

Der Fachkongress Deutschlands
für IT- und Cyber-Sicherheit bei
Staat und Verwaltung

PITS 20.-21. September
2023
Public-IT-Security

Digitales Immunsystem

20.-21. September 2023,
Telekom Hauptstadtrepräsentanz
Berlin

WLAN einschalten
und mit **Telekom**
verbinden

Browserfenster öffnet sich,
Online gehen tippen – fertig!
Es wird kein Passwort benötigt.



Digitales Immunsystem

Das Immunsystem ist das Abwehrsystem des menschlichen Körpers. Ein digitales Immunsystem ist für die deutsche Verwaltung ebenso lebenswichtig wie das menschliche: Verwaltungen und kritische Infrastrukturen sind immer neuen Cyberangriffen ausgesetzt. Wie ein Immunsystem den Körper vor Schadstoffen, Krankheitserregern und krankmachenden Zellveränderungen schützt, braucht die Verwaltung Schutz vor Ransomware, DDoS, Zero-Day-Angriffen oder Phishing-E-Mails.

Dabei unterscheiden Mediziner zwischen einem angeborenen Schutzschild, welches von Geburt an aktiv ist und einem erworbenen Schutzschild, das sich erst im Laufe des Lebens entwickelt.

Wenn das Immunsystem reibungslos funktioniert, macht es sich nicht bemerkbar. Wenn die körpereigene Abwehr aber versagt, weil sie geschwächt ist oder gegen besonders aggressive Krankheitserreger nichts ausrichten kann, wird man krank. Gleiches gilt für die Verwaltung: Nachhaltige Angriffe oder Engpässe können erhebliche Störungen der öffentlichen Sicherheit auslösen. Es braucht Maßnahmen, die nach erfolgreichen Angriffen auch Schäden beseitigen können.

Oft haben Erreger, die dem Körper bisher noch unbekannt sind, leichtes Spiel, die Abwehr zu schwächen oder gar mit schädlichen Viren in das System einzudringen. Ein gesundes Immunsystem braucht daher stetige Innovationen, die den Schutz erhöhen. Bedrohungen müssen frühzeitig erkannt und abgewehrt werden, dass die überlebensnotwendigen Organe und Tätigkeiten weiterarbeiten können. Bei bestimmten Erregern führt aber nur der erste Kontakt zu einer Erkrankung – zum Beispiel bei Kinderkrankheiten wie den Windpocken. Auch dafür müssen Medikamente und präventive Maßnahmen entwickelt werden, denn einen Systemausfall oder eine flächendeckende Störung des digitalen Immunsystems darf sich die deutsche Verwaltung nicht leisten.

