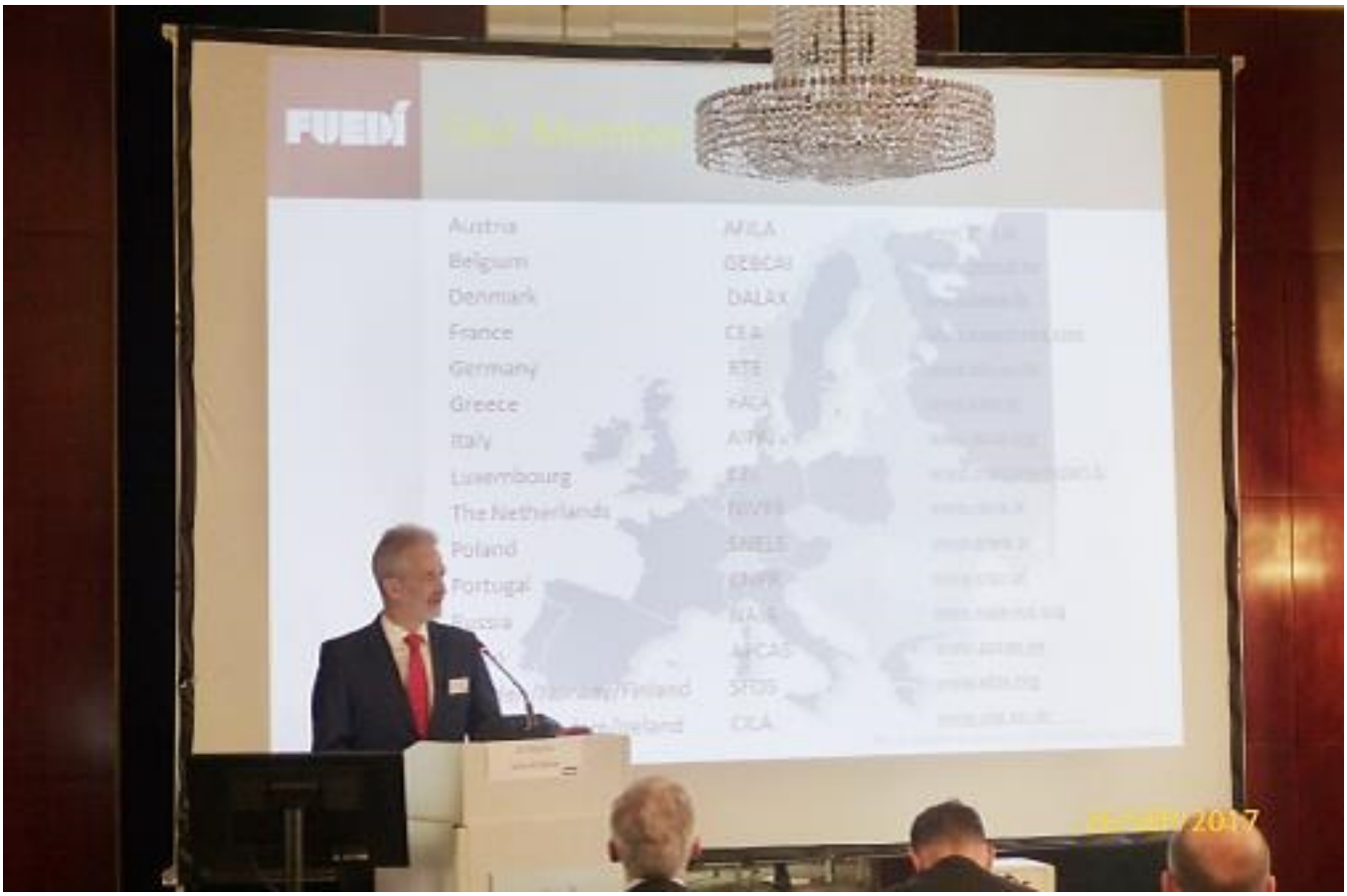
FUEDI

NEWS



LOSS ADJUSTERS VS. AUTHORISED EXPERTS – QUO VADIS?

At the end of September, the international FUEDI conference took place in Vienna amid great interest. Around 90 participants listened to the presentations of the top speakers invited. Martin Schörkhuber, the chairman of AFILA and president of FUEDI, is very satisfied with the lively participation.

