ENGLISH EDITION

42
32

The Softwarepark Hagenberg Magazine | Edition 2018

softwarepark
hagenberg

Information Security

4232 CONTENTS

Dear Readers,

Softwarepark Hagenberg's diversity is also reflected in the work carried out with our partners from research, education and business and is deeply rooted in our structures.

First of all, four brief statements on the subject of Information Security:

Photo: JKU

University President Prof. Mag. Dr. Meinhard Lukas
President of Johannes Kepler University and Head of Softwarepark Hagenberg

Information Security – most certainly existential

Technological security is all-embracing; the topic of Information Security is existential. A hack can affect us all and have far-reaching consequences. With its expertise in this sector, Softwarepark Hagenberg is now setting new standards that combine synergy effects with the constantly growing Linz Institute of Technology (LIT) which are valuable and sustainable for the entire location. The team of committed scientists is a driving force to be reckoned with, a pacesetter and a sounding board.

Photo: FH OÖ

FH-Prof. DI Robert Kolmhofer
Head of Secure Information Systems Department, University of Applied Sciences Upper Austria

Information Security affects everyone – especially in 2018

You hear and read about IT Security incidents and successful cyber attacks on an almost daily basis. This is why it's all the more important to transport the necessary Information Security/IT Security/data protection expertise in an applicable manner for companies, organisations and authorities.

The Softwarepark is the ideal location for an exciting and informative year of events for the Information Security Year 2018 by the Department of Secure Information Systems of the University of Applied Sciences Upper Austria with its internationally recognised security study programmes and research activities, the JKU, SCCH, consulting firms in the Information Security sector and many IT companies.

Editorial

Photo: SWPH

Dr. Sonja Mündl
Manager Softwarepark Hagenberg

The countdown has started!

The GDPR will be in force within the EU as of 25 May, 2018. For many people this means ruthlessly clearing their jungle of data – and the very first thing is to take an inventory of all the data they have stored.

In keeping with this year's main theme "Information Security", Softwarepark Hagenberg is dedicating itself to numerous events, such as the exciting event series for IT experts, the Security Forum and the Long Night of Research, which are held at Softwarepark Hagenberg (more information on page 19).

Photo: STIWA Group

Dipl.-Ing. Thomas Führer, MSc
Chairman of the Softwarepark Hagenberg company network

Ahead of the Information Security hype

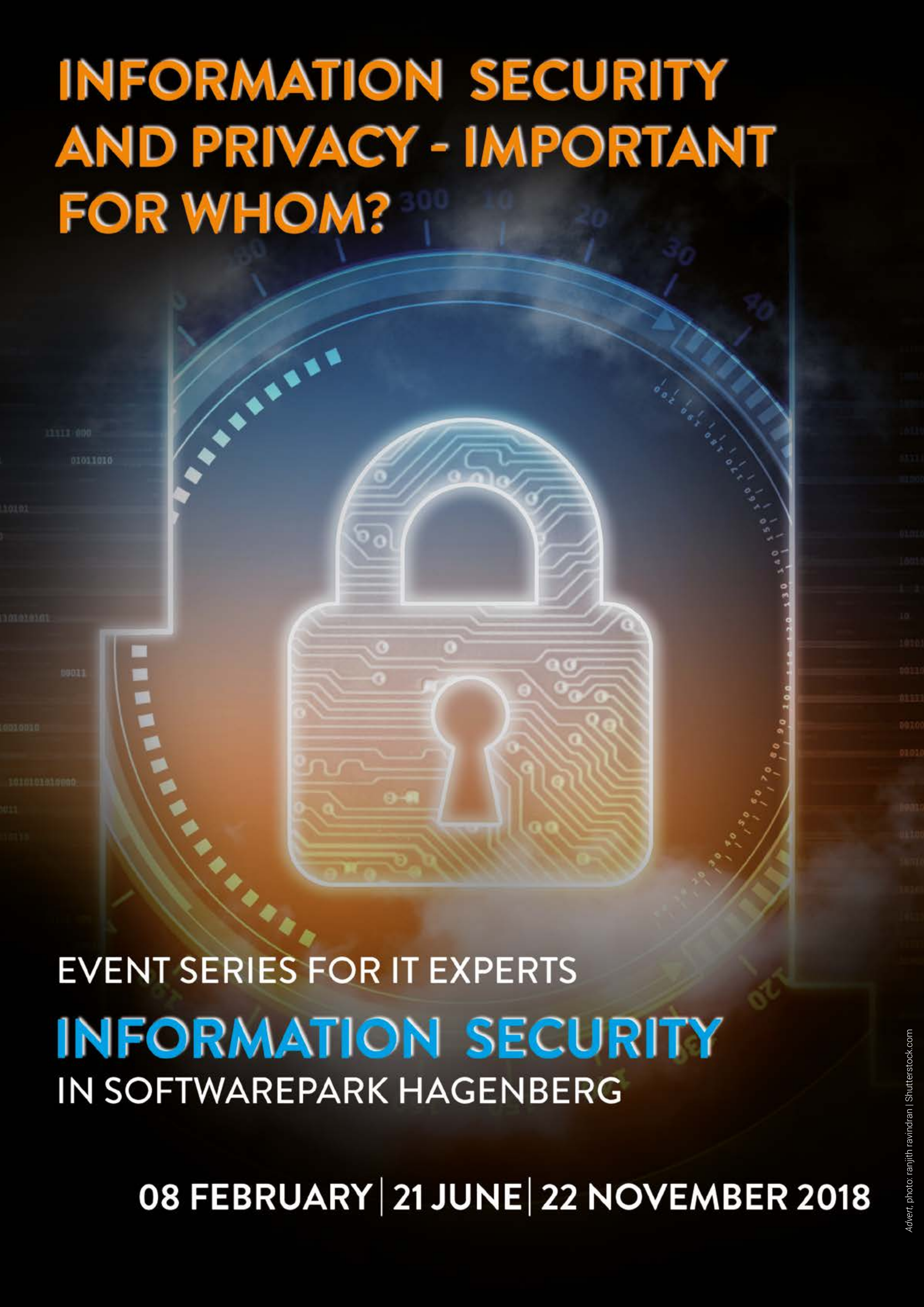
At Softwarepark Hagenberg more than 75 companies and training and research institutions work together on IT Security. In 2000, with the foundation of the first degree courses in computer and media security, the importance of Information Security arrived in Hagenberg long before the current hype. Access to graduates provides companies with permanent specialists with extensive know-how. Both the Softwarepark and its customers benefit from this.