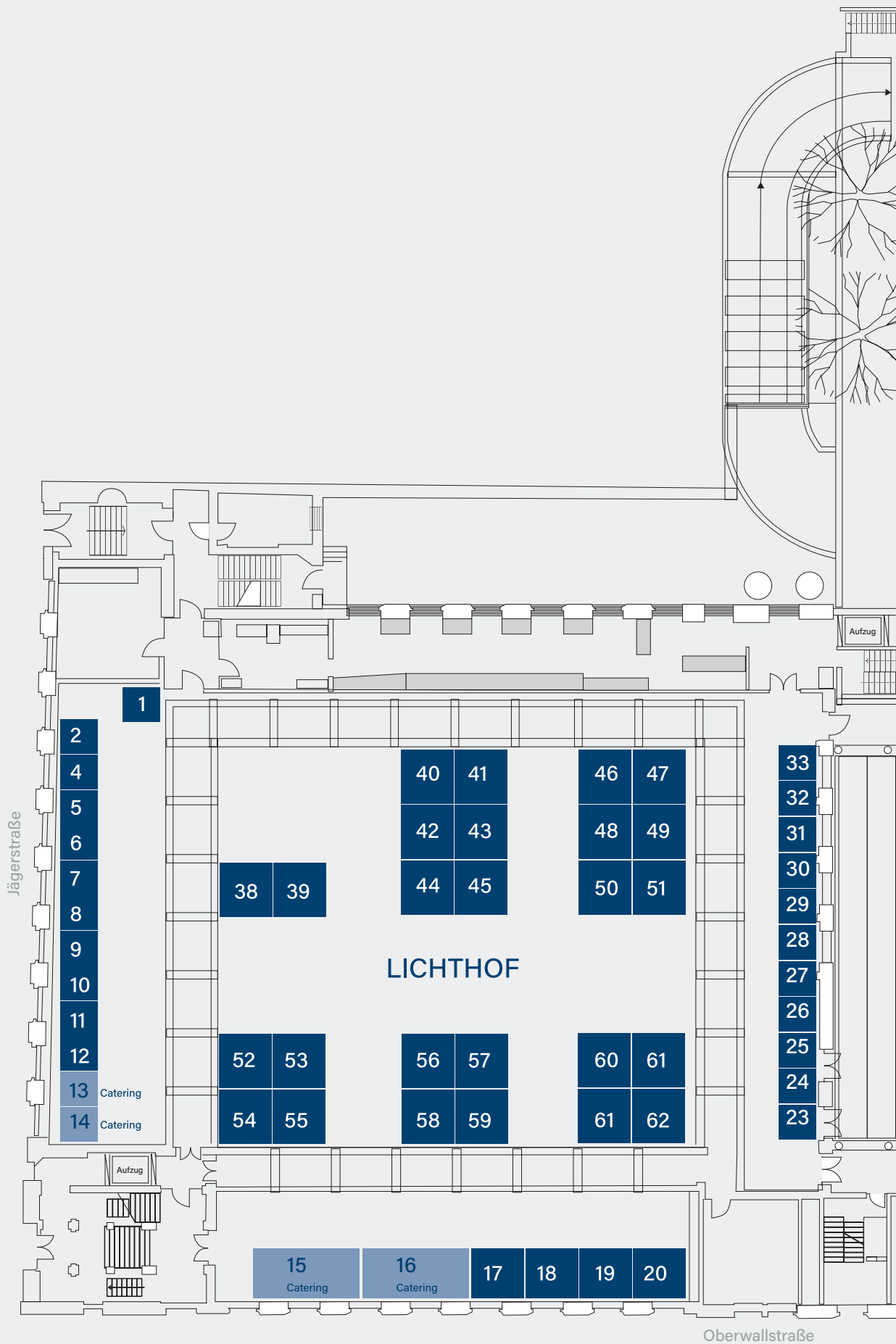
Die PITS 2023 widmet sich vollumfänglich dem digitalen Immunsystem. Im Fokus des Kongresses stehen die elementaren Fragen der Cyber-Sicherheit für Staat und Verwaltung. Die PITS wird als reale Veranstaltung durchgeführt. Zumindest in diesem Aspekt heißt es damit back to the roots – selbstverständlich mit angemessenen Abstandsregeln und einem modernen Hygienekonzept.