In his opening speech, the industry expert discussed in detail the topic „Loss Adjusters vs. Authorised Experts - where is the European insurance industry going „. In the following interview, Martin Schörkhuber revisits the cornerstones of the conference and asks himself how the merging of loss adjusters and experts might be in the future.

AFILA News: What were the main topics of the FUEDI Conference?

Martin Schörkhuber**:** One main topic was: „What can we, as experts or loss adjusters, do for the insurance industry and how can we better present ourselves on the market?“ We also discussed how the job description could be better presented at the European level. I gave an insight into the different situations in different countries to show that it is important to create a high European level.

What is your approach?
There are very good local systems in each country. Due to the international business, it is important for there to be uniform certifications and quality standards. These should be distributed and made known in the insurance industry and among customers. We simply must push development here!

Would the „Doku Tool“ presented at the FUEDI conference be an opportunity to work uniformly in the future?
Martin Schörkhuber: This tool affects certain areas and is used for major or prolonged losses or construction projects. It‘s about using more IT and also working with mobile solutions. Also, that it can be accessed by several people, resulting in teamwork and ultimately the client or insurer is provided with understandable documents. That is the essence of „Doku Tool“.

More EDP also means that you have new attack surfaces. Keyword cyberrisks. How sensitive is such data?
Very sensitive, because it often affects personal space. But also company-internal premises are shown. This opens areas that nobody wants to make public.

In Austria, Loss Adjuster Experts are known more as experts. How different is the profession in Europe?
What is known as Loss Adjuster in England is known as Loss Adjusting Expert here. A very long and complicated name. There are differences in every language, but most of the time internationally Expert or Loss Adjuster remains, even though it is actually more an expert, who is also familiar with the insurance industry. Thus, the

task is actually a combination of both fields, which are handled by a single person in the settlement of claims. This sector is not really perceived as such in public. Except in the Czech Republic, where certification as a loss adjuster is available. The way in continental Europe will, in my opinion, be that it will be dealt with more on the basis of expert.

Has this complexity developed, or has it always been so extensive?
Martin Schörkhuber: Due to technical developments, it used to be easier. Also, the business was not yet so internationally interdependent. Today, the overall developments are simply necessary. Think of big companies that are represented somehow in all countries. Of course they want cases of loss to be well handled in all countries.

Will it be easier in the future due to the efforts of a common chamber?
Martin Schörkhuber: Things are changing, business and the economy are changing as well. Keyword Industry 4.0. Our way of working will change as well.

Does the European Environmental Liability Directive also play a role?
Martin Schörkhuber: Losses are getting bigger and bigger. Therefore, more and more demands are made for the original state to be restored as quickly as possible. That is what this directive is for.

Experts meet at the FUEDI conference. What can the individual persons, apart from specialist input, take along with them?
Martin Schörkhuber: It's obvious that everything is becoming more and more networked and extensive. Teamwork plays an increasingly important role, so that everything happens fast enough. Communication has to become faster and faster and still meet high demands. In my view, it's a matter of time. Such conferences make it possible to expand one's network and keep up with the times.

CYBERRISKS - CHALLENGES FOR COMPANIES

Verena Bec www.it-safe.atker is responsible for cybersecurity in the information and consulting division of the Austrian Federal Chamber of Commerce. Among other things, she is responsible for the initiative , the goal of which is to promote IT security in small and medium-sized companies. Verena Becker gave a summary at the FUEDI conference:

Cybercrime
This has now overtaken the lucrative „business" of drug and human trafficking worldwide. In Austria, damage amounting to EUR 1.6 billion to EUR 2 billion is caused annually by digital industrial espionage. 3 out of 4 companies have been victims of cyberattacks in the past 12 months, with the telecom and financial sectors being particularly popular targets. However, it is a fatal fallacy to believe that only large companies are affected. Companies of all sizes and industries need to protect themselves, it can also affect anyone in the private sector. However, often it is not criminal activities that lead to massive problems. The famous defective hard drive, mere misuse, or the notebook which gets forgotten while travelling, lead to far more data loss than cybercrime.

EU Data Protection Regulation
In their own interests companies do well to take appropriate care of their data. However, with the new EU Data Protection Regulation which comes into force next May, massive penalties can also be imposed in cases of personal data breaches. The current data protection law already stipulates that companies have to take appropriate technical and organisational measures to protect their data. Management cannot surrender strategic responsibility, privacy and data security have top priority.

Risk analysis
Ideally, organisations take stock of their IT infrastructure and data, and then conduct a risk analysis. From this, appropriate technical and organisational measures can be deduced.

