

Exklusiv:

- Live-Hacking auf Smartphone & Co.
- Cyber-Abwehr beim israelischen Militär

Handelsblatt Konferenz

Cybersecurity 2011.

Das Strategieforum für Politik, Wirtschaft und Militär

► 13. und 14. September 2011, Hotel Pullman Schweizerhof, Berlin

Was unternehmen Deutschland, EU und NATO gegen Cyber-Attacken?



Horst Flätgen,

Vizepräsident, Bundesamt für Sicherheit in der Informationstechnik (BSI)

Dr. Udo Helmbrecht,

Direktor, European Network and Information Security Agency (ENISA)

Generalleutnant Kurt Herrmann,

Direktor, NATO Communication and Information System Services Agency (NCSA)

Ministerialdirektor Martin Schallbruch,

IT-Direktor, Bundesministerium des Innern

Aus der Praxis: Wie schützen sich die Key-Player der Wirtschaft?



Michael Bartsch,

Vertriebsleiter Sichere Mobile Kommunikation, T-Systems

Dr. Johann Fichtner, Leiter Cyber Emergency Readiness Team (CERT), Siemens

Jörg Peter, Vorstandsvorsitzender, Arbeitsgemeinschaft für Sicherheit in der Wirtschaft e. V. (ASW); Leiter Corporate Protection and Security, Bosch

Dr. Andreas Rohr, Leiter Cyber Forensics, RWE

Kontrollierte Offensive: Ist Angriff die neue Verteidigung in der Online-Welt?



Dr. Rainer Baumgart, Vorstandsvorsitzender, secunet;

stv. Vorstandsvorsitzender, TeleTrusT Deutschland e.V.

Dr. Sandro Gaycken, Technik- und Sicherheitsforscher, Freie Universität Berlin

Jürgen Maurer, Vizepräsident, Bundeskriminalamt (BKA)

Frank Rieger, Sprecher, Chaos Computer Club

Diskutieren Sie mit diesen und vielen weiteren Top-Referenten!

Besuchen Sie uns im Internet:

<http://vhb.handelsblatt.com/cybersecurity>

Konzeption und Organisation:

EUROFORUM
The Conference Company

Handelsblatt

Substanz entscheidet.

Neue Herausforderungen – gemeinsame Lösungen

Alle zwei Sekunden werden in Deutschland Computer über das Internet angegriffen. Bundes- und EU-Behörden, Unternehmenszentralen, Militär-Hauptquartiere, Träger kritischer Infrastrukturen – wesentliche Säulen von Wirtschaft und Gesellschaft stehen unter digitalem Dauerfeuer.

Laut Schätzungen von Europol beläuft sich der weltweite Schaden durch Cyber-Angriffe auf jährlich rund eine Billion Dollar. Um zu gewährleisten, dass Deutschland in dieser veränderten Bedrohungslage sicher ist, müssen **Politik, Wirtschaft und Militär** gemeinsam Lösungen finden.

Diskutieren Sie mit hochrangigen Referenten aus dem In- und Ausland:

- Wie rüsten sich **Deutschland, EU und NATO** gegen Online-Attacken?
- Wie schützen führende Unternehmen wie **RWE, Siemens und T-Systems** sensible Daten und kritische Infrastrukturen?
- Wie verändern sich **Kriegsführung, Sicherheitspolitik, Wirtschaftsschutz sowie Völker- und Strafrecht**, wenn unsichtbare und unberechenbare Angreifer aus dem Netz zuschlagen?

Die Handelsblatt Konferenz Cybersecurity 2011 bringt exklusiv Experten und Entscheidungsträger aus allen relevanten Bereichen zusammen. Profitieren Sie vom interdisziplinären Austausch und erhalten Sie strategische Einblicke zur Bewertung einer neuen Gefahrensituation.

► Wen treffen Sie auf dieser Konferenz?

