Jetzt anmelden!
16. September 2015, Berlin

Cyber Security Challenge GERMANY

Cyber Security Challenge Germany

Die Konferenz

Viele Unternehmen sind durch Cyberangriffe großen Risiken ausgesetzt. Häufig besteht ein Informationsdefizit, wie sich die Unternehmen schützen können. Daran müssen und wollen wir gemeinsam arbeiten.

In zentraler Berliner Lage im **Humboldt Carré, Gendarmenmarkt** findet die **zweite Cyber Security Challenge Germany Konferenz** am **16. September 2015** statt. Wir zeigen Ihnen Gefahren und die Möglichkeiten der Prävention auf. Das unabhängige Konferenz-Programm wurde von TeleTrusT, if(is) und heise Events erstellt und richtet sich an Entscheider, Unternehmer, IT-Sicherheitsbeauftrage und IT-Experten.

In einer **begleitenden Ausstellung** werden führende IT-Sicherheitsunternehmen die Produkte präsentieren, die Ihre Daten vor Cyberangriffen schützen können.

Auf der **Recruting-Messe** (Match Making) haben Sie als Unternehmen die Möglichkeit vor Ort mit Schülerinnen und Schülern sowie mit Studierenden ins Gespräch zu kommen. Schülerinnen, Schüler und Studierende haben **kostenlosen Eintritt** zur Recruting-Messe.

Der Wettbewerb

Begleitend zur Konferenz findet das Finale der Cyber Security Challenge Germany statt. Hier werden die besten Schülerinnen, Schüler und Studierende Deutschlands um die Krone als Nachwuchs-Cyber-Security-Talent kämpfen.

Die Onlinequalifikation für das Finale in Berlin endet am 03. August 2015, bis zu einschließlich diesem Datum ist die Anmeldung und Teilnahme unter www.cscg.de möglich. Als Teilnehmer der Konferenz haben Sie die Möglichkeit mit den Talenten von morgen in Kontakt zu treten. Die **Preisverleihung** wird im **Anschluss zur Konferenz um 18.30 Uhr** im festlichen Ambiente mit anschließender Feier stattfinden.

Der kostenlose Zutritt zur Recruiting-Messe für Schülerinnen und Schüler sowie Studierende kann unter **cscg@teletrust.de** erfragt werden.

www.cybersecuritychallenge.de/konferenz

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Projekt der Initiative:
IT-Sicherheit IN DER WIRTSCHAFT
www.it-sicherheit-in-der-wirtschaft.de

Kooperationspartner:
if(is) internet-sicherheit.
TeleTrusT Pioneers in IT security.
Heise Medien

Konferenzprogramm
(Änderungen vorbehalten)