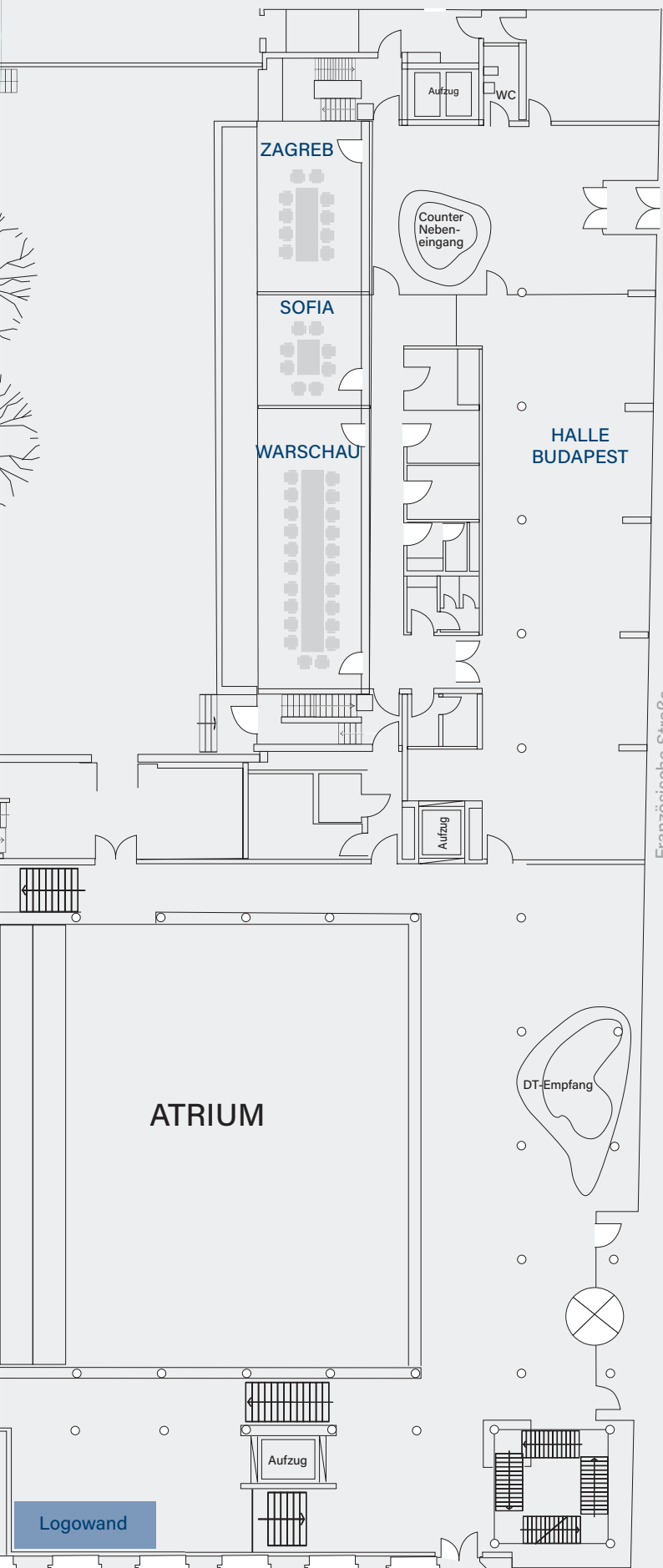
Als Treffpunkt der IT-Verantwortlichen von Bund, Ländern, Kommunen, den Streitkräften, Europäischen Polizeibehörden, den Nachrichtendiensten, der NATO, den Anbietern von Sicherheitslösungen und der Wissenschaft ist die Public-IT-Security (PITS) seit über zehn Jahren eine entscheidende Plattform für den Austausch zu neuen Trends der IT-Sicherheit.



Kongresspartner 2023







- 1 Proofpoint
- 2 Datawarehouse
- 4 FutureDat
- 5 FutureDat
- 6 BOC / Watchguard
- 7 AP Sensing
- 8 HiScout
- 9 HiScout
- 10 Secunet
- 11 Tixeo
- 12 Wagner Group
- 17 FB-Pro
- 18 slinf
- 19 Rotes Sofa
- 20 Rotes Sofa
- 23 Enginsight
- 24 Imperva
- 25 Splunk
- 26 Fortinet
- 27 Materna
- 28 Allgeier CyRis
- 29 Trellix
- 30 Exeon Analytics
- 31 QGroup
- 32 Cyberark
- 33 Netskope
- 38 Sophos
- 39 Fast LTA
- 40 Computacenter / Checkpoint
- 41 Genua
- 42 Computacenter / Checkpoint
- 43 Greenbone
- 44 Cybersense
- 45 Trend Micro Deutschland
- 46 Igel Technology
- 47 Behörden Spiegel
- 48 Skyhigh Security
- 49 Behörden Spiegel
- 50 Rubrik Germany
- 51 Rohde & Schwarz
- 52 Palo Alto
- 53 Kaspersky
- 54 Veeam / Purestorage
- 55 Bayoosoft
- 56 Cisco
- 57 Asconit
- 58 Google Cloud
- 59 VMRay
- 60 Adva Network Security
- 61 Sentinel One
- 62 Zscaler
- 63 SVA

