 9001/2015 for quality management systems-Requirements serves here as a good example of how quality management systems should be designed, under point 8.4 page 38 “Control of externally provided processes, products, and services” and point 8.4.1 “The organization shall determine the controls to be applied to externally provided processes, products, and services” [25]. However, this refers to the quality management system and not safety.

Therefore, the ISO/IEC 27001, Information Technology-Security, techniques-information security management systems-requirements, specifies the requirements for setting up, implementing, maintaining and continuously improving a documented information security management system, while taking into account the context of an organization. This is also confirmed by the Federal Office for Information Security [26].

Both standards applied together allow the realization of a proper assessment of suppliers in terms of product quality and IT security. At least it is a good way to orientate on these standards.

The router technology itself allows data packets to be transferred between the computer and the network, but how secure is it? Most routers today do not only use Local Area Network (LAN) technology, but also Wireless Local Area Network (WLAN) technology, so that users cannot only connect to the Internet via a cable but also wirelessly. Therefore, today's router manufacturers use the following encryption methods:

• WPA2 (Wi-Fi Protected Access 2) can use this WLAN encryption up to 256-bit to hide the entered password phrase.

Besides, the key is used asymmetrically. This means that the whole key does not always have to be used to encrypt the plaintext, but only parts of it can be used in different permutations.

• TKIP (Temporal Key Integrity Protocol) The protocol provides a kind of algorithm for encoding the WLAN key.

• CCMP (Counter-Mode/CBC-MAC Protocol) CCMP is the next step in encryption protocols providing a 128-bit long key, each with 48-bit long initialization vectors. A mixture of different encryptions is used so that the key can hardly be read out [27].

A software company is a company that focuses on the development, production, and distribution of software, for example operating systems, computer programs, and application programs [28].

Also, these manufacturers, like for example Microsoft and Apple are responsible for developing protected applications.

Since historically whole operating systems have been switched off by e.g. malware attacks, some software companies have specialized in the development of security software, like Kaspersky Lab or Symantec Corporation with Norton or McAfee.

These offer additional protection for better data security on standard computers in private households, right up to the entire IT infrastructure. We will discuss the IT infrastructure later.

II) Internet service provider (ISP) is an organization that provides services for accessing, using, or participating in the Internet [29]. This is shown in the following “Fig. 13”.

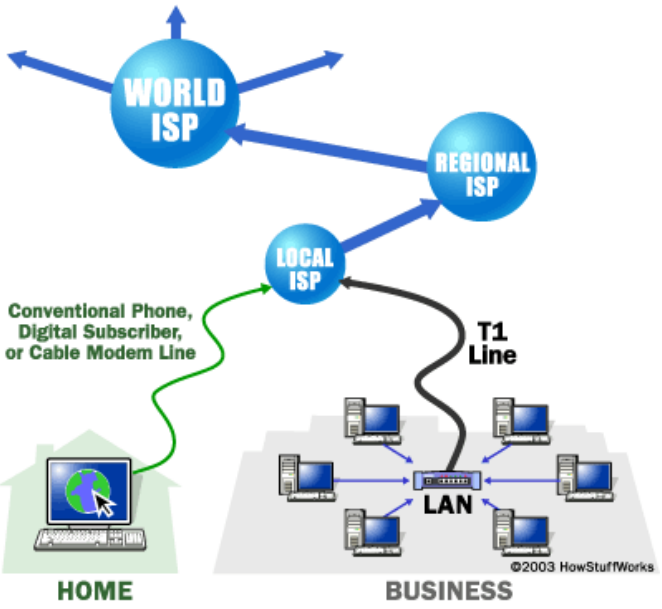

Fig. 13. Working system of a Internet service provider [30]

This means that the entire data flow runs over the networks provided by service providers. Internet service providers offer services by connecting private households, companies, and organizations to each other via their networks. They must also enable secure data traffic. Already today Internet Service Providers offer with their services not only access to the Internet, but also their own routers as OEM products with predefined standards for communication [31]. By getting predefined products delivered by router manufacturers and offering them under their own name the Internet Service Providers want to ensure that private households use WLAN application protected routers to get more data security when connecting to the internet.

The Facebook data scandal in which the English data analysis company Cambridge Analytica gained unauthorized access to data of more than 50 million Facebook users during the US election campaign to mobilize supporters of today's US President Donald Trump and at the same time deter potential voters of the opposing candidate Hillary Clinton from voting [32], has shown that data protection and data security play an enormous role in our society. Even election campaigns can be manipulated directly or indirectly. Such incidents must be counteracted.

