

IT Security

Technology Report

Vienna, May 2020

Dear readers,

Vienna is among the top five ICT metropolises in Europe. Some 6,200 ICT enterprises generate sales of around 20 billion euros annually. The approximately 8,900 national and international ICT companies in the "Vienna Region" (Vienna, Lower Austria and Burgenland) are responsible for roughly two thirds of the total turnover of the ICT sector in Austria.

According to various studies, Vienna achieves especially high marks for innovative power, comprehensive support for start-ups, and its strong focus on sustainability. Vienna also occupies top positions in multiple "Smart City" rankings. Enhancing the location's appeal still further are its researchand technology-friendly climate, its geographical and cultural vicinity to the growth markets in the East, the high quality of its infrastructure and education system, and last but not least, the best quality of life worldwide.

With its "Vienna 2030" strategy, the Federal Capital is focusing on those topics in which the city is already particularly successful, and thus wants to provide answers to the major challenges of the coming years - from climate change to digitalization. In these areas, Vienna wants to be among the world leaders in the next ten years and develop particularly powerful innovations ("Wiener Lösungen"). One of Vienna's top issues is "Wiener Digitalisierung". Here, cyber security is a major focus, and the establishment of a Cyber Security Hub is being implemented as one of the lead projects.

In order to make optimal use of this location's potential, the Vienna Business Agency functions as an information and cooperation platform for Viennese technology developers. It networks enterprises with development partners and leading economic, scientific and municipal administrative customers, and supports Viennese enterprises with targeted monetary funding and a variety of consulting and service offerings.

This technology report provides an overview of the various trends and developments in the field of cyber security, as well as current data and facts about Vienna as a location.

Your Vienna Business Agency team



EFRE



Contents

- ^{5.6}
 1. IT Security –
 From Optional to Compulsory
- ^{s.7} 2. Cyber Treats are Ubiquitous
- ^{S.8} 3. International Development: Massive Costs through Cyberattacks
- ^{s.10} 4. Situation in Austria

S.10	4.1	Current Data
S.11	4.2	No "Plan B"
S.12	4.3	Commitment Increased

S.14	5. Market Overview Vienna
S.14	5.1 Number and Structure
S.15	5.2 Customers
S. 16	6. Education, Research and Networks
S.16	6.1 Vienna Cyber Security and Privacy Research Center (VISP)
S.17	6.2 Online Advice
S.17	6.3 CryptoParties and Events
S.18	7. Trends
S.19	8. Services of the Vienna Business Agency
S.21	9. Companies in Vienna
S.31	10. Imprint

IT Security – From Optional to Compulsory

Cyber Threats are Ubiguitous



Nowadays, information and communication technologies affect all areas of life as well as all important economic sectors. The number of Internet users and smartphones, as well as the general variety of digital offerings keeps increasing. The linking of billions of devices ("Internet of Things") has multiplied the benefits of digital technologies; however, it has also increased the opportunities for assaults and misuse.

Apart from typical malware, attacks on companies and industrial espionage are booming. Due to the increased use of mobile phones and tablets - especially of own personal devices ("Bring Your Own Device") - companies are confronted with new risks regarding IT security. Whether it relates to "Industry 4.0", Cloud Computing or classic office solutions: Stable networks, a reliable infrastructure and traditional IT security are no longer optional but compulsory.

For some time now, focus has shifted from protecting individual PCs to the entire IT infrastructure system. It is essential to address this topic long before an attack has been initiated. Information technology must be considered and integrated in the planning stages for all areas. Consequently, IT security has acquired an increasingly strong overall strategic dimension, also as a location factor for the entire Viennese economy.

Almost half of the world's population (2016: 44%) is connected to the Internet in some way. In Europe, more than 510 million people - over 90% - use the Internet. This connectivity offers many opportunities but at the same time harbours many dangers. According to the WEF Global Risk Report¹ published in 2017, the probability of falling victim to a cyberattack or data theft ranks among the five highest risks worldwide. Each year the number of threats increases and the accompanying landscape undergoes swift and manifold changes. While previously DDoS (distributed denial-of-service) attacks were most common, APTs (advance persistent threats) and ransomware are now on the rise. According to the Austrian Criminal Police Office, between the years 2016 and 2017, the latter saw the strongest increase - by a full 186%. This rapid upswing is reflected through numerous incidents, one of the most interesting being an attack on the South Korean web hosting provider Nayana: The company paid a record sum of 1,3 billion won (1,14 million US dollars) in order to regain access to their encrypted data.²

Increased connectivity of different devices with the Internet (Internet of Things, or IoT for short) has significantly aggravated the threat of cyberattacks. Today, the average European household possesses 14 IoT-devices. Most are vulnerable and use very weak - sometimes even unchangeable - passwords, enabling attackers to gain easy access to, and control of, those devices. Furthermore, interconnection means that attackers can also access other devices and the data contained therein. Many individuals and companies are unaware that by having a smart-TV in their office, for instance, sensitive data from other computers could be stolen. Consequently, inadequate - or non-existent - prevention measures are taken against this lurking danger.

The use of new technology will impose additional security requirements on companies. Artificial intelligence is one

example which presents a severe threat potential. An international research group led by the Max-Planck-Institute for Informatics in Saarbrucken presented a procedure called "Deep Video Portraits"³ in this context that allows people to create fake videos ("deep fakes"). This technology could be used in various problematic ways including for damaging the reputation of political opponents or other important members of society.