09:00	Registrierung
10:15	**Eröffnung und Begrüßung durch das Bundesministerium für Wirtschaft und Energie und die Projektbeteiligten** Prof. Dr. Norbert Pohlmann, Leiter if(is) - Institut für Internet-Sicherheit, Westfälische Hochschule, Gelsenkirchen, Vorstandsvorsitzender TeleTrusT – Bundesverband IT-Sicherheit e.V.
10:30	KEYNOTE - **Informationssicherheit 4.0** **"Ein Erfahrungsbericht aus der Wirtschaft, aktuelle Bedrohungen und Gegenmaßnahmen"** Stephan Gerhager, Chief Information Security Officer (CISO), Allianz Deutschland AG
11:15	Kaffeepause
11:40	**"Cyberangriffe: Die Einschläge kommen näher!"** Michael Goedeker, CEO, Auxilium Cyber Security GmbH
12:10	**"Gamifying Security Awareness"** Jürgen Grieshofer, Managing Director, Awarity Training Solutions
12:40	**"Managed PKI & the world according to eIDAS"** Dr. Kim Nguyen, Geschäftsführer, D-Trust/Chief Scientist Security, Bundesdruckerei
13:00	Mittagspause
14:00	**"Phishing für Phortgeschrittene"** Marco Krause, Security Engineer, ING-DiBa AG
14:30	**"Zero-Day Hunting – Wie White-Hat Hacker agieren"** Andreas Falkenberg, Senior Security Consultant, SEC Consult
15:00	**"IT-Sicherheitsrisiken: Haftung und Versicherung"** RA Dr. Axel Frhr. v. d. Bussche, LL.M. (LSE), Fachanwalt für IT-Recht, TaylorWessing
15:30	**"Der Brandschutz des 21. Jahrhunderts - VdS-Cyber-Security für KMU"** Sebastian Brose, Stv. Abteilungsleiter Firmen und Fachkräfte, VdS Schadenverhütung GmbH
15:50	Kaffeepause
16:10	**Abschlussvorträge der Wettbewerbsteilnehmer**
16:50	**"Tutorial zur Collaborated Security – 8 Agenten in einem Pass Space: Wie kann die defensive Strategie der immer höheren Burgmauern und tieferen Gräben überwunden werden?"** Ulf Ziske, CEO, KikuSema GmbH Sophie Ziske, Schülerin, IT Gymnasiet Skövde/Schweden
17:20	**"Hacking für Deutschland!? Aufgaben und Herausforderungen der Cyberabwehr im BSI".** Andreas Könen, Vizepräsident Bundesamt für Sicherheit in der Informationstechnik
17:40	**Schlusswort und Verabschiedung** Prof. Dr. Norbert Pohlmann, Leiter if(is) - Institut für Internet-Sicherheit, Westfälische Hochschule, Gelsenkirchen, Vorstandsvorsitzender TeleTrusT – Bundesverband IT-Sicherheit e.V.
18:00	Ende der Veranstaltung
18:30	**Preisverleihung mit anschließender Feier** Prof. Dr. Norbert Pohlmann, Leiter if(is) - Institut für Internet-Sicherheit, Westfälische Hochschule, Gelsenkirchen, Vorstandsvorsitzender TeleTrusT – Bundesverband IT-Sicherheit e.V. Gertrud Husch, Leiterin des Referates "Sicherheit und Notfallvorsorge in der IKT" und Initiative "IT-Sicherheit in der Wirtschaft"

Weitere Informationen und Anmeldung unter

www.cybersecuritychallenge.de/konferenz

Vortragsdetails (Änderungen vorbehalten)

10:30 KEYNOTE - **Informationssicherheit 4.0**

"Ein Erfahrungsbericht aus der Wirtschaft, aktuelle Bedrohungen und Gegenmaßnahmen"

Stephan Gerhager, Chief Information Security Officer (CISO), Allianz Deutschland AG

Die IT spielt in unserem Alltag – ob privat oder beruflich – eine immer größere Rolle. Rund 45 Millionen Deutsche besitzen ein Smartphone, Wearables sind an vielen Handgelenken. Immer mehr Geräte sind internetfähig und vernetzt – von der Waschmaschine bis zum Auto. Der Alltag wird immer digitaler. Und viele Menschen sind überzeugt: Digital ist besser. Auf der anderen Seite stellt der Hackerfilm „Who am I" die These auf: „Kein System ist sicher". Was bedeutet das für diese neuen „smarten" Systeme, für unsere Gesellschaft und Wirtschafts-unternehmen?

Die Keynote beschäftigt sich mit den wichtigsten Informationssicherheitsrisiken und zeigt anhand zahlreicher Beispiele die aktuelle Bedrohungslage, gängige Hacking- und Angriffsmethoden sowie Gegenmaßnahmen und deren Grenzen auf.

Der Vortrag gibt damit einen Einblick in die tägliche Arbeit eines Informationssicherheitsmanagers: Was sind seine Aufgaben? Vor welchen Herausforderungen steht er? Untermauert werden die Thesen durch eine Live-Hacking-Demonstration.

Dipl. Inf. (FH) Stephan Gerhager ist seit 2012 Chief Information Security Officer der Allianz Deutschland AG. Zuvor hatte er die gleiche Position bei der E.ON Energie AG und davor bei der AUDI AG, in welcher er davor 4 Jahre in der IT-Security-Gruppe als Spezialist für Web-Applikations-Sicherheit und Hacking-Technologien beschäftigt war. Darüber hinaus forscht er seit Ende 2010 im Bereich "Cybersicherheit im zukünftigen Smart Grid" und vernetzten Fahrzeugen. Bereits seit 1995 arbeitet er im Bereich Software Development und IT-Sicherheit. Er hält regelmäßig Vorträge und Gastvorlesungen an verschiedenen deutschen Hochschulen sowie internationalen Experten-konferenzen zum Thema Informationssicherheit und Angriffs- bzw. Hacking-Technologien.