08.00 Uhr	Einlass, Registrierung und Eröffnung der Ausstellung	
08.40 Uhr	Eröffnung des Kongresses und Begrüßung der Teilnehmenden Dr. Eva-Charlotte Proll, Herausgeberin und CDO, Behörden Spiegel Reinhard Wolski, Generalmajor a.D., Behörden Spiegel	
08.45 Uhr	Cyberresilienz in Kritischen Infrastrukturen Johann Saathoff, Parlamentarischer Staatssekretär bei der Bundesministerin des Innern und für Heimat	
09.00 Uhr	Capture the Flag: Defending Taiwan's Democracy from Foreign Interference Audrey Tang, Digitalministerin Taiwan	
09.15 Uhr	IT-Sicherheit, quo vadis? Und wieso, wehalb, warum? – denn, wer nicht fragt bleibt dumm Dirk Arendt, Director Public Sector, Trend Micro Deutschland	
09.30 Uhr	Aktuelle Herausforderungen der IT-Sicherheit Dr. Dirk Häger, Abteilungsleiter Operative Cyber-Sicherheit, Bundesamt für Sicherheit in der Informationstechnik	
09.50 Uhr	Digitales Immunsystem - durch Security by Design und Transparenz Jochen Michels, Head of Public Affairs Europe, Kaspersky	
10.05 Uhr	Gemeinsam stark: Eine kooperative Vision für Cybersicherheit Dr. Michael Zimmer, Referatsleiter Informationssicherheit, Cybersicherheit, Niedersächsisches Ministerium für Inneres und Sport	
10.20 Uhr	Zero Trust als wirkungsvolle Basis für Resilienz Michael Hlevnjak, Key Account Director Bundesbehörden, Google	
10.35 Uhr	Operation am offenen Herzen – Cybersicherheit in Zeiten exponentiellen Wachstums Moderation und Impuls: Prof. Dr. Haya Shulman, Leiterin der Abteilung Cybersecurity Analytics and Defences (CAD), Fraunhofer-Institut für Sichere Informationstechnologie SIT Andreas Könen, Abteilungsleiter „Cyber- und Informationssicherheit“, Bundesministerium des Innern, für Bau und Heimat Vincent Strubel, Generaldirektor der französischen Cybersicherheitsbehörde ANSSI Florian Schütz, Delegierter des Bundes für Cybersicherheit, Nationales Zentrum für Cybersicherheit Schweiz General Armin Fleischmann, Unterabteilungsleiter Cyber/Informationstechnik, Bundesministerium der Verteidigung	
11.30 Uhr	Kaffeepause	
12.00 Uhr	EXPERTENRUNDE 1	
	Die Wände haben Ohren – Kommunikation mit Fernzugriff, Homeoffice-Geräten und privaten Netzwerken	Angriffs- und Einbruchserkennung
	Von menschlicher zu maschineller Geschwindigkeit – Automatisierung in der Cyber-Sicherheit	Live-Simulation eines Cyber-Angriffs: Wie würden Sie reagieren?
	Cybersecurity als Service – Sinn oder Unsinn für Staat und Verwaltung?	Es operiert immer ein Team – Schutz vor Cyber-Angriffen vielfältiger gestalten
13.15 Uhr	Mittagspause	
14.45 Uhr	EXPERTENRUNDE 2	
	Von der ersten Hilfe für Kommunen zu ganzheitlicher IT-Security-Governance	NIS2-Umsetzungsgesetz – Herausforderungen und Lösungsansätze
	Schutz vor Zero-Day-Angriffen und Phishing-E-Mails	IT-Security als Treiber der Digitalisierung
16.00 Uhr	Kaffeepause	
16.30 Uhr	Vorbeugung, Antibiotika und Innovationen – welcher Arzt verschreibt den besten Schutz? Moderation: Dr. Eva-Charlotte Proll, Herausgeberin und CDO, Behörden Spiegel Dr. Dirk Häger, Abteilungsleiter Operative Cyber-Sicherheit, Bundesamt für Sicherheit in der Informationstechnik Generalmajor Jürgen Setzer, Stellvertretender Inspekteur, Kommando Cyber- und Informationsraum, CISO der Bundeswehr Dr. Sven Stephen Egyedy, Leiter Informations- und Kommunikationstechnik und Chief Technology Officer, Auswärtiges Amt Dirk Arendt, Director Public Sector, Trend Micro Deutschland	
17.30 Uhr	Sicher in die IT-Zukunft: Innovationen in der IT und die Gestaltung effektiver IT-Sicherheit Gregor Keller, Director Sales Engineering, Zscaler Germany	
17.45 Uhr	Resilienz und Business Continuity Management Moderation und Impuls: Sabine Griebisch, Managing Director, GovThings Dr. Patrick Grete, Referatsleiter Virtualisierung und Cloud-Sicherheit, Bundesamt für Sicherheit in der Informationstechnik Dr. Claudia Warken, Vizepräsidentin, Cybersicherheitsagentur Baden-Württemberg	
18.45 Uhr	Abendempfang	