Let’s network!
We look forward to meeting you at our exciting events under the banner of "Information Security Park Hagenberg".

JKU JOHANNES KEPLER UNIVERSITÄT LINZ

softwarepark hagenberg business research education

Softwarepark Hagenberg is a research, training and business location. As a spin-off of Johannes Kepler University (JKU) Linz, it was founded by Univ. Prof. Dr. Bruno Buchberger who still contributes significantly to innovation in Upper Austria to this day. The Softwarepark is distinguished by its state-of-the-art infrastructure, as well as a diverse network of experienced industry experts, young creative people and students who are eager for knowledge. This synergy in particular is a major part of the recipe for success; Softwarepark Hagenberg is a place for communication and meeting, where around 2,800 people work, research, teach, learn and live.



SURE SUCCESS!

The Softwarepark Hagenberg event series.

In 2016 a group of experts consisting of representatives of the companies, research institutes and educational institutions of Softwarepark Hagenberg was formed to develop a new Hagenberg event series as a joint forum for inspiration, presentation, cooperation and communication both internally and externally.

The five-man team, consisting of Dipl.-Ing. Thomas Führer, MSc (STIWA Group), DI (FH) Thomas Kern (University of Applied Sciences Upper Austria Campus Hagenberg), DI Theodorich Kopetzky (Software Competence Center Hagenberg – SCCH), Dr. Sonja Mündl (Softwarepark Hagenberg) and A.Univ.Prof. Dipl.-Ing. Dr. Wolfgang Schreiner (Research Institute for Symbolic Computation (RISC) of the JKU), concretised this idea and implemented it in 2017 over the course of several consecutive open events. Within the framework of lectures by invited renowned experts from business and science, the participants shall learn more about current trends and the resulting IT requirements in order to deepen selected topics and discuss possible solutions together in a subsequent discussion.

A highly relevant guiding theme every year

The consensus was quickly reached to define an overarching, highly relevant guiding theme for all participants each year. And so, the first cycle in 2017 was dedicated to the topic of "Automotive Computing". Together with international experts, three well-attended events were held to discuss the new challenges facing information technology, in particular mobility of the future, the increasingly important role that data analysis will play in the automotive sector and how the increasing safety and security requirements in autonomous driving can be met.

In the past, the topic of Information Security in particular has usually been neglected somewhat. However, with the fast growing volume of information processing and increasingly networked systems in increasingly complex application areas, the resulting threatpotential is also on the rise. Last but not least, the European General Data Protection Regulation, which enters into force on 25 May 2018, hovers above companies' heads like a sword of Damocles.

Sword of Damocles European General Data Protection Regulation

A close inspection of security measures in respect of technology, architecture and management is therefore essential. However, it also presents the opportunity not only to set up state of the art infrastructure, but also to be able to better design data management and business processes.

For this reason, the main theme of events in 2018 will be "Information Security". Once again, we will turn an examining light on the subject from different perspectives together with renowned experts. These subjects include the Internet of Things, embedded systems, smart cloud services, critical infrastructures, agriculture and food, health care and medical technology, as well as legal aspects.

Seeing as law in IT Security is such a hot topic, the title of the opening event on 8 February, 2018 says it all: "Sword of Damocles – Protecting critical infrastructures"

We hope you're there right from the start! Because the Softwarepark Hagenberg event series is sure to be a success!

DI (FH) Thomas Kern
FH OÖ Campus Hagenberg, Head of Center of Excellence

Photo: Nata-Lia | Shutterstock.com

Advert

Information Security at the organisational (Information Security Management) and technical level (IT Security) has become an integral part of our digitally connected world. We receive reports about security incidents every day, be it hacks from Internet platforms or company servers, weak points in the firmware of products that lead to security gaps or data leaks that were only made possible by the exploitation of inadequate Information Security measures. It is necessary to take a holistic approach throughout the product lifecycle in terms of technology and organisation in order to ensure Information Security.

Walter Unger will talk about "Cyber Defence - which capabilities do we need?" at the kick-off event on February 8, 2018. Softwarepark Hagenberg asked him for an interview ahead of the presentation.

Mag. Walter J. Unger
Chief of Staff

Photo: Ministry of Defence/private

"Disruption or even destruction of strategic infrastructures can have serious consequences for the well-being of the population."