11:40 **"Cyberangriffe: Die Einschläge kommen näher!"**

Michael Goedeker, CEO, Auxilium Cyber Security GmbH

Spätestens jetzt wird auch dem letzten Zweifler klar sein: Die Bedrohungen durch Cyberangriffe sind realer, als viele es bisher glauben mochten. Schmerzhaft mussten das unsere Deutsche Bundesregierung die französische TV-Gruppe TV5 Monde oder auch Firmen wie Sony, adidas oder insbesondere kritische Infrastrukturen in der letzten Zeit merken. Die Einschläge kommen näher und es wird deutlich: Solche Szenarien können nicht nur unsere Nachbarn treffen, sondern auch Deutschland, deutsche Organisation als auch Firmen gleichgültig welcher Größe! Eine breit angelegte und tiefergehende Aufklärung von Wirtschaft, Industrie und Bürgern ist erforderlich. Sensibilisierung für Gefahren aus dem Netz steht dabei an oberster Stelle. Moderne Unternehmen müssen sich jedoch selbst auch in die Pflicht nehmen und sich die Frage stellen: Wie sieht es bei meinen eigenen Mitarbeitern mit dem Thema IT- und Datensicherheit aus? Unternehmen stehen damit auch in der Pflicht, ihre Mitarbeiter aufzuklären und deren Bewusstsein für Daten und IT-Sicherheit zu schulen.

Der Vortrag gibt einen aktuellen Überblick über die reale Bedrohungslage, zeigt Informationsquellen und Ansätze zur Selbsthilfe auf.

Michael (Mike) Goedeker kann auf eine langjährige IT Karriere zurück blicken, in welcher er sich erfolgreich vom IT Administrator zum Berater und dann Direktor für IT-¬ und Sicherheits-¬ Firmen ‚hochgearbeitet' hat. Die Kunden, Partner als auch Hersteller schätzen an Mike seine enthusiastische, motivierte Art, seine Kreativität als auch sein Durchhaltevermögen auch in schwierigen Situationen. Er war und ist für seine Kunden in Projekten national als auch international in der Beratung von IT Architekturen bis zum Thema Cyber- Sicherheit tätig.

12:10 **"Gamifying Security Awareness"**

Jürgen Grieshofer, Managing Director, Awarity Training Solutions

Selbst hochspezialisierte Firewalls, IDS, IPS, Spamfilter und wie sie alle heißen mögen, können uns nicht vor Low-Tech Attacken wie einem simplen Anruf, ein Notizzettel mit dem Passwort unter der Tastatur oder Trickbetrug schützen. Unwissenheit und Sorglosigkeit sind die Grundbausteine für erfolgreiche Social-Engineering Angriffe. Doch wie kann man die Mitarbeiter motivieren, trainieren und proaktiv an der Sicherheit im Unternehmen teilhaben lassen?

Jürgen Grieshofer ist Geschäftsführer und Gesellschafter der Awarity Training Solutions GmbH, sowie der 4CKnowLedge OG. Er hat die Höhere Technische Lehranstalt Wels für Elektrotechnik abgeschlossen und hat danach Erfahrung mit Industriellen Steuerungen, Netzdesign und IT-Sicherheit gemacht. In seiner Freizeit unterstützt er Projekte und Vereine wie OWASP, Cyber Security Austria, IoT Vienna und Funkfeuer (Freifunk).

Vortragsdetails (Änderungen vorbehalten)

12:40 **"Managed PKI & the world according to eIDAS"**
Dr. Kim Nguyen, Geschäftsführer, D-Trust/Chief Scientist Security, Bundesdruckerei

Vortragsbeschreibung:
Managed PKI als effizienter Business work flow und die Rolle von PKI im Kontext der EU Verordnung.

