TIDING

MAGAZINE OF BUSINESS HANSE

IT-SECURITY

Alexander Moiseev, Kaspersky:

„Wir wissen, wie groß der Eisberg ist, aber er wächst in alle Richtungen“

“We know how big the iceberg is, but it’s growing in all directions”

MEINUNG/ OPINION

Es gibt keine Alternative zu Europa

There is no alternative to Europe

Deutschland 4,50€
ISSN 2363-8842

9 780201 379624

N° 03
–
NOVEMBER 2015

TREU

treu-kommunikation.de

Marion Köhn
Geschäftsführerin Wirtschaftsbund Hanse
General Manager Business Hanse

Unternehmen in Gefahr?

Die Zahl der Angriffe auf die IT-Sicherheit von Unternehmen ist seit 2009 sprunghaft um 66 Prozent gestiegen. Dies ist das Ergebnis der Global State of Information Security Survey, einer weltweiten Erhebung, die die Beratungsgesellschaft PwC jährlich zusammen mit den Fachmagazinen CIO und CSO durchführt. Der Studie zufolge entstand 2013 weltweit ein Verlust von geschätzten 2,7 Millionen Dollar pro Angriff. Doch nicht nur Unternehmen werden Opfer von Hackerangriffen: Erst im Mai wurde bekannt, dass Trojaner in das IT-System des Deutschen Bundestages eingeschleust und Daten gestohlen wurden.

IT-Sicherheit wird immer wichtiger und immer schwieriger umzusetzen. Da die Angriffe natürlich auch vor Unternehmen der Wirtschaftshanse nicht haltmachen – aktuelle Statements von Mitgliedern lesen Sie ab Seite 25 – beleuchten wir in dieser Ausgabe der „Tiding" das Problem von unterschiedlichen Seiten: Im Interview (Seite 6) erklärt der Europachef von Kaspersky, einem Unternehmen für Cybersicherheit, wie Sie sich schützen können. Der Chaos Computer Club wiederum, der Hackern eine Plattform gibt, betont, es könne keinen 100-prozentigen Schutz geben (Seite 18). Auch die wichtigsten Ergebnisse der PwC-Studie haben wir komprimiert auf Seite 14 für Sie dargestellt.

Ich hoffe, dass wir mit diesem breiten Informationsangebot zum Nachdenken anregen und nützliche Debatten in Ihrem Unternehmen anstoßen. Dazu passen die vielen Interviews, die Ihnen verschiedene Denkansätze aus unterschiedlichen Blickwinkeln näherbringen.

Wenn auch Sie schon Erfahrungen mit IT-Sicherheit gemacht haben, bin ich gespannt auf Ihre Erkenntnisse. Schreiben Sie es uns – ich freue mich darauf! •

Companies at risk?

The number of attacks on corporate IT security has increased by a staggering 66 per cent since 2009. This is the result of the Global State of Information Security Survey that is carried out annually by consulting firm PwC together with the CIO and CSO trade magazines. According to the study, a loss of an estimated $2.7 million per attack was incurred worldwide in 2013. But not only companies are becoming victims of cyber attacks: Just in May of this year we learned that Trojans had been introduced into the IT system of the German Bundestag and data were stolen.

IT security is becoming ever more important and increasingly difficult to implement. Since the attacks obviously do not spare Business Hanse companies, either – current statements of members can be found starting from page 25– we are highlighting the problem from various angles in this issue of "Tiding": In an interview (page 6), the European Head of Kaspersky, a company for cyber security, explains how to protect yourself. Chaos Computer Club, in turn, which is giving hackers a platform, stresses that there cannot be 100 per cent protection (page 18). The main findings of the PwC study are summarised on page 14.

I trust that this wide range of information will encourage you to reflect on your own company's situation and to spark useful debates. The numerous interviews in this issue will introduce you to several approaches from various angles.

If you have already had experience with IT security as well, I am curious to find out about your conclusions. Drop us a line – I look forward to hearing from you! •

Alexander Moiseev

Alexander Moiseev verantwortet seit Juli 2013 als Europa-Geschäftsführer von Kaspersky Lab alle europäischen Niederlassungen. Moiseev begann seine Karriere bei Kaspersky 2006 als Manager Unternehmensentwicklung für Italien und Israel, bevor er 2008 Geschäftsführer für Italien und den Mittelmeerraum wurde. Ab 2011 verantwortete er als Leiter des Bereiches Globale Partnerschaften & Sponsoring die Sponsoring-Projekte des Unternehmens – das größte davon ist die Partnerschaft mit Ferrari, was dem passionierten Rennfahrer besonders gut gefällt.

„Wir wissen, wie groß der Eisberg ist, aber er wächst in alle Richtungen“

* *English article on page 10*

Alexander Moiseev, General Manager Europa bei Kaspersky Lab

Tiding: Der Deutsche Bundestag ist von einem Hackerangriff überrascht worden. Haben virtuelle Angriffe zugenommen oder werden sie im Moment in der Öffentlichkeit nur mehr wahrgenommen?

Moiseev: Tatsache ist, dass es immer mehr und immer ernstere Hackerangriffe gibt, da die Möglichkeiten in einer elektronischen und auf Daten vertrauenden Welt stark zunehmen. Kaspersky Lab entdeckt täglich etwa 325.000 verschiedene Schadprogramme – und das mit zunehmender Tendenz. Viele Unternehmen glaubten eine Zeit lang, sich durch den Einsatz virtueller Server gegen Schadprogramme schützen zu können – etwa indem Software nicht mehr lokal vor Ort, sondern virtuell in der Cloud liegt. Die schlechte Nachricht ist aber, dass die meisten Schadprogramme nicht zwischen physischen oder virtuellen Maschinen unterscheiden und in beiden Umgebungen gleichermaßen zerstörerisch wirken können. Es hat nur die Zahl der Angriffsvarianten erhöht.

Sehen wir nicht nur die Spitze des Eisberges, ist das Problem in Wirklichkeit viel größer?

Wir sehen viele Schadprogramme und wissen über viele Angriffe Bescheid. Es stimmt jedoch, dass eine sehr große Menge immer noch unentdeckt bleibt. Kriminelle sind immer besser ausgerüstet und schaffen es immer häufiger, ihre Taten zu verbergen. Ich wäre daher ausgesprochen überrascht, wenn es nicht weitaus mehr Angriffe gäbe, von denen Unternehmen gar nichts mitbekommen. Aber meiner Meinung nach sehen wir viel mehr als die Spitze des Eisbergs. Es wäre wohl besser zu sagen, dass wir den Eisberg eher aus der Sicht eines Fisches als aus der Sicht eines Vogels sehen. Wir wissen daher ziemlich genau, wie groß der Eisberg heute ist, aber er wächst in alle Richtungen.

Glauben Sie, Unternehmen melden Hackerangriffe den zuständigen Stellen und machen einen Angriff öffentlich oder kehrt man das Problem aus Angst vor der Reaktion der Kunden lieber unter den Tisch?

Ich glaube, dass Unternehmen Angriffe heutzutage häufiger melden, da sie sich des enormen Risikos sehr wohl bewusst sind, wenn sie solche Angriffe nicht melden. Abhängig von der Größe und den Auswirkungen der Angriffe sind Meldungen in einigen Ländern mittlerweile sogar zwingend vorgeschrieben. Ich bin mir aber auch sicher, dass es immer noch Unternehmen gibt, die die Behörden nicht verständigen oder Informationen über einen Angriff verheimlichen. Diesen Firmen würde ich dringend empfehlen, die Auswirkungen zu bedenken, die ein unehrlicher Dialog mit den Stakeholdern hat. Wenn man bedenkt, dass die meisten Unternehmen vom Vertrauen und Wohlwollen ihrer Kunden leben, kann eine Aushöhlung dieses Vertrauens schlimmere Auswirkungen haben als die Meldung eine Angriffs. Insbesondere bei bekannten Unternehmen besteht die Gefahr, dass ein Angriff trotz aller Geheimhaltung an die Öffentlichkeit gelangt. Um ehrlich zu sein, kann ich mir nicht vorstellen, wie ein Unternehmen damit langfristig durchkommen kann.

Vom Sicherheitsaspekt heraus können wir uns gegen Angriffe umso besser schützen, je mehr wir wissen und je mehr Informationen wir über Angriffe und Hacks teilen. Letztlich dient es nur den Interessen der Internetkriminellen, wenn wir Angriffe unter den Teppich kehren, und setzt andere Unternehmen (und deren Kunden) weiteren Risiken aus.

Was können Unternehmen tun, um sich wirklich zu schützen?

Der beste Schutz besteht darin, es allen Möchtegern-Angreifern unglaublich schwierig zu machen. Dies erreicht man durch mehrere Sicherheitsstufen: Schutz von Endgeräten, Patch-Management, mit dem Sicherheitslücken in Programmen und Betriebssystemen automatisch geschlossen werden,

Anwendungskontrolle, Verschlüsselung, mobile Sicherheit und natürlich Netzwerkschutz sowie eine solide Verteidigung an der Grenze, also eine Firewall.

Darüber hinaus müssen Führungskräfte und Mitarbeiter kontinuierlich fortgebildet werden, weil die überwiegende Mehrheit der Angriffe auf menschlichen Fehlern oder Fahrlässigkeit beruht. Und wenn es einem mit der Sicherheit seines Unternehmens ernst ist, sollte man Sicherheits-Dienstleistungen und Analyse-Tools nutzen, um Probleme zu stoppen, bevor sie beginnen. Außerdem sollte ein guter Sicherheitsbeauftragter eingestellt werden, dessen Ratschläge und Empfehlungen auch befolgt werden sollten.

Ziel ist es, das eigene Unternehmen zu einem wirklich frustrierenden Ziel für Angreifer zu machen, die auf den ersten Blick erkennen sollen, dass sie nicht genug Zeit, Geld, Wissen und Geduld haben, um hier reinzukommen. Angreifer sollen möglichst schnell das Interesse verlieren und – das klingt jetzt negativ – das Unternehmen als „zu schwierig" einstufen und sich andere Ziele suchen.

Wissen Unternehmen überhaupt, welche ihrer Daten Schutz brauchen und welche nicht?

Wahrscheinlich nicht. Das IT-Marktforschungsinstitut Gartner schätzt, dass 80 bis 90 Prozent der Daten in Unternehmen unstrukturiert in Datenbanken liegen und deshalb oft weniger gut geschützt sind.

Wenn Sie das mit Schätzungen kombinieren, nachdem sich das weltweite Datenvolumen bis 2020 um das 1.000-Fache erhöht, malt dies ein ziemlich düsteres Bild. Sollte dieses Szenario Wirklichkeit werden, müssen Unternehmen einstufen, welche Daten vertraulich sind und Schutz benötigen (wahrscheinlich ein weitaus geringerer Prozentsatz, als dies derzeit standardmäßig erfolgt) und welche Daten weniger privat sind. Darüber hinaus müssen wichtige Daten zukünftig wahrscheinlich auf einem viel höheren Niveau geschützt werden als heute, da sie für Angreifer sicher noch interessanter werden. Kurz gesagt: Der Einsatz wird viel höher werden.

Wenn dies tatsächlich in den nächsten fünf Jahren so kommt, werden Unternehmen gezwungen sein, ihre Datenschutzstrategien zu überdenken. Mit anderen Worten: Wer sich derzeit noch nicht bewusst ist, welche Daten Schutz brauchen und welche nicht, wird es bald sein müssen.

Kennen IT-Dienstleister in Europa sich mit der Abwehr von Hackerangriffen aus?

Es ist unglaublich schwierig, diese Frage zu beantworten, da es wirklich vom jeweiligen Unternehmen abhängt und wo dessen individuelle Prioritäten liegen. Es gibt so viele Faktoren: die Unternehmensgröße, die Industrie, in der man tätig ist, die Art, wie man IT verwendet. Dann kann es von den handelnden Personen und deren Blick auf das Thema abhängen. Firmen mit Führungsteams und Gremien, die ein höheres Sicherheitsbewusstsein und mehr Respekt für die Rolle des Sicherheitsbeauftragten haben, werden natürlich besser gerüstet sein. Leider erkennen zu viele Unternehmen die Bedeutung von IT-Sicherheit, Erhaltung und Pflege so lange nicht, bis sie ein Opfer werden.

Welche Qualifikation muss ein interner IT-Sicherheitsmann aufweisen?

Ich bin nicht sicher, ob ich darauf eine gute Antwort habe. Es kann je nach den Bedürfnissen des Unternehmens und der besonderen Rolle/Jobbeschreibung unterschiedlich sein. Ein interner IT-Sicherheitsmann muss auf jeden Fall zukunftsorientiert und anpassungsfähig sein und die Fähigkeit besitzen, unter Druck ruhig und rational zu arbeiten.

Sollte man interne Lösungen suchen oder externe Unternehmen beauftragen?

Ich kenne nicht allzu viele Unternehmen, die die Ressourcen und/oder das Know-how haben, um ihre Sicherheitslösungen selbst zu entwickeln. Zwar können Teile einer IT-Lösung intern konstruiert werden, aber in der Regel verlassen sich Unternehmen auf externe Anbieter, um auf verlässliche Expertenlösungen zugreifen zu können.

Was kostet es, einen effektiven Schutz aufzubauen?

Die Kosten können stark variieren. Es gibt keine 100-prozentig effektive Lösung und kein einzelnes Produkt, das die Sicherheit eines Unternehmens gewährleisten kann. Es gibt einen neuen Denkansatz, der besagt, dass unsere Definition von IT-Sicherheit neu definiert werden sollte: dass nicht alle Bedrohungen abgewehrt werden können, dass aber Daten nicht gestohlen und Verluste auf ein Minimum reduziert werden.

Gibt es Schätzungen über die Schadensummen, die einem Unternehmen entstehen können?

Das hängt von der Art des Angriffs ab. Wenn es sich zum Beispiel um eine einfache Distributed Denial of Service (DDoS) Attacke handelt, die Ausfallzeiten, aber keinen Datenverlust verursacht, kann wirklich nur der Umsatzverlust gemessen werden. Ich muss allerdings zugeben, dass es auch einen Imageschaden geben kann, der jedoch nicht wirklich messbar ist. Wenn Angreifer andererseits in der Lage sind, Millionen von Dollar von einem Unternehmen zu stehlen, könnten die Kosten astronomisch sein.

Auf jeden Fall haben wir in Analysen errechnet, dass es zwischen 50.000 US-Dollar bis zu vielen Millionen kosten kann, wobei die durchschnittlichen Kosten einer Datensicherheitsverletzung in einer großen Organisation auf 1,6 Mio. US-Dollar geschätzt wurden.

Gibt es überhaupt echten Schutz oder sind die Hacker immer einen Schritt weiter?

Es gibt proaktive Ansätze, aber Tatsache ist, dass ein Großteil der Forschung und daraus resultierende Maßnahmen als Reaktionen erfolgen. Wenn man sich vor Augen hält, dass Hacker Kriminelle sind, die online arbeiten – und dass wir Verbrechen niemals vollständig ausmerzen werden – macht es keinen Unterschied, ob die Täter im Internet arbeiten oder durch die Straßen streifen. Die Kunst besteht darin, die Sicherheit auf ein Niveau zu bringen, das als starkes Abschreckungsmittel für Kriminelle wirkt. Stellen Sie es sich so vor: Ich kann nicht garantieren, dass in meinem Haus nicht eingebrochen wird, wenn ich abends unterwegs bin. Dennoch sperre ich die Tür zu, schließe die Fenster, ziehe die Vorhänge zu, mache das Außenlicht an und aktiviere meine Alarmanlage. Ich mache es schwer für Kriminelle, mich zu berauben, und sende ihnen eine klare Botschaft: „Es wird nicht einfach sein – such' besser anderswo."