According to an online survey of 1009 respondents aged 18 and over in Germany in 2018 on the user reaction to data protection allegations against Facebook in Germany the usage has changed quite a bit. When asked: “Have you logged out of Facebook or at least temporarily deactivated your account?” it resulted, that 50% continue to use Facebook quite normally, 31% do not use Facebook, 6% have already temporarily deactivated their Facebook account but are now using it again, 3% had temporarily deactivated their Facebook account, 4% have logged out of Facebook and 6% gave no information. This can be seen in the following “Fig. 14”.

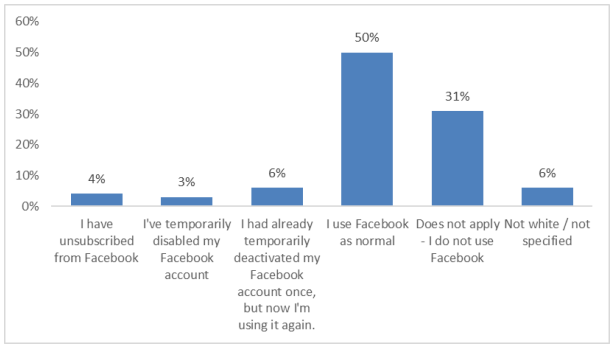

Fig. 14. Survey on user reaction to data protection allegations against Facebook in Germany 2018 [33]

As it can be seen, 4% have completely logged out of Facebook and another 9% have temporarily deactivated their Facebook account.

The reaction was not that big, but it can be stated that privacy and security are still important for Facebook users. More responsible actions on the part of the providers are demanded, e.g. by the BSI [34].

What about companies, what contribution do they make?

4) Companies need to take security precautions how they handle customer data.

On the one hand the state with the GDPR takes the enterprises into the duty to provide data security, however, how does this look like:

The 2018 survey of 503 industrial companies with ten or more employees on organizational IT security measures in Bitkom Research revealed the following: Which of the following organizational or process-related security measures are already in use in your company or are you planning to use in the future?

The definition of access rights for certain information takes place 100%. Clear classification/labeling of company secrets takes place in 84% of the answering companies, 80% define clear rules for the handling of sensitive information, 77% define access rights for certain rooms in the company, 66% define special regulations for taking IT and telecommunications equipment on business trips, 50% use the Clean Desk Policy (forcing employees to clean up their desks at the end of the day), 49% can be certified for security (like ISO 27001; BSI basic protection or similar), 35% carry out an information security management system (ISMS) and 34% carry out regular security audits. These are shown in the following “Fig. 15”.

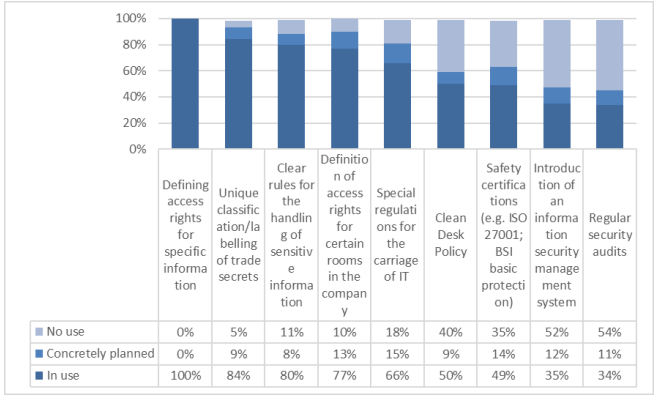

Fig. 15. Survey on organizational IT security measures in companies 2018 [35]

The approaches of the entrepreneurs are promising, but as you can see from the results of the survey, there is still some catching up to be done in the areas of regular security audits and information security management systems, among others; these are not used in over 50% of the companies, so there is a lot of potential for improvement.

It is also interesting to note that the statement on data security differ by educational attainment. The higher the level of educational attainment, the more the interviewees rate data security as "rather uncertain".

As early as 2011, 342 respondents with an intermediate secondary school certificate rated data security on the Internet as "rather insecure" by 41%, and of the 252 respondents with a university degree, as many as 51% rated it as "insecure" [36].

From the above aspects, it can be concluded that there is a will for data security, but this must also be ensured, but how? The answer can be given by IT security measures.

III. TECHNICAL AND OTHER REQUIREMENTS

IT security

Data security can only be implemented if IT security is also guaranteed. The following steps must be taken to ensure the security of any IT system. See the following “Fig. 16”.