Cloud services represent an additional new threat factor in this regard. More and more companies make use of cloud service providers (CSPs) and store elements of their databases, analyses and other information technology functions on external servers. As a result, any impairment or loss of those cloud-based solutions can disrupt or even interrupt all business operations. One example of a recent cloud server fault took place in July of 2018 when several popular applications of Google and other companies including Snapchat, Spotify and Discord became temporarily inoperative. Another example is the fault, in September 2018, of large parts of a Texan cloud server-centre running Microsoft Azure which affected customers worldwide.4

Therefore, the task of protecting sensitive information and IT equipment has become much more comprehensive. Also, the legal requirements of the European GDPR (General Data Protection Regulation) or the NIS-Directive (Directive on Security of Network and Information Systems) have created additional work for companies.

www.weforum.org/reports/the-global-risks-report-2018

2

1

www.bundeskanzleramt.gv.at/dam/jcr:aa859448-de81-44b2-af72-9a99376296d7/ Cybersicherheit_Bericht2018.pdf

3

gvv.mpi-inf.mpg.de/projects/DeepVideoPortraits/

www.heise.de/newsticker/meldung/Blitzschlag-in-den-USA-stoert-Azure-Active-Directory-4155496.html

International Development: Massive Costs through Cyberattacks

8

August and 5th of September. This affected approximately 380,000 debit or credit cards.⁸

The expenses for cyber security increase not just because of the rising risks but also due to new business desires (e.g. data protection) and changes in the industry (e.g. loT). Gartner estimates the worldwide growth of expenses in 2019 at 8.7% (124 billion US dollars) compared to just 3.2% for IT in general.⁹

The importance of the IT security sector worldwide is reflected in the current figures: Cyberattacks against companies have doubled in the last five years. Correspondingly, the market for fighting cybercrime has massively increased: In April 2018, experts estimated its worth at 1,5 trillion US dollars (Bromium 04/2018). The costs incurred by cybercrime, on the other side, amount to 6 trillion US dollars (Forbes 07/2017).

Moreover, Symantec found that one out of every 13 online requests leads to malware. Lately, malware targeting operating systems such as Microsoft Windows has been increasingly detected. The rate of email spam is also constantly growing and currently constitutes some 55% of mails received. The number of attacks on IoT-devices saw a sharp – and incredible – 600% increase between the years 2016 and 2017. Additionally, there was a 13% increase in the number of reported vulnerabilities such as EternalBlue or Meltdown, and for industrial controls an increase of some 29%⁵.

IBM has published a global study on the costs of data leaks: $\frac{6}{2}$



The data presented in the study corresponds with another international study conducted by EY, which estimates the extent of damage caused by data leaks at approximately 3.2 million euros.⁷ There are many examples of data leaks: In 2013, three billion Yahoo-accounts were hacked, resulting in stolen mailing addresses and phone numbers. In 2016, Uber fell victim to a hacking attack in which sensitive data such as addresses or given names were also stolen. A more recent incident concerns British Airways: In 2018, there was a hacking attack on the airline that stole the personal data as well as the bank account information of customers who booked flights via the company's website or app between the 21st of

www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

6

5

www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=55017055USEN&

7 www.ey.com/Publication/wwLUAssets/EY_Global_Information_Security_Survey_ 2018_-_Oktober/\$FILE/EY%20Global%20Information%20Security%20Survey 2018.pdf 8

www.forbes.com/sites/bishopjordan/2018/09/09/british-airways-hacked/ #555cc04967ae

9

Gartner, "2019 Worldwide Security Spending Projection."



According to the study, the costs of incidents with less than 10,000 data sets amount to <u>2.1 million US dollars</u> whereas the incidents with more than 50,000 data sets are <u>5.7 million US dollars</u>.

197 DAYS

are needed on average to detect a data leak.

The following factors help increase or reduce the costs of a data leak:

COST PUSHERS (TOP 5)

- Participation of third parties (Outsourcing)
- Comprehensive cloud migration
- Compliances errors
- Comprehensive use of mobile platforms
- Lost or stolen devices

MORE THAN 1 MILLION US DOLLARS

could be saved by companies that fix their data leak in less than 30 days.

COST SAVINGS (TOP 5)

- Incident response team for security emergencies
- Extensive use of encryption
- Integration into the business continuity management
- Trainings for staff
- Sharing information on threats

Situation in Austria

4.1 Current Data

According to a study by KPMG¹¹, two out of every three Austrian companies will become victims of cybercrime. Especially medium-size and large companies are being targeted. Attacks focus in particular on human-associated weak points. Phishing, malware/ransomware and social engineering rank among the most common attack-types.

Recently, strong increases have been seen in the use of ransomware and advanced persistent threats (APT), whereas distributed denial-of-service (DDoS) attacks appear to have peaked and are now in decline:



There has been a general increase in cybercrime cases whereas conventional criminal offenses are decreasing. The ongoing trend of influencing public opinion, as seen for example during elections via social media platforms, is evident in Austria too.¹²

Austrian companies operating in the area of critical infrastructure as well as the cyber security sector react to continually growing threats by allocating more money for cyber security measures and the ongoing implementation of novel security actions. Another trend is increased staffing in information and data security-related functions.

An assessment of 2018 cyber security trends are shown in the BKA report "Cyber Sicherheit 2018":

- Attacks will be more complex and frequent. The main motivation of attacks lies in monetarization.
- Cloud security will be an essential topic. An increase in the dependence of companies on cloud providers is to be expected.
- The European Union's NIS-Directive (Directive on Security of Network and Information Systems) and GDPR (the General Data Protection Regulation) will place considerable demands on companies.
- The importance of organizational measures (such as risk management) will increase in contrast to mere technical measures in the future.

Different Methods of Cyberattacks

RANSOMWARE	Ransomware is contain. Perpet unlocking their and enrich ther
ADVANCED PERSISTENT THREATS (APT)	An ATP is a del a very target-ou the victim's cou in order to spy,
DISTRIBUTED DENIAL-OF-SERVICE (DDOS)	With a DDoS-a a website or ar server. In some

4.2 No "Plan B"

Therefore, our economic system will face great challenges. "We are hardly prepared for potential strategic shocking incidents. We lack a plan B in many sections in order to handle bigger disruptions or total breakdowns. The first step starts with the knowledge of threats," states Herbert Saurugg of Cyber Security Austria (CSA).

Due to the interconnection of entire ecosystems, the dependence on energy and information increases. "Thus, simple mistakes can have tremendous consequences and cause accidents. Even our energy and water supply, communication as well as the entire infrastructure could be threatened," warns Herbert Dirnberger of CSA.

In the last few years, there have been an increasing number of attacks on industrial systems and "Triton" – a highly sophisticated piece of malware – shows us that such attacks could also affect safety systems. "Future attackers will not be satisfied with finding weak points in existing systems but will actively work on integrating weak points in engineering processes," explains Edgar Weippl, research director of SBA Research and head of the CD-lab SQI.

Sebastian Bachmann of Ikarus Security Software focuses on a particularly critical section: "In the last few years, there has been an increasing amount of online-banking fraud cases which show the – in this form – unprecedent potential of the malware business. Often, administrators and security experts themselves do not know how to deal with such new threats adequately."