The classic minimum measures are decent data backup, virus protection, firewalls and security updates. Still one of the most frequently used security measures is that involving passwords. It is necessary to specify that these be suitably complex, be changed regularly and be kept confidential.

To prevent hackers, different passwords must be used for different applications.

Staff training

This clearly shows that in addition to their technical homework, it is imperative for companies to involve every single employee in safety measures. The example of blackmail Trojans shows that simply clicking on a single malware-encrypted e-mail attachment can cause data to be encrypted throughout the network. To prevent such incidents, only targeted and regular staff training helps.

Integral process

It is important to understand that IT security is not a one-off project in the IT department, but an integral process that affects the entire company. The good news is that companies can protect themselves from most risks with a few basic measures.

How can the Chamber of Commerce help?

The Austrian Federal Chamber of Commerce has been providing practical IT security support for companies for many years with www.it-safe.at. On www.it-safe.at companies can find the following free of charge:

- Online guide it-safe with individual evaluation http://www.it-safe.wkoratgeber.at/
- Checklist for one-man businesses
- Security guide for small and medium businesses
- Safety manual for employees
- Short videos
- Blog with current hints

If companies want to get help from an external consultant, they can visit the UBIT Security Experts Group website https://www.wko.at/itsecurity to find a consultant in their area.

Mag. Verena Becker, BSc
Bundessparte Information und Consulting
Wirtschaftskammer Österreich

Wiedner Hauptstraße 63, 1040 Wien

T +43(0)590900-3176
F +43(0)590900-288
od. 113176
E ic@wko.at
W www.wko.at/ic
W www.it-safe.at

SMES IN THE SIGHTS OF CYBERCRIMINALS

Cybersecurity is and remains an important topic, which was not left out at the FUEDI conference. Even though IT security is now accepted as an important competitive factor in virtually all companies, there are still significant security vulnerabilities. Cybercrime has now become a real „economic branch“, says VdS CEO Dr. Robert Reinermann, who also pointed out in his speech at the FUEDI conference that it is often made too easy for attackers. Particularly small and medium-sized companies are a very worthwhile target for digital attacks due to the often weaker protective measures. Incidentally, on average, digital attacks are not noticed until after about 200 days. A conversation with Dr. Robert Reinermann on protective measures, important updates and VdS guidelines.

How exactly do digital attacks work?

Dr. Reinermann: In the ideal case digital access to the company is secured. However, the same applies as for every castle: With the necessary skills and enough time for undiscovered attacks, many security mechanisms can be overcome at some point. Then cyberattackers gain access to customer data, patents, processes, plans and prices. Digital knowledge theft threatens the existence of entire companies! Almost all computers and even many production facilities, which are often digitally maintained or whose utilisation is closely monitored, are now connected via the Internet. This also permits plenty of access to virtually all digitally stored data and digitally controlled processes in companies.

What can cyberattacks do?

It takes time until production processes are optimally set up. During this time, it can happen that the associated IT infrastructure security level is no longer up-to-date. Again and again we hear from production managers that important security updates were not installed, because the few minutes to import them, and particularly the often necessary system restart, disrupt operations too much. The VdS cyber risk assessments show far too frequently: particularly automation systems which operate 24/7 have not seen an update for a long time. The digital gates are thus wide open to all cybercriminals.

So updates protect?

Without regular updates, even semi-competent hackers can easily gain access. Minimal programme sabotage is enough and already the attacked company can no longer work and consequently no longer deliver.

What happens exactly?

Not even special cyber skills are required, because countless malware variants are freely available on the Internet. Attack tools can be purchased on the Darknet for a few dollars or bitcoins – and are often even available with a guarantee of success! In addition, there are the well-known viruses and Trojans, huge numbers of which threaten every computer via the Internet.

How can companies protect themselves?

With guideline 3473, „Cyber security for small and medium-sized enterprises (SME)“, VdS has created the first IT security standard especially for medium-sized businesses. And we offer this pragmatic solution on the Internet free of charge. VdS 3473, as well as 3473-1 especially for industrial control systems, contain all relevant information and the usual VdS practical assistance to ensure reliable organisational and technical implementation of information security.

What does VdS 3473 do? How exactly can these guidelines protect SMEs?