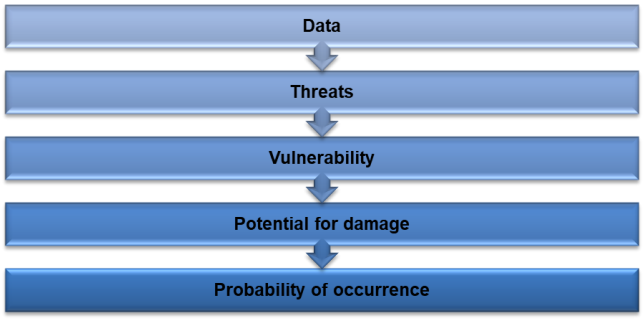

Fig. 16. Steps to Review IT Security [37]

The first step is to define the data to be protected and then identify the potential threats that could compromise that data.

Then the vulnerability of the own IT system is checked, and the expected damage is determined when the threat occurs.

The probability of these threats occurring must then be determined. In order to minimize the probability of occurrence, appropriate technical and organizational measures must be taken.

In 2017, around 3.7 billion euros were spent on IT security in Germany. According to the source, spending in 2019 will amount to around 4.4 billion euros. This shows that companies are already investing enormous sums in IT security and are continuing to expand them. This can be seen in the following “Fig. 17”.

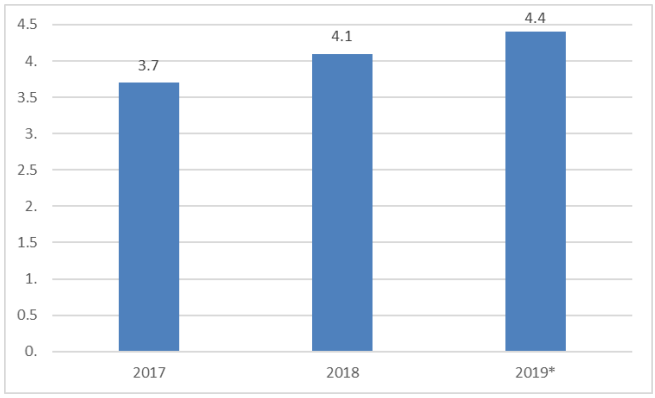

Fig. 17. Expenditure on IT security in Germany in 2017 and forecast to 2019 (in billions of euros) [38]

Already today, software companies that have focused on security software development offer solutions. Starting with simple antivirus programs up to complete solutions for corporations, like the applications for the "Data Center Infrastructure Management" (DCIM).

The DCIM is the convergence of IT and building functions within a company. DCIM's goal is to provide administrators with a holistic view of a data center's performance so that energy, equipment, and buildings can work together as efficiently as possible [39].

This helps to increase IT security in the data centers to protect the IT infrastructure from risks such as power failure, overheating, fire, debris loads, burglary or other causes. As a result, data centers are now monitored automatically. Due to the large number of components and operating parameters to be monitored, large amounts of data are generated that can be structured and evaluated by the DCIM software.

According to a forecast by the International Data Corporation (IDC) [40] about the volume of the annually generated digital data volume worldwide, the data volume in the year 2025 will increase to 175 Zettabyte. By comparison, in 2018 there were just 33 Zettabytes, an increase by a factor of 5.3. One Zettabyte is a unit of measurement for storage capacity and stands for 10^{21} bytes [41]. This can be seen in the following “Fig. 18”.

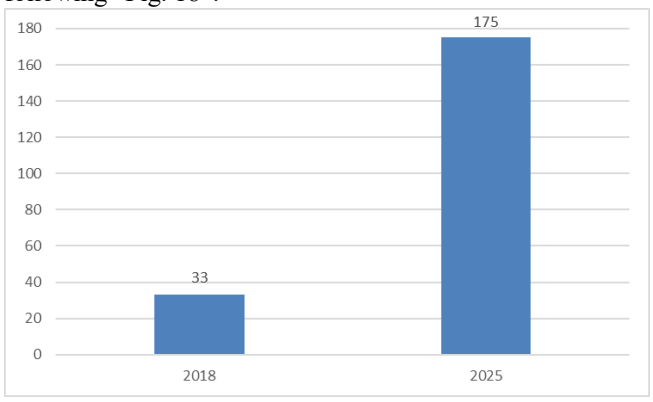

Fig. 18. Global data volume forecast for 2025 (in zettabyte) [42]

IT infrastructure

The term IT infrastructure is not clearly defined.