According to a report from the Austrian Criminal Police Office, the number of cybercrime incidents in 2017 saw an increase of more than 52.6% over the previous year. Some examples of recent incidents involving Austrian institutions are $\frac{10}{2}$:

- <u>WannaCry (05/2017)</u>: Ransomware, which encrypted the content of the targeted system's hard drive. Following the payment of a ransom, the hard disk was decrypted. Several countries, including Austria, were affected.
- <u>NotPetya (07/2017)</u>: Another ransomware attack targeting countries that maintain business relations with the Ukraine. The goal was a deliberate sabotage of the Ukrainian infrastructure.
- <u>Nationalist hacker groups (since 08/2016)</u>: Several facilities of Austria's critical infrastructure fell victim to DDoS-attacks by foreign nationalist hacker groups. The attacks affected the National Bank of Austria as well as the websites of the Austrian Parliament and various ministries.

https://home.kpmg/at/de/home/insights/2018/05/cyber-security-studieoesterreich-2018.html

10 www.bundeskanzleramt.gv.at/dam/jcr:aa859448-de81-44b2-af72-9a99376296d7/ Cybersicherheit_Bericht2018.pdf 12

www.bundeskanzleramt.gv.at/dam/jcr:aa859448-de81-44b2-af72-9a99376296d7/ Cybersicherheit_Bericht2018.pdf

11

is a type of malware that locks computers or encrypts the data they etrators blackmail their victims by demanding a ransom in exchange for r screens or decrypting their data. They play with the fears of the people emselves at their expense.

liberate attack on one or several victims. The perpetrator proceeds in riented manner. Meticulous attempts are made to gain access to both mputer and local network. The attacker wants to stay undiscovered , and to gather as much data – and do as much damage – as possible.

attack, it is possible to attack several computers at once (as a Botnet), in entire network infrastructure. This can quickly lead to a fault of the ie cases, the attack serves as a distraction for a bigger data theft.

g inndle arts g of the simuse icaed," sing ighacks t be but

4.3 Commitment Increased

How important new threats have become is demonstrated by the many initiatives of different political, scientific and civic organizations:

With the "Österreichische Strategie für Cyber Sicherheit"¹³, the Austrian government adopted a complex concept for the protection of cyber rooms and the people in virtual rooms. The report "Cyber Sicherheit 2018"¹⁴ summarizes the current threats as well as national and international developments. According to the report, there has been a significant increase in cyber espionage and cybercrime activities.

Cyber Security Austria (CSA), a non-profit association, has the aim of raising awareness for cyber security in Austria. In doing so, it wants to address different stakeholders from the areas of politics, economy, and science but at the same time also society itself. The activities and outputs of Cyber Security Austria include various publications, presentations and project collaborations in which existing knowledge on cyber security is linked and passed on to others.

On E-Day, one of the best-known events of the Austrian Chamber of Commerce, as well as at the TELEFIT road show for SMEs, the topic of cyber security is a regular fixture in the agenda.

The Computer Emergency Response Team Austria (CERT.at) serves as a contact for cyber security in the national environment. It connects other CERTs and CSIRTs (Computer Security Incident Response Teams) from the areas of critical infrastructure and information and communication technology (ICT) and issues warnings and tips for SMEs. The CERT of the City of Vienna (Wien CERT) is operated by the city's Municipal Department 01–Wien Digital.

13

www.bmi.gv.at/504/files/130416_strategie_cybersicherheit_WEB.pdf

14

https://www.bundeskanzleramt.gv.at/themen/cyber-sicherheit-egovernment.html



shares of the federal government to 1 share of the federal states. The Vienna Business Agency provides funding for Vienna. Currently, the Business Agency supports 15 COMET centres and projects.

Cyan Network Security specializes in Proxy technology and web-filter solutions. With some 100 employees, Bacher Systems is one of the largest service providers and offers a comprehensive product range for IT security. This includes solutions in the areas of Privileged Access Security, Data Security, Mobile Security, and Cloud Security and Network Security, as well as risk management for SIEM (Security Information and Event Management) systems.

Developments in Vienna follow the international trend of specialization in the IT security sector. In addition to the traditional IT security for company networks, there is now increasing supply and demand for security in the mobile sector and in industrial areas, as well as in the "Internet of Things". No clear boundary between consulting companies and providers and developers of own solutions can be drawn. The IT Security Expert Group in the Professional Association of Management Consultancy and Information Technology (UBIT) of the Austrian Chamber of Commerce (Wirtschaftskammer), points out the large number of one-person companies in the sector. Those - mostly specialized - lone fighters in the IT security field are mainly service providers but the boundary between them is obscuring. Adaption for the customer environment also has its development part. Here the transitions are guite seamless.

The focus on aspects of IT security is a consequence of the immense and crucial expertise, which is involved. There are in all likelihood more than 200 actual security experts in Vienna, who are usually focused on specific aspects. Markus Klemen, CEO of SBA Research explains: "The lack of highly qualified experts in the cyber security area will increase in the next years. As a Viennese research institution, we want to address this challenge together with our partner institutions in the future, for example with special course formats. In doing so we want to focus even more on the promotion of women in this area – female experts in the IT security area

actor for years. It develops independent products, especially in the fields of network security, industrial security and endpoint security. Another developing and innovative company is Cryptas, which is internationally active and specializes in strong authentication. It offers professional solutions in the areas of access control, integrity security and digital identity. Other companies are focused on specific aspects of IT security: The Viennese Company KiwiSecurity¹⁶ for example provides software for video analysis in the high-security sector and has attracted international attention for its video surveillance technique, which at the same time protects privacy. T3K-Forensics¹⁷ specializes in the area of digital forensics, whereas RadarServices¹⁸ offers solutions for IT security monitoring.

Vienna is Austria's most important location for information

technology and therefore also for IT security.¹⁵ Thus, many

companies offer services in this area. Forty in particular gain

a significant proportion of their revenue from respectively

pursuing their own research and development activities in this

Ikarus Security Software GmbH has been an established

5.1 Number and

Structure

area.