Kim Nguyen studierte Mathematik und Physik an der Universität Göttingen, am Trinity College in Cambridge (UK) sowie der Universität/Gesamthochschule Essen. Im Jahre 2001 wurde ihm von der Universität/GH Essen (Lehrstuhl Prof. Dr. Gerhard Frey) der Doktortitel in reiner Mathematik für eine Arbeit zu den Zusammenhängen von klassischen zahlentheoretischen Problemen, elliptischen Kurven und kryptographischen System verliehen. Von 2001-2003 war er bei Phillips Semiconductors (jetzt NXP Semiconductors) in Hamburg beschäftigt, dort beschäftigte er sich maßgeblich mit der sicheren Umsetzung von asymmetrischen kryptographischen Algorithmen auf Smartcards. Seit 2004 ist er bei der Bundesdruckerei GmbH in Berlin tätig. Hier übernahm er unterschiedliche Aufgaben in den Bereichen Entwicklung und Marketing und war zudem an der Umsetzung des elektronischen Reisepasses sowie des neuen Personalausweises beteiligt. Seit 2011 ist er als Chief Scientist Security im Entwicklungsbereich der Bundesdruckerei GmbH tätig. Seit Juni 2012 hat er zusätzlich die Geschäftsführung der D-Trust GmbH übernommen. Im Mai 2015 wurde ihm der Titel „Fellow" verliehen.

14:00 **"Phishing für Phortgeschrittene"**
Marco Krause, Security Engineer, ING-DiBa AG

In diesem Vortrag werden die psychologischen Tricks, die bei dieser Teil-Disziplin von Social Engineering eingesetzt werden vorgestellt. IT Experten wähnen sich häufig in Sicherheit, sind bei gezielten Attacken (Spear-Phishing) jedoch ebenso anfällig für die Ausnutzung menschlicher "Schwachstellen". Der größte Cyberbankraub aller Zeiten "Carbanak" hat mit einem Paukenschlag verdeutlicht, wie wichtig das Thema Phishing aktuell bereits ist.

Anhand der Betrachtung der Entwicklung von Phishing Mails von der Vergangenheit bis zur Gegenwart wird ein deutlicher Trend der Professionalisierung sichtbar, welcher sich zukünftig noch stärker ausprägen wird. Die bisherigen Sicherheitsmaßnahmen wie zum Beispiel Security Awareness Trainings reichen vielleicht für schlecht gemachte Massen-Attacken, aber einem relativ simplen Spear-Phishing Angriff halten diese auf Compliance bedachten Schulungen nicht stand. Diesem Trend lässt sich nur durch eine neue Herangehensweise entgegenwirken, welche in diesem Beitrag aufgezeigt werden.

Marco Krause hat 15+ Jahre Erfahrung in der IT Branche, darunter als System Administrator bei einem Vertragspartner des US DoD, Security Consultant bei NTT Com Security (Germany) GmbH und Security Engineer bei der ING-DiBa AG. Er ist zertifiziert durch GIAC (GSEC, GSNA) und diverse Hersteller.

14:30 **"Zero-Day Hunting – Wie White-Hat Hacker agieren"**
Andreas Falkenberg, Senior Security Consultant, SEC Consult

Kernaufgabe eines White-Hat Hackers ist die Identifikation von konkreten Schwachstellen in IT Produkten. Dies findet im Regelfall im Rahmen von Sicherheitsüberprüfungen für Kunden statt. Zusätzlich hierzu werden kundenunabhängig einer Laborumgebung IT Produkte großer Hersteller auf Herz und Nieren geprüft. Im Zuge dessen können weitere Schwachstellen identifiziert werden. Nach Identifizierung einer Schwachstelle ist die Arbeit für den White-Hat Hackers allerdings noch nicht beendet. So wird die Schwachstelle den Herstellern kommuniziert und nach Behebung veröffentlicht – mit zum Teil interessanten Feedback auf Herstellerseite. Der Vortrag gibt einen Einblick in die täglich Arbeit eines „White-Hat" Hackers – Beginnend mit der Identifikation einer Schwachstelle bis hin zur Veröffentlichung des öffentlichen Advisories.