Theresian Military Academy 1979-1982, Commander and Head of Squad and Central Agency of the Ministry of Defence (BMLV) since 1982; 1988-1991 General staff training; 1998-1999 Federal Executive training, 1999-2000 Commander of Anti-Tank Battalion 1; 2001-2009 Head of Electronic Defence, 2006-2008 Head of the Interministerial Working Group Strategy "ICT Security", 2009 Head of the ICT Security Division, Head of the Cyber Defence & ICT Security in the Defence Office since May 2013, currently Head of the Cyber Defence Centre.

What are operators of essential services and operators of critical infrastructure and what is their significance for the state (society, economy, government, executive, national defence)?
Critical infrastructures are organisations or institutions with (vital) strategic importance for the state community, the failure or disruption of which can lead to long-term supply shortages or other dramatic consequences for large population groups. State and society can only function if infrastructures such as telecommunications, energy supply (electricity, oil, gas), banking, finance and transport, healthcare (including food and drinking water supply and disposal), emergency and rescue services, government and public administration (including police, customs and the armed forces) are available without significant disruption. These infrastructures are the backbone of a successful economy, a vibrant research community, a transparent state and a free society.

Why is it so important to protect these critical network and Information Security infrastructures?
States have always been dependent on their strategic infrastructures. The digitisation and networking of strategic infrastructures and all areas of society leads to a massive dependence on the availability, confidentiality and integrity of stored data, the functionality of ICT infrastructures and the smooth flow of huge amounts of data over complex networks. Disruption or even destruction of these infrastructures can have serious consequences for the health, safety or economic and social well-being of the population or the effective functioning of state institutions.

The "Cyber Security Act", which is due to come into force in Austria in 2018, is often spoken of in public. Why is cyber security vital for essential services?
The business location, services of general interest, society and the state depend on the functioning of strategic infrastructures and the flow of information and communication. Therefore protecting these infrastructures is of strategic importance! Not only for the state but also for many companies!

Are there publicly known examples of cyber attacks on operators of essential services?
In the last two years there have been numerous examples of attacks of this kind internationally and in Austria. At the end of 2016, cyber attacks paralysed the power supply in Ukraine. Hundreds of thousands of people were without electricity for up to 48 hours. The attempt to set up a botnet paralysed about 900,000 German Telekom routers. In May 2017, the blackmail software NonPETYA took mere minutes to cause Maersk, one of the world's largest logistics companies, several hundred million dollars in damage. In February 2016, Telekom Austria was the target of a DDoS attack, which led to mobile data services being unavailable to a large number of customers for several hours. Between September 2016 and December 2017 there were numerous politically motivated DDoS attacks on websites of Austrian institutions (including Vienna Airport, the Ministry of Foreign Affairs, the Ministry of Defence, the National Bank, the parliament, the website of the then still presidential candidate Van der Bellen, the website of a political party, etc.).

Paid contribution

CYBER DEFENCE

An interview with Mag. Walter J. Unger, Chief of Staff, Head of Department of Cyber Defence Centre & ICT Security at the Ministry of Defence Office.

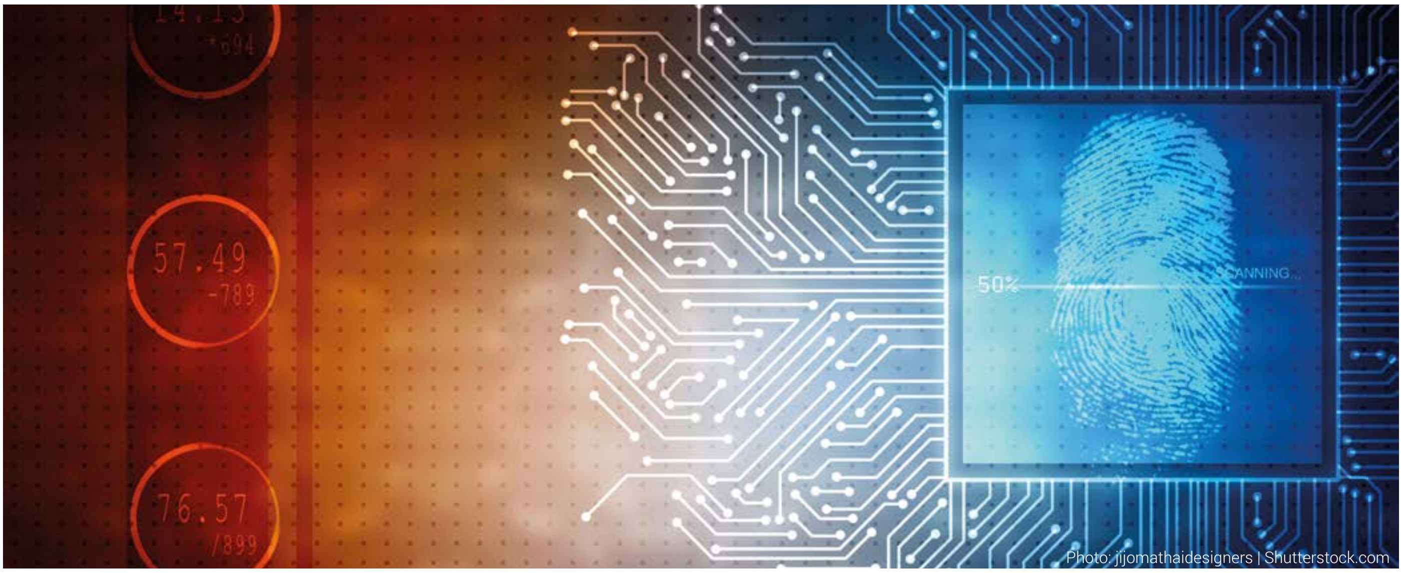


Photo: jijomathaidesigners | Shutterstock.com

The Austrian Armed Forces (ÖBH) are also permanently exposed to attacks. On average, about 60,000 events are registered per day. After analysis, there is around one concrete attack per day. These are often widespread mass attacks, but some targeted attacks have the hallmarks of international cyber espionage campaigns.