In addition to its activities as a research institution, SBA Research also offers security-related services. It operates in a network of national and international specialists whose expertise lies mainly in the technical area. With more than 100 employees, SBA Research is now the largest research center in Austria exclusively dealing with information security. SBA is a COMET centre. These centres are jointly funded by the federal government and the federal states at a ratio of 2

15 www.wien.gv.at/wirtschaft/standort/pdf/ikt-standort.pdf

16

www.kiwisecurity.com/?lang=de

17

www.t3k-forensics.com/de

18 www.radarservices.com/de are unfortunately still very rare." Joe Pichlmayr (Ikarus) of firms this and refers to the knowledge and the exciting p jects of the competence centre SBA Research (see chapter "Education, Research and Networks").

One big advantage Vienna offers when compared we other countries or cities is its tight network of experts as cializing in different security issues, regardless of whether the authority, industry or research areas. Many agents knew each other well and often work together in different asset ations or platforms. This simplifies the transfer of contar and creates an important advantage in the defence aga bigger attacks. Public initiatives such as the Computer Engency Response Team (CERT)¹⁹ constitute important action the promotion of connections and competences in Vier

The City of Vienna also reacts to recent development in the Digital Agenda Vienna: "Due to the increasing digization of many services and processes it is essential to enthe residents' trust in the security of our IKT systems, of and services."²⁰

5.2 Customers

The clients of IT security companies in Vienna vary great Besides small enterprises and law firms, there are also m large companies such as e.g. Siemens AG Austria, which m use of these agencies.

Despite the increasing sensitization for IT securit companies, there remains a great need for information particular, SMEs with fewer employees are often unawar the great importance this issue has for their companies. cording to Markus Klemen, CEO of SBA Research, the of sequence is that small and medium-sized businesses reg IT security measures as a kind of "luxury". At best, they penetration tests or security checks at the end of a proj "An early integration of security considerations would be m more reasonable in terms of costs since architectural flaw which can – if at all – only be resolved with significant artional costs could be prevented. There is not enough will ness yet to do so, though."

A special advantage of Viennese IT security comparis their proximity to their clients. In this way a trusted r tionship can be built, which is very important in this fie especially if sensitive data and areas are affected. Anot obvious factor is the agglomeration of international firms organizations in the city.

15

con-			
pro-			
the			
the			
WILLI			
spe-			
er in			
now			
soci-			
acts			
ainst			
mer-			
tors			
nna			
onte			
itali			
Itali-			
sure			
data			
atly.			
nanv			
nako			
lane			
h			
ty in			
n. In			
re of			
. Ac-			
con-			
gard			
use			
ject.			
nuch			
laws			
addi-			
lina-			
iiiig-			
nies			
rela-			
eld –			
other			
and			

19 www.cert.at

Education, Research and Networks

the AIT Austrian Institute of Technology, which operates the Centre for Digital Safety & Security.²² It addresses mainly the assurance of operative efficiency and reliability of all critical infrastructures, and the development and supply of forwardlooking technologies.

Important R&D issues at AIT include: command and control systems for use in crisis and catastrophe management, cyber security (AIT Cyber Range), big data and blockchain technologies, secure and reliable systems, latest sensor technologies and systems for the protection of critical infrastructures and digital identity management through modern biometric sensors, intelligent cameras and video analysis. new sensor technology and security on a physical level.

The funding programme KIRAS is a focused initiative which emphasizes the protection of critical infrastructures. KIRAS supports national research projects which increase the security of all members of society. This is also the aim of the A-SIT Secure Information Technology Center Austria. A-SIT is a non-profit association of institutional members with a public-law character.²³

6.1 Vienna Cyber Se-curity and Privacy Research Center (VISP)

Vienna and the Vienna Region have an excellent academic basis in the field of IT security and privacy. The TU Vienna, the University of Vienna and IST Austria, the three top institutions in this field, there are currently 10 professorships for Cyber Security and Privacy. These research institutions have successfully applied for 5 grants from the European Research Council - this is unique in international comparison.

Since 2020, the three institutions have been bundling their activities under a common roof in order to coordinate their activities even better and to make them more visible internationally. With the foundation of the Vienna Cyber Security and Privacy Research Center, the following goals are to be achieved:

- Initiation of cross-institutional internationally visible research activities
- Training opportunities for security experts for industry and science
- Support for regional start-ups
- Attracting international companies in this field.

21 https://www.secpriv.tuwien.ac.at/home/

22

https://www.ait.ac.at/ueber-das-ait/center/center-for-digital-safety-security/

23	
https://www.a-sit.at/	

6.2 Online Advice

An easily accessible information platform can be found at www.onlinesicherheit.gv.at. This strategic measure of the national IKT security strategy helps companies with the identification of possible IT security issues. The portal provides information on current security threats as well as events and publications relating to those issues.

The portal is operated by the A-SIT Secure Information Technology Center on behalf of the Federal Ministry for Digital and Economic Affairs. It offers impartial advice and assistance to accomplish more security in the digital world.

The portal gives a comprehensive overview of potential threats from the use of conventional computers up to mobile devices. It provides information on how to act properly when using the Internet, for example when online shopping, and has a section that deals with the correct use of the Internet for children. In addition, it addresses the topic of interconnected devices - the Internet of Things (IoT).

The quality of training offers and research institutions in the IT security sector in Vienna has recently improved from an already solid level. Besides central institutions such as the Technical University of Vienna (TU Vienna), there are extensive programmes on offer, also from universities of applied sciences. Due to a new head of its Security and Privacy group²¹

(Prof. Matteo Maffei) the TU Vienna has extended its offerings significantly. Main focal points are cryptography, web security, and mobile systems as well as applications of cryptography for electronic currencies, and cloud and data analysis in consideration of privacy. TU Vienna is regularly among the world's best at the international hacker competition iCTF (International Capture The Flag). TU Vienna also participates in the International Secure Systems Lab (iSecLab), an association of five international system and security research laboratories

The FH Campus Wien has a Competence Centre for IT-Security, and the Applied University FH Technikum Wien offers a research and development specialisation in Secure Services, eHealth and Mobility. Both applied universities offer master's degree programmes in this field. Vocational schools such as the TGM Institute of Technology or the HTBLVA (Higher Technical College) Spengergasse complement the training offers

SBA Research is the biggest Austrian competence centre for applied research in the area of IT security. It works closely with the TU Vienna, other universities and a large network of different companies. More than 100 researchers analyse the IT security of systems, ranging from traditional company IT to the security of production systems. Many sessions and courses offer a simple and solid insight into the state of science and technology.