Kritische Stimmen warnen davor, Ihre Software oder die der US-amerikanischen Konkurrenz zu nutzen, da die Geheimdienste der entsprechenden Länder dann direkt und einfach auf die so geschützten Computer zugreifen könnten. Was antworten Sie Ihren Kritikern?

Es ist eine abgedroschene und, um ganz ehrlich zu sein, grundlose Geschichte. Kaspersky Lab ist eine unabhängige, globale Organisation mit Büros in Europa, Amerika, dem Nahen Osten, Afrika und dem asiatisch-pazifischen Raum. Wir sind derzeit in 200 Ländern und Regionen weltweit tätig und haben mehr als 270.000 Firmenkunden.

Unsere Mission ist es, alles und jeden vor jeder Bedrohung zu schützen – weltbekannte Unternehmen wie Ferrari ebenso wie Ihren lokalen Autohändler um die Ecke. Wir beraten Regierungen in Europa und im Rest der Welt und arbeiten regelmäßig mit Strafverfolgungsbehörden und größeren Exekutivbehörden wie Interpol und Europol zusammen – mit beiden pflegen wir formelle Partnerschaften. Ich glaube nicht, dass jemand weitere Argumente braucht. •

Kaspersky Lab

Kaspersky Lab ist das weltgrößte privat geführte Unternehmen für Cybersicherheit und schützt nach eigenen Angaben zurzeit mehr als 400 Millionen Nutzer in rund 200 Ländern. Laut IT-Marktforschungsunternehmen IDC zählte Kaspersky 2014 zu den vier erfolgreichsten Anbietern von IT-Sicherheitslösungen für Privatkunden.

Kaspersky Lab is the world's largest privately held enterprise for cybersecurity and by its own account currently protects over 400 million users in some 200 countries. According to IT market research firm IDC, Kaspersky ranked among the four most successful providers of IT security solutions for private customers in 2014.

Alexander Moiseev

Alexander Moiseev was appointed Kaspersky Lab's Managing Director Europe in July 2013, taking responsibility of all European offices. Alexander joined Kaspersky in 2006 as Business Development Manager for Italy and Israel, before being appointed Managing Director for Italy and the Mediterranean in 2008. Since 2011, he has worked as Head of Global Partnerships and Sponsorships with responsibility for the company's sponsorship projects, the biggest of which is the partnership with Ferrari, much to the delight of the avid race driver.

"We know how big the iceberg is, but it's growing in all directions"

Alexander Moiseev, General Manager Europe at Kaspersky Lab

Tiding: The German Bundestag has been surprised by a hacking attack. From your perspective, have virtual attacks increased or are they only perceived more in the public and discussed more in the media at the moment?

Moiseev: The reality is that the increased opportunities presented by an ever more digital and data-reliant world means cyber-attacks are increasing in volume and severity. In fact, Kaspersky Lab is now detecting 325,000 unique malware samples daily, and this is increasing all the time. The bad news for organisations that believe that they can escape attacks by implementing virtualization is that most malware does not discriminate between physical or virtualized machines and can be equally destructive in either environment.

Are we only seeing the tip of the iceberg? Is the problem actually much bigger?

We can see the majority of malware, and we know about the majority of attacks taking place, but it's true that there is still a very large amount of malware and a large number of attacks that remain undetected. Criminals are getting more advanced and better at hiding their work. So I would be hugely surprised if there weren't more attacks taking place that companies are completely in the dark about. But realistically, I think we can see much more than the tip of the iceberg. It would be more accurate to say that we are seeing the iceberg from the fish's point of view, as opposed to the bird. So we have a pretty good handle on how big that iceberg is, but it's definitely growing in all directions.

Do you think companies report hacker attacks to the competent authorities and make attacks public or is the issue rather kept under the table for fear of customer reaction?

I think companies are nowadays reporting attacks more frequently. I believe the bulk of them understand the huge risk they take by not doing so.

In some countries, depending on the size and implications of the breach, reporting is now mandatory. But still, there are organisations out there that I'm sure routinely fail to alert authorities or make information about a breach public. To those organisations, I would strongly recommend that their boards and executives reconsider the implications of failing to have an open and honest dialogue with their stakeholders. When you consider that most organisations live and die by earning the trust and goodwill of their customers, an erosion of that trust can have far worse implications than reporting a breach.

For large and very well-known companies in particular, the risk of the breach being made public, despite their best efforts, is typically quite high. To be frank, I can't see how any business could feasibly get away with it in the long-term.

Purely from a security standpoint, the more we know and share information about breaches and hacks, the better we can protect against future attacks. Ultimately, sweeping attacks under the carpet only serves the interests of the cybercriminals, putting other organisations (and customers) at further risk.

What can companies do to effectively protect themselves?

Right now, the best way to protect your company is to make sure it is incredibly tough for any would-be attackers. You achieve this by implementing multi-layer security – endpoint protection, patch management, application control, encryption, mobile security, and of course network protection and a solid perimeter defence (ie, a firewall).

On top of this, you need ongoing education of your executives and employees because the vast majority of attacks on companies involve some element of human oversight, error or negligence. And if you are serious about your company's security, you should make-use of

intelligence services and predictive analysis tools to stop problems before they start. The final piece of the puzzle is to hire a good CISO, and importantly, listen to their advice and recommendations.

In the end, the goal is to make your organisation a genuinely frustrating target for attackers. You want them to take one look and think … I just don't have the time, money, knowledge, and patience to get past all of this. You want them to lose interest quickly and it sounds bad to say it, but ultimately, you want them to put you in the "too-hard basket" and look elsewhere.

Are companies even aware which of their data need to be protected and which do not?

The answer is "probably not". IT research company Gartner estimates that 80-90% of existing data in organisations is non-structured in databases and therefore often less well protected.

When you combine this with estimates that the volume of data being collected each day in the world will increase up-to 1000 fold by 2020, it paints a fairly bleak picture. If this scenario is true, companies will need to evaluate which data is confidential and needs protection (most likely a lot lower percentage than is currently the norm) and what is of a less private nature. What's more, the data being protected will need to be protected to a much higher level than it is today as it will likely be of greater interest to attackers. In short, the stakes will be much higher.

If this is how it looks in 5 years' time, companies will be forced to rethink their data protection strategies. So if they are not currently aware of what needs protection and what doesn't, they soon will be.

Do IT service providers in Europe know how to defend against hacking attacks?

It's incredibly hard to answer this as it really depends on the organisation and where their individual priorities lie. There are so many factors – their size, the industry they operate within, the way they use IT. Then it can depend on the people within those organisations and their own approach to security. Companies with executive teams and boards that are more security aware and have more respect for the CISO role will naturally be better equipped to defend against hackers. Unfortunately, too many companies don't realise the importance of IT security health and hygiene until they've become a victim.

What qualifications does an internal IT security person need to have?

I don't really think I can provide a good answer for this. It can vary depending on the needs of the organisation and the particular role/job description. They certainly need to be forward-thinking, adaptable and know how to operate calmly and rationally under pressure.

Should companies always be looking for internal solutions or rather hire external providers?

I can't think of too many organisations that would have the resources and/or expertise to develop their security solutions themselves. Admittedly, some parts of a solution can be engineered internally, but generally companies rely upon external providers to source expert solutions they can rely upon.

What does it cost to build up effective protection?

The cost can vary greatly. It should be kept in mind that there is no 100% effective solution, and no single product can guarantee your organisation's security. In fact, there is a school of thought now that says that our definition of "winning" in security should be redefined not as blocking all threats, but ensuring data is not ex-filtrated and losses are kept to a minimum.

Are there any estimates of the amounts of loss that companies may incur?

It depends on the attack. For instance, if it's a simple Distributed Denial of Service (DDoS) attack that causes downtime, but no data leakage, the expense can only really be measured in loss of sales, although I do acknowledge that in some instances there is perhaps a degree of reputational damage (but that's not really measurable). If, on the other hand, the attackers were able to steal millions of dollars from companies, the costs can be astronomical.

In any case, we've done some high-level analysis that suggests it can cost anywhere from $50,000 to many millions, with the average cost of a data breach in a large company/enterprise estimated at $1.6m.

Is there even any real protection or will hackers always be one step ahead?

There are protections that are proactive approaches to security, but the nature of the game is that much of the research and resulting measures for prevention are reactively driven. When you think about it, hackers are simply criminals

operating online … and we will never completely stamp out crime … it's really no different whether the perpetrators are operating online, or prowling the streets. As stated earlier, the trick is to build security to a level that acts as a strong disincentive for criminals. Think of it like this, I can't guarantee that when I leave my home for a night out, it won't be burgled … but I still bolt the door, lock the windows, close my curtains, flick the porch light on and activate my home security alarm. I make it hard for the criminals to rob me and I send them a clear message: "It won't be easy … so you're better off looking elsewhere."

Critical voices warn against using your software or the software of US competitors, since the secret services of the respective countries could then directly and easily access the computers protected by such software. How do you answer your critics?

It's a tired, and to be quite frank, baseless story. Kaspersky Lab is a fiercely independent, global organisation with offices spanning Europe, The Americas, The Middle East, Africa and Asia Pacific. We currently do business in 200 countries and territories right around the world, and have over 270 thousand corporate customers.

Our mission is to protect everyone and everything from every threat. We protect companies of all sizes – some globally renowned like Ferrari, others smaller like your local car dealership.

We are advisors to governments throughout Europe and the rest of the world, and we regularly work alongside local law enforcement agencies, as well as larger LEAs such as Interpol and Europol – both of with which we maintain formal partnerships. I can't see how anyone would need any further convincing. •

Verlust von Geschäftsgeheimnissen kostet bis zu 2,2 Billionen US-Dollar

Investitionen in IT-Sicherheit werden für Unternehmen immer wichtiger

Die Zahlen und Daten auf dieser Seite stammen aus der Global State of Information Security® Survey 2015, einer weltweiten Erhebung der Unternehmensberatung Pricewaterhouse Coopers (PwC) und der IT-Magazine CIO und CSO. Die Umfrage für 2015 wurde von März bis Mai 2014 online durchgeführt: Die Leser der Fachmagazine CIO, CSO und Kunden von PwC wurden per E-Mail befragt. Die Ergebnisse beruhen auf den Antworten von mehr als 9.700 Führungskräften und IT-Verantwortlichen in über 154 Ländern.

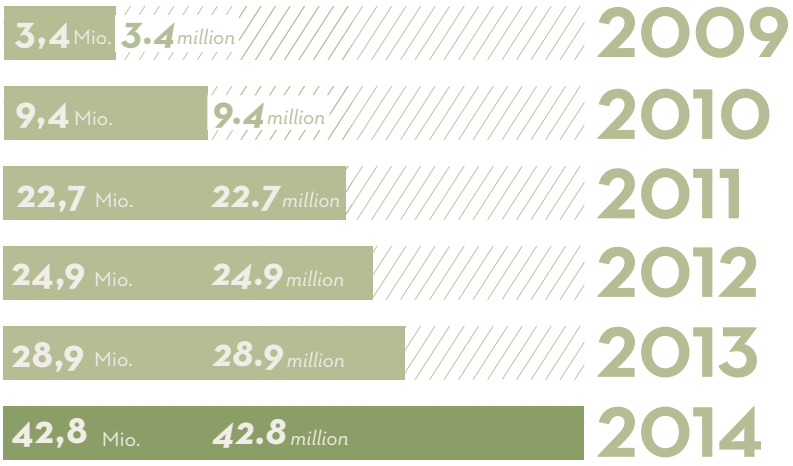
The financial impact of the loss of trade secrets may be up to $2.2 trillion annually

Investments in IT security are becoming ever more important for companies

All facts and figures on this page are from the Global State of Information Security® Survey 2015, a worldwide study of management consulting firm Pricewaterhouse Coopers (PwC) and of IT magazines CIO and CSO. The 2015 survey was conducted online from March 2014 to May 2014; readers of CIO, CSO and clients of PwC from around the globe were invited via e-mail to take the survey. The results are based on the responses of more than 9,700 CEOs, CFOs, CIOs, CISOs, CSOs, VPs and directors of IT and security practices across more than 154 countries.

Die Zahl entdeckter IT-Angriffe ist seit 2009 durchschnittlich jährlich um 66 Prozent pro Jahr gestiegen.

The compound annual growth rate of detected security incidents has increased 66% year-over-year since 2009.



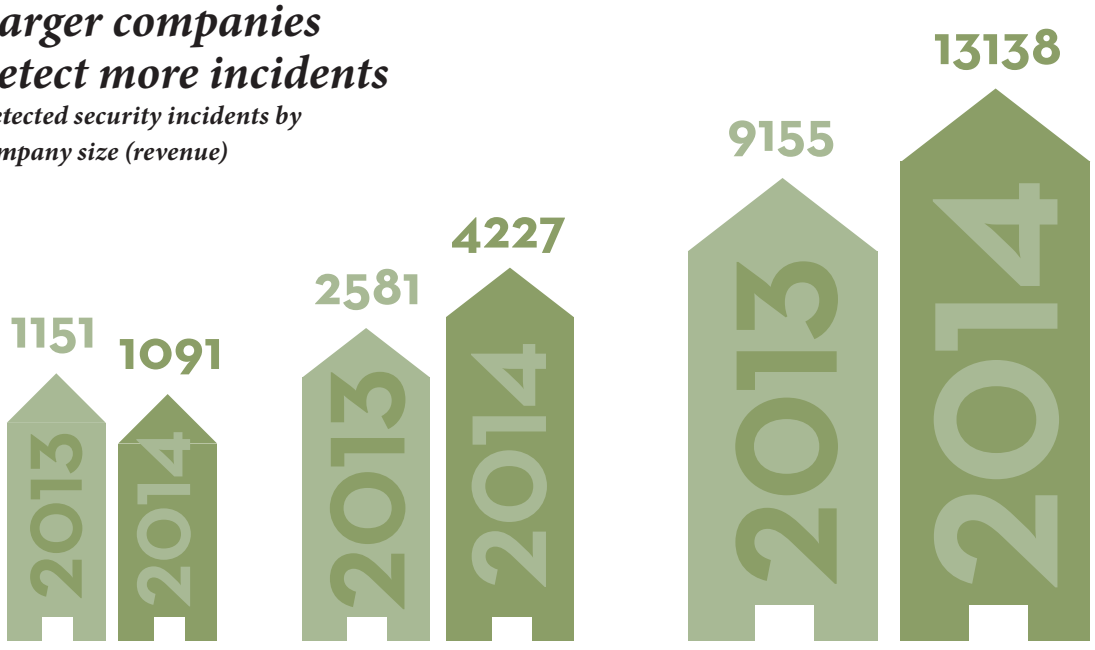
Gesamtzahl entdeckter Angriffe
Total number of detected incidents

Größere Unternehmen entdecken mehr Angriffe

Entdeckte Sicherheitsvorfälle nach Unternehmensgröße (Umsatz)

Larger companies detect more incidents

Detected security incidents by company size (revenue)



