Hessische Staatskanzlei

Hessische Ministerin für
Digitale Strategie und Entwicklung

HESSEN

Konferenz-Reader

Secure Smart Region Congress 2021

digitales.hessen

Inhalt

Grußworte

Prof. Dr. Kristina Sinemus 3

Peter Beuth 4

Keynotes 5

Sicheres Smartes Hessen 6

Cyber- und IT-Sicherheit in Hessen 8

Raus aus den Silos – Sicherheitsanforderungen für smarte Regionen 10

Post-Quantum-Kryptografie für Datenschutz und Sicherheit im Internet 11

Herausforderungen für sichere Kritische Infrastrukturen 12

Workshops 13

Datenplattformen und andere Digitalisierungsprojekte 14

Unterstützung durch zivile Hilfskräfte bei Cyber-Großschadenslagen 15

Governance von Cybersicherheit für Kommunen 16

Best Practices 17

Living Labs und innovative Ökosysteme 18

Die Sicherheit von Bürgerinnen und Bürgern sowie die Widerstandsfähigkeit von smarten Städten und Regionen verbessern 19

Die digitale Kommune – smart UND sicher! 20

Cybersicherheit in smarten Regionen – auch eine Frage verständlicher Zahlen! 21

Partizipation als zentrales Element der Smart Region 22

Gemeinsam zu einer nachhaltigen Sicherheitskultur 23

Protecting the IoT – Lösungen für vernetzte Systeme 24

Sichere 5G-basierte Lösung zur smarten Verkehrssteuerung 25

Erhöhte Sicherheit durch autonomes Verkehrsmanagement 26

Anwendungsorientierte Forschungsförderung in Hessen 27

Paneldiskussion 28

Statements 29

Impressum 31

„Wir sind in Hessen auf dem Weg zur Secure Smart Region!“

Liebe Leserinnen und Leser,

im Juli 2021 rief der Landkreis Anhalt-Bitterfeld wegen eines Cyberangriffs den Katastrophenfall aus – den ersten dieser Art in Deutschland. Der Vorfall hat eine neue Herausforderung ins öffentliche Bewusstsein gerückt: digitale Attacken auf unsere Kommunen.

Klar ist: Wir wollen smarte Kommunen, digitale Rathäuser und intelligente Mobilität. Das macht Hessen lebenswerter sowie umwelt- und klimafreundlicher. Um diesen Prozess zu unterstützen, haben wir die Geschäftsstelle Smarte Region Hessen eingerichtet und den Smart Region Congress etabliert. Hier beraten und unterstützen wir Kommunen, digitale Technologie einzuführen.

Doch je mehr sich Kommunen digitalisieren, desto stärker suchen Cyberkriminelle nach Einfallslöchern. Die Frage ist: Wie können sich Kommunen schnell digitalisieren und gleichzeitig ein hohes Cybersicherheits-Niveau beibehalten?

Das haben wir auf dem ersten Secure Smart Region Congress diskutiert. Hier haben wir Hessens Kommunen mit kompetenten Fachleuten aus Wirtschaft und Wissenschaft zusammengebracht. Zentrale Fragen waren: Wovor sollten sich smarte Kommunen schützen? Wie sollten sie es tun? Und wer kann ihnen dabei helfen? Dazu haben wir viele kluge Antworten gehört – auch aus Israel, einer der weltweit führenden Nationen in Cybersicherheit. Der Kongress hat uns einen großen Schritt weiter auf dem Weg zur Secure Smart Region Hessen gebracht. Die wichtigsten Ergebnisse und Erkenntnisse haben wir in dieser Dokumentation zusammengefasst. Vielversprechende Maßnahmen werden wir umsetzen und weiterentwickeln. Daran arbeiten Peter Beuth, der hessische Innenminister, und ich gemeinsam, um unser Ziel einer Secure Smart Region Hessen zu erreichen.

Prof. Dr. Kristina Sinemus
Hessische Ministerin für Digitale Strategie und Entwicklung

„Der Kongress zeigt, wie wichtig das Thema Sicherheit für alle Beteiligten in smarten Regionen ist."