08.00 Uhr	Einlass, Registrierung und Eröffnung der Ausstellung	
08.30 Uhr	Eröffnung des zweiten Kongresstages Prof. Dr. Ina Schieferdecker , Technische Universität Berlin	
08.45 Uhr	Grußwort Thomas Strobl , Stellvertretender Ministerpräsident und Minister des Inneren, für Digitalisierung und Kommunen des Landes Baden-Württemberg	
08.50 Uhr	Informationssicherheit im Saarland: Ganzheitlich. Ebenenübergreifend. Gemeinsam. Thorsten Sokoll , Landesbeauftragter für Informationssicherheit der Landesregierung (CISO) im Saarland und Vorsitzender der Arbeitsgruppe Informationssicherheit (AG InfoSic) des IT-Planungsrates	
09:05 Uhr	Security Plattform from best of breed to ways beyond Dr. Michael von der Horst , Managing Director Cyber Security Deutschland, Cisco Systems	
09.20 Uhr	Den Finger in die Wunde legen – Schwachstellen managen oder schließen? Moderation: Katharina Sook Hee Koch , Bundesamt für Sicherheit in der Informationstechnik Nikolas Becker , Leiter Politik & Wissenschaft, Gesellschaft für Informatik Catarina dos Santos-Wintz , Mitglied des Deutschen Bundestages (CDU/CSU) und Mitglied im Ausschuss für Digitales Dr. Dirk Häger , Abteilungsleiter Operative Cyber-Sicherheit, Bundesamt für Sicherheit in der Informationstechnik Dirk Kunze , Dezernatsleiter Ermittlungen Cybercrime/Cyber Recherche- und Fahndungszentrum, Landeskriminalamt NRW Dr. Jan Oliver Wagner , Vorstandsvorsitzender, Greenbone	
10.15 Uhr	Kaffeepause	
10.45 Uhr	Pitch 1: VS-NfD-Daten nativ mit iPhone und iPad nutzen Clemens A. Schulz , Director Endpoint Security, Rohde & Schwarz Cybersecurity Florian Vigyikan , agilimo Consulting	
11.05 Uhr	Pitch 2: Revolutionieren Sie Ihr SOC, indem Sie SIEM neu denken Anton Neidel , Major Account Manager Public Sector, Palo Alto Networks	
11.25 Uhr	Pitch 3: Kalte Pizza, Warme Cola – Malware Incident Response aus dem Blickwinkel der Cybercrime-Ermittlung Dr. Carsten Willems , CEO und Co-Founder VMRay Dirk Kunze , Dezernatsleiter Ermittlungen Cybercrime/Cyber Recherche- und Fahndungszentrum, Landeskriminalamt NRW	
11.45 Uhr	Pitch 4: Bedrohungslage – Trends & Treiber – Was ist ein Digitales Immunsystem und welche Aspekte sind wichtig ? Max Tammen , Major Account Manager Government, Check Point Armend Saliaj , Lead Consultant – Public Sector Security, Computacenter	
12.05 Uhr	Raumwechsel	
12.15 Uhr	EXPERTENRUNDE 3	
	Skalierungseffekte für Sicherheitsstandards – Sicherheit aus der Cloud	Ärztliche Schweigepflicht – VS-NfD schützt Bürger und Staat
	Gemeinsame Lagebilder, schlanke Cyber-Sicherheitsarchitektur und Gefahrenabwehr vom Land zum Bund	Im Dialog mit dem BSI: Zertifizierung, Zulassung, Audit etc. – Was ist wann sinnvoll?
13.30 Uhr	Mittagspause	
14.45 Uhr	EXPERTENRUNDE 4	
	Ransomware – Eine Seuche ohne Ende?	Starkes Rückgrat KRITIS – Mehr Pflichten gleich mehr Schutz?
	Cybercrime – Der Wurm im System	Es ist alles guuuuuut (wenn Sie mir Ihre Kontodaten geben) – Social Engineering als gesamtgesellschaftliche Gefahr
16.00 Uhr	Ende des Kongresses & Ausklang	

