

# CYBERSECURITY

FORUM FÜR DATENSICHERHEIT, DATENSCHUTZ UND DATENETHIK



Fotos: Andreas Henn



Über IT-Sicherheit in einer agilen Geschäftswelt sprach Stephan Halder, Senior Manager FRC, BDO AG Wirtschaftsprüfungsgesellschaft



Über das Billion-Dollar-Desaster diskutierten Arne Helemann (TÜV Rheinland i-sec GmbH), Abdou-Naby Diaw (Lufthansa Group), Hans-Wilhelm Dünn (Cyber-Sicherheitsrat Deutschland e.V.) und Dr. Haya Shulman (Fraunhofer-Institut für Sichere Informationstechnologie), moderiert von ZEIT-Redakteur Claas Tatje (v.l.)



Hessens Justizministerin Eva Kühne-Hörmann fordert eine Digitale Agenda für das Recht. Im Netz müssten dieselben Regeln gelten wie in der realen Welt.

## Drei Fragen an



**Björn Haan, Geschäftsführer Cybersecurity, TÜV Rheinland AG**

### Was waren die folgen-schwersten Ereignisse im Bereich Cybersecurity im letzten Jahr?

Wir konnten 2018 neue Angriffsmethoden beobachten. Diese konzentrierten sich auf die entdeckten Sicherheitslücken – genannt Meltdown und Spectre – in der Architektur vieler moderner Mikroprozessoren. Es könnte Jahre dauern, ehe diese Lücken geschlossen werden. Im weiteren Verlauf des Jahres sorgten die Attacken mit Ransomware auf die Stadt Atlanta sowie die Häfen von San Diego und Barcelona für Aufmerksamkeit. Ein beunruhigendes Zeichen dafür, dass Cyberkriminelle nun auch die für die Wirtschaft unverzichtbare Infrastruktur ins Visier nehmen.

### Was ist in diesem Jahr wichtig?

Die digitale Transformation stellt für Unternehmen und Organisati-

onen eine gewaltige Herausforderung dar. Es gibt eine Vielzahl an Risiken, die auch nach dem Inkrafttreten der EU-Datenschutz-Grundverordnung bestehen und beachtet werden müssen. Wir untersuchen als TÜV Rheinland, wie sich Cyberkriminalität auf die Operational Technology (OT) in der Industrie sowie auf das Internet of Things (IoT) auswirkt. Wir analysieren zudem, welchen Einfluss sie auf den anhaltenden Fachkräftemangel und das Management von Unternehmen hat. Des Weiteren beleuchten wir Methoden, u.a. das zielgerichtete Red Teaming, agile Sicherheit, Automatisierung, lernfähige Systeme und Big-Data-Analysen, die vermehrt in den Fokus der Cybersecurity rücken.

### Was können Unternehmen tun?

Ich bin davon überzeugt, dass existierende sowie zukünftige Probleme und Herausforderungen bei Cybersecurity und Datenschutz gemeistert werden können – auch wenn diese mitunter noch so überwältigend erscheinen. Dazu bedarf es entschlossenen Handelns und des unbedingten Willens, in das dringend benötigte Fachwissen zu investieren. Wir unterstützen Unternehmen auf diesem Weg und erreichen hier gemeinsam große Fortschritte.

## Tatort Internet

**Jeder weiß es, jeden kann es treffen: Mit der Digitalisierung nehmen auch Cyberattacken zu. Wie man sie erkennt und bekämpft, darüber diskutierten Sicherheitsexperten aus Wirtschaft, Wissenschaft und Politik auf der 2. Jahrestagung Cybersecurity am 15. Mai 2019 in Frankfurt am Main.**

Systemausfall, Wirtschaftsspionage, Sabotage, Wahlmanipulation – gezielte Angriffe von Cyberkriminellen verursachen nicht nur Schäden in Milliardenhöhe, sondern gefährden Freiheit und Wohlstand. »Weltweit registrieren wir über 800 Millionen Schadprogramme, und wir stehen erst am Anfang der Digitalisierung«, mahnte Arne Schönbohm, Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI), und stellte die umfangreichen Schutz-

maßnahmen der nationalen Cybersicherheitsbehörde vor – übrigens die größte in Europa. Er gab Einblicke in die dunkle Welt der organisierten Cyberkriminalität, vom Massenphänomen Identitätsdiebstahl über kompromittierte Software bis hin zu gravierenden Angriffen auf Hardware.

### Strategien zum Schutz der vernetzten Welt

Immer mehr Menschen, Maschinen und Services sind miteinander vernetzt und bieten damit Angriffsflächen für Attacken. Die größte Schwachstelle ist jedoch der Mensch: »Wir investieren Millionen in Cybersecurity«, betonte Chief Information Security Officer Abdou-Naby Diaw und erläuterte die Cybersecurity-Strategie der Lufthansa Group, »letztlich ist jedoch die »Awareness« der Bediener entscheidend.« Alle Referenten forderten dazu auf, in Bildung und Innovationen zu investieren, um die zunehmend digitalisierte Welt sicherer zu machen.

Doch wer sind die Täter, was treibt sie an? Zu Beginn des Jahres 2019 sorgte die Veröffentlichung von gestohlenen Daten von Politikern, Journalisten und Künstlern für Schlagzeilen. Die Überraschung: Dahinter steckte ein Einzeltäter! Der YouTuber Tomasz Niemiec sprach mit Moderator Claas Tatje, DIE ZEIT, über Insights aus der Hackerszene. Für Niemiec sind vor allem Geld und Geltungssucht die treibenden Faktoren.

### Rechtlich up to date sein

Von der schwierigen Suche nach den Tätern berichtete Dr. Volker Bützler, Staatsanwalt bei der Zentralstelle zur Bekämpfung der Internetkriminalität (ZIT) bei der Frankfurter Generalstaatsanwaltschaft: »Wenn Hacker im Auftrag des organisierten Verbrechens Malware verschlüsseln und weiterleiten, wo ist dann die Straftat passiert und wer ist der Geschädigte?«, fragte er und stellte fest: »Die bestehende Gesetzgebung hinkt hin-

terher.« In Zusammenarbeit u.a. mit dem FBI hat das ZIT unlängst dem Wall Street Market, einem der größten Handelsplätze im Darknet, und einer Plattform für Kinderpornografie ein Ende gesetzt – ein gutes Beispiel, wie wichtig die Zusammenarbeit bei der Bekämpfung der Internetkriminalität ist. Damit diese verbessert wird, wurde im April 2019 das Hessen Cyber Competence Center (Hessen3C) in Wiesbaden geschaffen. Hier arbeiten 20 Cybersicherheitsexperten aus Verwaltung, Polizei und Verfassungsschutz zusammen, um Cyberangriffe auf Landesbehörden und Kommunen, aber auch Unternehmen schneller zu erkennen und abzuwehren. Bis Ende des Jahres sollen es 50 Mitarbeiter werden. All dies ist jedoch nur erfolgreich, so Hessens Justizministerin Eva Kühne-Hörmann, »wenn wir Strafbarkeitslücken schließen. Das Recht muss mit den technischen und gesellschaftlichen Entwicklungen Schritt halten.«

Detaillierte Informationen zur 2. Jahrestagung Cybersecurity finden Sie unter [www.convent.de/cybersecurity](http://www.convent.de/cybersecurity)