Another important actor in the Austrian research field is

6.3 CryptoParties and Events

In Vienna, CryptoParties, aimed at providing easy access to topics such as privacy, the Internet, cryptography and other interesting and related subjects, take place regularly. In particular, topics of how to encrypt e-mails, hard drives, chats and phone calls, as well as anonymous surfing and how to publish things anonymously are addressed.²⁴

Moreover, the non-profit association Cyber Security Austria (CSA) focuses on dissemination of knowledge on cyber security by e.g. holding public events or publishing papers on the topic.²⁵

As early as 2012, the Austria Cyber Security Challenge (ACSC) was launched (www.verbotengut.at), which has since developed into a major European Cyber Security Challenge (ECSC) on the initiative of the CSA (www.europeancybersecuritychallenge.eu). The ACSC is Austria's first IT security talent search for the recruitment of young, gualified people. In future, this group will form the personnel backbone for the defence against national cyber-attacks. With this challenge, young talents are to be discovered and awarded prizes.

The AIT organises the "International Digital Security Forum" under the motto: "Global Discussion for a Connected World". In addition to presentations and discussions, numerous exhibitors will offer insights into current developments in the field of cyber security.

SBA organizes the annual conference "Sec4Dev - Conference & Bootcamp". It has a strong focus on practical, applicable, hands-on, and security-related content for people involved in software development. The goal is to make security one of the most relevant topics in the world of software development.

Services of the

It is not guite clear whether the implementation of IT in other sectors - e.g. cyberphysical systems, blockchain/smart contracts, usability - will result in new business opportunities. While some insist that collaboration will be more interdisciplinary and that specialists that build control or heating systems for instance will connect with IT security experts, others speak of "wishful thinking". In the long run, it is, however, guite likely that new options will evolve. Edgar Weippl, head of the CD-lab SQI and research director of SBA Research, is convinced that the engineering process of industrial systems can greatly benefit from the experiences of the software sector over the last 10 years:

> "The quality and the security of software saw a tremendous increase in the last decade. System builders should be able to draw on those experiences at the introduction of a secure development lifecycle in order to protect the engineering process better."

The ongoing technologization and connectedness of our society means that the number of cyberattacks will continue to increase in the future. Regarding Vienna as a business location, efficient measures need to be taken to focus on protecting critical infrastructure and sensitive knowledge, e.g. when thinking of economic espionage. In order to achieve this goal, it is necessary to ensure certain things:

First, investments in and capacities of the education sector for cyber security must continually expand. Education programmes at Austrian applied universities and other universities must be significantly increased in order to satisfy the needs of companies and authorities for well-gualified people. In Vienna, the University of Vienna and the Technical University of Vienna, as well as applied universities such as FH Technikum Vienna and FH Campus Vienna, are essential educational institutions that also conduct research and benefit from the research expertise of other research institutions such as SBA Research.

Although further investment in education is vital, this alone cannot fix the shortage of skilled labour. According to a report by the Austrian Federal Economic Chamber, the number of vacant positions in recent years has numbered around 5,000.26 Thus, it is also necessary to develop efficient and attractive concepts that recruit more people from abroad.

There has been a substantial increase in awareness by companies when it comes to cyber security in recent years. Many have already implemented numerous measures to ensure the security of their infrastructure and data. Nevertheless, it remains necessary to carry out awareness-raising activities especially for SMEs since many remain unaware of the seriousness of the problem. In this regard, it is important to take targeted measures to clarify and emphasise the big financial advantages of security investments for companies in the long run.

26 https://kurier.at/wirtschaft/fachkraeftemangel-it-spezialisten-fuer-kmu-kaum-nocheistbar/400357549

The objective of the Vienna Business Agency is the continuous development of international competitiveness by supporting both Vienna-based companies and their innovative strengths, and the sustainable modernization of the city as a business location. To achieve this, the Agency provides free consultations to all entrepreneurs in Vienna on the topics of business creation, business location or expansion, business support and financing. Furthermore, networking contacts in the Viennese economy are also made available. The Vienna Business Agency supports and helps businesses complete their research and development projects with both individual consulting and monetary funding. Depending on requirements, they will receive information about sponsorships, financing opportunities, possible development partners, research service providers, or research infrastructure, according to their needs. The Vienna Business Agency sees itself as a network of the Viennese ICT industry and supports businesses with

consultations, as well with distribution and networking among themselves. Events and workshops on topics from the field of ICT are held regularly.

Additionally, the Vienna Business Agency helps with company relocations or internationalization services. Assistance is provided to business founders and young entrepreneurs in the start-up area. Free workshops and training sessions on topics of everyday business are offered as well as small, affordable office spaces.

Founders Labs²⁷: Free intensive training over several weeks to get started.

All funding programs of the Vienna Business Agency can be found here:

https://viennabusinessagency.at/funding/programs

Vienna Business Agency



With the alphabetical listing on the following pages, we offer you an overview of selected companies from Vienna that offer services in the field of IT security. This list makes no claim to completeness.

Companies and Research Institutions

COMPANY/ RESEARCH INSTITUTION	DESCRIPTION	CONTACT/ WEBSITE
A.SYS	A.SYS offers a broad portfolio in the area of cyber secu- rity. The portfolio ranges from business antivirus soft- ware, DNS security service to a platform that can detect sensitive company information in the Darknet and Deep Web.	Seitenhafenstrasse 15/205 1020 Vienna T +43 1 585 76 36 office@asys.at Contact person: Hans Christian Singhuber <u>www.asys.at</u>
A1 CYBER RANGE	As Austria's largest telecommunication provider, A1 offers a comprehensive range of IT security services. In addition to its own firewall systems and software for secure data transmission, the company also features a training acad- emy where IT specialists from companies can intensify their skills.	Lassallestrasse 9 1020 Vienna T +43 800 664 444 664 business.loesungen@a1.net www.a1.net/a1-cyber-range
AUSTRIAN INSTITUTE OF TECHNOLOGY	AIT is the largest non-university research institution in Austria. It deals with various topics in the IT field, includ- ing cyber security. On the one hand, AIT conducts re- search into the development of new security technologies. On the other hand, established technologies and tools for strengthening critical infrastructures are offered and taught in special workshops and training courses.	Giefinggasse 4 1210 Vienna T +43 1 50550-4100 markus.kommenda@ait.ac.at <u>www.ait.ac.at/dss</u>
ANOVIS	Anovis has been active in the field of IT security since 2004 and exhibits an extensive range of different prod- ucts. In addition to general consulting activities, Anovis also supports the entire conception, implementation and operation of network and data centre infrastructures if required.	Rennweg 97–99 1030 Vienna T +43 1 7124070 office@anovis.com www.anovis.com