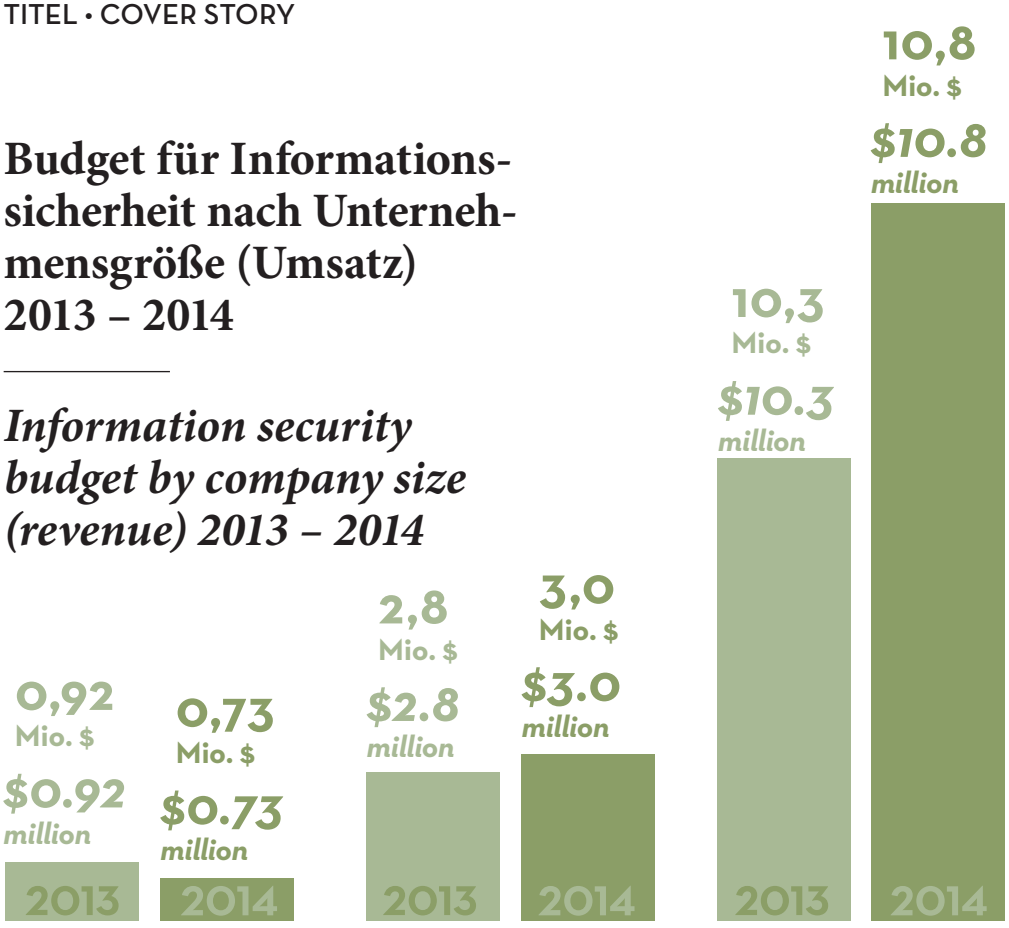
Klein
Umsatz < 100 Mio. US-$
Small
Revenues less than $100 million

Mittel
Umsatz 100 Mio. - 1 Mrd. US-$
Medium
Revenues $100 million - $1 billion

Groß
Umsatz > 1 Mrd. US-$
Large
Revenues more than $1 billion

Budget für Informationssicherheit nach Unternehmensgröße (Umsatz) 2013 – 2014

Information security budget by company size (revenue) 2013 – 2014



Klein
Umsatz < 100 Mio. US-$
Small
Revenues less than $100 million

Mittel
Umsatz 100 Mio. - 1 Mrd. US-$
Medium
Revenues $100 million - $1 billion

Groß
Umsatz > 1 Mrd. US-$
Large
Revenues more than $1 billion

Auf Grundlage der Weltbank-Schätzung des weltweiten Bruttoinlandsproduktes von 74,9 Billionen US-Dollar für 2013 kostet der Verlust von Geschäftsgeheimnissen zwischen 749 Milliarden und 2,2 Billionen US-Dollar jährlich.

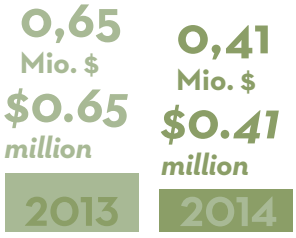
Using the World Bank's annual global GDP estimate of $74.9 trillion in 2013, loss of trade secrets may range from $749 billion to as high as $2.2 trillion annually.

Angriffe verursachen bei größeren Unternehmen höhere Kosten

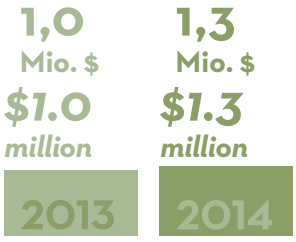
Durchschnittliche finanzielle Verluste durch Sicherheitsvorfälle 2013 – 2014

Incidents are more costly to large organisations

Average financial losses due to security incidents, 2013 – 2014



Klein
Umsatz < 100 Mio. US-$
Small
Revenues less than $100 million

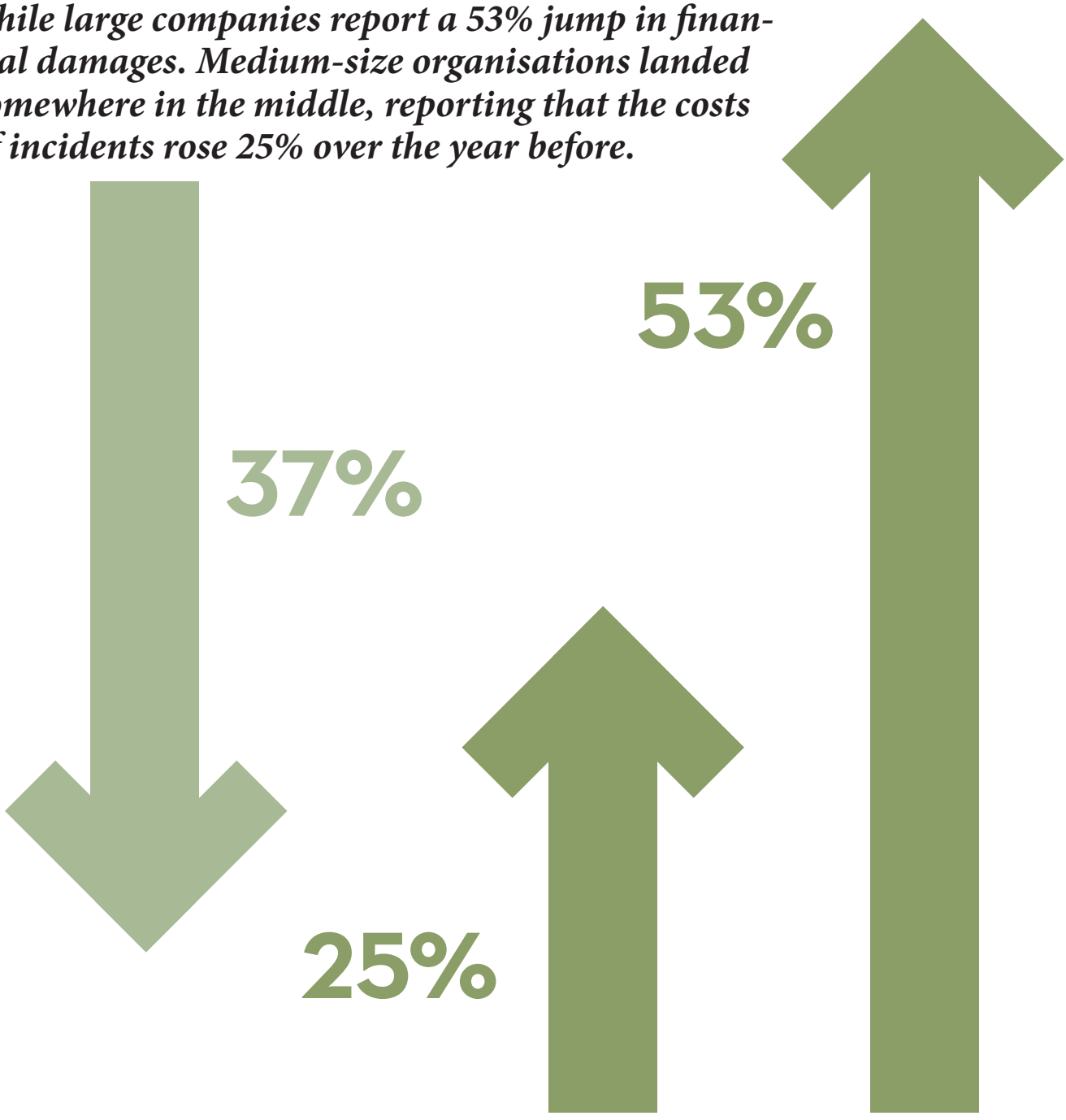


Mittel
Umsatz 100 Mio. - 1 Mrd. US-$
Medium
Revenues $100 million - $1 billion

Groß
Umsatz > 1 Mrd. US-$
Large
Revenues more than $1 billion

Kleine Unternehmen geben an, dass die Kosten, die Angriffe verursachten, im Vergleich zum vergangenen Jahr sogar um 37 Prozent zurückgegangen sind. Bei großen Unternehmen gab es dagegen einen Anstieg von 53 Prozent. Mittelständler landeten dazwischen und gaben einen Kostenanstieg von 25 Prozent gegenüber dem Vorjahr an.

Small companies report that the cost of incidents actually decreased 37% compared with last year, while large companies report a 53% jump in financial damages. Medium-size organisations landed somewhere in the middle, reporting that the costs of incidents rose 25% over the year before.



Dirk Engling

Dirk Engling, 37, studierte Informatik und arbeitet als selbstständiger Programmierer unter anderem an elektronischen Problemlösungen für die Software von Mobiltelefonen, an hoch-skalierenden Netzwerkdiensten und kryptographischen Systemen. In seiner Freizeit arbeitet Engling seit 12 Jahren als ehrenamtlicher Sprecher des Chaos Computer Club und an diversen Projekten als Autor freier Software.

„Hacker kochen auch nur mit Wasser“

* *English article on page 22*

Dirk Engling, Sprecher des Chaos Computer Club, erklärt, wie sich Unternehmen gegen Angriffe schützen können

Tiding: Der Deutsche Bundestag ist von einem Hackerangriff überrascht worden. Überrascht Sie das?

Engling: Die IT des Deutschen Bundestages muss ihr System mit Software-Komponenten aufbauen, die sehr verschieden und von unterschiedlicher Qualität sind. Das macht es für Angreifer leichter. Und dabei kommt es kaum drauf an, ob diese Bestandteile kommerziell hergestellt oder als quelloffene Software verteilt werden. Angriffe auf fast jede Art von Software wurden in den vergangenen Jahren festgestellt. Es gibt immer wieder Schwachstellen, die nach Entdeckung von Sicherheitsforschern oder Hobbyisten nicht den Herstellern gemeldet wurden und dann teilweise auf dem Schwarzmarkt gehandelt werden. Selbst eine auf Computereinbrüche spezialisierte Firma wie das „Hacking Team“ aus Italien wurde im Sommer 2015 kurzfristig von Unbekannten übernommen. Dies zeigt, dass selbst die Spezialisten Schwierigkeiten haben, ihre Systeme zu sichern. Man muss ferner sehen, dass gerade die IT des Bundestags mit gewählten Vertretern des Volkes konfrontiert ist. Diese wollen sich im Zweifel ungern einschränken lassen bei dem, was sie mit dem wilden Zoo ihrer mitgebrachten Hardware tun und lassen dürfen.

Wer, glauben Sie, steckt dahinter? Ausländische Geheimdienste oder Hacker, die Lust auf Provokation hatten?

Die korrekte Identifikation des Angreifers ist ein komplexer Vorgang und es ist schwer zu sagen, wer dahintersteckt. Selbst wenn die als Angriff erkannten Netzwerk-Verbindungen von Computern aus Russland, China oder Korea stammen, ist noch lange nicht gesagt, dass es sich dabei nicht nur um gehackte Computer mit gestohlenen Windows-Lizenzen in Baku, einem mit gestohlenen Kreditkartendaten bezahlten Server im Großdatenzentrum in Taiwan oder einem gelangweilten Schüler handelt. Gern wird auch von den Administratoren eines angegriffenen Netzwerks ein Schnellschuss der Art „Die Chinesen waren‘s“ abgegeben, um mit Verweis auf den angeblich übermächtigen Gegner die Schuld an der zu laxen Sicherung des Netzwerks von sich zu weisen. Natürlich ist der Bundestag für einen Hacker ein prestigeträchtiges Ziel. Ist hingegen die großflächige und auffällige Infiltration der IT ein brauchbares Werkzeug für einen Geheimdienst, der etwas auf sich hält? Eher nicht.

Sehen wir nicht nur die Spitze des Eisberges, ist das Problem in Unternehmen in Wirklichkeit viel größer?

In vielen großen und sehr hierarchisch aufgestellten Firmen mit eigener Abteilung für Unternehmenssicherheit gibt es stringente und zentral gesteuerte Vorschriften, was auf Dienstrechnern installiert sein darf. Somit können die Systeme viel strikter abgeschottet werden und Reparaturen für bekannt gewordene Schwachstellen auch unternehmensweit durchgeführt werden. Je kleiner die Firma ist, desto geringer ist jedoch das Budget für die Firmen-IT und das Verständnis für Einschränkungen bei der Benutzung von Computern – wie das Installieren von eigener Software auf Dienstcomputern. Zuweilen verabschieden sich einige Unternehmen komplett vom Betrieb eigener IT-Dienste und nehmen kostenlose, webbasierte Lösungen in Anspruch, für die sie nicht mal einen belastbaren Vertrag im Falle von Nichtverfügbarkeit oder Datendiebstahl haben. Dies ist natürlich unverantwortlich und hat schon einigen Firmen die Existenz gekostet, deren Geschäftsführer sich danach verzweifelt an uns gewendet haben.

Glauben Sie, Unternehmen melden Hackerangriffe den zuständigen Stellen und machen einen Angriff öffentlich oder kehrt man das Problem aus Angst vor der Reaktion der Kunden lieber unter den Tisch?

Es hat sich gezeigt, dass die meisten Kunden recht träge sind und es schon massive Verletzungen von datenschutzrechtlichen Vorgaben braucht, um sie aufzuschrecken. Ein souveräner Umgang mit Datenverlust verbunden mit der Beschreibung von Maßnahmen zur Verbesserung der Situation

hinterlässt meist ein wesentlich professionelleres Bild beim Kunden.

Eine Meldepflicht besteht bereits, wird aber von den meisten Betroffenen nicht befolgt. Hier müssen abschreckendere Strafen für den Fall eines nicht-gemeldeten Angriffs aber noch mal die Bereitschaft erhöhen.

Ich persönlich verwende bei allen Firmen speziell markierte E-Mail-Adressen und Kundendaten, um bei einem späteren Datenverlust die betroffene Firma anhand der aufgetauchten Informationen identifizieren zu können. Hierbei stellte sich heraus, dass erfolgreiche Attacken sehr häufig nicht kommuniziert werden. Für den Kunden ist das ein Desaster, da er sich nicht darauf einstellen kann, dass bestimmte persönliche Daten im Umlauf sind, die wiederum für Identitätsdiebstahl nutzbar sind.

Können sich Unternehmen überhaupt effektiv schützen?

Natürlich gibt es diverse datenschutz-gesetzliche Vorgaben, wie mit der eigenen IT und verarbeiteten Daten von Kunden umzugehen ist. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) ist dabei auch gern behilflich, diese Verpflichtungen umzusetzen.