- For an operating system developer, only the computer is "his" IT infrastructure, which he can use but not influence.
- For an application developer, the operating system is part of the IT infrastructure.
- For a "normal" user, from "his" perspective, all applications belong to the IT infrastructure, possibly also his internet phone (VoIP).

One can conclude that the IT infrastructure is the totality of all buildings, networks, hardware, and software. See also figure 13.

The IT infrastructure as a whole offers a lot of potential vulnerability. If this is protected, threats can be detected much earlier, fended off and the consequences of an attack mitigated. See figure 16: “Steps to Review IT Security” and the explanation of “DCIM”.

Threats of the Internet

There is a risk of losing your data or infecting a computer with malware. In 1992 the first computer virus "Michelangelo" caused a media hysteria. And even today, most Internet users, 61% of respondents, consider malware infestation to be the most important threat that could arise from using the Internet. According to the BITKOM survey, 54% of all Internet users in Germany gained experience with criminal incidents within the last 14 years, almost 40% of them were infected with malware [43].

The police recorded cases of cybercrime in Germany from 2014 to 2017 show that this has increased by a factor of 3.2 from 26,986 police recorded cases in 2004 to 85,960 in 2018.

This can be seen in the following “Fig. 19”.

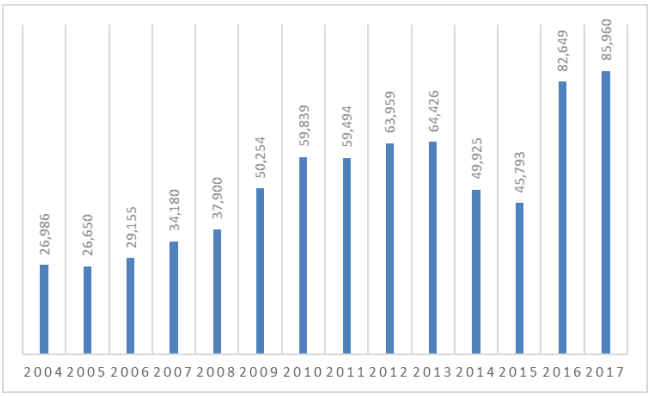

Fig. 19. Police recorded cases of cybercrime in Germany until 2017 [44]

The use of the Internet can be dangerous. The threats can be shown by the statistics of a survey on the concrete incidents of cybercrime in selected countries worldwide in 2017, in which 254 companies in the USA, Germany, Japan, Great Britain, France, Italy, and Australia were examined. In 2017, too, malware is the leader in cybercrime with 98%, followed by phishing & social engineering with 69%, web-based attacks with 67%, botnets with 63%, malicious codes with 58%, denial of service attacks with 53%, stolen devices with 43%, malicious insiders with 40% and ransomware with 27% occurrence. This is shown graphically in the following “Fig. 20”.

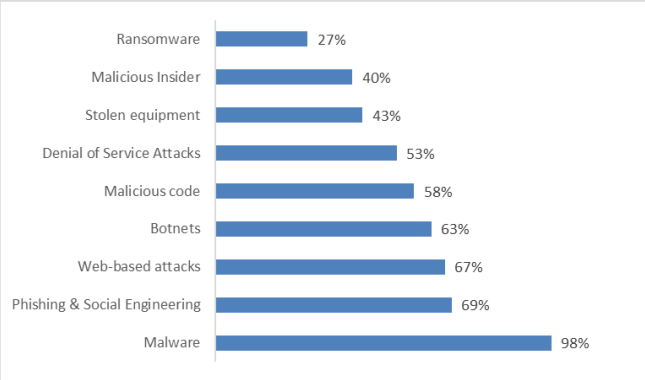

Fig. 20. Survey on cybercrime incidents in enterprises worldwide 2017 [45]

Malware: Software (such as viruses, worms, etc.) that can penetrate computer systems and cause interference or damage [46].

Phishing: Obtaining other people's data (such as password, credit card number, etc.) with fake e-mails or websites [47].

Social Engineering: Influencing people (in computer networks) to induce them to behave in a particular way, often with unfair intent [48].

Web-based attacks: Are attacks on web pages and web servers [49].

Botnets: A larger number of computers that have been infected with malware and networked without the knowledge of their operators [50].

Malicious code: Malicious code is the kind of harmful computer code or web script designed to create system vulnerabilities leading to back doors, security breaches, information and data theft, and other potential damages to files and computing systems [51].

Denial of Service Attacks: A Denial of Service (DoS) attack impairs the functionality of services and restricts the availability of services to users and businesses [52].

Stolen equipment: Internal company equipment is stolen.