Chapter 9, Companies in Vienna

Companies in Vienna

COMPANY/ RESEARCH INSTITUTION	DESCRIPTION	CONTACT/ WEBSITE	C RI IN	COMPANY/ ESEARCH NSTITUTION	DESCRIPTION	CONTACT/ WEBSITE
A-TRUST	A-Trust is a qualified trust service provider for electron- ic certificates and offers various solutions in this area. Its portfolio includes Handy-Signatur as a digital signing tool as well as software and cash register certificates.	Landstrasser Hauptstraße 1b The Mall E02 1030 Vienna T +43 1 71321510 office@a-trust.at <u>www.a-trust.at</u>	CE E-I GC	ERT.AT/ -CERT/ OVCERT	CERT.at is the Austrian national CERT (Computer Emer- gency Response Team). It acts as a contact for IT secu- rity, network CERTs and CSIRTs (Computer Security Incident Response Teams) from the areas of critical infrastructure & ICT and supports SMEs with general warnings and tips.	Karlsplatz 1/2/9 1010 Vienna T +43 1 505641678 team@cert.at <u>www.cert.at</u>
BACHER SYSTEMS	Bacher Systems features a comprehensive choice of different IT security solutions: It offers solutions in the areas of privileged access security, data security, mobile security, cloud security and network security as well as risk management to SIEM (Security Information & Event Management) systems.	Wienerbergstr. 11/B9 (Tower B) 1100 Vienna T +43 1 601260 info@bacher.at www.bacher.at	CH	HANGE-IT	Change-IT operates in the field of cyber security for SMEs. It offers holistic solutions in the areas of applica- tion security, business continuity in the event of data loss and access control to simplify work processes.	Lerchenfelder Strasse 70–72/5 1080 Vienna T +43 699 17992940 office@change-it.at www.change-it.at/security
BECHTLE	Bechtle considers itself a provider of integrated solutions in the field of cyber security. The company's portfolio includes consultancies in the area of threat prevention and information security as well as solutions in the area of application and cloud security.	Technologiestrasse 8 1120 Vienna T +43 1 570040 office.at@bechtle.com Contact person:		ORETEC	CoreTEC fully specializes in IT security and can therefore offer a high level of quality and services. This includes various penetration tests, consulting and support activ- ities of companies with regard to their system security policy, security training as well as consultancy and prepa- rations for ISO 27001 certifications.	Ernst-Melchior-Gasse 24/DG 1020 Vienna T +43 1 50372730 www.coretec.at
BITMAN	Bitman already has many years of experience in the field of IT security. The company offers various solutions for the development and management of secure and flexible systems for its customers. Bitman can also be consulted	Robert Absenger www.bechtle.com/at Engerthstrasse 227 1020 Vienna T +43 664 524 9612	CF	RYPTAS	CRYPTAS concentrates on strong authentication within the IT security area. The company offers professional solutions in the field of access protection (multi-factor authentication), integrity assurance (data encryption, digital signatures) and digital identity (portal notifications, identity federation).	Franzosengraben 8/4th Floor 1030 Vienna T +43 1 355530 office@cryptas.com www.cryptas.com
BRAINLOOP AUSTRIA	systems for its customers. Bitman can also be consulted in the event of acute situations. The internationally operating company Brainloop is char- acterized by a wide range of modern technologies in	office@bitman.at www.bitman.at Gonzagagasse 19/3 1010 Vienna	CY	YAN	cyan as an internationally operating company features a high variety of products based on future-oriented tech- nologies in the IT security field. Its customers include insurance companies, governments, banks and game providers. They offer solutions in the fields of OnNet Security, Personal Protection & Authentication.	Wiedner Gürtel 13 1100 Vienna office@cyansecurity.com www.cyansecurity.com
	the field of IT security. This includes firewall systems, 256-bit SSL/TLS encryption and document fingerprint technology. The company also offers hosting in ISO 270001-certified data centres in several European coun- tries.	T +43 1 361 9790 info@brainloop.de <u>www.brainloop.com/de</u>	CS	SA	Cyber Security Austria is a non-profit association with the goal to create a sensitization for the topic of IT se- curity. It wants to address different stakeholders such as politicians, business people, and scientists, but also society as a whole. Its activities range from publications and lectures to project collaborations in which existing knowledge is networked and communicated.	Blechturmgasse 11 1050 Vienna office@cybersecurityaustria.at www.cybersecurityaustria.at