Eine gute Administration kann sich gegen den überwiegenden Teil der im Umlauf befindlichen und neu bekannt gewordenen Angriffe recht effektiv schützen, wenn die Korrekturen schnell eingespielt und die Systeme regelmäßig überprüft werden. Ein speziell zugeschnittener Angriff hingegen ist auch sehr teuer. 100-prozentige Sicherheit ist nicht herzustellen, aber eine mittelständische Firma kann ziemlich sicher sein, dass ein Konkurrent mit dem Ziel Industriespionage die Ressourcen nicht aufbringen kann. Er wird sich eher Zugang über soziale Kniffe verschaffen, wie dem Überraschungsanruf als angeblicher Systemadministrator, um in den Besitz von Passwörtern zu gelangen.

Hier hat sich als hilfreich herausgestellt, die Angestellten einzubeziehen und sie nicht wortlos mit den als „Gängelungen" wahrgenommenen Schutzmaßnahmen zu konfrontieren. Es gilt, zwischen lähmender Paranoia und fahrlässigem Schludrian maßvoll abzuwägen.

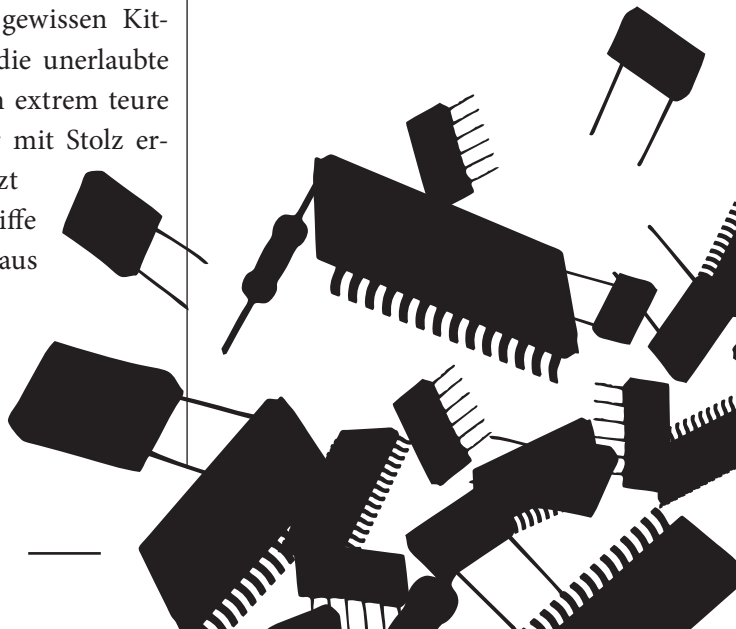
Gehen wir mal weg von den „Opfern" und schauen uns die andere Seite an: Warum hacken Hacker?

Zunächst einmal bedeutet „hacken", einen kreativen und nicht sofort offensichtlichen Weg zu finden, ein Problem zu lösen. Eine Software so zu überlisten, dass sie Dinge tut, für die sie nicht geschrieben wurde, ist auch eine Art „Hack". Diese Konnotation des Worts wurde wegen des gefährlichen Klangs von der Presse dann auch dankbar verbreitet.

Es ist nicht von der Hand zu weisen, dass das Eindringen in Computersysteme auch mit einem gewissen Kitzel verbunden ist und die unerlaubte Kontrolle über zuweilen extrem teure IT-Systeme den Hacker mit Stolz erfüllen kann. Nicht zuletzt erfolgen aber viele Angriffe zum Broterwerb – etwa aus plumpen kriminellen Beweggründen, um Zugangsdaten für Banken auszuspähen – oder im Auftrag von Geheimdiensten, Armeen und Kriminellen, um Wirtschaftsspionage oder Auslandsaufklärung zu betreiben.

Gibt es überhaupt echten Schutz oder sind die Hacker immer einen Schritt weiter?

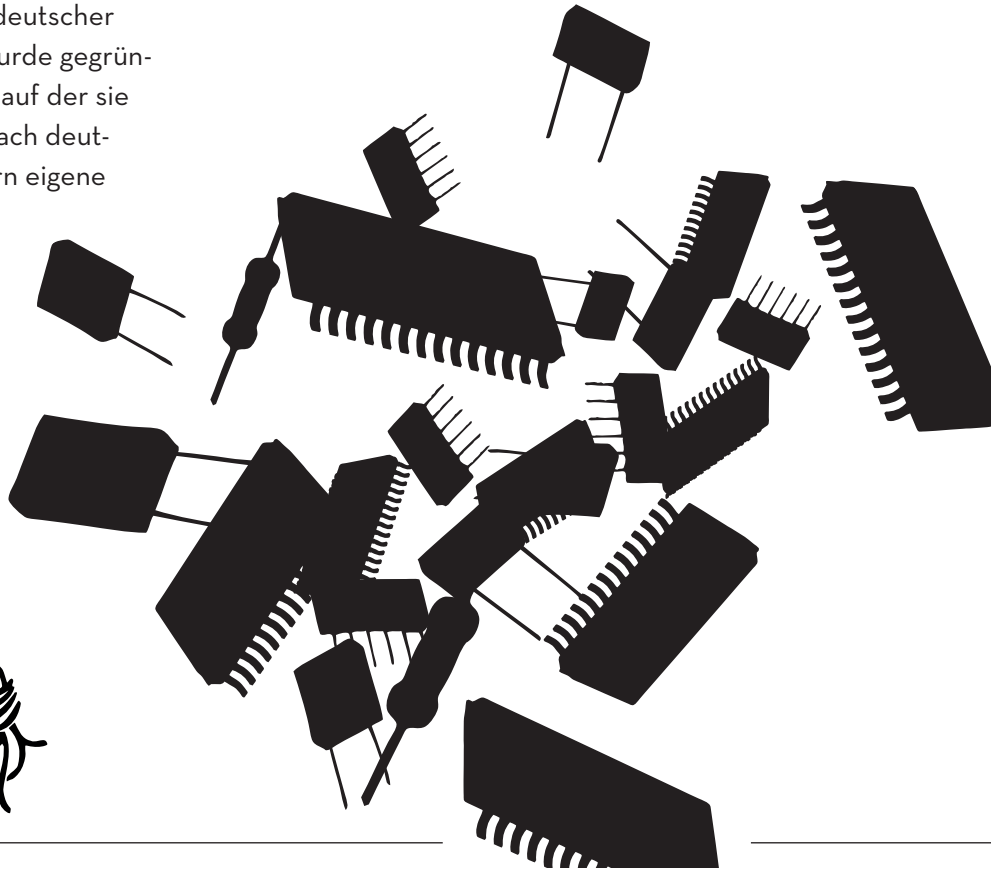
100-prozentigen Schutz kann es nicht geben, allerdings kochen auch Hacker nur mit Wasser und haben keine magischen Fähigkeiten, jedes Computersystem der Welt zu infiltrieren. Die Tatsache, dass viele große Unternehmen ihre IT recht gut unter Kontrolle haben, sollte Hinweis genug sein, dass man mit ein wenig gesundem Menschenverstand benutzbare Systeme hinreichend absichern kann. •



Der Chaos Computer Club (CCC) ist ein deutscher Verein mit knapp 6.000 Mitgliedern. Er wurde gegründet, um Hackern eine Plattform zu geben, auf der sie über ihre Aktivitäten berichten können. Nach deutschem Vorbild haben sich in vielen Ländern eigene Gruppen für Hacker gegründet.

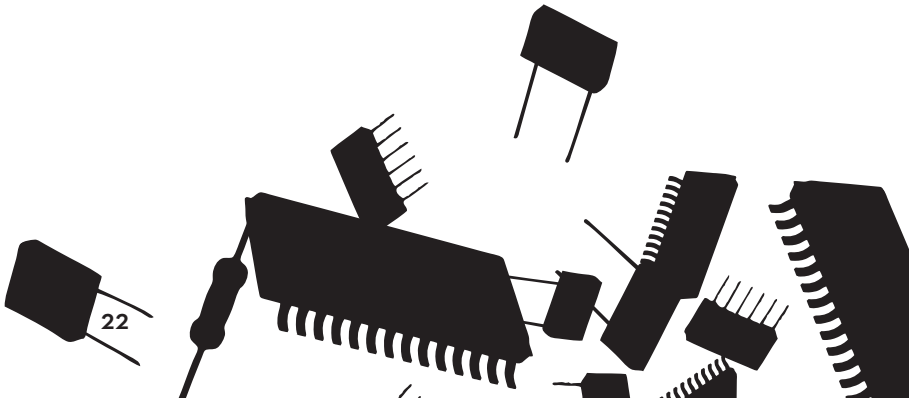
Chaos Computer Club (CCC) is a German association with some 6,000 members. It was founded in order to give hackers a platform on which they can report on their activities. Based on the German model, groups for hackers have been set up in many countries

CHAOS COMPUTER CLUB



Dirk Engling

Dirk Engling, 37, studied computer science and worked as an independent programmer, including on electronic problem solutions for the software of mobile phones, of highly scalable network services and cryptographic systems. In his spare time, Engling worked as voluntary spokesman of Chaos Computer Club for 12 years and on various projects as the author of open-source software.



"Hackers are putting on their trousers one leg at a time"

Dirk Engling, spokesman of Chaos Computer Club, explains how companies can protect themselves against attacks

Tiding: The German Bundestag has been caught off guard by a cyber attack. Does that surprise you?

Engling: The IT of the German Bundestag has to build its system with software components that are very different from each other and of different quality. That makes it easier for attackers. And it hardly matters whether these components are produced commercially or distributed as open-source software. Attacks on almost every type of software were detected in recent years. There are always vulnerabilities that are not reported to manufacturers after their discovery by security researchers or hobbyists and which then may be traded on the black market. Even a firm specialising in computer attacks such as the Italian "Hacking Team" was taken over for a short time by unknown individuals in the summer of 2015. This shows that even specialists have difficulties in securing their systems. It must also be considered that the IT of the Bundestag is confronted with elected representatives of the people. They generally show a reluctance to being restricted in what they can do with the wild zoo of hardware they are bringing along.

Who do you think is behind this? Foreign secret services or hackers who felt like provoking?

The correct identification of the attacker is a complex process and it is difficult to say who is behind it. Even if the network connections of computers used in an attack originate from Russia, China or Korea, it is still a long way from being said that this is not just a hacked computer with stolen Windows licenses in Baku, a server paid for with stolen credit card data in a large data centre in Taiwan or if it is a student who is just bored. Rushing to conclusions such as "It was the Chinese" is also a convenient tactic employed by the administrators of an attacked network, in order to place the blame for too lax network security on the allegedly superior opponent. Of course, the Bundestag is a prestigious target for a hacker. Is the extensive and conspicuous infiltration of the Bundestag IT a useful tool for a self-respecting secret service, however? I would doubt it.

Are we not only seeing the tip of the iceberg? Is the problem in companies in reality much greater?

In many large and very hierarchically organised firms with their own corporate security department, there are stringent and centrally controlled rules on what may be installed on office computers. Thus, the systems can be strictly sealed off and repairs for known vulnerabilities are made company-wide. The smaller the firm is, however, the less budget is available for company IT and the lower is the understanding for limitations in the use of computers – such as the installation of one's own software on office computers. At times, some companies fully outsource the operation of their own IT services and use free, web-based solutions for which they do not even have an enforceable contract in the event of unavailability or data theft. This is of course irresponsible and has already cost some firms their existence, whose managers then desperately contacted us.

Do you think companies report hacker attacks to the responsible authorities and make an attack public or is the problem rather swept under the table for fear of customer reactions?

It has been shown that most customers are quite lethargic and it requires massive violations of privacy law rules, in order to startle them. Confident handling of data loss associated with describing the measures for improving the situation for the most part leaves a significantly more professional image with customers.

While there is a reporting duty, it is not observed by most of those affected. More dissuasive penalties in the event of unreported attacks are necessary to increase preparedness.

I personally use specially marked email addresses and customer data at all firms, in order to be able to identify the firm concerned by means of the information revealed in the case of a subsequent data loss. It turned out that

successful attacks are very frequently not communicated. That is a disaster for customers since they cannot respond to the fact that certain personal data are in circulation, which in turn can be used for identity theft.

Can companies effectively protect themselves at all?

Of course, there are various requirements under privacy law regarding how to deal with corporate IT and processed data of customers. The Federal Office for Information Security will also gladly help to implement these obligations.

Good administration can quite effectively protect against the major part of known and newly discovered attacks if corrections are quickly implemented and systems are regularly checked. A custom-made attack, however, is also very expensive. There cannot be 100 per cent security, but a medium-sized firm can be fairly certain that a competitor with the aim of carrying out industrial espionage will be unable to afford the resources. It will rather gain access through social gimmicks, such as the surprise caller posing as an alleged system administrator, in order to gain access to passwords.

Here it has proven helpful to involve the employees instead of simply confronting them with protective measures perceived as "patronising". It is important to find a moderate balance between paralysing paranoia and being a negligent person.

Let's move away from the "victims" and take a look at the other side: Why are hackers hacking?

For a start, "hacking" means finding a creative and not immediately obvious way to solve a problem. To outwit software so that it does things for which it was not written is also a type of "hack". This connotation of the word was then gladly spread by the press because it sounded so dangerous.

It cannot be dismissed that the penetration into computer systems is also associated with certain titillation and the unauthorised control over sometimes extremely expensive IT systems can fill hackers with pride. But many attacks are not least occurring to earn someone a living – for instance, for crude criminal motivations in order to uncover access data for banks – or on behalf of secret services, armies and criminals in order to conduct industrial espionage or reconnaissance abroad.

Is there any real protection or will the hackers always be one step ahead?

There cannot be 100 per cent protection. Hackers also are putting on their trousers one leg at a time, however, and have no magic capabilities to infiltrate any computer system in the world. The fact that many large companies have their own IT under quite good control should be adequate proof that with a little common sense usable systems can be sufficiently protected. •

Wie schützen Sie Ihr Unternehmen gegen Bedrohungen aus dem Internet?

Fünf Statements aus der Wirtschaftshanse

Five statements from Business Hanse

How do you protect your company against threats from the Internet?