Andreas Falkenberg arbeitet seit vielen Jahren als professionaler White-Hat Hacker. Durch Sicherheitsüberprüfungen in internationalen Projekten in Europa, Asien und den USA kann auf ein breites Erfahrungsspektrum zurückgegriffen werden; beginnend mit simplen Webseiten bis hin zur Core-Banking Applikationen. Andreas Falkenberg hat den Master in IT-Sicherheit / Informationstechnik an der Ruhr-Universität Bochum abgeschlossen. Neben diversen Talks auf Veranstaltungen ist er zudem Dozent am Technikum Wien."

Vortragsdetails (Änderungen vorbehalten)

15:00 **"IT-Sicherheitsrisiken: Haftung und Versicherung"**
RA Dr. Axel Frhr. v. d. Bussche, LL.M. (LSE), Fachanwalt für IT-Recht, TaylorWessing

Die Bedrohung der IT-Sicherheit von außen und von innen gehören mittlerweile zum Unternehmensalltag. Zunächst nur als beklagenswerter "Unfall" wahrgenommen, ist den Unternehmen mittlerweile bewusst, sich mit dem Cyberrisiko - gewissermaßen auf der Schattenseite der Digitalisierung - konkret auseinandersetzen zu müssen. Hierbei spielen als präventive Maßnahme das Herausarbeiten der Haftungsfragen und die Versicherbarkeit der neuartigen Risiken eine zentrale Rolle.

Axel Freiherr von dem Bussche ist Head der Practice Area Technology, Media & Telecoms und koordiniert zudem Taylor Wessings internationale US Group für Deutschland. Er ist spezialisiert auf die Technologie-Branche und den Bereich Datenschutz. Seine Beratungsschwerpunkte sind die Begleitung von Transaktionen, Software-Lizenzierung, Outsourcing, F&E-Projekte, branchenspezifische Vertragsgestaltungen, Internet- und Glücksspielrecht sowie Fragen der Regulierung. Er begleitet interne Prozesse im Bereich Konzerndatenschutz, einschließlich Verhandlungen mit Betriebsräten. Ein besonderer Schwerpunkt ist die Beratung in Angelegenheiten mit Auslandsbezug sowie die Betreuung expandierender ausländischer Mandanten in Deutschland.

15:30 **Der Brandschutz des 21. Jahrhunderts - VdS-Cyber-Security für KMU**
Sebastian Brose, Stv. Abteilungsleiter Firmen und Fachkräfte,
VdS Schadenverhütung GmbH

Die Unternehmenssicherheit mit ihren klassischen Handlungsfeldern Brandschutz, Security (Schutz gegen Einbruch, Diebstahl, Sabotage) und Naturgefahren (z.B. Überschwemmung, Starkregen) muss heute um den Aspekt der Informationssicherheit ergänzt werden. Die Nutzung moderner IT zur Bewältigung von betriebswirtschaftlichen, logistischen und technischen Geschäftsprozessen in Unternehmen, sowie der Anschluss an das Internet, sind heute unabdingbare Erfordernisse, um im weltweiten Wettbewerb bestehen zu können. Die Digitalisierung und die Vernetzung bieten aber auch eine breite Angriffsfläche für Cyber-Kriminelle, Daten und Know-how von Unternehmen abzugreifen oder die Betriebsabläufe empfindlich zu stören. Mit den Richtlinien "VdS-zertifizierte Cyber-Security" (VdS 3473) stellt VdS erstmalig eine Leitlinie zur Verfügung, mit der sich kleine und mittlere Unternehmen (KMU) angemessen vor Cyber-Gefahren schützen und dies durch ein Zertifikat einer unabhängigen Institution belegen können.

16:10 **Abschlussvorträge der Wettbewerbsteilnehmer**

Die Abschlussvorträge der Wettbewerbsteilnehmer ermöglichen den SchülerInnen und StudentInnen nach der eigentlichen Challenge am 15.09. nochmals Bonuspunkte zu sammeln. Jedes der vier Teams präsentiert anhand von jeweils zwei Challenges einer Jury sein technisches Wissen aber auch seine Fähigkeit, dieses verständlich darzustellen. Denn auch im Job muss man nicht nur Sicherheitslücken finden, sondern auch Vorschläge für erste Maßnahmen aufzeigen können und den Sachverhalt auch dem Management klarmachen können.

