JAHRESTAGUNG

# CYBERSECURITY

FORUM FÜR DATENSICHERHEIT, DATENSCHUTZ UND DATENETHIK

**26. FEBRUAR 2018, FRANKFURT AM MAIN**

Fotos: Andreas Henn

Über den Schutz vor Cyberattacken diskutierten, moderiert von Jens Tönnesmann, DIE ZEIT (2. v. l.), Christoph Bornschein, CEO, TLGG GmbH, Dr. Sven Herpig, Leiter Transatlantic Cyber Forum, und Prof. Dr. Marco Gercke, Direktor, Cybercrime Research Institute GmbH (v. l.)

»Nex« (alias Claudio Guarnieri), Amnesty International, Mitbegründer »Security Without Borders«, über White Hat Hacker

Rege Debatte über »Erfolgreiche Recovery nach einem Angriff«, moderiert von Stefan Schmitt, DIE ZEIT (2. v. l.): Ghazaleh Koohestanian, CEO, Re2You GmbH, Ralph Langner Direktor, Langner Communications GmbH und Prof. Dr. Tobias Heintges, Medizinischer Geschäftsführer, Lukaskrankenhaus Neuss (v. l.)

## »Always on« – immer in Gefahr?

**Immer mehr Menschen, immer mehr Dienste und Geräte sind online vernetzt. Die Analyse und Verknüpfung der daraus entstehenden Daten führen zu nie da gewesenen Möglichkeiten. Für Wirtschaft, Wissenschaft und Gesellschaft – aber auch für Kriminelle. Wie Unternehmen Cyberangriffen trotzen können, stand im Fokus der ersten Jahrestagung Cybersecurity.**

Systemausfall, Verlust von Daten, von Know-how oder gar Identitätsdiebstahl – Cyberattacken gegen Staat, Unternehmen und Gesellschaft nehmen zu und verursachen Schäden in Milliardenhöhe. Jeden kann es treffen. Doch das ist kein Grund, so das Fazit der Referenten, in Schreckstarre zu verfallen und die Chancen, die die Digitalisierung bringt, anderen zu überlassen. Vielmehr gilt es, sich der Risiken bewusst zu sein, das Wissen um Cybersecurity auszubauen und Strategien zum Schutz der vernetzten Welt effektiv umzusetzen.

### Das unterschätzte Risiko

Welches Ausmaß Cyberangriffe auf Staat und Gesellschaft haben können, zeigte IT-Sicherheitsexperte Ralph Langner, Direktor der Langner Communications GmbH. Als einer der Ersten analysierte er die Stuxnet-Malware, die 2010 gezielt iranische Atomanlagen manipulierte. Kritische Infrastrukturen, wie Wasser- und Stromversorgung, aber auch die Produktion sind vernetzt und daher angreifbar. »Alles, was programmierbar ist, kann auch umprogrammiert werden! Wir erleben immer wieder Hackerangriffe im Bereich Big Data. Und dies sind keine heroischen Einzelkämpfer, wie gerne in den Medien dargestellt, sondern Organisationen in Nationalstaaten und Banden der organisierten Kriminalität, die oft mit staatlicher Billigung oder gar Unterstützung arbeiten. Ihnen geht es nicht um einzelne Firmen, sondern um den Zugang zu wichtigen Branchen.« Durch die Vernetzung sämtlicher Prozesse erlauben es Schwachstellen in der Kette, diese in ihrer Gesamtheit zu beeinflussen. In Anbetracht dieser Gefahren stellt man sich unweigerlich die Frage: »Warum nicht einfach so weitermachen wie bisher?« Langner konterte: »Die digitale Transformation und die Industrie 4.0 sind längst Teil unserer Wirtschaft und nicht mehr aufzuhalten.«

### Der Teufel steckt im Detail

Doch wie kann sich die Wirtschaft nun konkret gegen weltweite Attacken schützen? Alle Referenten forderten eindringlich dazu auf, in den Betrieben Fachwissen aufzubauen, und rieten zu einer Cybersecurity-Strategie, die nicht nur den bestmöglichen Schutz sensibler Daten beinhaltet, sondern auch mögliche Sicherheitslücken rechtzeitig identifiziert und regelmäßige Schulungen umfasst. »In der Realität scheitert es oft schon an der regelmäßigen Aktualisierung der Software«, betonte Prof. Marco Gercke, Direktor der Cybercrime Research Institute GmbH. Doch nicht nur das: Für Johannes Behrends, Leiter der Cyber-Spezialeinheit von Aon Risk Solutions Deutschland, ist es wichtig, das »Risikobewusstsein der Mitarbeiter zu schärfen sowie deren IT-Zugriffsrechte festzulegen, zu kontrollieren und bei ihrem Ausscheiden auch zu entziehen«. Empfehlenswert sind auch Cyber-Versicherungen, die nicht nur die Ertragsausfälle übernehmen, sondern unter anderem auch die Kosten für das Krisenmanagement und die IT-Forensik, wenn es zur Katastrophe gekommen ist. Langner riet: »Gute Recovery beginnt Jahre vorher, nicht erst im Notfall, mit Back-up-Plänen und mit einem erprobten Systemwiederherstellungsplan. Je komplexer die Anlage, desto länger dauert dies!«

Detaillierte Informationen zu der Jahrestagung Cybersecurity finden Sie unter www.convent.de/cybersecurity

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

**Wie gelingt die digitale Transformation?** Cybersecurity ist kein Nice-to-have, sondern muss »serienmäßiger« Bestandteil sein – von Services, Produkten und Geschäftsprozessen. Außerdem brauchen wir höhere Sicherheitsstandards für die Geräte im Internet der Dinge. Cybersecurity-Prüfungen und Zertifizierungen für vernetzte Geräte werden wahrscheinlicher.

**Welche Rolle spielt der Mensch?** Mehr denn je brauchen wir kluge Köpfe mit einem umfassenden Verständnis für Businessprozesse und Cybersecurity. Die Aus- und Weiterbildung des Fachkräftenachwuchses ist so existenziell wie die regelmäßige Qualifizierung des IT-Fachpersonals in Unternehmen.

**Welche Tipps geben Sie Unternehmen?** Ergreifen Sie Chancen, ohne die Risiken zu vernachlässigen – und zwar auf Basis einer robusten Cybersecurity-Strategie. Passen Sie diese Strategie zudem regelmäßig an, denn Cyberkriminelle finden immer wieder neue Mittel und Wege für einen Angriff.


Veranstalter: CONVENT.de – Ein Unternehmen der ZEIT Verlagsgruppe
Mitveranstalter: TÜVRheinland® Genau. Richtig.
Veranstaltungspartner: IHK Industrie- und Handelskammer Frankfurt am Main
Förderer: AIG, C/M/S/ Hasche Sigle, Symantec., TOSHIBA Leading Innovation
In Zusammenarbeit mit: DIE ZEIT