Malicious Insider: Employees of a company steal or delete data from the company for financial or personal reasons [53].

Ransomware: Form of malware that kidnaps data. The attacker encrypts the data of the victims and demands a ransom for the private key [54].

Other hazards include the illegal use of personal data, fraud in online banking or online shopping, and harassment or bullying on the Internet.

IT transparency

IT transparency is becoming increasingly important. Due to the diversity of IT, it is becoming increasingly important not what IT can deliver as data, but what is important for the user and must be used to keep an overview of business processes and make them more dynamic. Above all, today's IT must increase data transparency and data quality. Besides, IT must improve communication between those involved and offer the possibility of joint data evaluation.

Software-Upgrades

Each software program must meet its specifications and fulfill the functions expected by the client. Therefore, each program must survive verification and validation during and after the implementation. During the verification phase, it is checked whether the program meets the specified requirements and during the validation phase, it is checked whether the system meets the wishes and needs of the customers and if it can be adapted to them [55].

Due to the changes in the part of the IT and thus also the change of ideas and wishes of the customers, the software must also be constantly adapted to the changed requirements of the users. The installation of an improved Enterprise-Resource-Planning (ERP) version (release change or upgrade) is very complex due to the effort involved [56].

The scope of the functionalities of an ERP system is so large that the software must be adapted to a company through customizing. Comprehensive definitions or even programming of additional modules is necessary for the system. A lot of time must also be planned for data migration.

Besides, depending on changes in the scope of functions, users may have to be offered further training.

IV. RESULTS

Protective measures

The survey in Germany on protective measures against cybercrime in 2018 of 1025 respondents aged 18 and over, regarding which of the protective measures they take (against cybercrime and cyberthreats) has revealed that 68% use a current antivirus program and firewall, 56% hide password/ pin when entering, 46% install immediately available updates, 44% use secure passwords according to BSI recommendation, 32% make a backup copy, 24% encrypt e-mail communication, 21% encrypt data (e.g. photos), 19% do not use social networks, 17% do not use online banking, 5% do not buy on the Internet and 5% do not use any of it. This can be seen in the following “Fig. 21”.

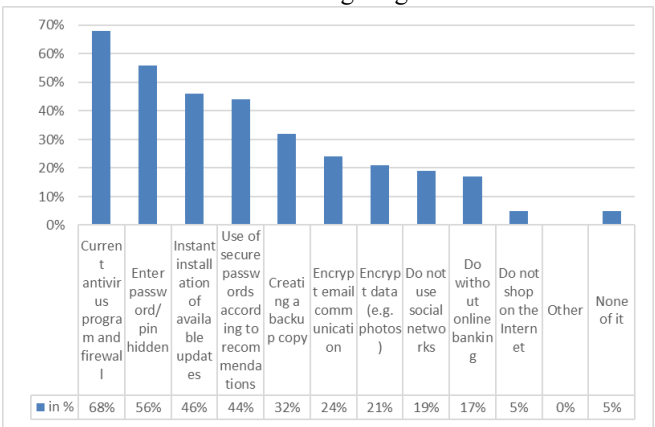

Fig. 21. Survey in Germany on protective measures against cybercrime 2018 [57]

Mobile devices must be particularly well protected against unauthorized access to the data stored on them, as they are much easier to get into the hands of strangers than stationary computers. A variety of access controls have already been developed to protect against unauthorized use, such as the entry of a password, access via a chip card or the use of biometric features [58].

When entering passwords, one should pay attention to an encrypted internet connection, this can be read in the address bar, if a hyperlink begins with https://.

To minimize the security risk, you should make sure that the antivirus software and the version of the Internet browser are always up-to-date and that the firewall is switched on.
„An optimal protection of the enterprise can be realized only over a holistic solution. In particular, the consideration of individual security requirements is of decisive importance for effective protection "[59].

V. CONCLUSION

The trend towards digitalization already arrived in the German real estate market. IT brings help, and the requirements are defined.

There are already today high standards of the state, for example defined by the GDPR or BSI in Germany. Enterprises work on the realization of the best possible security concepts and even private households are making efforts to take appropriate precautions to prevent the exploitation of their data and to advance digitalization accordingly. IT brings help but is still only an instrument that is operated by people, and people also make mistakes. Neither the state, nor the enterprises, nor private households can counteract these errors individually completely, people are active in all areas and can permit errors accordingly. Only joint action can bring more security.