Konferenzteilnehmer erhalten durch die Präsentationen einen ganz besonderen Einblick in den Hacker-Wettbewerb.
Sie werden staunen, wie groß das Fachwissen der Finalisten bereits ist!

Vortragsdetails (Änderungen vorbehalten)

16:50 **"Tutorial zur Collaborated Security – 8 Agenten in einem Pass Space: Wie kann die defensive Strategie der immer höheren Burgmauern und tieferen Gräben überwunden werden?"**
Ulf Ziske, CEO, KikuSema GmbH
Sophie Ziske, Schülerin, IT Gymnasiet Skövde/Schweden

Noch immer ist eine Keyhole-Security (Schlüssellochsicherheit) üblich. Videoclips illustrieren, wie "gehackte" Identifizierung und Authentifizierung in bekannten Filmen dargestellt wird. Es zeigt sich: Eine Überwindung der Keyhole-Security durch die schrittweise Überführung in eine Welt der Collaborated Security (Sicherheit durch Zusammenarbeit) und Diversifikation ist notwendig. Eine Live-Demo lüftet den Schleier, der über den 8 Agenten in einem Pass Space liegt.

Demonstriert wird: nicht wie man etwas hackt, sondern wie mehrere Agenten bzw. Instanzen gemeinsam eine Authentifizierung durchführen und wie man den Zugang zu "schützenswerten Gütern" eines Jugendlichen (Fotos, App-In-Einkäufe, Zugang zu Social Media Plattformen) sicherer machen kann. Parallel werden folgende Aspekte diskutiert: Multi Instance Authentifizierung vs. Multifaktor Authentifizierung, Pass Space & Entropie, Scrambled Secrets Verschlüsselung durch Vermischung.

Dieser Einblick in zukünftige Sicherheitsmechanismen ist für IT-Sicherheitsexperten, CISO, CIOs, Unternehmer und Nachwuchstalente gleichermaßen interessant.

Ulf Ziske ist Gründer und Geschäftsführer der KikuSema GmbH. Er ist der Erfinder und der Entwickler der vielmals ausgezeichneten IT-Sicherheits-App "FabulaRosa and the Five New Protocols". Seine Ausbildung als Diplom-Wissenschaftsorganisator und seine jahrzehntelange Tätigkeit als Systementwickler ermöglichen es ihm zukünftige Herausforderungen an die Informationssicherheit nicht nur zu erkennen, sondern diese direkt in Applikationen umzusetzen. Sein Standpunkt ist es, dem Anwender zu ermöglichen, mit Hilfe von Authentifizierungstechnologie unabhängig und selbständig zu handeln.

Sophie Ziske ist eine 17jährige Schülerin am schwedischen IT Gymnasiet in Skövde, zweisprachig (de/sv) und als "Digital Native" aufgewachsen. Sie ist eine exzessive Anwenderin alle Dienste, die im Internet zu Verfügung stehen: Social Media, Dienste schwedischer Behörden und Banken über E-Legitimation, Cloud-Dienste etc. pp.

17:20 **"Hacking für Deutschland!? Aufgaben und Herausforderungen der Cyberabwehr im BSI".**
Andreas Könen, Vizepräsident Bundesamt für Sicherheit in der Informationstechnik

17:40 **Schlusswort und Verabschiedung**
Prof. Dr. Norbert Pohlmann, Leiter if(is) - Institut für Internet-Sicherheit, Westfälische Hochschule, Gelsenkirchen, Vorstandsvorsitzender TeleTrusT – Bundesverband IT-Sicherheit e.V.

18:00 Ende der Veranstaltung

18:30 **Preisverleihung mit anschließender Feier**

Prof. Dr. Norbert Pohlmann, Leiter if(is) - Institut für Internet-Sicherheit, Westfälische Hochschule, Gelsenkirchen, Vorstandsvorsitzender TeleTrusT – Bundesverband IT-Sicherheit e.V.

Gertrud Husch, Leiterin des Referates "Sicherheit und Notfallvorsorge in der IKT" und Initiative "IT-Sicherheit in der Wirtschaft"