What can the effects of cyber attacks be for the public?
Damage to individuals is mainly caused by the misuse of personal data, cyberbullying and cybercrime. Companies, authorities, etc. must expect extortion using encryption Trojans or DDoS attacks. Know-how, companies and trade secrets are threatened by cyber espionage. Sabotage attacks can cause major financial damage and damage to a reputation if customer data is stolen. Attacks against individual critical infrastructures could, for example, cause a blackout. Large-scale attacks on Austria's sovereignty are also not unthinkable. For this reason, the Austrian Ministry of Defence has been commissioned to prepare the national defence, including cyberspace.

Is it already possible to find out who might be classified as an operator of essential services in Austria, or how can you tell if you might be affected as an operator of essential services?
About 400 companies are counted among the critical infrastructure in Austria. The Federal Chancellery is currently analysing which companies are to be classified as operators of essential services. This list must be ready by autumn 2018 at the latest, the companies will be informed in writing.

To what extent are the suppliers or service providers of operators of essential services also covered by the EU's NIS Directive?
When you think about cyber security, it quickly becomes clear that the entire lifecycle of an important ICT system must be considered. Ultimately, a holistic, systematic approach includes personnel, organisational, infrastructural and technical security measures. It is therefore logical that suppliers, service providers, partners and customers must be taken into account in the security plan.

What protective measures should operators of essential services take from May 2018?
Operators shall take appropriate organisational and technical measures to avoid disruptions to the availability, integrity, authenticity and confidentiality of their network and information systems, components or processes relevant to the functioning of the services they operate. State of the art methods must be employed. The NIS Directive provides for state-of-the-art safety standards. These standards are currently being developed by a working group at the Federal Chancellery.

Who will be responsible for monitoring the measures taken by operators of essential services in Austria?
Operators must provide the Federal Minister of the Interior with appropriate evidence of compliance with the requirements of Para. 1. every two years at the minimum. The Federal Minister of the Interior may inspect the network and information systems and documents to check compliance with the requirements and is authorised to demand measures to establish the safety requirements.
According to the draft NIS law, three NIS authorities will be established for this purpose: one at the Federal Chancellor, one at the Minister of the Interior and one at the Minister of Defence.

>>>

CYBER DEFENCE

Interview with Mag. Walter J. Unger. continued.

What role will the Ministry of Defence play with respect to operators of essential services?
The Ministry of Defence (BMLV) is the NIS authority for all military matters. It has not yet been decided whether the Ministry of Defence will also have responsibility for those operators of essential services that are of particular importance for the task of national defence.

What measures does an operator of essential services have to take in the event of a cyber attack being carried out which affects the critical infrastructure it operates?
In addition to preventive measures for self-protection and defence against ongoing attacks, the operator of essential services must immediately report a security incident to the computer emergency team responsible for it, which immediately forwards the report to the Federal Minister of the Interior.

Of course, a new directive/law will only be taken seriously if there are also penalties for infringements. What penalties can an operator of essential services face if the measures required by the EU NIS Directive are not implemented?
Anyone who refuses to cooperate, to provide information or evidence or to inspect or implement the recommendations, or who fails to comply with the obligation to report security incidents, will face fines of up to EUR 50,000.00 and, in the case of repeated incidents, up to EUR 100,000.00.

Paid contribution

THE HUMAN FACTOR

Key component of Information Security.

Information Security is ubiquitous, not least because of current incidents in the media. The STIWA Group has been investing more and more in the topic of Information Security for decades and uses the competences from Softwarepark Hagenberg.

The STIWA Group is located in Softwarepark Hagenberg with its business units Manufacturing Software, Laboratory Automation and Building Automation. Information Security is particularly relevant for the STIWA Group in these areas as highly sensitive production, plant or patient data are processed with the software solutions of the group worldwide.

Creating consciousness

Globally networked production, which requires fully automated data management and machine-to-machine communication, among other things, requires the processing of large amounts of data. This data can contain confidential information about production processes, part quality and employees for example. Not only fundamental aspects such as network security must be mastered: employees must also develop an awareness of practices such as social engineering and phishing. The STIWA Group understands this not only from the point of view of the software developer for manufacturing automation, but also from the point of view of the plant constructor and the customer: At its headquarters in Attnang-Puchheim, the company manufactures high-performance assembly lines; in Gampern, the STIWA Group uses its production facilities and software to manufacture parts and components for the automotive industry. The holistic approach to Information Security in the company also developed from this comprehensive view on the subject: "The human factor must be taken into account when evaluating the security risks in the production environment as well as security gaps in technical systems," says Alexander Schwarz, Information Security Manager at STIWA.

Comprehensive measures

In order to guarantee the best possible level of data protection, the STIWA Group employs intensive training and further education measures. To this end, the company has developed its own security awareness programme in which regular training courses on the subject raise awareness of possible attacks. In addition, a security guide supports employees in their daily work. Regular newsletters warn of current waves of attacks and increase the workforce's attention to specific topics. If there are current threats, special measures are also communicated. Another part of the current Security Awareness Programme is a specially introduced column for Information Security in the staff newspaper, in which current topics from the area of Information Security are discussed by experts.

www.stiwa.com

Photo: HYWARDS | istock.com

Paid contribution

DISCONSULTING

Data protection and Information Security.