Kay-Uwe Moosheimer
Geschäftsführer MySecondWay, Böblingen/Deutschland
General Manager MySecondWay, Böblingen/Germany

„Als IT-Unternehmen, das eigene Produkte und Dienstleistungen anbietet, ist Security für uns täglich relevant. Gerade in unserem Tätigkeitsfeld – wir beraten Kunden im Bereich Big Data und bieten Predictive Analytics an, bei dem wir mit Analysetools Vorhersagen treffen – ist Cloud Computing ein wichtiges Thema. Die Speicherung und Verarbeitung sehr großer Datenmengen in der Cloud bringt Kosteneinsparungen und damit klare Wettbewerbsvorteile. Jedoch garantiert kaum ein Anbieter, dass außer dem Nutzer wirklich niemand Zugriff hat. Geschäftsprozesse und deren Daten können daher nicht einfach in die Cloud übernommen werden. Wir unterstützen unsere Kunden dabei, sensible Daten in sicheren Bereichen inhouse abzulegen und unkritische Daten in der Cloud zu speichern. Das verändert jedoch die bestehenden Geschäftsprozesse, denn bisher konnte auf alle Informationen sofort und einfach zugegriffen werden. Wenn jedoch sensible Daten nicht von unkritischen getrennt werden können, müssen diese verschlüsselt werden, bevor sie aus dem Unternehmen in die Cloud gelangen. Und bei der Bearbeitung wird ad hoc wieder entschlüsselt. Hier ist es wichtig, Aufwand, Kosten, praktikables Arbeiten und Sicherheitsbedürfnis genau abzuwägen.“ •

“As an IT company offering proprietary products and services, security is relevant for us on a daily basis. Especially in our field of work – we advise customers in Big Data and offer Predictive Analytics – cloud computing is an important topic. For our customers, we are achieving cost savings by storing and processing very large data volumes in the cloud, thus offering them clear competitive advantages. There is hardly a provider, however, that guarantees that really no one has access to the data except the user. It is therefore not possible to simply transfer business processes and their data into the cloud. We support our customers in storing sensitive data in secure areas in-house and in storing non-critical data in the cloud. This, however, changes the existing business processes, since previously all information could be easily and immediately accessed. If, however, sensitive data cannot be separated from non-critical data, they must be encrypted, before they are moved to the cloud. And during processing these data, they will be decrypted again. Here it is important to precisely weigh effort, costs, feasible working methods and security requirements”. •

Jens Deyerling
Geschäftsführer Kreislauf Partner, Münster/Deutschland
General Manager Kreislauf Partner, Münster/Germany

„Wir sind ein Beratungshaus mit den Themenschwerpunkten Kreislaufwirtschaft, M & A und Finanzstrukturen. Unsere Kunden sind Kommunen und Unternehmen im In- und Ausland. Das Thema IT-Sicherheit steht bei uns weit oben auf der Agenda. Dies schon deshalb, weil unser Know-how vor allem in elektronischen Dokumenten niedergelegt ist. Wir sind zu dem Ergebnis gekommen, dass es keine absolute Sicherheit gibt. Wir arbeiten natürlich mit Firewalls und Antivirenprogrammen. Unsere Hardware ist aber grundsätzlich offen für USB-Sticks und Internetnutzungen. Es besteht eine automatische Synchronisation zu Handy und Notebook. Wir informieren natürlich die Mitarbeiter und sagen, was erlaubt ist und was nicht. Schlussendlich vertrauen wir dabei aber auf die Intelligenz unserer sehr überschaubaren Mitarbeiterzahl von fünf Personen mit Zugriff auf die Systeme. Wir arbeiten mit einer Cloud, die auf deutschen Servern arbeitet. So haben wir wenigstens deutsche Datenschutzregeln." •

"We are a consulting company focusing on recycling management, M&A and financial structures. Our customers are municipalities and German and foreign corporations. The topic of IT security ranks very high on our agenda simply because our know-how is mainly laid down in electronic documents. We have arrived at the conclusion that there is no absolute security. Of course, we are working with firewalls and anti-virus programs. Our hardware, however, is generally open to USB sticks and Internet use. There is automatic synchronization with mobile phones and notebooks. Obviously, we inform our employees and tell them what is permitted and what is not. Ultimately, however, we rely upon the intelligence of our small staff of five persons with access to the systems. We are working with a cloud provider, which operates on German servers. Thus, at least we are subject to German data protection rules". •

„Fast jeden Monat werden wir mit Angriffen konfrontiert. Ein Kunde hat uns beispielsweise gerade informiert, dass wir bestimmte E-Mails nicht öffnen dürfen, weil ein Trojaner an sein gesamtes Adressbuch versendet wurde. Daher wird es immer schwieriger, einen Absender oder eine Betreff-Zeile als ungefährlich einzustufen. Selbst unser externer Dienstleister kann nicht alle Angriffe abwehren. Bei einem besonders schweren Angriff auf unsere Homepage Anfang des Jahres musste unsere Internetseite sogar eine Zeit lang komplett abgeschaltet werden, was für unser Unternehmen hohe Verluste bedeuten kann. Der Angriff dauerte vier Stunden. In der Spitze wurden über eine Million Verbindungen von mehreren tausend Rechnern registriert. Infolgedessen waren unser Internet-Anschluss und die Firewall völlig überlastet. Wir konnten den Angriff letztendlich abwehren, indem die Attacke in eine andere Richtung gelenkt werden konnte. Und natürlich haben wir die zuständigen Sicherheitsbehörden eingeschaltet." •

"We are confronted with attacks almost every month. To give you an example, one of our customers has just warned us not to open certain emails because a Trojan was sent to his entire address book. It is therefore getting more and more difficult to classify a sender or a subject line as harmless. Even our external service provider cannot ward off all attacks. At the beginning of the year, an especially severe attack on our website forced us to shut it down completely for some time, which can result in high losses for our company. The attack lasted four hours. At the peak, we registered more than one million connections from several thousand computers. As a result, our Internet connection and the firewall were completely overloaded. In the end, we were able to fight back by steering the attack into another direction. And, of course, we have notified the responsible authorities". •

Mitglied der Wirtschaftshanse, Name der Redaktion bekannt *Member of Business Hanse, Name withheld*

Dirk Diestelhorst
Partner bei der Johannes Müller Wirtschaftsberatung, Bünde/Deutschland
Partner at business consulting firm Johannes Müller Wirtschaftsberatung, Bünde/Germany

„Wir legen sehr viel Wert darauf, dass unsere Mitarbeiter wissen, worauf es ankommt. Daher sensibilisieren wir sie für Sicherheitsthemen in gesonderten Schulungen und üben das Verhalten bei verdächtigen Vorgängen. Wir erklären den Umgang mit Kennwörtern, verwalten alle Zugangsdaten zentral und verschlüsselt und trennen strikt zwischen Administrator- und Benutzerrechten. Außerdem achten wir darauf, dass unsere Mitarbeiter keine Daten auf ‚privaten' Medien sichern. Darüber hinaus sind natürlich alle gängigen Infrastrukturmaßnahmen im Einsatz wie eine zentrale Firewall und Spam-Filter für den gesamten Maileingang." •

"We place high value on our employees knowing what is important. Therefore, we ensure in separate training sessions that they are sensitive to security issues and practice how to act when suspicious activity occurs. We explain to them how to deal with passwords, manage all access data centrally and encrypted and draw a strict distinction between administrator and user rights. Moreover, we make sure that our employees do not back up any data on 'private' media. In addition, of course, all common infrastructure measures are used, such as a central firewall and spam filters for all incoming emails". •

Dennis Blackmore
Geschäftsführer Learning Resources, King's Lynn/Großbritannien
Managing Director Learning Resources, King's Lynn/Great Britain

„Als wachsendes Unternehmen nehmen wir IT-Sicherheit sehr ernst, um unsere Geschäfts-, Mitarbeiter- und Kundendaten zu schützen. Wir arbeiten eng mit einem lokalen IT-Unternehmen zusammen um sicherzustellen, dass wir in Bezug auf Datenschutz und Sicherheit ständig auf dem neuesten Stand sind und schnell Gegenmaßnahmen ergreifen können, wenn dies mal nötig werden sollte. Daher haben wir vor kurzem erst neue, moderne Systeme installiert – einen Server und eine Telefonanlage mit Fernzugriff. Das bringt uns die Flexibilität, auch außerhalb des Unternehmens zu arbeiten und im Krisenfall auf wichtige Daten zugreifen zu können, um das Geschäft ohne Unterbrechung weiterführen zu können." •

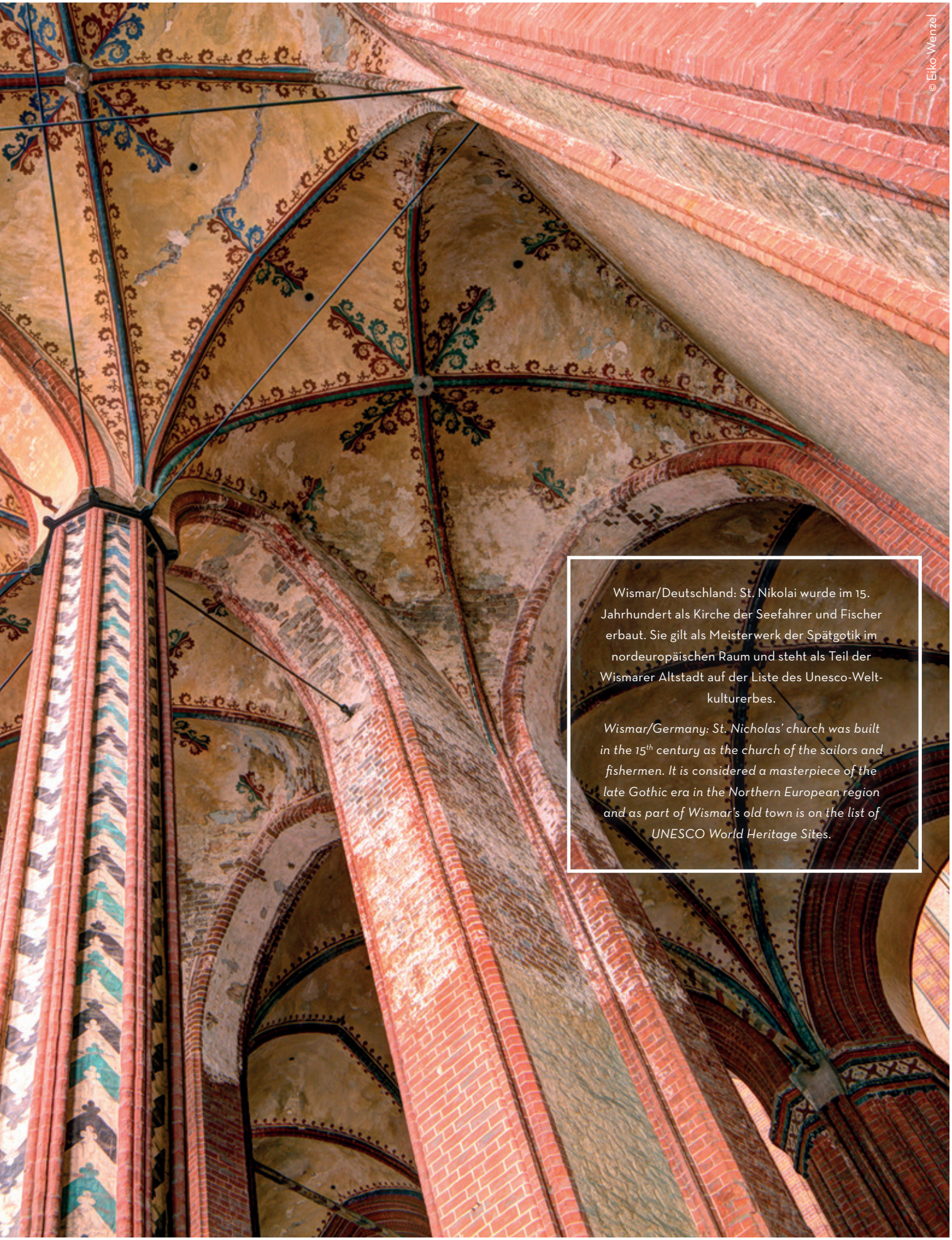
"As a growing company we take our IT security very seriously, in order to protect our business, employee and customer data. We work closely with a local IT partner company to ensure that we continually stay abreast of changes to data protection and IT security and have strong measures in place to act quickly where necessary. The innovative systems we have recently installed – a new server and phone system which facilitates remote access – offer us the flexibility to work remotely and access key data in case of a crisis, to guarantee business continuity". •

VON GIEBELN, BLENDEN, TÜRMEN UND BÖGEN

OF GABLES, BLIND WINDOWS, TOWERS AND ARCHES

Unterwegs auf der Europäischen Route der Backsteingotik

Travelling along the European Route of Brick Gothic



© Eiko Wenzel

Wismar/Deutschland: St. Nikolai wurde im 15. Jahrhundert als Kirche der Seefahrer und Fischer erbaut. Sie gilt als Meisterwerk der Spätgotik im nordeuropäischen Raum und steht als Teil der Wismarer Altstadt auf der Liste des Unesco-Weltkulturerbes.

Wismar/Germany: St. Nicholas' church was built in the 15th century as the church of the sailors and fishermen. It is considered a masterpiece of the late Gothic era in the Northern European region and as part of Wismar's old town is on the list of UNESCO World Heritage Sites.

Gdańsk/Polen: Der Vorläufer der St.-Katharinen-Kirche entstand vermutlich bereits 1185 unter Fürst Sobiesław I., der hier eine Holzkirche errichten ließ. Im 13. Jahrhundert entstand der erste Steinbau, der im 14. und 15. Jahrhundert umfangreich ausgebaut wurde. Die Kirche ist die älteste der Stadt und beherbergt heute ein Uhrenmuseum.

Gdańsk/Poland: The precursor of St. Catherine's Church was likely already started in 1185 under Prince Sobiesław I., who had a wooden church built here. In the 13th century, the first stone structure arose, which was extensively expanded in the 14th and 15th centuries. The church, the oldest one in the city, today houses a clock museum.

Rot leuchten Kirchen, Rat- und Giebelhäuser von Haderslev in Dänemark über das deutsche Lüneburg bis Płock im polnischen Masowien. Auf der gesamten Strecke prägt die Backsteingotik das Landschaftsbild. 2002 wurde die „Europäische Route der Backsteingotik" ins Leben gerufen, die heute 36 Städte verbindet. •


© Eiko Wenzel

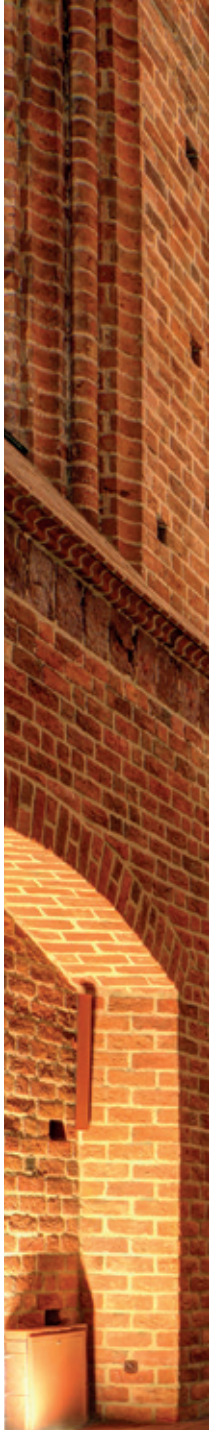
Haderslev/Dänemark: Die Domkirche St. Marien geht auf die Mitte des 12. Jahrhunderts zurück. 1525 wurden hier erstmals im Königreich Dänemark Luthers Lehren verkündet, elf Jahre früher als anderswo im Land.

Haderslev/Denmark: The Cathedral of Our Lady dates back to the middle of the 12th century. Luther's ideas were preached here for the first time in Denmark in 1525. Other churches only followed suit 11 years later.

© Europäische Route der Backsteingotik

Stargard Szczeciński/Polen: Das „Protzenhaus“ aus dem 15. Jahrhundert mit der „Stargarder Blende“, einer besonders reichen Verzierung des Giebels. Das Gebäude gehört zu den schönsten spätgotischen Bauten Polens.

Stargard Szczeciński/Poland: The “Gothic House”, built in the 15th century, featuring walls filled with “Starograd Blenda”, an especially rich ornamentation of the gable. The building is among the most beautiful late Gothic structures in Poland.



Szczecin/Polen: Die St.-Johannes-Evangelist-Kirche hat seit ihrer Errichtung im 14. Jahrhundert einiges durchgemacht: Gebaut für ein Franziskanerkloster wurde sie im 16. Jahrhundert zum Krankenhaus umgebaut und später als protestantisches Gotteshaus genutzt. Während der Napoleonischen Kriege wurden hier Lebensmittel gelagert. Heute gehört die Kirche dem katholischen Pallottiner-Orden.

Szczecin/Poland: Since its establishment in the 14th century, St. John's Church has undergone a lot of changes: Built for a Franciscan monastery, it was converted into a hospital in the 16th century and later was used as a Protestant house of worship. During the Napoleonic Wars food was stored here. Today the church belongs to the Catholic Pallottine Order.