COMPANY/ RESEARCH INSTITUTION	DESCRIPTION	CONTACT/ WEBSITE	COMPANY/ RESEARCH INSTITUTION	DESCRIPTION	CONTACT/ WEBSITE
CYBERTRAP	Founded in 2015, CyberTrap focuses on cyber security for government organizations and large enterprises. Through a self-developed deception solution, attacks on sensitive IT systems can be prevented and the resulting damage avoided. Moreover, attackers are also unknow- ingly redirected into an own isolated environment in which she can be monitored.	Auerspergstrasse 4/7 1010 Vienna T +43 1 8904700 contact@cybertrap.com www.cybertrap.com	GEKKO IT-SOLUTIONS	For more than 20 years, GEKKO it-solutions has oper- ated as a service provider in the IT security sector. Its portfolio ranges primarily from consulting and support of data in the area of firewall network security, encryp- tion, disaster recovery to general backups.	Wiegelestrasse 10 1230 Vienna T +43 1 710 5656510 office@gekko.at Contact person: Thomas Hofstätter
DELOITTE	Deloitte is characterized both by its strong internation-	Renngasse 1/Freyung			www.gekko.at
	of cyber security, Deloitte supports companies in carry- ing out risk analyses of their IT systems, fulfilling legal & security-related requirements in this area and establish- ing comprehensive identity & access management.	T +43 1 537007950 office@deloitte.at Contact person: Mag. Alexander Ruzicka <u>www2.deloitte.com/at</u>	HACKNER SECURITY INTELLIGENCE	Hackner Security Intelligence was founded in 2010 with the aim of expanding the existing range of IT security audits to include physical security and social engineering. The offer ranges from general IT penetration tests, to vulnerability management up to special security trainings, in which employees of companies are taught important knowledge on IT security.	Franz-Josefs-Kai 27/3B 1010 Vienna T +43 1 2052300 office@hackner-security.com www.hackner-security.com/1
EXPRESSFLOW	expressFlow concentrates on the development of mobile applications in the field of IT security. With its own Secure- Beam App, files from existing cloud memories can be encrypted, divided into pieces and then distributed ran- domly as data blocks to the existing cloud storage. The app provides real-time information on accesses and changes to the respective files.	Pater-Schwartz-Gasse 11A 1150 Vienna contact@expressflow.com Contact person: DI Dr. Martin Vasko <u>www.expressflow.com</u>	HXS	The company HXS covers a wide range of different fields in the business IT world. With regard to their cyber se- curity solutions, they offer not only individual IT security risk analyses but also comprehensive firewall and anti- virus systems, backups and consulting sessions to raise awareness.	Millergasse 3 1060 Vienna T +43 1 3441344 office@hxs.at Contact person: Lorenz Bindhammer, BSc (WU) <u>www.hxs.at</u>
UNIVERSITY OF APPLIED SCIENCES FH CAMPUS VIENNA	FH Campus Vienna has an IT security competence cen- tre and a part-time Master's programme in IT Security. There is also a cyber security team which deals with penetration tests, ethical hacking, capture-the-flag com- petitions and cryptography challenges.	Favoritenstrasse 226 1100 Vienna T +43 1 606 68 77-6600 office@fh-campuswien.ac.at www.fh-campuswien.ac.at/de/	IKARUS SECURITY SOFTWARE	IKARUS Security Software offers a comprehensive range of security products for both home users and enterprise networks. Applications are available for the fields of net- work protection, industrial security and endpoint protec- tion.	Blechturmgasse 11 1050 Vienna T +43 1 589950 office@ikarus.at www.ikarussecurity.com/at
UNIVERSITY OF APPLIED SCIENCES FH TECHNIKUM WIEN	FH Technikum Wien offers both an R&D focus on fields as Secure Services and eHealth & Mobility as well as a master's degree in IT Security. Every year, the Master's programme in IT Security, together with the Faculty of Computer Science, organizes an event called Security Potpourri where the latest developments are presented by experts from the industry.	Höchstädtplatz 6 1200 Vienna T +43 1 333 40 77-0 its@fh-campuswien.ac.at www.technikum-wien.at	INFRAPROTECT®	Lack of safety awareness and a lack of safeguards favour cyberattacks in many SMEs. INFRAPROTECT special- izes in risk analysis according to applicable standards and laws which includes the creation of precise action plans and training employees in security awareness and correct behavior in critical situations.	Ghegastrasse 3/5/5.2 1030 Vienna T +43 1 9741706 office@infraprotect.com www.infraprotect.com

COMPANY/ RESEARCH INSTITUTION	DESCRIPTION	CONTACT/ WEBSITE	COM RESI INST	/PANY/ EARCH TITUTION	DESCRIPTION	CONTACT/ WEBSITE
KAPSCH BUSINESSCOM	Kapsch BusinessCom acts as a digitization partner for companies. In the area of IT security, they offer solutions for the prevention of IT attacks, network protection through firewalls and encryption as well as general mon- itoring software for the detection of irregularities. More- over, they also offer own workshops for advanced train- ing in the field of IT security. A separate report on cyber security has also been published in the meantime.	Wienerbergstrasse 53 1120 Vienna T +43 508110 kbc.info@kapsch.net www.kapsch.net	RADAI	R CYBER RITY	Radar Cyber Security offers its customers comprehen- sive tools and services for their cyber security: Their portfolio ranges from IT and OT security monitoring to advanced cyber threat detection, IT and OT risk detec- tion and log data analytics (also called SIEM) to CDC as a service.	Zieglergasse 6 1070 Vienna T +43 1 92912710 office@radarcs.com <u>www.radarcs.com</u>
KIWISECURITY SOFTWARE	KiwiSecurity is a leading provider of video analysis and video control centre solutions that transform video sur- veillance into a proactive tool. Due to an intelligent eval- uation of relevant picture information, video surveillance is automated for the first time.	Guglgasse 15 1110 Vienna T +43 1 9971039 office@kiwisecurity.com www.kiwisecurity.com	REDPU	ULS IT & RITY SOLUTIONS	redPuls IT & Security Solutions is characterized by its great choice of IT security solutions. In addition to their Next Generation Firewall, it also offers solutions for Network Web Cloud Ransomware Protection, DDoS Preventing, Mobile Device Security as well as general penetration tests and network monitoring tools: IT inci- dent management and IT malfunction management concepts are developed and implemented together with the customer.	Neulinggasse 29/2/13 1030 Vienna T +43 1 512 11220 office@redpuls.com <u>www.redpuls.com</u>
KPMG	KMPG offers a wide range of cyber security products. They carry out audits to identify and assess specific risks of IT systems, provide individual guidelines for risk minimization and the establishment of protective meas- ures, and support companies in the event of acute cy- berattacks.	Porzellangasse 51 1090 Vienna T +43 1 31332 <u>home.kpmg/at/de/home/</u> industries/technology.html	SBAR	RESEARCH	SBA Research is a COMET centre of excellence for IT security located in Vienna. In cooperation with TU Vienna as well as some other international institutions, a dual approach of scientific research and practice-oriented implementation offers a unique range of services, from research cooperations to penetration tests. It covers security aspects of future key areas such as	Floragasse 7 1040 Vienna T +43 1 5053688 office@sba-research.org www.sba-research.org
MAG MENTAL ACROBATICS GROUP™	MAG Mental Acrobatics Group features a comprehensive portfolio for enterprise IT security. In addition to docu- mentation, audits and training, a variety of different hard- ware and software solutions are offered to ensure opti- mal protection of critical networks and infrastructures.	Arsenal Objekt 16 Top 66 1030 Vienna T + 43 1 40600970 office@magsecurity.at			Al, IoT/Industry 4.0, secure software development and security in digitization. Moreover, they also conduct different kinds of of training courses.	
	The company also has expertise in social security and legal issues (DSGVO).	www.magsecurity.at	SEC C	CONSULT	SEC Consult has great expertise in the fields of cyber and application security. In addition to general security checks of IT systems of companies and authorities, its portfolio also includes activities in process management	Leopold-Ungar-Platz 2/3/3 1190 Vienna T +43 1 89030430 office@sec-consult.com
PWC AUSTRIA	PwC helps companies protect themselves against digi- tal threats. With experts in the fields of information se- curity, data protection, digital identity, IT/OT security, awareness and business continuity management, PwC ensures that companies are prepared in the event of a cyberattack. PwC accomplishes a paradigm shift among employees and integrates cyber security into all business processes.	Donau-City-Strasse 7 1220 Vienna T +43 1 50188-0 cyber.austria@pwc.com Contact person: Georg Beham <u>www.pwc.at/cyber</u>			to ensure legal requirements. Solutions for the imple- mentation of security measures in software development are also offered.	www.sec-consult.com