Liebe Leserinnen und Leser,

der erste Secure Smart Region Congress der Hessischen Staatskanzlei, Geschäftsbereich der Ministerin für Digitale Strategie und Entwicklung, mit Unterstützung des Hessischen Ministeriums des Innern und für Sport wurde sehr positiv aufgenommen. Das zeigt, wie wichtig das Thema Sicherheit für alle Beteiligten in smarten Regionen ist.

Wir haben uns über die wertvollen Beiträge von Mitarbeiterinnen und Mitarbeitern unserer Verwaltung, Wissenschaftlerinnen und Wissenschaftlern sowie Start-ups gefreut. Auch unsere Gäste aus Israel haben uns interessante Anregungen gegeben, wie sichere smarte Regionen und Städte gelingen können. Das alles hilft uns, die Digitalisierung in Hessen weiter voranzubringen.

Ich wünsche Ihnen viel Freude und viel Spaß mit dieser Dokumentation, die Ihnen wichtige Ideen und Impulse des Kongresses vorstellt.

Peter Beuth
Hessischer Minister des Innern und für Sport

Mehr Informationen über alle Angebote des HMdIS:
https://innen.hessen.de/Sicherheit/Cyber-und-IT-Sicherheit

Keynotes

Welche Visionen gibt es in Hessen zum Ausbau smarter Regionen und Städte? Wie können sich Kommunen schnell und effektiv digitalisieren und dabei ein hohes Niveau bei der Cybersicherheit beibehalten? Und vor welchen Herausforderungen müssen Kommunen sich schützen, wenn sie smarte Regionen schaffen?

Die Keynotes gaben Antworten darauf!

Sicheres smartes Hessen

Cyber- und IT-Sicherheit in Hessen

Raus aus den Silos – Sicherheitsanforderungen für smarte Regionen

Post-Quantum-Kryptografie für Datenschutz und Sicherheit im Internet

Herausforderungen für sichere Kritische Infrastrukturen

Keynotes

Sicheres smartes Hessen

„Hessen soll bis 2030 eine Smart Region werden – ein Bundesland mit smarten Regionen und Kommunen als Zukunftsorte, die hohe Lebensqualität und Nachhaltigkeit bieten."

Mit der fortgeschriebenen Strategie „Digitales Hessen – Wo Zukunft zuhause ist" ist das Ziel klar definiert. Hessen soll bis 2030 eine Smart Region werden – ein Bundesland mit smarten Regionen und Kommunen als Zukunftsorte, die hohe Lebensqualität und Nachhaltigkeit bieten, weil sie klug, passgenau und innovativ auf digitale Anwendungen setzen und Daten als Grundlage ihres Handelns nutzen.

Schon heute ist Hessen ein wichtiger Hotspot der europäischen Smart-Region-Entwicklung. Pilotkommunen wie Darmstadt, Eichenzell oder Kassel finden mit ihren Innovationen bundesweit Beachtung. Ob urbane Datenplattformen, umweltsensitive Verkehrssteuerung oder digitale Tools zur Bürgerbeteiligung: Smart-Region-Anwendungen made in Hessen schaffen konkrete Mehrwerte für Bürgerinnen und Bürger vor Ort.

Auf dem Weg in diese digitale Zukunft sind wichtige erste Schritte gemacht: Mit der virtuellen Geschäftsstelle Smarte Region wurde eine Einheit geschaffen, die der wachsenden Smart-Region-Community in Hessen als Plattform zur Verfügung steht und ihr attraktive Angebote für Austausch, Vernetzung, Beratung und Wissenstransfer unterbreitet. Hierzu zählen insbesondere der jährliche Kongress „Digitale Städte, Digitale Regionen", ein Infoportal mit einer Best-Practice-Datenbank sowie verschiedene Fachinformationen und FAQs. Über die Förderung smarte Kommunen und Regionen im Programm Starke Heimat stehen hessischen Kommunen zudem pro Jahr 16 Millionen Euro für die Entwicklung und Umsetzung innovativer Vorhaben zur Verfügung.

So gelingt es, gute Ideen für die Smart Region Hessen noch schneller umzusetzen und die Innovationskraft in die Breite aller hessischen Kommunen zu tragen.