- Geschäftsführer und leitende Mitarbeiter aus Unternehmen und Behörden, insbesondere Verantwortliche der Bereiche
 - Unternehmenssicherheit (CSO)
 - IT/IT-Sicherheit (CIO/CISO)
 - Technologie/F&E (CTO)
 - Emergency Response (CERT/CSIRT)
 - IT-gestützte Produktionssysteme
 - Risk Management & Business Continuity
 - Recht & Compliance
 - Business Development
- Führungskräfte aus Militär, Sicherheits- und Verteidigungsindustrie
- Kanzleien, Beratungen und Dienstleister
- Branchenverbände und -organisationen aus den Bereichen Unternehmens- und IT-Sicherheit, Sicherheits- und Verteidigungsindustrie, Technologie und Compliance

Info-Telefon: 02 11 . 96 86 – 36 14

Haben Sie Fragen zu dieser Konferenz?
Wir helfen Ihnen gerne weiter.



Konzeption und Inhalt
Cliff Lehnen
Konferenz-Manager
EUROFORUM
E-Mail: cliff.lehnen@euroforum.com



Organisation
Kristin Langer
Konferenz-Koordinatorin
EUROFORUM
E-Mail: kristin.langer@euroforum.com

Erster Konferenztag Dienstag, 13. September 2011

8.30 – 9.00

Empfang mit Kaffee und Tee, Ausgabe der Tagungsunterlagen

9.00 – 9.15

Eröffnung durch den Veranstalter und den Vorsitzenden des ersten Konferenztages

Prof. Dr. Michael Waidner, Leiter, Fraunhofer-Institut für Sichere Informationstechnologie (SIT), Darmstadt; Lehrstuhl für Sicherheit in der Informationstechnik, Technische Universität Darmstadt

9.15 – 9.45

IMPULSVORTRAG

Höchste Zeit für klare Worte: Zum Stand der Cybersecurity-Debatte

- Gefahr erkannt, Gefahr benannt: Cyberwar – Cybercrime – Cybersecurity
- Falsche Definitionen – falsche Maßnahmen – neue Gefahren
- Einordnung Cybersecurity: Wer sind die Angreifer? Wer ist gefährdet? Welche Gefahren bestehen?

Dr. Sandro Gaycken, Technik- und Sicherheitsforscher, Freie Universität Berlin

Cyber-Sicherheit für Deutschland und Europa: Die Politik in der Verantwortung

9.45 – 10.15

Nationales Handeln in internationaler Kooperation: Die Cyber-Sicherheitsstrategie für Deutschland

- Cyber-Sicherheit stärken: Vom einzelnen PC bis zur kritischen Infrastruktur
- Das Nationale Cyber-Abwehrzentrum: Ziele und Arbeitsweise
- Der globale Cyber-Raum: Zusammenwirken für Cyber-Sicherheit weltweit

Ministerialdirektor Martin Schallbruch, IT-Direktor, Bundesministerium des Innern

10.15 – 11.00

DISKUSSIONSRUNDE

Bedrohung ohne Grenzen: Supranationale Verantwortung und Sicherheitsstrategien in der Cyber-Abwehr

- Die Rolle Deutschlands als EU- und NATO-Mitglied
- Wie verhalten sich überstaatliche Allianzen bei Cyber-Attacken?
- Wie lässt sich der Cyberwar völkerrechtlich einordnen?

Moderation: Dr. Rüdiger Scheidges, Redaktion Wirtschaft und Politik, Handelsblatt

Es diskutieren:

- **Horst Flätgen**, Vizepräsident, Bundesamt für Sicherheit in der Informationstechnik (BSI)
- **Dr. Udo Helmbrecht**, Direktor, European Network and Information Security Agency (ENISA)
- **Generalleutnant Kurt Herrmann**, Direktor, NATO Communication and Information System Services Agency (NCSA)
- **Prof. Dr. Wolff Heintschel von Heinegg**, Vizepräsident der Europa-Universität Viadrina, Frankfurt (Oder), Lehrstuhl für Öffentliches Recht, insbes. Völkerrecht, Europarecht und ausländisches Verfassungsrecht

11.00 – 11.15

Fragen an die Referenten und Diskussion

11.15 – 11.45

Pause mit Kaffee und Tee

Bekämpfung von Cyber-Gefahren: Perspektive Sicherheitspolitik und Militär

11.45 – 12.15

Infowar before Infowar:

Will the cyber threat change the face of warfare?