COMPANY/ RESEARCH INSTITUTION	DESCRIPTION	CONTACT/ WEBSITE		COMPANY/ RESEARCH INSTITUTION	DESCRIPTION	CONTACT/ WEBSITE
SECURITECTS	Securitects is a professional IT and information security consultant. They support companies in the implementa- tion of the ISO 27001 standard in the form of security guidelines, processes and procedures. Securitects also specializes in penetration testing and IT forensic analysis. Both together provide companies with a comprehensive overview on the security level of their IT systems and clear recommendations for action where required. Per-	Schelleingasse 8/9 1040 Vienna T +43 1 9666471 office@securitects.com <u>www.securitects.com</u>	THALES AUSTRIA	As an international company, Thales is a global player in the field of cyber security. Its portfolio ranges from data encryption to big data analysis and threat intelligence, allowing the threat potential of cyberattacks to be as- sessed at any time, to its own cyber security centers where external threats in IT systems can be analyzed by customers in real time and responded to immediately.	Handelskai 92 1200 Vienna T +43 1 277110 office.at@thalesgroup.com www.thalesgroup.com	
	27001 and secure software development round out the offer.			T-SYSTEMS AUSTRIA	As a corporate customer arm of Deutsche Telekom, T-Systems supports the planning and implementation of customized security solutions such as cyber defense, security assessments, IP DDoS Security, incident re-	Rennweg 97–99 1030 Vienna T +43 057 0570 security-info@t-systems.at
SELECT-IT	SELECT-IT offers a wide range of own product solutions in the field of IT security. This includes e.g. firewall and virus solutions. They also offer management and moni- toring services so that problems can be responded to quickly by remote monitoring. The company is further	Schuhfabrikgasse 17/3/4 1230 Vienna T +43 1 36191010 office@select-it.at			sponse, SlaaS to protect the IT infrastructure, managed firewall services for companies, and with its own secu- rity operations centre in Vienna.	www.t-systems.at
	operating in the field of IT security for educational insti- tutions.	www.select-it.at		TECHNICAL UNIVERSITY OF VIENNA	The Technical University of Vienna (TU) offers the fol- lowing focuses in the security area: cryptography, web security, mobile systems as well as applications of cryp- tography for electronic currencies, cloud and data anal-	Karlsplatz 13 1040 Vienna T +43 1 58801-0 pr@tuwien.ac.at
ÖSTERREICH	As a large international corporation, Siemens strongly supports the concern to raise awareness for IT security at various levels. In addition to a Charter of Trust, which was published together with many other companies, Siemens is also active at events such as Graz Security Week.	Siemensstrasse 90 1210 Vienna T +43 1 517070 kontakt.at@siemens.com <u>new.siemens.com</u>			ysis while preserving privacy. It is also involved in the International Secure Systems Lab (iSecLab), an associ- ation of five international system and security research laboratories.	www.tuwien.at
T3K-FORENSICS	TT3K-Forensics works as a service and training con- sultant for national and international law enforcement agencies in the field of mobile forensics. This includes the securing and evaluation of mobile devices and cloud data, forensic trainings and workshops with authorities in Europe as well as solutions in the field of mobile se- curity for the detection and defense of threats to mobile devices.	Jacquingasse 51/3 1030 Vienna T +43 1 9971033 office@t3k.ai www.t3k-forensics.com		XSEC	As a cyber security company, XSEC checks the securi- ty of companies in various areas. The companies' em- ployees are also evaluated with regard to their own procedures. In addition, training courses on IT security and consulting interviews with companies are held in which central points in the area of IT security such as the ISO 27001 standard are explained. XSEC can also be requested as an external consultant, e.g. in the area of data protection.	Mayerhotgasse 6, 5th Floor 1040 Vienna T +43 69910242048 bboeck@xsec.at Contact person: DI Mag. Mag. Benjamin Böck <u>www.xsec.at</u>
TECHBOLD	techbold offers a wide range of product solutions in the field of cyber security: Besides audits to assess the cur- rent security status of IT systems, the company's port- folio also includes firewalls, data backups and anti-spam solutions.	Dresdner Strasse 89 1200 Vienna T +43 1 3434333 office@techbold.at www.techbold.at				



10.

Imprint

Vienna Business Agency. A service offered by the City of Vienna. Mariahilfer Strasse 20 1070 Vienna viennabusinessagency.at

Contact Bernhard Schmid Technology Services T +43 1 25200-521 schmid@wirtschaftsagentur.at

Text and Editing eutema GmbH Lindengasse 43/13 1070 Vienna

Design seitezwei.com

Photos Vienna Business Agency/Karin Hackl, Vienna Business Agency/Klaus Vyhnalek

31

Technology reports are available on the following topics:

- Big Data & Al
- Cloud-Computing
- E-Government
- E-Health
- E-Commerce
- FinTech
- Enterprise Software
- Entertainment Computing
- IT-Security
- Internet of Things
- Mobile Computing
- User Centered Design
- Visual Computing

The digital versions can be found at www.viennabusinessagency.at/technology/let-s-talk-innovation/ digital-technologies/



The information and networking services are co-financed by the European Regional Development Fund as part of the "IC3 Innovation by Co-Operation, Co-Creation and Community Building" project.



The information and networking services are co-financed by the European Regional Development Fund as part of the "IC3 Innovation by Co-Operation, Co-Creation and Community Building" project.



Contact

Vienna Business Agency. A service offered by the City of Vienna. Mariahilfer Strasse 20 1070 Vienna viennabusinessagency.at