The EU General Data Protection Regulation applies to every company

The new EU General Data Protection Regulation (GDPR) came into force on 24 May 2016 and will come into force on 25 May 2018 under the new Austrian Data Protection Act. This also implements the uniform EU law on the protection of personal and sensitive data in Austria. Specifically, the GDPR prescribes data protection measures for the processing of personal data in the organisational and technical areas according to the state of the art, reporting obligations, regular audits and effectiveness tests. Instead of the DVR notification, the person responsible must provide a list of applications relevant to the GDPR and nominate a data protection officer under certain conditions. Violations of the GDPR could result in severe fines of up to several million euros, regardless of the size of the company. Timely, professional implementation of the GDPR requirements is therefore unavoidable.

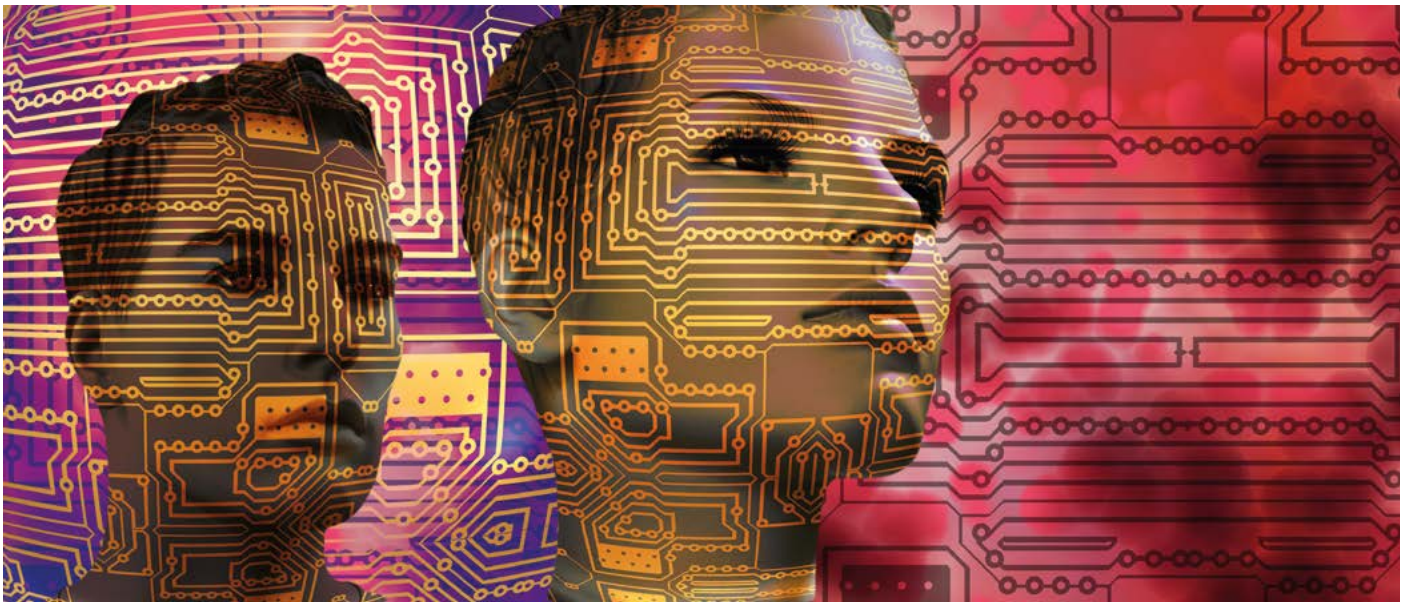
Consulting competence through competent partners

In cooperation with the law firm Prof. Hintermayr & Partner, which specialises in data protection and Information Security law, UNINET assists Austrian companies using the consulting product "DISconsulting - Datenschutz und Informationssicherheit" (data protection and Information Security) to perform targeted analysis in order to identify the obligations of companies with regard to the requirements of the GDPR and to be able to achieve the necessary implementation measures for the protection of personal data and applications. The Information Security/IT Security Part is handled by UNINET's experts, who have many years of experience in the field of ICT/IT Security/Information Security consulting in a variety of projects for SMEs, large corporations and multinational companies. The data protection and Information Security part of the consulting service is provided by the law firm Prof. Hintermayr & Partner, by the IT law expert FH-Prof. Dr. Peter Burgstaller, LL.M. This bundling of technical and legal expertise permits comprehensive coverage of all relevant issues with regard to the requirements of the GDPR.

Data protection and Information Security assessment

The core areas of DISconsulting include collection, which personal data is processed in which applications, the analysis and assessment of risks within the framework of processing, the analysis of existing Information Security measures and which additional technical and organisational measures (data protection-friendly settings, security of processing) are to be implemented. In addition, the legally required measures, such as the maintenance of a processing directory or the information and reporting obligations in the event of data protection incidents, are defined.

www.uninet.at



Paid contribution

TIGHT-KNIT

The security forum for Information Security experts

Photo: jijomathaidesigners | Shutterstock.com

Hagenberger Kreis (HK) is an association of students of the Department of Secure Information Systems of the University of Applied Sciences Upper Austria Campus Hagenberg which currently has approx. 550 members. The association has set itself the goal of improving public awareness of Information Security and remaining in contact with each another even after graduation.