Churches, town halls and gabled houses exhibit the red glow – stretching all the way from the Danish town of Haderslev to the German city of Lüneburg and on to the Polish city of Płock in the Masovian Voivodeship. The landscape across the entire route is characterized by the red brick Gothic style. In 2002, the "European Route of Brick Gothic" was established and today connects 36 cities. •

„Es gibt keine Alternative zu Europa“

* *English article on page 37*

Zukunftsforscher Ulrich Reinhardt erklärte beim Wirtschaftsforum der Hansestadt Brilon/Deutschland, dass Europa mehr ist als ein Wirtschaftsraum und weiter zusammenwachsen muss

Ulrich Reinhardt

Ulrich Reinhardt, 45, ist Wissenschaftlicher Leiter der Stiftung für Zukunftsfragen. An der Fachhochschule in Heide/Deutschland ist der studierte Erziehungswissenschaftler und Psychologe Professor für Empirische Zukunftsforschung. Seine Forschungsschwerpunkte umfassen den gesellschaftlichen Wandel, das Freizeit-, Konsum- und Tourismusverhalten sowie die Europaforschung. Reinhardt ist Initiator und Ideengeber vieler Forschungsprojekte in Deutschland und Europa sowie Mitglied in verschiedenen Beraterkreisen.

Europa bestimmt seit Monaten die Schlagzeilen: Griechenland, die Ukraine, die Euro- und Schuldenkrise und jetzt die Flüchtlingspolitik sind Schlagworte, mit denen eher negative Entwicklungen assoziiert werden. Doch Europa besteht nicht nur aus Krisen und Problemen, hinter der Idee Europas steht viel mehr. Ulrich Reinhardt, Zukunftsforscher und Leiter der BAT Stiftung für Zukunftsfragen, referierte dazu auf dem Briloner Wirtschafsforum im September und zeigte dabei auf, wo die Chancen Europas liegen. Das Briloner Wirtschaftsforum fand im September zum 52. Mal statt. Eingeladen hatten die Stadt Brilon/Deutschland, Mitglied in der Wirtschaftshanse, und die Brilon Wirtschaft und Tourismus GmbH.

Tiding: Sie sind Zukunftsforscher und interessieren sich besonders für Europa. Wie viele Ihrer Überzeugungen mussten Sie in den vergangenen Jahren über Bord werfen?

Reinhardt: Keine. Ich glaube nach wie vor fest an Europa. Unabhängig von Krisen steht immer der Mensch im Mittelpunkt. Für mich ist Europa mehr als bloß ein Wirtschaftsraum. Es ist eine Wertegemeinschaft.

Welche Werte vereinen die Bürger in Europa?

Die Bürger Europas wünschen sich ein schnelles Ende der drohenden sozialen Erosion und sind mehrheitlich durchaus zu moralischen Erneuerungen bereit. Im Fokus stehen Werte, die auf ein Miteinander der Bürger ausgerichtet sind. Hierzu zählen Freundschaft und soziale Gerechtigkeit ebenso wie Verlässlichkeit.

In welche Richtung steuert Europa? Gibt es das eine Europa überhaupt?

Für mich gibt es keine Alternative zu Europa. Sicherlich ist es kein abgeschlossener Raum, sondern lebt und entwickelt sich weiter. In jeder Krise steckt auch eine Chance. Diese gilt es zu ergreifen, um gemeinsam eine positive Zukunft zu gestalten.

Doch für eine gemeinsame Zukunft braucht es ein Werte-Fundament. Die Flüchtlingskrise beweist nicht gerade, dass es diese gemeinsame Haltung gibt. Was muss geschehen, damit Europa mehr wird als ein Wirtschaftsraum?

Wir benötigen vor allem eines: Zeit! Jahrzehnte, teilweise auch Jahrhunderte alte nationale Traditionen, Verhaltensweisen und Ansichten lassen sich nicht per Vertrag von heute auf morgen verändern. Gerade die neuen Mitgliedsstaaten fürchten, nicht Teil einer Wohlstandsunion zu sein, die hilft, den Lebensstandard im eigenen Land zu erhöhen, sondern selber Hilfe leisten zu müssen. Hier helfen Aufklärung und gemeinsame Ziele.

Es gibt die europäische Idee in den Köpfen der Bürger und es gibt Brüssel. Wie weit haben sich die Institutionen von der ursprünglichen Vision entfernt?

Derzeit ist viel Krisenmanagement gefordert, weshalb kurzfristig eine Diskrepanz zwischen der Vision der Bürger und dem Handeln in Brüssel wahrgenommen werden könnte. Jedoch hat die Vision von Europa noch immer und auch langfristig gesehen in Brüssel Bestand.

Der Vorläufer der EU startete als „Friedensunion". Spielt diese Bedeutung des politischen Europas in den Köpfen junger Europäer überhaupt noch eine Rolle?

Frieden ist für die jungen Europäer zur Selbstverständlichkeit geworden. Noch nie in der Geschichte Europas konnte man auf eine so lange Friedensperiode zurückblicken. 70 Jahre ohne Krieg – das ist einzigartig. Auch wenn die Welt sich im Wandel befindet, nur wenige glauben an die Möglichkeit eines Krieges vor der eigenen Haustür.

Schreiben die Menschen diesen Erfolg auch Europa zu?

Wenn sie sich damit auseinandersetzen, bestimmt. Gleichzeitig schätzt man bekanntlich vieles erst, wenn es nicht mehr da ist. Um jedoch diese bittere Erfahrung nicht wirklich machen zu müssen, ist es notwendig, dass wir in Europa weiter zusammenwachsen.

Wo sehen Sie Europa 2050?

Ich bin Optimist und glaube an ein Idealszenario. In diesem sind die Vereinigten Staaten von Europa Realität und es werden in den Verhandlungen über einen Zusammenschluss von US und EU zukunftsweisende Entscheidungen getroffen, um die Lebensqualität dauerhaft zu sichern. •

STIFTUNG FÜR ZUKUNFTSFRAGEN

Die Stiftung für Zukunftsfragen in Hamburg wurde 2007 von British American Tobacco Germany gegründet. Sie setzt sich wissenschaftlich mit Zukunftsfragen auseinander und entwickelt Lösungsansätze für künftige Herausforderungen unserer Gesellschaft. Hervorgegangen ist die Stiftung aus dem BAT Freizeit-Forschungsinstitut, das 1979 gegründet wurde. 2009 wurde das Forschungsfeld auf Europa ausgedehnt.

FOUNDATION FOR FUTURE STUDIES

The Foundation for Future Studies in Hamburg was founded in 2007 by British American Tobacco Germany. It deals scientifically with future research and develops solution approaches for future challenges of our society. The foundation emerged from the BAT Leisure Research Institute, which was set up in 1979. In 2009, the research field was expanded to include Europe.

"There is no alternative to Europe"

At the Economic Forum of the Hanseatic city of Brilon/Germany, futurologist Ulrich Reinhardt stated that Europe was more than an economic area and must continue to grow closer

Ulrich Reinhardt

Ulrich Reinhardt, 45, is the Scientific Head at the Foundation for Future Studies. He holds a professorship for empirical future research at the university of applied science in Heide/Germany. His research focuses on social change, leisure, consumer and tourism behaviour as well as research on Europe. Reinhardt is the initiator and idea provider for many research projects in Germany and Europe as well as a member of various consultancy circles.

For months, Europe has been making headlines: Greece, Ukraine, the Euro and debt crisis and now the refugee policy are keywords associated with rather negative developments. Europe does not only consist of crises and problems, however; much more stands behind the idea of Europe. Ulrich Reinhardt, futurologist and Scientific Head of the BAT Foundation for Future Studies, gave a lecture at the Brilon Economic Forum in September and pointed out where the opportunities of Europe lie. The Brilon Economic Forum was held in September for the 52nd time. The invitation was issued by the city of Brilon/Germany, member of Business Hanse, and Brilon Wirtschaft und Tourismus GmbH.

Tiding: You are a futurologist and are particularly interested in Europe. How many of your beliefs did you have to throw overboard in recent years?

Reinhardt: None. I still believe firmly in Europe. Regardless of crises, the human being is always the focus. For me, Europe is more than merely an economic area. It is a community of values.

What values unite the citizens in Europe?

The citizens of Europe want a rapid end to the threatening social erosion and the majority are absolutely ready for moral renewals. The focus is on values that are oriented towards a cooperation of citizens. These include friendship and social justice as well as reliability.

In what direction is Europe heading? Does the one Europe exist at all?

For me, there is no alternative to Europe. Certainly it is not a closed space, but rather lives and develops further. Every crisis also offers an opportunity that must be seized in order to jointly create a positive future.

But a foundation of values is needed for a common future. The refugee crisis does not really demonstrate that this common attitude exists. What needs to happen for Europe to become more than an economic area?

We need one thing above all: Time! Decades-old, in part even centuries-old, national traditions, behaviour patterns and views cannot be changed per treaty overnight. Especially the new Member States fear not being part of a prosperity union, which helps to increase the standard of living in their own country, but rather to have to provide assistance themselves. Here, information and common objectives are helping.

There is the European idea in the minds of citizens, and then there is Brussels. How far have the institutions departed from the original vision?

At present, a lot of crisis management is required, which is why a discrepancy could be perceived in the short term between the vision of citizens and the activities in Brussels. The vision of Europe is still enduring, however, and in the long term in Brussels as well.

The precursor of the EU started as a "peace union". Does this meaning of the political Europe still play any role at all in the minds of young Europeans?

Peace has become a matter of course for young Europeans. Never before in the history of Europe could we look back on such a long period of peace. 70 years without war – that is unparalleled. Even if the world is undergoing change, only a few consider the eventuality of war on their own doorstep.

Do people ascribe this success to Europe?

If they think about it, they definitely do. At the same time, as we know, you appreciate many things only once they are no longer there. In order not to have to make this bitter experience, however, it is necessary that we continue to grow closer in Europe.

Where do you see Europe in 2050?

I am an optimist and believe in an ideal scenario in which the United States of Europe are a reality and forward-looking decisions will be made in the negotiations on the merger of the US and the EU, in order to ensure quality of life on a sustained basis. •

„Jetzt verstehe ich, was Hanse ist“

✱ *English article on page 42*

Mit dem Europäischen Hansemuseum wurde in Lübeck das größte Museum über die Geschichte der Hanse eröffnet

© Europäisches Hansemuseum / Foto: Thomas Radbruch

Rund 100.000 Ziegel wurden für die Fassade des Hansemuseums entworfen und in Dänemark aus Englischem Ton von Hand gefertigt.

Some 100,000 bricks were designed for the facade of the Hanse Museum and made in Denmark by hand from English clay.

„Die Hanse hat europäische Geschichte maßgeblich mitgeschrieben. Sie wirkte identitätsstiftend. Auf sie sind Wurzeln zurückzuführen, auf denen unser europäisches Miteinander auch heute noch beruht“, sagte Bundeskanzlerin Angela Merkel anlässlich der Eröffnung des Europäischen Hansemuseums in Lübeck, das im Mai nach dreijähriger Bauzeit eröffnet wurde. Insgesamt 50 Millionen Euro haben Neubau und Sanierung gekostet. 80 Prozent hat die in Lübeck ansässige Possehl-Stiftung beigetragen, der Rest wurde mit EU-Geldern und Unesco-Welterbemitteln finanziert.

Als niederdeutsche Kaufleute aus Soest, Münster, Groningen und Lübeck 1193 am Ufer des Flusses Newa landeten, ahnten sie noch nicht, dass sie eine mächtige Vereinigung mitbegründeten, die ab dem 14. Jahrhundert als „Dudesche Hense“ bekannt wurde. Was zunächst ein loser Verbund von Fernkaufleuten für anstehende Handelsgespräche in Nowgorod war, sollte sich in den nächsten Jahrhunderten zum einflussreichsten Wirtschafts- und Städteverbund Nordeuropas entwickeln. „Die Hanse war der erste große, erfolgreiche Wirtschaftsverbund Europas. Er hatte länger als ein halbes Jahrtausend Bestand. Wir haben vor gar nicht langer Zeit 50 Jahre Römische

Verträge gefeiert, die Europäische Union muss sich also noch anstrengen", sagte Angela Merkel am Eröffnungstag.

Die facettenreiche Geschichte der Hanse wird in Lübeck seit Ende Mai nun in einem eigenen Museum dargestellt: Das Europäische Hansemuseum zeigt die Entwicklung des Kaufmannsbundes von seinen Anfängen hin zu einer nordeuropäischen Großmacht mit einem Netz von mehr als 200 Partnerstädten. Die Besucher erfahren von Wagnis und Aufstieg, von einer Welt des Reichtums und der Macht, von Misserfolg und Kampf sowie von Todesgefahren und dem alles bestimmenden Glauben. Sie können besondere Schlüsselereignisse der Hansegeschichte in rekonstruierten Szenen erkunden und nachvollziehen, wie sich eben jenes Zusammentreffen an der Newa abgespielt haben könnte, während sie an zwei originalgetreu nachgebauten Koggen vorbeigehen.

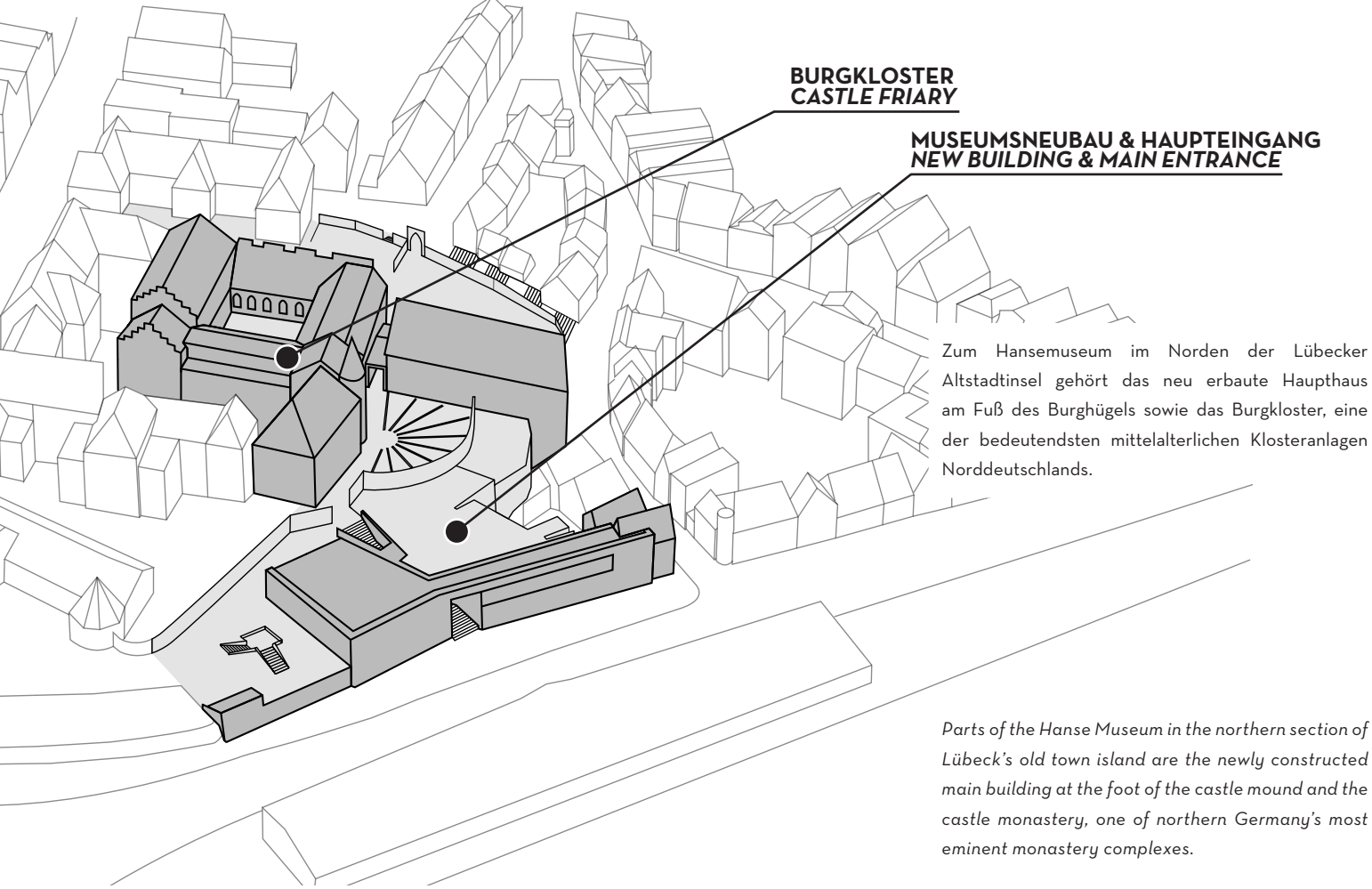
„Alle rekonstruierten Szenen basieren auf dem gegenwärtigen Forschungsstand und wurden mit großem Aufwand historisch so getreu wie möglich nachgebildet", sagt Direktorin Dr. Lisa Kosok. So erfahren die Besucher auch, wie es sich in den Kontoren zugetragen haben könnte: Sie betreten eine belebte Verkaufshalle in Brügge, den prunkvollen „Stalhof" in London und einen wichtigen Umschlagplatz für Stockfisch in Bergen. Am Beispiel Lübecks, dem damaligen „Haupt der Hanse", werden die Auswirkungen der Pest im 14. Jahrhundert dargestellt oder ein Hansetag mit Vertretern der Hansestädte in Szene gesetzt. Auch die nach dem Niedergang der Hanse einsetzenden Mythen- und Legendenbildungen werden thematisiert. „600 Jahre Wirtschaftsgeschichte werden so präsentiert, dass die Besucher sagen können ‚Jetzt verstehe ich, was Hanse ist!'", erklärt Björn Engholm, ehemaliger schleswig-holsteinischer Ministerpräsident und heute Mitglied im Beirat des Museums.