The cyber security standard VdS 3473 provides integral basic protection, which should be used comprehensively. In other words: highly exposed IT systems, or those which have „weaknesses that can be exploited via the network“ should be shut off from the rest of the IT infrastructure, e.g. by „limiting network traffic to the minimum necessary for functionality“. In this way companies can

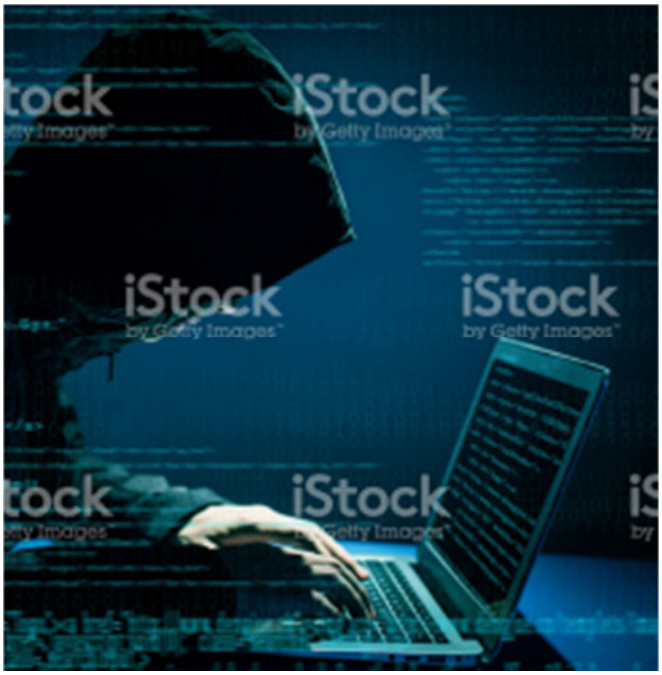
prevent security problems being introduced into their infrastructure.

What about ransomware?

With ransomware, the amount of damage depends on the type and amount of affected company data. In many companies, employees can access directories they do not need for their job, which increases the destructive impact of damaging software. A very simple countermeasure: VdS 3473 calls for structured administration of access and access rights. These are only to be approved „if they are necessary for the task performance of the respective user, or for the company's operational processes". And according to section 7.3, they are to be „promptly checked and adjusted as necessary" when a user's employment is terminated or changed. This will reduce the likelihood that malware introduced through email accounts can cause widespread damage. Very important are also the comprehensive backup guidelines. Locky, Wannacry, Petya and their stronger relatives which are sure to come, can run riot, the damage done is kept within very narrow limits.

What else matters?

Staff training is crucial. VdS 3473 demands that affected personnel be informed about hazards in target groups and instructed how to deal with the security measures. This staff training and sensitization must be planned, monitored and constantly improved. IT security works only if it is integrated in the enterprise. Criminals will always come up with something new - that's why the VdS standard's holistic orientation is so important.



Where do you see the main gateway for cyber criminals?

First and foremost, I would like to mention so-called phishing, in which cyber criminals obtain their victim's personal data via fake websites, e-mails or SMS. But browsers also have some significant weaknesses. The same applies to mobile devices. Companies interviewed by VdS themselves assess the degree of maturity of their IT security in this frequently used area as very critical.

Even more problematic in practice are shortcomings in the integral management approach to cyber security and the IT organisation itself. Both are lagging behind.

So what should be done?

Especially here very little can achieve a lot. Cost-effective and easily implementable little things, as recommended by the VdS 3473 guidelines, can make a very great difference:

Clear IT security policy is very important, including precise specifications for the private use of corporate IT, and especially for external employees - both are serious gateways to cyberattacks. A small step with a big impact is also that administrative access is reserved exclusively for the company's administrators. It is also very important to only grant access to the various areas of IT infrastructure if necessary for the fulfilment of a task. Another good tip is to define the necessary security requirements for every IT outsourcing and cloud computing project. The contract with each service provider should contain precise security requirements and the obligation to fulfil them.

What else is good to know?

Emergency planning and BCM measures are also far below average. In an emergency situation the only thing that really matters is getting the operation up and running again quickly: damage and the loss of business are always insured - but with every additional day of standstill due to destroyed systems, even the most satisfied customers will inevitably migrate to the competition. Particularly these uninsurable consequences of cyberattacks are ruining many companies.

Of course, your protection hints are particularly interesting - what recommendations do you have?