- Knowing more than the enemy: Why infowar has always existed
- The history of information warfare and the turn to cyberwar
- What are the essentially new challenges posed by cyber warfare?

Prof. Dr. Martin van Creveld, Emeritus, Hebräische Universität Jerusalem, einer der weltweit führenden Experten für Militärgeschichte, Strategie und zukünftige Konflikte [Vortrag in englischer Sprache]

12.15 – 12.45

EXKLUSIV

Cyber defence from the perspective of Israel

- Insight into potential operations in cyber space
 - The asymmetrical nature of cyber operations
 - Cyber defence case studies: The virtual threat is real
- Generalmajor a.D. Prof. Dr. Isaac Ben-Israel**, Vorsitzender des Israel National Council for Research and Development sowie der Israel Space Agency (ISA); Professor für Sicherheits- und Verteidigungspolitik an der Universität Tel-Aviv [Vortrag in englischer Sprache]



Michael Bartsch



Rainer Baumgart



Isaac Ben-Israel



Martin van Creveld



Johann Fichtner



Horst Flätgen



Sandro Gaycken

12.45 – 13.15

Cyber-Abwehr bei der NATO: Status quo und Ausblick

- Status der NATO-Operationen zum Thema Cybersicherheit
- Einblick in die Arbeit der NATO-Agentur für Kommunikations- und Informationssysteme (NCSA)
- Entwicklungsbedarf und -potential im Bereich der Cyber-Abwehr auf NATO-Ebene

Generalleutnant Kurt Herrmann, Direktor, NATO Communication and Information System Services Agency (NCSA)

„Cyber-Angriffe können heute ähnlich verheerend wirken wie herkömmliche Militärschläge. Die Bedrohung wächst exponentiell.“

13.15 – 13.30

Fragen an die Referenten und Diskussion

13.30 – 15.00

Gemeinsames Mittagessen

Dimensionen und Potentiale von Cyber-Abwehr und Online-Sicherheit

15.00 – 15.30

Die Mär von der absoluten Sicherheit im Netz:

Wogegen wir uns schützen können – und wogegen nicht

- Softwarefehler, Schwachstellen, etc.: Offene Türen für Hacker
 - Nach dem digitalen Erstschlag: Welche Herausforderungen Staat und Wirtschaft in Zukunft erwarten
 - Warum immer komplexere Angriffe neue Lösungsansätze erfordern
- Frank Rieger**, Sprecher, Chaos Computer Club

„Der Einsatz von Cyber-Waffen durch Staaten wird zur Normalität. Die Welt muss sich auf ein neues Zeitalter einstellen: Unsere bestehenden Sicherheitskonzepte sind nicht mehr ausreichend.“

15.30 – 16.15

DISKUSSIONSRUNDE

Geballte Defensive, kontrollierte Offensive:

Ist Angriff die neue Verteidigung in der Online-Welt?

- Proaktiv versus reaktiv: Wie weit darf Selbstschutz gehen?
- Abschreckung als Sicherheitsdoktrin im Online-Universum?
- Der Angriff als Option? Streitthema aktive Operationen

Moderation: Dr. Rüdiger Scheidges

Es diskutieren:

- **Dr. Rainer Baumgart**, Vorstandsvorsitzender, secunet Security Networks AG; stellvertretender Vorstandsvorsitzender, TeleTrusT Deutschland e.V.

• **Dr. Sandro Gaycken**

- **Brigadegeneral a.D. Friedrich Wilhelm Kriesel**, Berater des Vorstands, Deutsches Zentrum für Luft- und Raumfahrt; ehem. Kommandeur, Kommando Strategische Aufklärung (KSA)
- **Dr. Michael Meier**, Wissenschaftler in der Forschungsgruppe Cyber Defense, Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE)
- **Frank Rieger**

16.15 – 16.30

Fragen an die Referenten und Diskussion

16.30 – 17.00

Pause mit Kaffee und Tee

Gesamtstaatliche Cyber-Abwehr und -Diplomatie

17.00 – 17.30

Gefahr neu denken:

Cyber-Abwehr als gesamtstaatliche Herausforderung

- Warum wir Cyber-Sicherheit erst verstehen lernen müssen
- Wie wir uns bei der Cyber-Abwehr selbst im Weg stehen
- Was braucht es, um die neuen Gefahren gemeinsam zu meistern?