Die Wände haben Ohren – Kommunikation mit Fernzugriff, Homeoffice-Geräten und privaten Netzwerken

Raum: Bratislava

Moderation: **Katharina Sook Hee Koch**, Bundesamt für Sicherheit in der Informationstechnik
Dr. Günther Welsch, Abteilungsleiter “Krypto-Technologie und IT-Management“, Bundesamt für Sicherheit in der Informationstechnik
Dr. Michael Wendel, Referatsleiter, Informations- und Kommunikationstechnik, Bundeskanzleramt
Georg Hermann, Senior Sales Engineer, Netskope
Dr. Christoph Erdmann, Managing Director, Secusmart
Christian Eisenried, Global Head of Fed. & Central Gov. Sales, secunet

Angriffs- und Einbruchserkennung

Raum: Budapest

Moderation: **Sebastian Kosch**, Informationssicherheitsbeauftragter für das IM NRW, Ministerium des Innern des Landes Nordrhein-Westfalen
Ralf Sturhan, Geschäftsführer, Cybersense
Oliver Hilscher, Abteilungsleiter Informationstechnologie, Stadt Monheim am Rhein
Stefan Stein, Teamleiter CERT, Cyber Defense Center, gematik GmbH Berlin
Philip Goerd, Geschäftsführer, concentrade

Von menschlicher zu maschineller Geschwindigkeit – Automatisierung in der Cyber-Sicherheit

Raum: Zagreb

Moderation: **Guido Gehrt**, Stellvertretender Chefredakteur, Behörden Spiegel
Prof. Dr. Dirk Labudde, Professor für Forensik & Bioinformatik, Hochschule Mittweida
Michael Tullius, Sales Director Germany Exeon Analytics
Arnold Krille, Strategic Sales Manager, genua

Live-Simulation eines Cyber-Angriffs: Wie würden Sie reagieren?

Raum: Warschau

Während dieser Übung werden die Experten von Google Cloud und Mandiant mehrere Szenarien vorstellen, die auf realen Erfahrungen beruhen. Dies bietet den Teilnehmern die Möglichkeit, die einzigartigen Aspekte der Reaktion auf einen gezielten Sicherheitsangriff zu untersuchen.

Sergej Gilgenberg, Territory Account Manager Mandiant
Jochen Klotz, Consulting Sales Engineer Mandiant

Cybersecurity als Service – Sinn oder Unsinn für Staat und Verwaltung?

Raum: Atrium

Moderation: **Paul Schubert**, Redakteur, Behörden Spiegel
Martin Weiß, Senior Sales Engineer Public, Sophos
Danial Kamran, Global Solutions Engineer – Managed Detection and Response, Sophos
Andreas Daum, Rechtsanwalt, Noerr Partnerschaftsgesellschaft

Es operiert immer ein Team – Schutz vor Cyber-Angriffen vielfältiger gestalten

Raum: Prag

Moderation: **Peter-Michael Kessow**, Geschäftsführer, G4C German Competence Centre against Cyber Crime
Michael Dwucet, Referatsleiter CERT-Bund: Vorfallsbearbeitung und Verbindungsstelle Nationales Cyber-Abwehrzentrum, Bundesamt für Sicherheit in der Informationstechnik
Matthias Maier, EMEA Director, Splunk
Dr. Daniel Guagnin, Bereichsleiter Netze und Gesellschaft, nexus Institut für Kooperationsmanagement und interdisziplinäre Forschung und Mitglied im Bundesverband Smart City
Markus Wiegand, Stellvertretender Leiter, Hessen CyberCompetenceCenter (Hessen3C)
Roberto Concu, Account Executive, Rubrik