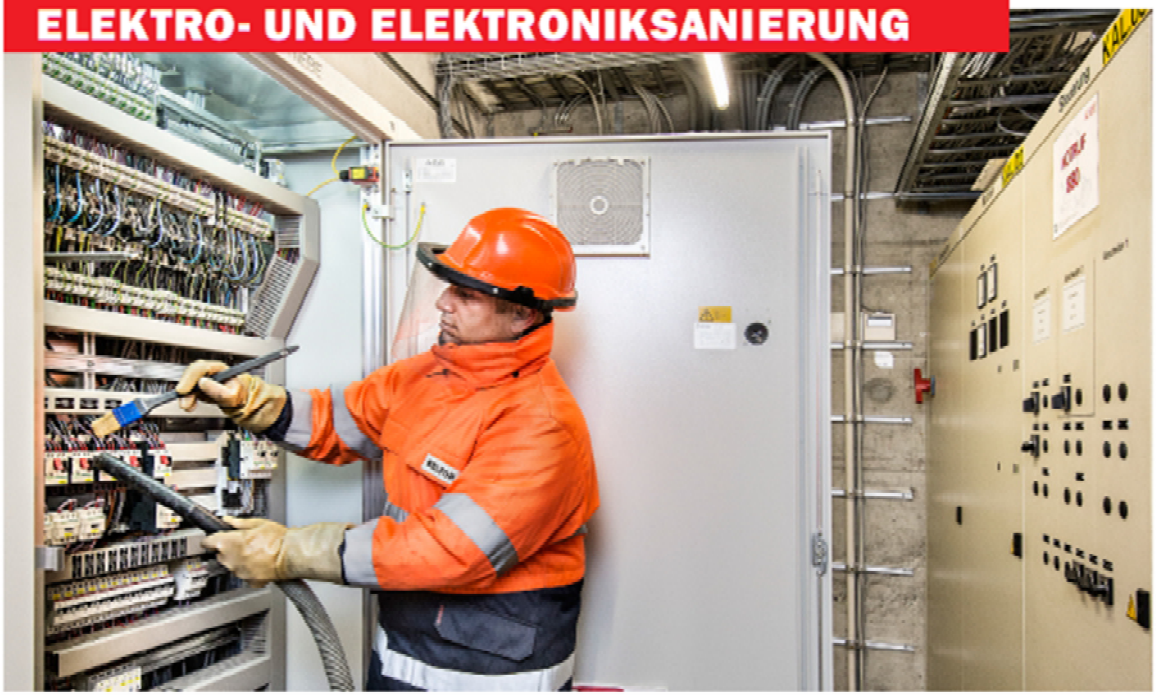
VdS offers a free Quick-Check on the Internet at www.vds-quick-check.de The offer is based on an approximately 20-minute self-assessment check and systematically assesses the security situation in companies with regard to organisation, technology, prevention and management. Thereafter, a compact and detailed report, including a traffic light system, will be prepared for immediate assessment. For all 39 questions, the report provides, where necessary, concrete recommendations for immediate closure of gateways.

BELFOR

SANIERT & ERNEUERT

FACT SHEET

ELEKTRO- UND ELEKTRONIKSANIERUNG



SCHNELLER WIEDER SCHALTEN

SANIERUNG VON ELEKTRONIK UND ELEKTRISCHEN ANLAGEN

SCHALTEN SIE UNS EIN. ZUR SICHERHEIT.

Was tun nach einem Brand? Oder einer Überschwemmung, Explosion oder anderen Katastrophen? Das Wichtigste: Ihr Betrieb muss möglichst schnell wieder ungestört laufen. Mit intakten Büros, Anlagen und Unterlagen.

Dazu brauchen Sie einen erfahrenen Partner – wie BELFOR. Wir haben die Experten und das Wissen, um Ihnen in diesen Fällen zur Seite zu stehen. Mit unserer langjährigen Erfahrung schätzen wir Risiken ab und sind in der Lage, Ihnen schnell und erfolgreich zu helfen.

WAS BELFOR SANIERT - EINIGE BEISPIELE

- Audio- und Videoelektronik
- Anlagen und Geräte für Pharma- und Lebensmittelindustrie
- Computer und Server
- Halbleiterindustrie: Front-End- & Back-End
- Laboranalytik (Prüf- und Messgeräte)
- Lokomotiven und Schiffselektronik
- Luft- und Raumfahrttechnologie
- Medizinelektronik (Therapie und Forschung)
- Prozess-Steuerungen für Fertigung und Überwachung
- Steuerungen für Kernkraftwerke
- Telekommunikationsanlagen