REFERENCES

1. R. Dobler, and D. Ittstein, "Digitalisierung. Interdisziplinär," p. 2, 2018
2. G. Vornholz, "Digitalisierung der Immobilienwirtschaft," page25, 2019
3. Statista GmbH, (2019. September 20). Umfrage zum zukünftigen Einfluss von Megatrends auf den Immobilienmarkt in Deutschland [Online] Available: https://de.statista.com/statistik/daten/studie/797769/umfrage/umfrage-zum-zukuenftigen-einfluss-von-megatrends-auf-den-deutschen-immobilienmarkt/
4. General Data Protection Regulation GDPR, (2019. September 20). [Online] Available: https://gdpr-info.eu/
5. W. Lassmann, "Wirtschaftsinformatik, Nachschlagewerk für Studium und Praxis" vol. 1, p 400, 2006
6. Statista GmbH, (2019. September 20). DSGVO Konformität von Unternehmen in Deutschland [Online] Available https://de.statista.com/infografik/13651/dsgvo-konformitaet-von-unternehmen-in-deutschland/
7. General Data Protection Regulation GDPR, (2019. September 20). [Online] Available: https://gdpr-info.eu/
8. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom), (2019. September 02). DSGVO Aufwand im laufenden Betrieb [Online] Available: https://www.bitkom.org/Presse/Presseinformation/Kaum-Fortschritt-bei-der-Umsetzung-der-Datenschutz-Grundverordnung.html#item-385
9. Statista GmbH, (2019. September 20). Meinungen zum Thema Datenschutz im Internet nach Geschlecht in Deutschland 2018 [Online] Available https://de.statista.com/statistik/daten/studie/911174/umfrage/meinungen-zum-thema-datenschutz-im-internet-nach-geschlecht-in-deutschland/
10. Statista GmbH, (2019. September 20). Umfrage zur Zuständigkeit für den Schutz von persönlichen Daten im Internet [Online] Available https://de.statista.com/infografik/16771/umfrage-zur-verantwortung-beim-thema-datenschutz/
11. Statista GmbH, (2019. September 20). Umfrage zum Schutz persönlicher Daten von Jugendlichen im Netz in Deutschland 2018 [Online] Available https://de.statista.com/statistik/daten/studie/505798/umfrage/schutz-persoenlicher-daten-von-jugendlichen-im-netz/
12. Statista GmbH, (2019. September 20). Umfrage zum Datenschutzverhalten von Jugendlichen in Deutschland 2018 [Online] Available https://de.statista.com/statistik/daten/studie/867410/umfrage/umfrage-zum-datenschutzverhalten-von-jugendlichen-in-deutschland/
13. A. Sodtalbers, C. Commerce, and A. Heise, "IT-Recht – Software-Recht, E-Commerce-Recht, Datenschutz-Recht" p. 271, 2010
14. A. Sodtalbers, C. Commerce, and A. Heise, "IT-Recht – Software-Recht, E-Commerce-Recht, Datenschutz-Recht" p. 271, 2010
15. Bundesamt für Sicherheit in der Informationstechnik, "Leitfaden Informationssicherheit – IT-Grundschutz kompakt," p. 11. 2011 [Online] Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Leitfaden/GS-Leitfaden_pdf.pdf?__blob=publicationFile&v=3
16. Statista GmbH, (2019. September 20). Einschätzung der Sicherheit von Daten im Internet in Deutschland bis 2018 [Online] Available https://de.statista.com/statistik/daten/studie/217842/umfrage/sicherheit-von-persoenlichen-daten-im-internet/
17. Statista GmbH, (2019. September 20). Einschätzung der Sicherheit von persönlichen Daten im Internet in Deutschland 2019 [Online] Available https://de.statista.com/statistik/daten/studie/872116/umfrage/einschaetzung-der-sicherheit-von-persoenlichen-daten-im-internet-in-deutschland/