Von der ersten Hilfe für Kommunen zu ganzheitlicher IT-Security-Governance

Raum: Prag

Moderation: **Teresa Ritter**, Senior Associate, GovTech Campus Deutschland
Sven Kindervater, Referent, Deutschland sicher im Netz e.V.
Holger Berens, Vorstandsvorsitzender, Bundesverband für den Schutz Kritischer Infrastruktur
Sabine Griebisch, Managing Director, GovThings
Christian Stuffrein, Referent für Digitalisierung, Deutscher Landkreistag
Alexander Sander, Policy Consultant, Free Software Foundation Europe (FSFE)
Ferdinand Alexander Gehringer, Innere- und Cybersicherheit, Konrad-Adenauer-Stiftung

NIS2-Umsetzungsgesetz – Herausforderungen und Lösungsansätze

Raum: Bratislava

Moderation: **Paul Schubert**, Redakteur, Behörden Spiegel
Michael Kalisch, CISO und BCM Manager, Rundfunk Berlin-Brandenburg
Prof. Dr. René Treibert, Institutsleiter Clavis – Institut für Informationssicherheit der Hochschule Niederrhein
Heiko Adamczyk, Business Development Manager OT Fortinet
Dr. Christian Polster, Geschäftsführer, Materna Radar Cyber Security
Clemens Körner, Landrat, Rhein-Pfalz-Kreis

Schutz vor Zero-Day-Angriffen und Phishing-E-Mails

Raum: Budapest

Moderation und Impuls: **Markus Wiegand**, Stellvertretender Leiter, Hessen CyberCompetenceCenter (Hessen3C)
Ralf Benz Müller, stellvertretender Vorstandsvorsitzender, eurobits e.V.
Jonas Spieckermann, Manager Sales Engineering Central Europe, WatchGuard Technologies
Timo Wember, Senior Solutions Engineer, CyberArk
Thomas Blumenthal, CEO und Chief Security Architect, QGroup

IT-Security als Treiber der Digitalisierung

Raum: Atrium

Moderation & Impuls: **Dr. Jan Remy**, CISO des Freistaats Bayern
Ralf Stettner, Abteilungsleiter Cyber- und IT-Sicherheit, Verwaltungsdigitalisierung, Hessisches Ministerium des Innern und für Sport und CISO der Hessischen Landesverwaltung
Thomas Menke, Referatsleiter Koordinierungsstelle für Cybersicherheit NRW und die Informationssicherheit im IM und im Geschäftsbereich, Ministerium des Innern des Landes Nordrhein-Westfalen
Franziska Weiß, Business Manager, BAYOOSOFT
Dr. Alexander Löw, Gründer und Geschäftsführer, Data-Warehouse
Christian Drieling, Sales Engineering Manager, Imperva

Skalierungseffekte für Sicherheitsstandards – Sicherheit aus der Cloud

Raum: Bratislava

Moderation: **Guido Gehrt**, Stellvertretender Chefredakteur, Behörden Spiegel
Impuls: **David Anders**, Referent Cybersicherheit, Bundesministerium des Innern und für Heimat
Susanne Dehmel, Mitglied der Geschäftsleitung, Bitkom
Prof. Dr. Dennis-Kenji Kipker, Professor für IT-Sicherheitsrecht, Hochschule Bremen
Binthu Vijayaratnam, Manager Sales Engineering, EMEA (Channel & Account Management), IGEL Technology

Ärztliche Schweigepflicht – VS-NfD schützt Bürger und Staat

Raum: Prag

Moderation: **Dr. Eva-Charlotte Proll**, Herausgeberin und CDO, Behörden Spiegel
Marc Akkermann, Bundesverband der Deutschen Sicherheits- und Verteidigungsindustrie e.V.
Clemens A. Schulz, Director Endpoint Security, Rohde & Schwarz Cybersecurity
Dr. Alexander Koenen, Geschäftsführung, Xecuro
Tassilo Singer, Strateg. Beratung im Bereich Informationssicherheit, Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITIS)