Der Rundgang startet mit einem Blick in die älteste Vergangenheit an der archäologische Grabungsfläche unter

© Europäisches Hansemuseum / Foto: Thomas Radbruch

Die archäologische Grabungsstätte zu Beginn der Ausstellung belegt die Anfänge der Besiedlung Lübecks um das Jahr 800 sowie die Stadtgründung 1143.

The archaeological dig at the beginning of the exhibition tells of the earliest settlement of Lübeck around 800 and the city's foundation in 1143.



Zum Hansemuseum im Norden der Lübecker Altstadtinsel gehört das neu erbaute Haupthaus am Fuß des Burghügels sowie das Burgkloster, eine der bedeutendsten mittelalterlichen Klosteranlagen Norddeutschlands.

Parts of the Hanse Museum in the northern section of Lübeck's old town island are the newly constructed main building at the foot of the castle mound and the castle monastery, one of northern Germany's most eminent monastery complexes.

dem heutigen Museums und erzählt von den Anfängen der Lübecker Besiedlung um das Jahr 800 und von der Stadtgründung 1143. Die Grabung, die vor Baubeginn durchgeführt wurde, dauerte drei Jahre und hat rund 10.000 unterschiedliche Fundstücke zutage gebracht, die zum Teil in die Ausstellung integriert wurden. Wertvolle Originalobjekte, seltene Dokumente, Gemälde und Sammlungsstücke veranschaulichen das Leben und Arbeiten der Hansekaufleute. Außerdem erfahren die Besucher an interaktiven Medienstationen und durch Informationsgrafiken wirtschaftliche Zusammenhänge, sehen Reiserouten und lernen das Alltagsgeschehen zur Zeit der Hanse kennen. Das Zusammenspiel von beeindruckenden Rauminszenierungen und neuester Museumstechnik zeigen ein informatives wie faszinierendes Bild von der Welt der Hanse und ihren Auswirkungen, die bis in unsere Gegenwart reichen. „Manche Spezifika Europas gehen auf die klassischen Hansekaufleute zurück. So kann man sehen, dass vieles, was wir heute vom Wirtschaftsleben erwarten, von den Hansen schon vorgelebt wurde", unterstreicht Engholm.

Zum Museum gehört außerdem noch das Burgkloster, eine der bedeutendsten mittelalterlichen Klosteranlagen Norddeutschlands. Der ehemalige Dominikanerkonvent aus dem 13. Jahrhundert wurde aufwendig saniert und restauriert. Besucher können sich die Schmuckfußböden in der Sakristei und im Hospital ansehen, Wandmalereien aus verschiedenen Epochen bestaunen und die für den Konvent äußerst bedeutsamen Schlusssteine der Gewölbe entdecken. Das Burgkloster war nach der Reformation Armenhaus, später Hospital, dann Gefängnis und ist mit einer baulichen Ergänzung auch heute noch Gerichtsgebäude.

Björn Engholm fasst die Aufgabe des neuen Museums so zusammen: „Die Kaufleute bildeten so etwas wie eine europäische Wirtschaftsgemeinschaft. Ich denke, sie waren sehr weit, gemessen an heute. Eigentlich sind sie der Nukleus eines Europa, wie wir es heute erhoffen. Positive Beiträge zu dieser fantastischen Idee Europa zu leisten, wird ein wichtiger Aspekt des Europäischen Hansemuseums sein." Angela Merkel will an die zentrale Erfahrung der Hanse anknüpfen, dass „wir gemeinsam stärker sind und mehr für alle erreichen, als wenn jeder für sich selbst agieren würde. Daher gibt es auch heute das Bemühen um Einigkeit in der Europäischen Union – immer wieder und in allen aktuellen Fragen." •

Besucher erleben in einem Nachbau des Hansekontors im norwegischen Bergen, wie Stockfisch im Jahr 1774 gelagert und gehandelt wurde.

In a replica of the Hanseatic trading post in Bergen, Norway, visitors experience how stockfish were stored and treated in 1774.

"Now I understand what the Hanse is"

The European Hanse Museum, the largest museum on the Hanseatic League's rich history, opened in Lübeck

"The Hanse has been a major factor in contributing to European history and added to its sense of identity. The roots on which our European cooperation is based today can be traced back to it", German Chancellor Angela Merkel said at the inauguration of the European Hanse Museum in Lübeck, which opened in May after a three-year construction period. New construction and renovation cost a total of 50 million euros. The Lübeck-based Possehl Foundation contributed 80 per cent, the rest was financed with EU funds and UNESCO World Heritage funds.

When Low German merchants from Soest, Münster, Groningen and Lübeck moored on the banks of the Neva river in 1193, they had no idea that they were among the founders of a powerful association, which came to be known as "Dudesche Hense" from the 14th century on. What was initially a loose alliance of merchants preparing for trade talks in the city of Novgorod evolved into the most influential economic and municipal network in Northern Europe over the following centuries. "The Hanseatic League was Europe's first large, successful economic association. It existed longer than half a millennium. Not long ago we celebrated the 50th anniversary of the Treaties of Rome, therefore the European Union still has a long way to go", Angela Merkel said on the opening day.

The Hanse's multifaceted history has now been on display in its own museum in Lübeck since the end of May: The European Hanse Museum illustrates the development from a group of merchants at its beginnings to becoming a major northern European power spanning a network of more than 200 affiliated towns and cities. The exhibition examines daring and advancement, a world of wealth and power, failure and struggle as well as mortal dangers and the all-pervasive influence of religion. Visitors are given the opportunity of discovering key events in the history of the Hanse in reconstructed scenes to comprehend just how that meeting at the Neva river could have taken place, while walking past two faithfully recreated cogs.

"All the reconstructed scenes are based on the latest state of research and no expense has been spared to make them as historically accurate as possible", said Dr Lisa Kosok, Managing Director of the Hanse Museum. As they walk through the exhibition, visitors can also see how things may have looked in the kontors, the Hanse's overseas trading posts: They can wander around a bustling market hall in Bruges, gaze at the splendour of the Steelyard in London and examine an important trading centre for stockfish in Bergen. Lübeck, known as the "Head of the Hanse", is used to portray the impact of the Black Death in the 14th century or as the stage a Hanse convention with representatives of the Hanseatic cities. The creations of myths and legends introduced after the decline of the Hanse are discussed as well. "600 years of economic history are presented such that the visitors can say 'Now I understand what the Hanse is!'" said Björn Engholm, former prime minister of Schleswig Holstein and today a member of the museum's advisory board.

The tour starts with a look into the oldest past at the archaeological excavation area underneath the present-day museum and tells of the beginnings of the Lübeck settlement around 800 and of the foundation of the city in 1143. The excavation, carried out before the start of construction, lasted 3 years and brought to light around 10,000 different finds, which were integrated in part into the exhibition. Valuable original objects, rare documents, paintings and collector items illustrate the life and work of the Hanseatic merchants. In addition, visitors find out economic correlations at interactive media stations and through information graphics, see itineraries and become familiar with the everyday events at the time of the Hanseatic League. The interplay of impressive space installations and the latest museum technology paint an informative and fascinating picture of the world of the Hanse and its impact, which extends up to our present day. "Some specific characteristics of Europe go back to the classical Hanse merchants. Thus, you can see that much of what we expect today from economic life was already practiced at the time of the Hanse", Engholm emphasized.

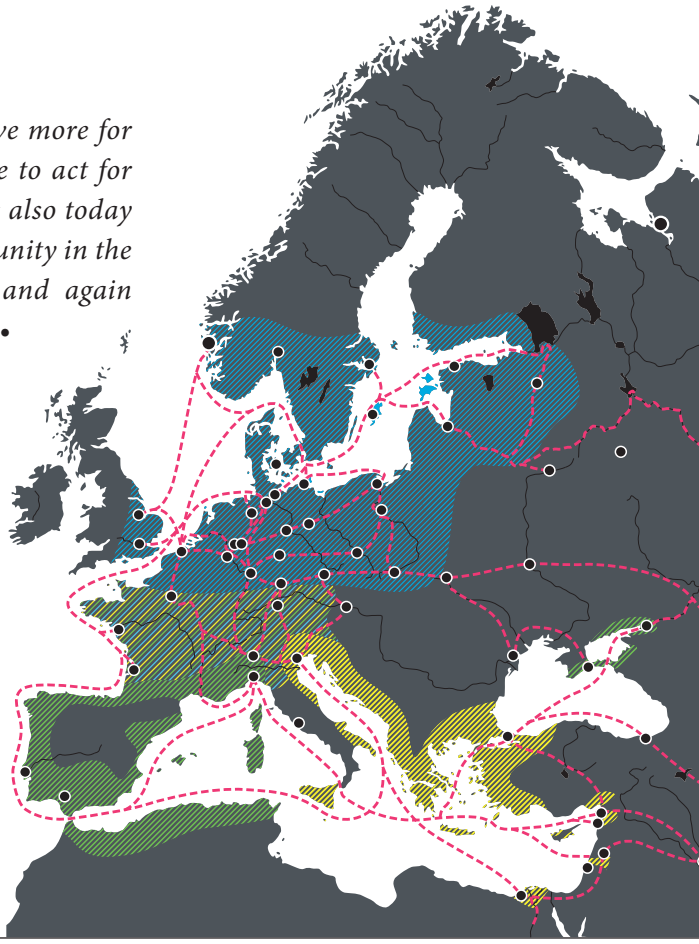
In addition, the Castle Friary one of the most important medieval convents in northern Germany, is another key element of the museum. The former Dominican friary dating from the 13th century was extensively refurbished and restored. Visitors can look at the ornamental floors in the sacristy and the infirmary, marvel at the frescoes from various periods and discover the keystones in the vaults, which are a defining element for the

Im Kapitelsaal des Burgklosters versammelten sich die Dominikaner.

The Dominicans gathered in the chapter room of the Castle Friary.

convent. After the Reformation, the castle monastery was a poor house, later a hospital, then a prison, and with a structural addition, it is a court building still today.

Björn Engholm summarised the task of the new museum: "The merchants formed something like a European economic community. I think, they were very advanced, compared to today. Actually they are the nucleus of a Europe, such as the one we are hoping for today. To provide positive contributions to this fantastic idea of Europe, will be an important aspect of the European Hanse Museum". Angela Merkel wants to take up the central idea of the Hanse that "together we are stronger and achieve more for everyone than if each were to act for himself. Therefore, there is also today the endeavour to work for unity in the European Union – time and again and on all current issues". •



Die Handelsrouten im 14. Jahrhundert gingen vom Gebiet der Hanse (blau) bis in den genuesischen (grün) und venezianischen (gelb) Handelsraum.

Trade routes in the 14th century extended from the Hanseatic territory (blue) to the Genoese (green) and Venetian (yellow) trading areas.

Gute Geschäfte per Handschlag

* English article on page 47

Paul Schockemöhle erklärt, warum es im Pferdehandel keine Verträge gibt, hier zählt allein der Handschlag

Tiding: Werden Geschäfte im Pferdehandel noch per Handschlag besiegelt?

Schockemöhle: Das ist in 80/90 Prozent der Fälle so. Es gibt schon einige Ausländer, die gern einen Vertrag wollen, aber das ist eigentlich die Ausnahme.

Woher kommt diese Tradition?

Pferde werden schon seit Ewigkeiten gehandelt – da gab es noch kein Papier und keine Verträge. Alles wurde per Handschlag besiegelt und im Pferdehandel ist das so geblieben.

Sind Sie damit schon mal auf die Nase gefallen?

Selten, sehr selten. Ich habe sicherlich schon 40.000 Pferde gehandelt und es gibt schon mal den ein oder anderen, der sich dann tatsächlich nicht an die Absprachen hält, aber normalerweise ist das kein Problem. Ich bin häufig auf Turnieren und dann kommt es vor, dass ich beim Springen ein Pferd sehe und es kaufe. Wenn hinterher andere dann mehr für das Pferd bieten, kann es schon mal sein, dass der Verkäufer vom Kaufvertrag per Handschlag nichts mehr wissen will. Aber normalerweise geht das gut.

Gibt es mehr Vertrauen unter Pferdehändlern als unter anderen Kaufleuten?

Ich glaube, Pferdehändler haben einen ähnlichen Ruf wie Autohändler, der ja nun nicht besonders gut ist. Aber Tatsache ist, dass sich die meisten an die mündlichen Absprachen halten.

Und das geht auch über die deutschen Grenzen hinweg?

Das gilt in der ganzen Welt.

Sie sind ja auch Inhaber einer Spedition. Gelten da ähnliche Regeln wie im Pferdehandel?

Nein, hier ist das anders. Normalerweise bekommen wir eine schriftliche Anfrage mit den besonderen Spezifikationen wie Anlieferung und Gewicht. Es werden ja auch andere Speditionen angefragt und der Preis abgefragt und erst dann kommt der Auftrag. Teilweise werden auch größere Verträge zum Beispiel mit Logistikunternehmen gemacht. Im Pferdehandel ist es dagegen so, dass das Pferd, das man kaufen möchte, nur noch vom Tierarzt begutachtet wird. Erst danach wird der Verkauf abgewickelt.

Und es gibt wirklich keine Vertragsunterlagen, die ausgetauscht werden?

Nein, nur die Rechnung für die Buchhaltung.