18. Bürgerliches Gesetzbuch Civil Law Book (2019. September 20), "Definition Verbraucher,"Vol 83 § 13 Verbraucher, 2019 [Online] Available https://www.gesetze-im-internet.de/bgb/BJNR001950896.html
19. Startpage BV, (2019. September 20). The world's most private search engine [Online] Available https://www.startpage.com/
20. Statista GmbH, (2019. September 20). Einsatz von Maßnahmen zum Schutz vor Datenmissbrauch im Internet 2017 [Online] Available https://de.statista.com/statistik/daten/studie/28771/umfrage/haltung-zu-sicherheitsrisiken-im-internet/
21. Produkthaftungsgesetz Product liability law (2019. September 20), "Definition Herrsteller, ProdHaftG § 4 Herrsteller, p. 2 [Online] Available www.gesetze-im-internet.de/prodhaftg/ProdHaftG.pdf
22. Produkthaftungsgesetz Product liability law (2019. September 20), "Definition Produkt, ProdHaftG § 2 Produkt, p. 1 [Online] Available www.gesetze-im-internet.de/prodhaftg/ProdHaftG.pdf
23. A. Yunlong Z. Zedtwitz, and D. Assimakopoulos, "Responsible Product Innovation: Putting Safety First" p. 289, 2017
24. R. Stair, and G. Reynolds, "Principles of Information Systems", p. 283, 2015
25. Quality management systems - Requirements (ISO 9001:2015), (2019. September 20) [Online] Available https://www.din.de/de/wdc-beuth:din21:235671251
26. Bundesamt für Sicherheit in der Informationstechnik, (2019. September 20), „"ISO 27001 Zertifizierung auf Basis von IT-Grundschutz" [Online] Available https://www.bsi.bund.de/DE/Themen/ZertifizierungundAnerkennung/Managementsystemzertifizierung/Zertifizierung27001/GS_Zertifizierung_node.html
27. E. Lauterschlag, (2019. September 20), "WLAN Verschlüsselung: Welche Methoden gibt es und welche ist am sichersten?" [Online] Available http://www.was-ist-malware.de/it-sicherheit/wlan-verschluesselung/
28. L. Nielsen, "ERP-Software in kleinen und mittelständischen Unternehmen: Ein optimiertes Vorgehensmodell," p. 11, 2014
29. Disha Experts "Olympiad Champs Cyber Class 7 with Past Olympiad Questions," p. 138, 2018
30. HowStuffWorks, (2019. September 20), "How Web Servers Work" [Online] Available https://computer.howstuffworks.com/web-server3.htm
31. Weka Medie publishing, (2019. September 20), "SpeedPort-Router zur Fritzbox machen" [Online] Available https://www.pc-magazin.de/ratgeber/speedport-fritzbox-hack-firmware-modding-download-anleitung-tutorial-2309816.html
32. Heise Medien GmbH & Co. KG, (2019. September 20), "Facebook-Datenskandal" [Online] Available https://www.heise.de/thema/Facebook_Datenskandal
33. Statista GmbH, (2019. September 20). Umfrage zur Nutzerreaktion auf Datenschutzvorwürfe gegen Facebook in Deutschland 2018 [Online] Available https://de.statista.com/statistik/daten/studie/821263/umfrage/nutzerreaktion-auf-datenschutzvorwuerfe-gegen-facebook-in-deutschland/
34. Bundesamt für Sicherheit in der Informationstechnik, (2019. September 20), " Datendiebstahl - BSI fordert verantwortungsvolles Handeln der Betreiber" [Online] Available https://www.bsi.bund.de/DE/Presse/Kurzmeldungen/Meldungen/news