One of the most important events for HK is the Security Forum, where various aspects of Information Security are discussed. Security experts from all over the world meet and present current security topics. The event takes place annually over two days on the campus of the University of Applied Sciences in Hagenberg. Approximately 200 visitors come, mainly from Austria, Germany and Switzerland. The event is organised exclusively by students - they are very proud that the Security Forum will take place for the 16th time on 2 and 3 May 2018.

The event is intended for interested parties with and without security know-how. Both administrators and managers of small and medium-sized enterprises should become aware of the everyday dangers of the IT world and learn how these dangers can be eliminated or circumvented.

The Security Forum consists of two parallel series of previous days, which are oriented towards technology and management. Every year, the Security Forum is distinguished by renowned speakers from all over the world who, as experts in their field, present a variety of aspects of Information Security. These show time and again the effects of Information Security on the digital world. Even the more “exotic” components such as building automation, cars, smart homes and industrial networks are affected. Ten years ago, Information Security did not play a role in these areas, but since Stuxnet, research in the field of industrial security has gained momentum.

Meeting point for security experts

Information Security used to be a mystical "black box", today it is widely known and weak points can be exploited with a mouse click. Tools for hacking industrial plants are now widely available. The way these systems are connected has also changed. They are no longer isolated and their proprietary operation also offers no protection. Today in the age of the "Internet of Things" (IoT) and "Industry 4.0", systems must be able to interact with each other. These systems are closely networked and must be accessible from anywhere. At the same time, their security must be guaranteed. These two opposing requirements will continue to occupy HK in the coming years.

www.securityforum.at

Paid contribution

SECURITY EXPERTS

University of Applied Scienes Upper Austria Campus Hagenberg - Degree courses in security since 2000.

As a trendsetter in the field of secure information systems, the University of Applied Sciences Upper Austria started research and training in 2000 with Information Security. Today, the department "Secure Information Systems" with currently 9 full-time professors and 600 graduates is one of the leading Information Security competence centres in Europe.

Occupying the top places in University rankings

Currently, two technical courses in Information Security and IT Security are offered at the Upper Austria University of Applied Sciences, Hagenberg Campus: Secure Information Systems Bachelor (SIB) and Master (SIM) as well as a part-time international Master's programme Information Security Management (ISM) which offers a solid foundation in Information Security management/data protection for prospective CISOs and data protection officers. Over 170 active students are selected by 9 full-time professors from Information Security & IT Security to focus on network technology and network security, cryptography, system and deployment planning, secure systems operations, malware, secure software design, Information Security management, big data and cloud security, forensic/incident analysis, authentication solutions/smart cards/PKI, secure company organisation/business processes as well as legal/compliance and over 50 business lecturers trained as experts in IT Security (with a focus on technical planning, implementation, operation and QA) and Information Security management (with a focus on ISMS, BCM, CIP, legal/compliance). The 6-semester Secure Information Systems Bachelor (SIB, 180 ECTS) offers sound training as a technical IT Security Professional, the 4-semester Secure Information Systems Master (SIM, 120 ECTS) deepens the training as an expert for Information Security with a research background. The in-service Information Security Management Master (ISM, 120 ECTS) offers in-service training as CISO/CSO/DSB with only 8 weeks of attendance in 2 years and uses innovative teaching and learning methods, such as e-learning with inverted classroom concepts. The department and its degree programmes have been ranked among the best in various university rankings for years. In the 2017 University of Applied Sciences ranking of the industry magazine, the Information Security Management Master immediately took first place among all Austrian IT Management degree programmes as a newcomer. The research group, which is part of the Secure Information Systems department and currently has 8 R&D employees, carries out ongoing research and development projects in close cooperation with the training company in the LABs of the SIM Master for domestic and foreign partners (industry, authorities, organisations, companies). A current highlight in the field of R&D is a project in cooperation with the Federal Chancellery/Cities Federation/Communal Confederation, where a handbook of measures is being developed to implement the Information Security requirements of the EU General Data Protection Regulation for all 2100 Austrian municipalities. Another current R&D highlight is a project with semiconductor sensor manufacturer ams (Graz/Unterpremstetten) in which IT Security protection mechanisms for coupling sensor chips and signal processing software are being developed. With projects in security research, the Department of Secure Information Systems at the University of Applied Sciences Upper Austria Campus Hagenberg has many years of experience, among others in two large FFG KIRAS projects (Cuteforce and Realtime Analyzer). With an R&D acquisition volume of approx. EUR 0.6 million per year, the department plays a major role in ensuring that the University of Applied Sciences Upper Austria is Austria's top research institution for years.

Many years of experience in security research projects

As a TeleTrusT regional office in Hagenberg, the Department of Secure Information Systems also offers international networking within the framework of Germany's largest IT Security industry association, which is based in Berlin and unites the who-is-who of the IT Security industry. The TeleTrusT Hagenberg regional office acts as an Austrian hub between the regional members and the international association, organising regular participation of TeleTrusT in events such as the Security Forum and the ICT Security Conference.

As an annual highlight, the "Hagenberger Kreis zur Förderung der digitalen Sicherheit" (Hagenberger Kreis for the promotion of digital security) (HK), the student association of the department of secure information systems, organises the Security Forum, which is one of the oldest IT Security conferences in German-speaking countries with over 200 (inter)national visitors. The Security Forum will take place this year for the 16th time on May 2-3, 2018 at the campus of the University of Applied Sciences Upper Austria in Hagenberg.