Gemeinsame Lagebilder, schlanke Cyber-Sicherheitsarchitektur und Gefahrenabwehr vom Land zum Bund

Raum: Budapest

Moderation & Impuls: **Markus Albert**, Informationssicherheitsbeauftragter, FITKO (Föderale IT-Kooperation)
Dr. Claudia Warken, Vize-Präsidentin, Cybersicherheitsagentur Baden-Württemberg (CSBW)
Anke Richter, Referatsleiterin Lage, strategische Auswertung und Kooperationen, Bundeskriminalamt
Dr. Lutz Viehweger, Referent, Koordinierungsstelle für Cybersicherheit NRW, Ministerium des Innern des Landes Nordrhein-Westfalen

Im Dialog mit dem BSI: Zertifizierung, Zulassung, Audit etc. – Was ist wann sinnvoll?

Raum: Atrium

Moderation & Impuls: **Dr. Barbara Held**, Behörden Spiegel
Matthias Intemann, Fachbereichsleiter Zertifizierungsverfahren, Bundesamt für Sicherheit in der Informationstechnik
Ingrid Wilke, Fachbereichsleiterin Zulassung und Bereitstellung von VS - und IT -Sicherheitssystemen , Bundesamt für Sicherheit in der Informationstechnik
Andreas Groß, Director Solutions Engineering, Germany, Trellix
Lars Kukuk, Bereichsleiter der Informationssicherheit und Chief Information Security Officer, Bundesagentur für Arbeit
Sebastian Kosch, Informationssicherheitsbeauftragter für das IM NRW, Ministerium des Innern des Landes Nordrhein-Westfalen

Ransomware – Eine Seuche ohne Ende?

Raum: Atrium

Moderation: **Prof. Dr. René Treibert**, Institutsleiter Clavis – Institut für Informationssicherheit der Hochschule Niederrhein
Thomas Biere, Referatsleiter Informationssicherheitsberatung für den Bund und Grundsatz, Bundesamt für Sicherheit in der Informationstechnik
Ralf Benz Müller, stellvertretender Vorstandsvorsitzender, eurobits e.V.
Stefan Mai, Senior Channel Account Manager, BlackBerry
Markus Klose, Account Executive, Pure Storage

Starkes Rückgrat KRITIS – Mehr Pflichten gleich mehr Schutz?

Raum: Budapest

Moderation: **Dr. Barbara Held**, Behörden Spiegel
Maximilian Haselberger, Mitglied, AG KRITIS
Benjamin Wetter, Leiter, Cyber-Reservistenarbeitsgemeinschaft (CRAG) Hamburg
Clemens Pohl, CEO, AP Sensing
Claudia Wolf, Head of Sales, Enginsight

Cybercrime – Der Wurm im System

Raum: Bratislava

Moderation: **Beatrix Jakobs**, Leiterin Zentrale IT-Stelle, Rheinland Pfalz
Anke Richter, Referatsleiterin Lage, strategische Auswertung und Kooperationen, Bundeskriminalamt
Jan Lemnitzer, Assistant Professor Department of Digitalization, Copenhagen Business School
Maximilian Heitkämper, Fachbereichsleiter Digitales und Verbraucherrecht, Verbraucherzentrale Rheinland-Pfalz

Es ist alles guuuuuut (wenn Sie mir Ihre Kontodaten geben) – Social Engineering als gesamtgesellschaftliche Gefahr

Raum: Prag

Moderation & Impuls: **Sandra Balz**, Bereichsleitung Mittelstand, Deutschland sicher im Netz
Stefan Becker, Referatsleiter Cyber-Sicherheit für die Wirtschaft, Bundesamt für Sicherheit in der Informationstechnik
Dr. Christian Schunck, Identity Management, Fraunhofer IAO
Richard Huber, Assoziierter Forscher Forschungsgruppe „Digitalisierung und vernetzte Sicherheit“, Fraunhofer Fokus

12.–13. März 2024

DIGITALER



STAAT

schneller, stärker, souveräner –

GEMEINSAM.

Andel's Berlin

SAVE THE DATE



[DIGITALER-STAAT.ORG](https://digitaler-staat.org)

Behörden Spiegel