Brigadegeneral a.D. Friedrich Wilhelm Kriesel

17.30 – 18.00

Vom Cyberwar zum Cyberpeace

- Vision Online-Frieden: Möglichkeiten der Cyber-Diplomatie
- Online-Rüstungskontrolle: Wie wir ein neues Wettrüsten verhindern
- Vorrangiges Ziel Cyberstabilität

Botschafter a.D. Dr. Henning Wegener, Vorsitzender, Permanent Monitoring Panel on Information Security der World Federation of Scientists

18.00 – 18.15

Abschlussdiskussion und Ende des ersten Konferenztages

Ab 19.00

Im Anschluss an den ersten Konferenztag lädt Sie das Handelsblatt zu einer gemeinsamen Abendveranstaltung ein. Lassen Sie den Tag in angenehmer Atmosphäre ausklingen und nutzen Sie die Gelegenheit, Ihr Netzwerk zu pflegen und neue Kontakte zu knüpfen.



Marco Gercke



W. Heintschel von Heinegg



Udo Helmbrecht



Kurt Herrmann



Stefan Krebs



Friedrich W. Kriesel

Zweiter Konferenztag Mittwoch, 14. September 2011

8.30 – 9.00

Empfang mit Kaffee und Tee

9.00 – 9.05

Eröffnung durch den Veranstalter und den Vorsitzenden des zweiten Konferenztages

Prof. Dr. Norbert Pohlmann, Geschäftsführender Direktor des Instituts für Internet-Sicherheit, FH Gelsenkirchen; Vorstandsvorsitzender, TeleTrust Deutschland e.V.

Impulsvorträge: Sicherheit für Staat und Wirtschaft

9.05 – 9.25

Kriminalität 2.0: Welche Gefahren deutschen Unternehmen über das Netz drohen

- Cybercrime: Herausforderung für Wirtschaftsunternehmen
 - Tatort Internet: Zur notwendigen Kooperation von Wirtschaft und Sicherheitsbehörden
 - Erforderliche Maßnahmen zur Bekämpfung von Cybercrime
- Jürgen Maurer**, Vizepräsident, Bundeskriminalamt (BKA)

„Die Bekämpfung der Internetkriminalität ist eine gesamtgesellschaftliche Aufgabe. Öffentliche Verwaltung, private Unternehmen sowie Bürgerinnen und Bürger müssen ihren Beitrag leisten – insbesondere zur Kriminalitätsverhütung.“

9.25 – 9.45

Unternehmensschutz heute: Die Bedeutung der Cybersecurity im ganzheitlichen Sicherheitskonzept

- Herausforderungen an die Corporate Security
 - Strategiekonzept Cybersecurity aus Sicht der ASW
 - Initiativen und Aktionen zum Schutz der Wirtschaft
- Jörg Peter**, Vorstandsvorsitzender, Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V. (ASW); Leiter Corporate Protection and Security, Robert Bosch GmbH

Schutz kritischer Infrastrukturen: Die Bereiche Energie und Finanzen

9.45 – 10.15

Cyber-Sicherheit als Teil der Unternehmenssicherheit im Energiesektor – das Beispiel RWE

- Vergleich der Bedrohungsvektoren über die Zeit
 - Erkennung von Angriffen und Ableitung von Gegenstrategien
 - Cyber-Forensik: Maßnahme umfassender Informationssicherheit
- Dr. Andreas Rohr**, Leiter Cyber Forensics, RWE AG

10.15 – 10.45

Online-Schutz des Finanzsystems am Beispiel einer Finanzgruppe

- Zeitgemäßer Online-Schutz bei der Finanz Informatik: Sicherheit für über 400 Finanzinstitute
 - Langfristige Planung, kurzfristige Reaktionsmöglichkeit
 - Schneller als die Angreifer: Strategien und Maßnahmen
- Stefan Krebs**, Leiter Informationssicherheit, Risiko-Management und Compliance sowie Organisationsentwicklung und interne IT, Finanz Informatik GmbH & Co. KG