Complete information about the department
Secure information systems
available at **www.fh-ooe.at/si**.

Paid contribution

Studying in Hagenberg

Photo: Vertigo3d | iStock.com

20 Bachelor and Master courses for a career in computer science, communication and media are available at the Hagenberg campus of the Upper Austrian University of Applied Sciences: from software engineering to media design, mobile computing and secure information systems to – completely new – automotive computing and data science.

Practice with a capital P

Students gain valuable practical experience in projects with partners from industry and in professional internships. There are around 100 partner universities worldwide to choose from for a semester abroad.

Study, research & work

In addition to the top-equipped university of applied sciences, the Softwarepark is home to over 75 companies and ten research institutes. The exchange of know-how, projects and internships or jobs benefit the students.

Top career opportunities

In addition to regular high rankings, the FH>>next Career Fair with over 135 exhibitors also shows how just in demand Hagenberg's graduates are. Graduates include founders of successful companies such as managing directors of Runtastic, Tractive, Loxone and Celum.

www.fh-ooe.at/campus-hagenberg

Photo: State of OÖ

Dr. Michael Strugl
Economic Advisor LH-Deputy

"The most important task is to network providers and interested parties – especially small and medium-sized enterprises – in the field of Information Security and data protection. This will also increase the international visibility of Upper Austria and strengthen the regional IT Security industry".

Paid contribution

SECURE SOFTWARE

Analytics and Information Security

Almost every modern technology we use is supported by IT. It is a reality that almost all new devices and machines are IP-based. They thus offer a port to the Internet, including the potential danger of cyber attacks. This also applies increasingly to large industrial production systems which, until recently, were completely isolated from the Internet. Fulfilling rigorous IT Security requirements is the basis for the successful implementation of Industry 4.0 with the vision of a seamless integration of entire value-added chains.

The Software Competence Center Hagenberg (SCCH) has established itself nationally and internationally as an Austrian COMET Centre of Excellence (Competence Center for Excellent Technologies) in close cooperation with Johannes Kepler University (JKU). SCCH's research work, with its two core competencies Data Science and Software Science, provides important impulses for Information Security. SCCH owes its success first and foremost to the close linking of expertise in these two domains and to the fruitful research cooperation with JKU.

For the next 5 years, the team of SCCH scientists has decided to tackle a research topic in the field of Information Security where these two core research competencies can be perfectly integrated, namely "Secure Software Analytics" (SSA). It will be driven not least by the fact that SCCH will be able to use its latest research results and methods from the field of data analytics (together with JKU institutes such as FAW) very profitably for emerging IT Security problems. The results of SSA research will be relevant to almost all software solutions of the future, including data protection and security, in distributed machine learning in cloud environments.

Software solutions for the future

Information Security is also a topic at FAW (JKU Linz - Institute for Application-Oriented Knowledge Processing). Among other things, it deals with access protection and anonymity of information, the balancing act between privacy and the general data evaluation.

The expected results of the work in the field of Secure Software Analytics should lead to new methods and tools for secure and sustainable software engineering in the next 5 years, which go beyond the state of the art. It holistically targets all steps of the transformation process from specification to secure code, including a comprehensive analysis of runtime monitoring.

This cooperative research, planned in close cooperation with industry, is aimed at the needs of the economy, where an increase in productivity in software development should ideally be achieved hand in hand with a rigorous integration of (software) security requirements.

www.scch.at
www.faw.at

Prof. Dr. A Min Tjoa
Software Competence Center Hagenberg GmbH (SCCH), Chief Scientific Officer

Photo: SCCH

"Secure Software Analytics is the indispensable precaution to ensure an intact immune system for Information Security."

a.Univ.-Prof. Dr. Josef Küng
Institute for Application-oriented Knowledge Processing (FAW), Johannes Kepler University Linz, Head

Photo: Private

"Authorisation and access control are central components of Information Security."

Paid contribution

SHOWING THE RED CARD

Limes Security pits their defence against a penetration test. An interview with Peter Panholzer.

Photo: Limes Security GmbH

Why compare football and penetration tests?

Like football, the majority of time that goes into penetration tests is spent in training and tactics, not on the pitch. Because unlike others, we don't just go at it blindly, instead we put a lot of energy into the preparation.

How is this preparation different?

We define goals and non-goals in a kick-off meeting with the customer. This allows us to concentrate on the relevant information and adapt our individual approach to the systems for testing. It is also tactically important for us to carry out a risk analysis with the respective company.

Why is this risk analysis so important?

Generally speaking, simply identifying technical errors is not sufficient. You also need to know your architectural and procedural weaknesses. Therefore, understanding the entire system with all its data flows and interfaces is of primary importance. Then we consider what things can happen and what the effects would be. Based on the data, concrete attack routes and threats are finally identified. If countermeasures already exist, they should of course be employed.

Like footballers you spend a lot of time on training and tactics, how does that help you with the test itself?

The knowledge gained from the risk analysis enables us to test specifically and efficiently for weak points, though we also use standards such as ISO 27000 or IEC 62443 to guide us. For the test itself, we rely on recognised testing tools and we also implement our own if required. We also stay in constant consultation with system administrators to ensure that they are able to react quickly to results. However, our team is excellently prepared for tests on critical systems and plants due to our extensive experience in the industrial sector.

So, a penetration test is like a football game, where you deliver peak performance in a short time to identify defensive gaps?