_yahoo_BSI_fordert_verantwortungsvolles_Handeln_23092016.html

35. Statista GmbH, (2019. September 20). Umfrage zu organisatorischen IT-Sicherheitsmaßnahmen in Unternehmen 2018 [Online] Available https://de.statista.com/statistik/daten/studie/444794/umfrage/umfrage-zu-technischen-it-sicherheitsmassnahmen-in-unternehmen/
36. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom), (2019. September 20). "Datenschutz im Internet – Eine repräsentative Untersuchung zum Thema Daten im Internet aus Nutzersicht," p. 23, 2011 [Online] Available https://www.bitkom.org/sites/default/files/file/import/BITKOM-Publikation-Datenschutz-im-Internet.pdf
37. Compendio-Autorenteam, "Informatik für technische Kaufleute und HWD, Grundlagen mit Beispielen, Repetitionsfragen und Antworten sowie Übungen," vol. 1, p. 167, 2009
38. Statista GmbH, (2019. September 20). Ausgaben für IT-Sicherheit in Deutschland bis 2019 [Online] Available https://de.statista.com/statistik/daten/studie/1041736/umfrage/ausgaben-fuer-it-security-in-deutschland/
39. TechTarget Germany GmbH, (2019. September 20). "Data Center Infrastructure Management (DCIM)," [Online] Available https://www.computerweekly.com/de/definition/Data-Center-Infrastructure-Management-DCIM
40. Research International Data Corporation, Inc. [Online] Available https://www.idc.com/about
41. TechTarget Germany GmbH, (2019. September 20). "Definition Zettabyte," [Online] Available https://www.computerweekly.com/de/definition/Zettabyte
42. Statista GmbH, (2019. September 20). Prognose zum weltweit generierten Datenvolumen 2025 [Online] Available https://de.statista.com/statistik/daten/studie/267974/umfrage/prognose-zum-weltweit-generierten-datenvolumen/
43. Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom), (2019. September 20)."Datenschutz im Internet – Eine repräsentative Untersuchung zum Thema Daten im Internet aus Nutzersicht," p. 21, 2011 [Online] Available https://www.bitkom.org/sites/default/files/file/import/BITKOM-Publikation-Datenschutz-im-Internet.pdf
44. Statista GmbH, (2019. September 20). Polizeilich erfasste Fälle von Cyberkriminalität in Deutschland bis 2017 [Online] Available https://de.statista.com/statistik/daten/studie/295265/umfrage/polizeilich-erfasste-faelle-von-cyberkriminalitaet-im-engeren-sinne-in-deutschland/
45. Statista GmbH, (2019. September 20). Umfrage zu den Vorfällen von Cybercrime in Unternehmen weltweit 2017 [Online] Available https://de.statista.com/statistik/daten/studie/499324/umfrage/vorfaelle-von-cybercrime-in-unternehmen-weltweit/
46. Bibliographisches Institut GmbH, „Duden - Deutsches Universalwörterbuch: Das umfassende Bedeutungswörterbuch der deutschen Gegenwartssprache," vol. 8, p. 1159, 2016
47. Bibliographisches Institut GmbH, „Duden - Deutsches Universalwörterbuch: Das umfassende Bedeutungswörterbuch der deutschen Gegenwartssprache," vol. 8, p. 1346, 2016
48. Bibliographisches Institut GmbH, „Duden - Deutsches Universalwörterbuch: Das umfassende Bedeutungswörterbuch der deutschen Gegenwartssprache," [Online] Available https://www.duden.de/rechtschreibung/Social_Engineering
49. ITservice Sustemhaus, (2019. September 20). "Webbasierte Angriffe steigt weiter an" [Online] Available http://www.pc-doktor-blog.de/webbasierte-angriffe-steiger-weiter-an-mehr-als-4-500-angriffe-pro-tag/
50. Bibliographisches Institut GmbH, „Duden - Deutsches Universalwörterbuch: Das umfassende Bedeutungswörterbuch der deutschen Gegenwartssprache," [Online] Available https://www.duden.de/rechtschreibung/Botnet
51. Kaspersky Labs GmbH, (2019. September 20). "What is Malicious Code?" [Online] Availablehttps://www.kaspersky.com/resource-center/definitions/malicious-code
52. TechTarget Germany GmbH, (2019. September 20). "Definition Denial of Service (DoS)," [Online] Available https://www.computerweekly.com/de/definition/Denial-of-Service-DoS
53. PINNOW & Partner Unternehmens- und Technologieberatungsgesellschaft mbH., (2019. September 20). " Unterschätztes Risiko Insider-Angriff," [Online] Available https://www.datensicherheit.de/aktuelles/unterschaetztes-risiko-insider-angriff-27834
54. TechTarget Germany GmbH, (2019. September 20). "Definition Ransomware," [Online] Available https://www.computerweekly.com/de/definition/Ransomware
55. I. Sommerville, "Software Engineering", vol. 8, p. 556, 2007
56. M. Hesseler, and M. Görtz, Marcus, "Basiswissen ERP-Systeme – Auswahl, Einführung & Einsatz betriebswirtschaftlicher Standardsoftware", vol. 1, p. 362, 2007
57. Statista GmbH, (2019. September 20). Umfrage in Deutschland zu Schutzmaßnahmen gegen Internetkriminalität 2018 [Online] Available https://de.statista.com/prognosen/952937/umfrage-in-deutschland-zu-schutzmassnahmen-gegen-internetkriminalitaet
58. M. Wind, and D. Kröger, "Handbuch – IT in der Verwaltung" p. 276,2006
59. Research International Data Corporation, Inc., (2019. September 20). "Mehr Mobilität erfordert bessere Lösungen für mehr Sicherheit beim Einsatz mobiler Endgeräte" [Online] Available https://www.it-times.de/news/idc-mehr-mobilitat-erfordert-bessere-losungen-fur-mehr-sicherheit-beim-einsatz-mobiler-endgerate-12763/

AUTHORS PROFILE

Georg Rockel is a Ph.D. Scholar in the Department of Economics and Management, Mendel University Brno, Czech Republic.

Linard Barth is a Ph.D. Scholar in the Department of Economics and Management, Mendel University Brno, Czech Republic.