10.45 – 11.00

Fragen an die Referenten und Diskussion

11.00 – 11.30

Pause mit Kaffee und Tee

Cyber-Sicherheit in der Unternehmenspraxis

11.30 – 12.00

Aktuelle Cyberattacken:

Wie Siemens auf die Herausforderung Cybersecurity reagiert

- Technische und organisatorische Anforderungen an effektive Cybersecurity
 - Herausforderungen für Anbieter von Lösungen für kritische Infrastrukturen
 - Der Beitrag der Forschung zur Unternehmenssicherheit
- Dr. Johann Fichtner**, Global Technology Field Leader und Leiter des weltweiten Cyber Emergency Readiness Teams (CERT), Siemens AG

12.00 – 12.30

Geschäftsmodell Computerkriminalität – einfach (un)sicher

- Was Cyber-Kriminalität für Hacker so attraktiv macht
- Mit welchen Mitteln und Methoden ein erfolgreiches Cybercrime-Unternehmen aufgebaut werden kann
- Ausblick auf Wirtschafts- und Industriespionage als Mittel zum Zweck

Michael Bartsch, Vertriebsleiter Sichere Mobile Kommunikation, T-Systems International GmbH; Arbeitskreisleiter Öffentliche Sicherheit im Bundesverband ITK und Medien (Bitkom)

„In einer globalen Internetgesellschaft ist Cyber-Kriminalität sehr einfach und sehr lukrativ – und deshalb extrem attraktiv. Die Motivation der Täter ist dabei ausschließlich finanzieller Natur.“



Jürgen Maurer



Michael Meier



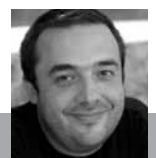
Klaus Mochalski



Jörg Peter



Norbert Pohlmann



Frank Rieger

12.30 – 13.00

Deep Packet Inspection: Basistechnologie für zukünftige Sicherheitsarchitekturen

- Zuverlässige Erkennung von gut- und bössartigen Kommunikationsmustern
- Whitelisting- und Blacklisting-Ansätze zum Schutz kritischer Infrastrukturen
- Deep Packet Inspection im praktischen Einsatz

Klaus Mochalski, Executive Vice President Market Development, ipoque GmbH, a Rohde & Schwarz Company

13.00 – 13.20

Rechtsfreier Raum Internet? Möglichkeiten der strafrechtlichen Verfolgung von Cyber-Kriminellen

- Fremde Server, falsche Namen, verdeckte Identitäten: Wer trägt Schuld beim Cyber-Angriff?
- Attacken aus dem Ausland: Welches Recht gilt?
- Hacker-Bekämpfung: Welche Maßnahmen sind legal?

Prof. Dr. Marco Gercke, Direktor, Cybercrime Research Institute

13.20 – 13.30

Fragen an die Referenten und Diskussion

Gemeinsamer Aperitif vor dem Mittagessen auf freundliche Einladung von



13.30 – 14.45

Gemeinsames Mittagessen

Best Practices für eine zukunftssichere Wirtschaft

14.45 – 15.30

LIVE-Hacking

„Einmal nicht aufgepasst...!“ – Smartphone, Notebook, USB & Co.: Sicherheitslücken to go für Profi-Hacker



Diese und weitere Angriffs-Szenarien werden live präsentiert:

- Handys als Abhör-Wanzen: Wer hört mit beim Geschäftstelefonat?
- Shop till you drop: Angriffe auf Shop-Systeme
- Sicher mit Passwort? Attacken auf den Passwortschutz in Windows und Bios
- Trojaner der Zukunft aus dem USB-Stick

Sebastian Schreiber, Geschäftsführer, SySS GmbH

15.30 – 16.00



TRIALOG

Online-Sicherheit in der Wirtschaft – heute und in Zukunft

- Nachholbedarf: Cybersecurity für den Mittelstand
- Welche Best Practices allen Unternehmen nützen
- Zukunftssicher: Recruiting und Ausbildung von Fachkräften zur Cyber-Gefahrenabwehr

Prof. Dr. Norbert Pohlmann im Gespräch mit:

- Michael Bartsch
- Jörg Peter

16.00 – 16.15

Abschlussdiskussion und Ende der Konferenz



Andreas Rohr



Martin Schallbruch



Rüdiger Scheidges



Sebastian Schreiber



Michael Waidner



Henning Wegener

Gastgeber des Aperitifs



ipoque ist der führende europäische Anbieter von Deep-Packet-Inspection-Lösungen für Internet-Traffic-Management und Netzwerkmonitoring, die kommerziellen und institutionellen Netzbetreibern eine

effektive Analyse, Verwaltung und Optimierung ihrer Netzwerkressourcen ermöglichen. Mit über 250 Installationen in mehr als 60 Ländern betreut das 2005 in Leipzig gegründete Unternehmen heute ein weltweites Netz von Kunden und Partnern.

ipoque, Neumarkt 29-33, 04109 Leipzig, www.ipoque.com

Ansprechpartner: Klaus Mochalski, EVP Market Development, Telefon: 0341.59403053

E-Mail: klaus.mochalski@ipoque.com



ROHDE & SCHWARZ steht seit über 75 Jahren für Qualität und Innovation in den Bereichen sichere Kommunikation sowie Überwachungs- und Ortungstechnik. ROHDE & SCHWARZ liefert

interoperable und leistungsfähige Kommunikationssysteme, die im Einsatz- oder Krisenfall die zeitnahe Koordination ziviler, behördlicher und militärischer Einsatzkräfte gewährleisten. Für Unternehmen, Regierungsstellen, Bundeswehr und die NATO entwickelt und produziert die ROHDE & SCHWARZ zudem Kryptolösungen. Mit seinen Empfängern, Peilern, Signalanalytoren, Antennen zur Erfassung, Ortung und Analyse von Funkkommunikationssignalen ist ROHDE & SCHWARZ seit vielen Jahrzehnten in den Bereichen innere und äußere Sicherheit ein zuverlässiger Partner.

ROHDE & SCHWARZ GmbH & Co. KG, Mühlendorfstraße 15, 81671 München, www.rohde-schwarz.com

Telefon: 089.4 12 91 37 74, Fax: 089.4 12 91 37 77, E-Mail: CustomerSupport@rohde-schwarz.com

Förderer



Die **secunet Security Networks AG** ist einer der führenden deutschen Anbieter für anspruchsvolle IT-Sicherheit. Im engen Dialog mit ihren Kunden – Unternehmen, Behörden und internationale Organisationen – entwickelt secunet leistungsfähige Produkte und fortschrittliche IT-Sicherheitslösungen. Damit sichert secunet nicht nur sensible IT-Infrastrukturen mit besonderen

Hochsicherheitsanforderungen, sondern erzielt auch intelligente Prozessoptimierungen und schafft nachhaltige Mehrwerte.

secunet Security Networks AG, Kronprinzenstraße 30, 45128 Essen, www.secunet.com

Ansprechpartner: Jens Westphal, Bereichsleiter Business Security, Telefon: 02 01.54 54 – 2032, Fax: 02 01.54 54 – 1325, E-Mail: Jens.Westphal@secunet.com

Kooperationspartner



SECURITY insight ist die Fachzeitschrift für Sicherheits-Entscheider, denen die oberflächliche Berichterstattung auf Fachchinesisch nicht genügt. Die Zeitschrift zeigt Lösungen aus der Praxis für die Praxis, erklärt die komplexen Zusammenhänge und schafft mit Hintergrundberichten Perspektiven für die tägliche Sicherheitsarbeit. Die Zeitschrift orientiert sich am Informationsbedürfnis der

Sicherheits-Entscheider, hinter die Kulissen des Sicherheitsmarktes zu blicken, um auf seiner Bühne wirken zu können. Ergänzend dazu ist www.security-insight.com das Internetportal für die schnelle Informationssuche.



Der IT-Sicherheitsverband **TeleTrust Deutschland e.V.** wurde 1989 gegründet und umfasst mehr als 110 Mitglieder aus Industrie, Wissenschaft, Forschung und öffentlichen Institutionen sowie Partnerorganisationen aus Deutschland und Europa. In Projektgruppen zu aktuellen Fragestellungen der IT-Sicherheit und des Sicherheitsmanagements tauschen die Mitglieder ihr Know-how aus.