Braucht man vielleicht auch deswegen keine schriftlichen Verträge, weil Sie sich untereinander kennen? Ist die Branche eher klein?

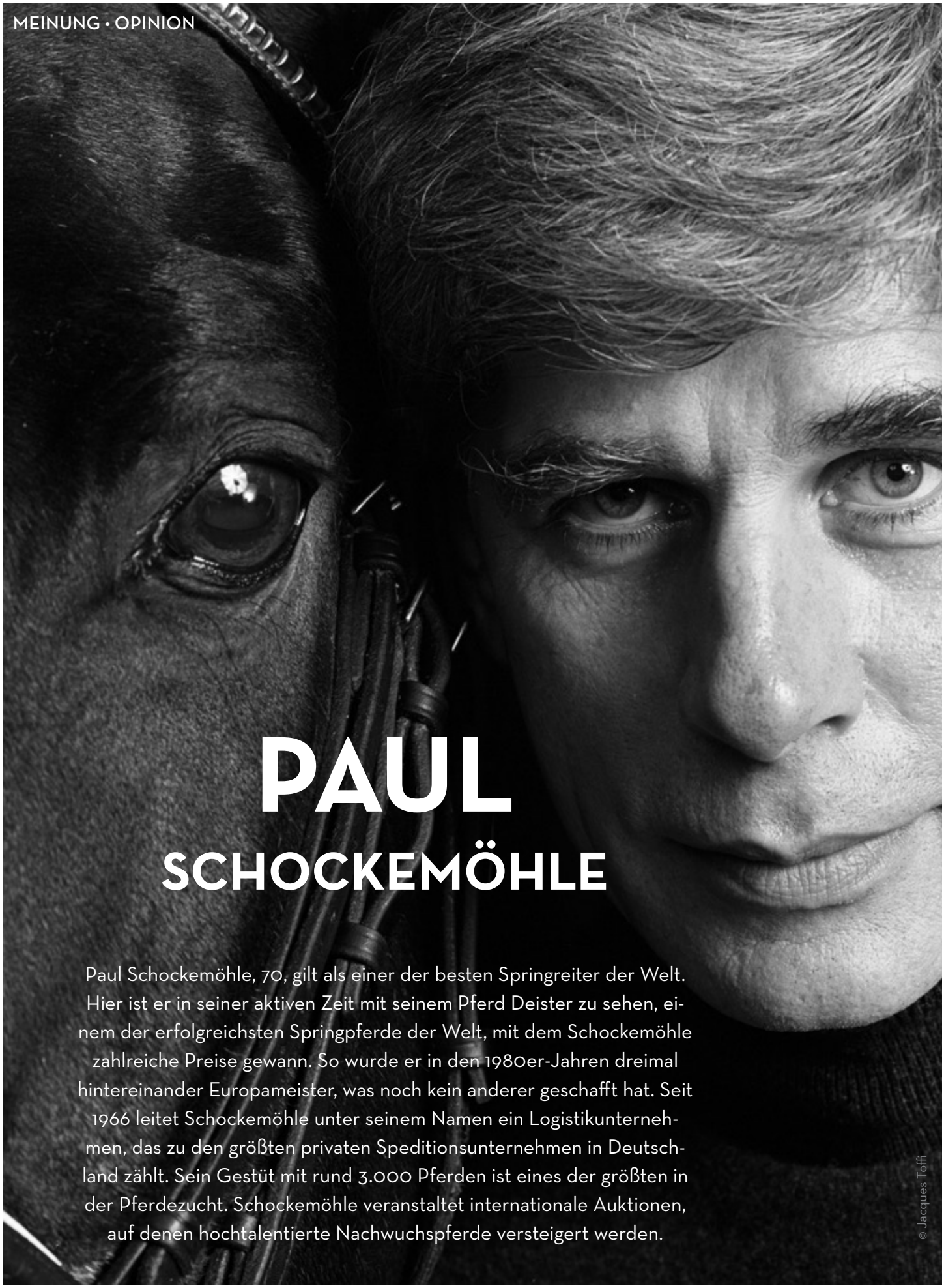
Nein, so klein auch wieder nicht, aber wie überall im Leben so trifft man sich auch hier immer zweimal. Es gibt ja auch viele, die Pferde ausbilden und dann verkaufen wollen. Aber es ist natürlich nicht wie im Supermarkt, das ist klar.

Hätten Sie in Ihrer Spedition auch gern weniger schriftliche Verträge und mehr Absprachen per Handschlag?

Nein, eigentlich nicht. Ich habe es gern, wenn die ausgehandelten Konditionen dann auch festgehalten werden. Dann gibt es nachher auch keinen Ärger. Beim Pferd ist das ein bisschen was anderes: Ein Pferd muss nur noch den Tierarzt passieren. Das Geschäft ist einfacher.

Kennen Sie zufällig noch andere Kaufleute, die so vertrauensvoll handeln?

Es gibt meines Wissens nur wenige Branchen, die das so machen. Ich kenne natürlich Kaufleute, wo ein Wort ein Wort ist und wo man nichts aufschreiben muss, aber das ist dann schon eher der Sonderfall – und absolut personenbezogen. •



PAUL SCHOCKEMÖHLE

Paul Schockemöhle, 70, gilt als einer der besten Springreiter der Welt. Hier ist er in seiner aktiven Zeit mit seinem Pferd Deister zu sehen, einem der erfolgreichsten Springpferde der Welt, mit dem Schockemöhle zahlreiche Preise gewann. So wurde er in den 1980er-Jahren dreimal hintereinander Europameister, was noch kein anderer geschafft hat. Seit 1966 leitet Schockemöhle unter seinem Namen ein Logistikunternehmen, das zu den größten privaten Speditionsunternehmen in Deutschland zählt. Sein Gestüt mit rund 3.000 Pferden ist eines der größten in der Pferdezucht. Schockemöhle veranstaltet internationale Auktionen, auf denen hochtalentierte Nachwuchspferde versteigert werden.

Paul Schockemöhle, 70, is considered one of the best show jumpers in the world. Here a picture from his time as a competitor with his horse Deister, one of the world's most successful show jumping horses, with which Schockemöhle won many prizes. In the 1980s, he was European Champion three times in a row, a feat that no other horseman has ever accomplished. Since 1966, Schockemöhle has managed a logistics company under his name, which is among the largest private forwarding companies in Germany. His stud farm with some 3,000 horses is one of the largest in the horse-breeding field. Schockemöhle organises international auctions, at which highly talented budding young horses are auctioned off.

Good transactions sealed by a handshake

Paul Schockemöhle explains why there are no contracts in horse trading; it is only the handshake that counts

Tiding: Are transactions in the horse trade still sealed by a handshake?

Schockemöhle: Yes, in 80 to 90 per cent of the cases. There are some foreigners, who would like to have a contract, but that is actually the exception.

Where does this tradition come from?

Horses have been traded since time immemorial – since there was no paper and there were no contracts. Everything was sealed by a handshake and that has remained the case in the horse trade.

Have you ever fallen flat on your face?

Rarely, very rarely. I have probably already traded 40,000 horses and there have occasionally been one or two, who then in fact did not abide by the agreement, but normally that is not a problem. I am often at tournaments and I may see a horse in show jumping that I want to buy. If someone else offers more for the horse afterwards, it can sometimes happen that the seller wants to forget about a purchase agreement sealed by a handshake. But normally it works out well.

Is there more trust among horse traders than among other merchants?

I believe horse traders have a reputation similar to that of car dealers, which is not especially good. But the fact is that most abide by verbal agreements.

And is that also the case beyond the borders of Germany?

That applies all over the world.

You are also the owner of a forwarding company. Do the same rules apply there as in the horse trade?

No, there it is different. Normally we receive a written enquiry with particular specifications such as delivery and weight. The enquiries are also sent to other forwarding companies and only after pricing, an order is placed. Sometimes also larger contracts are made with logistics companies. In the horse trade, on the other hand, the horse that you would like to buy is only examined by the veterinarian, after which the sale is processed.

And there are really no contract documents that are exchanged?

No, only the invoice for accounting.

Are written contracts perhaps not needed because you know each other? Is the industry rather small?

No, it is not that small, but as in life in general, you always meet twice. There are many individuals who train horses and then want to sell them. But, of course, it is not like in the supermarket, that much is clear.

Would you prefer to have fewer written contracts in your forwarding company as well and more agreements sealed by a handshake?

No, not really. I like it if the negotiated terms are then also recorded. So, afterwards there is no trouble, either. In the case of horses, that is a bit different: A horse must only pass a veterinarian examination. The business is simpler.

Do you happen to know other merchants who do business so trustingly?

To my knowledge, there are only a few industries that do so. Of course, I know merchants with whom a word is a word and where nothing needs to be written down, but that is then already a special case – and absolutely specific to the individual. •

IMPRESSUM • LEGAL NOTICE

HERAUSGEBER
Wirtschaftsbund Hanse e. V.
Projektleitung: Marion Köhn
Rathausplatz 1, D-32052 Herford
presse@businesshanse.com
www.businesshanse.com

REDAKTION
Marion Köhn (V. i. S. d. P.)
Isabel Melahn, Bodo Scheffels
newskontor GmbH, Düsseldorfer Straße 23,
D-40878 Ratingen
isabel.melahn@newskontor.de,
bodo.scheffels@newskontor.de
www.newskontor.de

REDAKTIONELLE MITARBEIT
Huw Sayer, Business Writers Limited, 2 Oatfield Chase,
Norwich NR14 8GU, Großbritannien
huw@business-writers.co.uk
www.business-writers.co.uk
Nico Popp, newskontor GmbH

ÜBERSETZUNGEN
Rob Wouk
Lilli Translations
P. O. Box 18223, Sarasota, FL 34276, USA
rob@lillitranslations.com
www.lillitranslations.com

ART DIREKTION
Jean-Marc Vieregge
TREU Gesellschaft für
Kommunikation mbH & Co. KG
Bahnhofstraße 13, D-32105 Bad Salzuflen
vieregge@treu-kommunikation.de
www.treu-kommunikation.de

GRAFIK
Judith Klingen
newskontor GmbH
judith.klingen@newskontor.de

VERTRIEB UND ANZEIGEN
Anke Walker
newskontor GmbH
Telefon: +49 176 729 37 727
anke.walker@newskontor.de

Es gelten die Mediadaten von Juli 2015.

AUFLAGE
5.000 Stück

DRUCK
Industrie+werbedruck
Hermann Beyer GmbH+Co.KG
Salzufler Straße 184, D-32052 Herford
www.iwdruck.de

Die „Tiding" kostet pro Heft 4,50 Euro inkl. MwSt. zzgl. Zustellgebühr.

ISSN 2363-8842

PUBLISHER
Wirtschaftsbund Hanse e. V.
Project Management: Marion Köhn
Rathausplatz 1, 32052 Herford, Germany
presse@businesshanse.com
www.businesshanse.com

EDITORIAL DEPARTMENT
Marion Köhn (responsible)
Isabel Melahn, Bodo Scheffels
newskontor GmbH, Düsseldorfer Straße 23,
40878 Ratingen, Germany
isabel.melahn@newskontor.de,
bodo.scheffels@newskontor.de
www.newskontor.de

EDITORIAL ASSISTANCE
Huw Sayer, Business Writers Limited, 2 Oatfield Chase,
Norwich NR14 8GU, United Kingdom
huw@business-writers.co.uk
www.business-writers.co.uk
Nico Popp, newskontor GmbH

TRANSLATION
Rob Wouk
Lilli Translations
P. O. Box 18223, Sarasota, FL 34276, USA
rob@lillitranslations.com
www.lillitranslations.com

ART DIRECTION
Jean-Marc Vieregge
TREU Gesellschaft für
Kommunikation mbH & Co. KG
Bahnhofstraße 13, 32105 Bad Salzuflen, Germany
vieregge@treu-kommunikation.de
www.treu-kommunikation.de

ARTWORK
Judith Klingen
newskontor GmbH
judith.klingen@newskontor.de

SALES AND ADVERTISING
Anke Walker
newskontor GmbH
Telefon: +49 176 729 37 727
anke.walker@newskontor.de

Information is based on the July 2015 media data.

CIRCULATION
5,000 copies

PRINT
Industrie+werbedruck
Hermann Beyer GmbH+Co.KG
Salzufler Straße 184, 32052 Herford, Germany
www.iwdruck.de

Price per issue EUR 4.50 including VAT plus delivery charge.

ISSN 2363-8842

Werte als Fundament

Werden Sie Mitglied in der Wirtschaftshanse

MITGLIED IM WIRTSCHAFTSBUND HANSE

Im Wirtschaftsbund Hanse schließen sich Unternehmen, Städte, Hochschulen, Verbände oder auch Privatpersonen aus europäischen Hansestädten zusammen, um die alten Werte verstärkt ins Geschäftsleben zu integrieren. Das Ziel: Die Zusammenarbeit über Grenzen hinweg zu fördern, vertragliche und regulatorische Hürden zu überwinden und damit mehr Freiraum für unternehmerisches Handeln zu schaffen. Alle Mitglieder der Wirtschaftshanse haben ihre Zustimmung zum Werteverständnis eines ehrenwerten Kaufmanns bekräftigt – bei dem das gesprochene Wort und der Handschlag wichtige Grundlagen für vertrauensvolle Geschäftsbeziehungen sind.

Werden auch Sie Mitglied im Wirtschaftsbund Hanse. Wir freuen uns auf Sie.

Den Mitgliedsantrag und die Satzung finden Sie unter www.businesshanse.com. •

Values as foundation

Membership in Business Hanse

MEMBER OF BUSINESS HANSE

Business Hanse is an association of enterprises, cities, universities, federations and private individuals from European Hanseatic cities to increasingly integrate the old values into business life. The objective: To promote cooperation across borders to overcome contractual and regulatory hurdles and thus to create more space for entrepreneurial activity. All members of Business Hanse affirmed their consent to an honourable merchant's understanding of values – where the spoken word and the handshake form important bases for business relations made in trust.

How to become a member in Business Hanse? We are looking forward to welcoming you.

For membership applications and statutes, see www.businesshanse.com. •

MITGLIEDER/ MEMBERS

DER STÄDTEHANSE/ OF THE HANSEATIC CITY LEAGUE

in den baltischen Staaten und Weißrussland

—

in the Baltic States and Belarus

Estland/Estonia

1. Narva
2. Tallinn
3. Pärnu
4. Viljandi
5. Tartu

Lettland/Latvia

6. Valmiera
7. Limbaži
8. Straupe
9. Cēsis
10. Koknese
11. Rīga
12. Kuldīga
13. Ventspils

Litauen/Lithuania

14. Kaunas

Weißrussland/Belarus

15. Polozk
16. Vitebsk

THE 36TH INTERNATIONAL HANSEATIC DAYS

WELCOME TO THE HANSEATIC DAYS

Explore the Hanseatic history of Bergen

Join the **Hansebusiness** seminar, be inspired by relevant common issues such as entrepreneurship and innovation. Bring your own stand to Bergen and present your company to a large audience. Use this opportunity to connect with companies in Western Norway!

Enjoy **Hansa Market**, **HanseARTworks**, **Hansachef competition** and **Youth Hansa** for the younger delegates. We can promise colorful street parades and spectacular opening and closing seremonies, and a city filled with music and joy.

BERGEN
NORWAY

9-12 JUNE 2016

HANSEATIC DAYS

PAST IS FUTURE

hansa2016.no
#hansa2016

CITY OF BERGEN

BERGEN OG OMLAND HAVNEVESEN
PORT OF BERGEN

BERGEN NÆRINGSRÅD

COX

ZACHARIASBRYGGEN