Exactly. In order to prioritise the identified attack paths, we evaluate the gaps we find using CVSS. We then recommend economically sensible countermeasures. The results are presented as a report which contains both a management summary and a detailed description for the technicians. This gives our customer the opportunity to remedy the weak points found themselves or with the help of our experts.

Is everything complete after the analysis?

No. It is absolutely essential to repeat penetration tests in order to stay up to date. What's more, regular training helps to increase the security level in the company.

www.limessecurity.com

Photo: Limes Security GmbH

Peter Panholzer, MSc

Managing Director, Limes Security GmbH

> “In contrast to football, security is a game with no rules.”

Paid contribution

ON EVERYBODY'S LIPS

The EU General Data Protection Regulation will enter into force on 25 May, 2018.

The first Data Protection Act came into force in Austria in 1980. Data protection is therefore a relatively new field of law. It has so far received a manageable amount of attention among both entrepreneurial and media minds. This will change from 25 May, 2018, when much stricter rules and obligations will come into force.

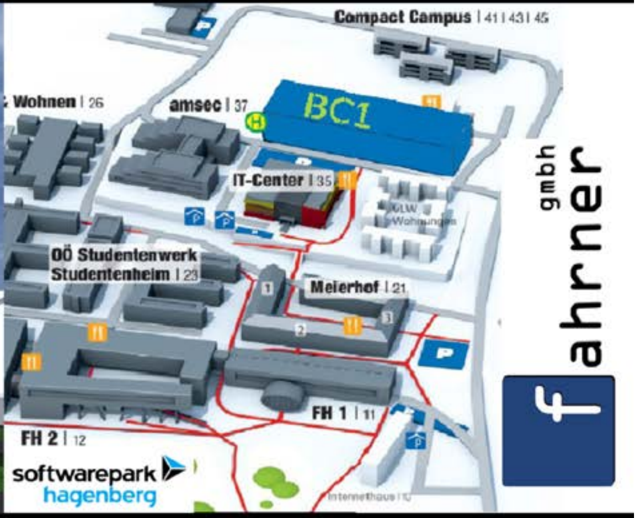
Technological progress, the sometimes careless handling of data, the passion for collecting that companies have and the desire to draw conclusions automatically from the flood of data on the purchasing habits of customers – all this was considered by the European Commission in order to establish a uniform and high level of data protection throughout Europe. The result of these efforts is the basic EU General Data Protection Regulation.

The topic of data protection goes hand in hand with technical and organisational measures to guarantee a level of protection and make it demonstrable to third parties. That is why the IT cluster with the Information Security Network (ISN) has committed itself to the topics of information security and data protection.

The ISN carries out educational work and imparts the appropriate and sensible handling of the new regulation using experts. In addition, companies looking for solutions to their challenges can take advantage of free orientation assistance.

www.itcluster.at

ITC IT CLUSTER



2018 HIGH LIGHTS

2

8 FEBRUARY 2018
Kick-off event for the Softwarepark Hagenberg
event series on Information Security
University of Applied Sciences Upper Austria Campus Hagenberg

4

13 APRIL 2018
Long night of research 2018
IT-Center, amsec IMPULS

5

2-3 MAY 2018
Security Forum 2018
University of Applied Sciences Upper Austria Campus Hagenberg

6

21 JUNE 2018
2nd event of Softwarepark Hagenberg
IT expert series Information Security
amsec IMPULS

7

16-18 JULY 2018
Kids Uni Hagenberg
University of Applied Sciences Upper Austria Campus Hagenberg

8

15-31 AUGUST 2018
European Forum Alpbach 2018
Alpbach, Tirol
For dates go to www.alpbach.org

10

16-17 OCTOBER 2018
IKT-security-conference 2018
Congress Center Alpbach, Tirol

18 OCTOBER 2018
Fh>>next Career Fair for IT and media
University of Applied Sciences Upper Austria Campus Hagenberg

11

22 NOVEMBER 2018
3rd event of Softwarepark Hagenberg
IT expert series Information Security
Hagenberg Castle

+

MANY MORE EVENTS
www.softwarepark-hagenberg.com/veranstaltungen

IMPRINT & DISCLOSURE IN ACCORDANCE WITH § 25 MEDIA ACT
Purpose: Information on current developments in the IT industry. The magazine is published annually. Softwarepark Hagenberg is an initiative of the Province of Upper Austria and a spin-off of the Johannes Kepler University. Softwarepark Hagenberg is run by Business Upper Austria - OÖ Wirtschaftsagentur GmbH.
Media owner (issuer) and publisher: Business Upper Austria – OÖ Wirtschaftsagentur GmbH, Address of the editorial office: Hauptstraße 90, 4232 Hagenberg, Telephone: +43 7236 3343 0, Fax: +43 7236 3343 590, email: office@softwarepark-hagenberg.com, www.softwarepark-hagenberg.com. Responsible for the content: DI (FH) Werner Pamminger, MBA. Editorial office: Dr. Sonja Mündl. Graphics layout: Agency Sara Aschauer, MA, BSc, www.sarai-creations.com. Photographic material: Title image: jijomathaidesigners/Shutterstock.com. All of other images, unless otherwise stated. Softwarepark Hagenberg. Guest contributions may not necessarily reflect the opinion of the publisher. Attached documents are paid information services produced by Softwarepark Hagenberg for its partners. Despite careful preparation, all information is provided without guarantee; liability is excluded.

Grammatical gender has been avoided for an easy reading experience. Any formulations include both genders.