TeleTrust äußert sich zu politischen und rechtlichen Fragen, organisiert Veranstaltungen und Veranstaltungsbeteiligungen und ist Trägerorganisation der „European Bridge CA“ (Bereitstellung von Public-Key-Zertifikaten für sichere E-Mailkommunikation) sowie des Zertifikates „TeleTrust Information Security Professional“ (T.I.S.P.).



Die **ASW – Arbeitsgemeinschaft für Sicherheit der Wirtschaft e.V.** – ist der Zusammenschluss der Spitzenverbände der Deutschen Wirtschaft (DIHK, BDI, BDA), aller regionalen Sicherheitsverbände sowie mehrerer Branchenverbände in Sicherheitsfragen.

Die Mitgliedsorganisationen der ASW vertreten in ihrer Gesamtheit über vier Millionen Unternehmen und Selbstständige. Die ASW ist damit die Zentralorganisation der Deutschen Wirtschaft in Sicherheitsfragen und versteht sich als Netzwerk und Forum in der Unternehmenssicherheit. Sie vertritt die Sicherheitsinteressen der deutschen Wirtschaft gegenüber Politik, Staat und Gesellschaft.

Sponsoring und Ausstellungen:

Im Rahmen der Veranstaltung besteht die Möglichkeit, dem exklusiven Teilnehmerkreis Ihr Unternehmen und Ihre Produkte oder Dienstleistungen zu präsentieren. Ihre Fragen zu Sponsoring- und Ausstellungsmöglichkeiten sowie zur Zielgruppe beantwortet Ihnen gerne:



Anne Katrin Ruhkamp
Teamleiterin
Sponsoring/Ausstellungen
Telefon:

02 11.96 86 – 37 31

Fax: 02 11.96 86 – 47 31

E-Mail: anne.ruhkamp@euroforum.com

(Kenn-Nummer)

Cybersecurity 2011.

Das Strategieforum für Politik, Wirtschaft und Militär

- Profitieren Sie vom interdisziplinären Austausch mit Referenten aus dem In- und Ausland
- Diskutieren Sie Best-Practices zur Cyber-Abwehr kompakt in nur zwei Tagen
- Erhalten Sie Einblicke in die zentralen Trends und Entwicklungen im Bereich Cybersecurity
- Treffen Sie Top-Entscheidungsträger in angenehmer Atmosphäre ohne Zeitdruck
- Beteiligen Sie sich aktiv an den Debatten um Angriff und Verteidigung in der Online-Welt

Bitte ausfüllen und faxen an: 02 11.96 86-40 40

- Ja, ich nehme am 13. und 14. September 2011 in Berlin teil** zum Preis von € 2.099,- p. P. zzgl. gesetzl. MwSt. (P1200435M012)
- Sonderpreis für Vertreter des Militärs, der Politik, der Ministerien und des diplomatischen Dienstes: € 1.449,- p.P. zzgl. gesetzl. MwSt.**
[Ich kann jederzeit ohne zusätzliche Kosten einen Ersatzteilnehmer benennen.]
[Im Preis sind ausführliche Tagungsunterlagen enthalten.]
- Ich kann nicht teilnehmen. Senden Sie mir bitte die **Tagungsunterlagen** zum Preis von € 399,- zzgl. MwSt. zu. [Lieferbar ab ca. 2 Wochen nach der Veranstaltung.]
- Ich interessiere mich für **Ausstellungs- und Sponsoringmöglichkeiten.**
- Ich möchte als Dankeschön für meine Teilnahme **das Handelsblatt kostenlos für zwei Monate erhalten.**
- Ich möchte meine Adresse wie angegeben korrigieren lassen.
[Wir nehmen Ihre Adressänderung auch gerne telefonisch auf: 0211.9686-3333.]

Name, Vorname	
Position/Abteilung	
Telefon	Fax
E-Mail	Geb.-Datum (TTMMJJJJ)

Die EUROFORUM Deutschland SE darf mich über verschiedenste Angebote von sich, Konzern- und Partnerunternehmen wie folgt zu Werbezwecken informieren:
Zusendung per E-Mail: Ja Nein per Fax: Ja Nein

Firma
Anschrift
Branche
Ansprechpartner im Sekretariat

Datum, Unterschrift

Bitte ausfüllen, falls die Rechnungsanschrift von der Kundenanschrift abweicht:

Name
Abteilung
Anschrift

Wer entscheidet über Ihre Teilnahme? Ich selbst oder Name: _____

Position: _____

Beschäftigtenzahl an Ihrem Standort: bis 20 21-50 51-100 101-250 251-500 501-1000 1001-5000 über 5000

Teilnahmebedingungen. Der Teilnahmebetrag für diese Veranstaltung inklusive Tagungsunterlagen, Mittagessen, Pausengetränken und Abendessen pro Person zzgl. MwSt. ist nach Erhalt der Rechnung fällig. Nach Eingang Ihrer Anmeldung erhalten Sie eine Bestätigung. Die Stornierung (nur schriftlich) ist bis 14 Tage vor Veranstaltungsbeginn kostenlos möglich, danach wird die Hälfte des Teilnahmebetrages erhoben. Bei Nichterscheinen oder Stornierung am Veranstaltungstag wird der gesamte Teilnahmebetrag fällig. Gerne akzeptieren wir ohne zusätzliche Kosten einen Ersatzteilnehmer. Programmänderungen aus dringendem Anlass behält sich der Veranstalter vor.

Datenschutzinformation. Die EUROFORUM Deutschland SE verwenden die im Rahmen der Bestellung und Nutzung unseres Angebotes erhobenen Daten in den geltenden rechtlichen Grenzen zum Zweck der Durchführung unserer Leistungen und um Ihnen postalisch Informationen über weitere Angebote von uns sowie unseren Partner- oder Konzernunternehmen wie der Handelsblatt GmbH zukommen zu lassen. Wenn Sie unser Kunde sind, informieren wir Sie außerdem in den geltenden rechtlichen Grenzen per E-Mail über unsere Angebote, die den vorher von Ihnen genutzten Leistungen ähnlich sind. Soweit im Rahmen der Verwendung der Daten eine Übermittlung in Länder ohne angemessenes Datenschutzniveau erfolgt, schaffen wir ausreichende Garantien zum Schutz der Daten. Außerdem verwenden wir Ihre Daten, soweit Sie uns hierfür eine Einwilligung erteilt haben. Sie können der Nutzung Ihrer Daten für Zwecke der Werbung oder der Ansprache per E-Mail oder Telefax jederzeit gegenüber der EUROFORUM Deutschland SE, Postfach 11 12 34, 40512 Düsseldorf.

Zimmerreservierung. Im Tagungshotel steht ein begrenztes Zimmerkontingent zum ermäßigten Preis zur Verfügung. Bitte nehmen Sie die Reservierung direkt im Hotel unter dem Stichwort Handelsblatt-/EUROFORUM-Konferenz vor. Änderungen vorbehalten.

Ihr Tagungshotel.
Am Abend des ersten Veranstaltungstages lädt Sie das Hotel Pullman Schweizerhof herzlich zu einem Umtrunk ein.



Datum und Ort:
13. und 14. September 2011
Hotel Pullman Schweizerhof
Budapester Str. 25, 10787 Berlin
Telefon: +49 (0) 30 . 26 96 0

Wir über uns. Handelsblatt Veranstaltungen vermitteln Ihnen in hochkarätigen Konferenzen und Seminaren wichtige Wirtschaftsinformationen zu aktuellen Themen. Wir bieten damit Führungskräften aus Wirtschaft und Industrie Foren für Know-how-Transfer und Meinungsaustausch. Mit der Planung und Organisation der Veranstaltungen haben wir die EUROFORUM Deutschland SE beauftragt.

Anmeldung und Information

per Fax: +49 (0)2 11.96 86-40 40

telefonisch: +49 (0)2 11.96 86-36 14
[Kristin Langer]

Zentrale: +49 (0)2 11.96 86-30 00

schriftlich: EUROFORUM Deutschland SE
Postfach 11 12 34, 40512 Düsseldorf

per E-Mail: anmeldhb@euroforum.com

im Internet: <http://vhb.handelsblatt.com/cybersecurity>