Keynotes

Sicheres smartes Hessen

Nur gilt bei all den Vorteilen smarter Städte und Regionen: Je digitalisierter sie sind, desto mehr Angriffsflächen haben Cyberkriminelle. Entsprechende Vorsichtsmaßnahmen lassen sich aus der Cybersicherheitsforschung ableiten. Mit dem Nationalen Forschungszentrum für angewandte Cybersicherheit ATHENE mit Sitz in Darmstadt hat Hessen einen international renommierten und strahlenden Leuchtturm der Cybersicherheitsforschung. Um ATHENE herum bildete sich in Darmstadt ein starkes Ökosystem in den Themen Cybersicherheit und Privatsphärenschutz: zum Beispiel mit zahlreichen Ausgründungen und Initiativen wie dem Competence Center for Applied Security Technology. Außerdem zeichnete die Bundesregierung den Standort Darmstadt bereits 2017 zum Digital Hub Deutschlands für das Thema Cybersicherheit aus.

Von den Forschungsergebnissen profitieren Kommunen und Unternehmen dank eines ebenso effizienten wie praxisorientierten Wissenstransfers. Hier spielt das House of Digital Transformation eine besondere Rolle. Es vernetzt als Teil der Hessischen Innovationsstrategie Wirtschaft, Wissenschaft und Politik. Dies ebenfalls als Partner der Geschäftsstelle Smarte Region.

Um gleichermaßen smart wie sicher zu sein, können unsere Kommunen zudem auf Start-ups sowie kleine und mittlere Unternehmen zählen, die auf Cybersicherheit spezialisiert sind. Durch das kürzlich vom Land Hessen novellierte Vergabe- und Tariftreuegesetz finden beide Seiten fortan leichter zueinander, da es ermöglicht, bei Vergaben grundsätzlich auch den Aspekt der Innovation zu berücksichtigen. Konkrete Hinweise zu smarter Vergabe finden sich auf der Homepage der Geschäftsstelle Smarte Region.

Hinweis
Mehr Informationen über alle Angebote der Geschäftsstelle Smarte Region:
https://www.smarte-region-hessen.de/

Denis Liebetanz
Hessische Staatskanzlei
Hessische Ministerin für
Digitale Strategie und Entwicklung
Referat Institutionen der
Digitalisierung und Smart Region

www.digitales.hessen.de

Sebastian Köster
Hessische Staatskanzlei
Hessische Ministerin für
Digitale Strategie und Entwicklung
Referat Institutionen der
Digitalisierung und Smart Region

www.digitales.hessen.de

Keynotes

Cyber- und IT-Sicherheit in Hessen

2021 hat die weitreichenden Folgen von Sicherheitsangriffen auf (öffentliche) Infrastrukturen deutlich vor Augen geführt, u. a. mit dem Ausrufen des ersten Cyberkatastrophenfalls in Deutschland.

In Hessen steht das Thema Cybersicherheit seit vielen Jahren weit oben auf der Agenda: Unser Ziel ist eine bedarfsorientierte Sicherheitsarchitektur, bei der alle Akteure aus Wirtschaft, Verwaltung, Wissenschaft und über die Ebenen Bund, Land und Kommunen hinweg zusammenarbeiten. Hessen hat derzeit eine führende Stellung unter allen 16 deutschen Ländern inne. Wir bieten zahlreiche zielgerichtete Angebote in den Bereichen Prävention, Detektion, Reaktion, aber auch Vernetzung an, die wir kontinuierlich ausbauen. Unsere wichtigsten Initiativen sind:

Angebote für kleine und mittlere Unternehmen (KMU) und Kommunen

Das Hessen CyberCompetenceCenter (Hessen3C) als zentrale Kompetenzstelle im Bereich Cybersicherheit, u. a. mit

- MIRT – das Mobile Incident Response Team unterstützt Kommunen und KMU primär IT-forensisch vor Ort
- Warn- und Informationsdienst zu Aspekten der Cyber- und IT-Sicherheit
- 24/7-Verfügbarkeit und Hilfe für betroffene Kommunen und Unternehmen
- Beratungen vor Ort
- Durchführung von Informations- und Awareness-Veranstaltungen

Spezielle Angebote für Kommunen

- Kommunales Dienstleistungszentrum Cybersicherheit (KDLZ-CS): Passgenaue Unterstützung und konkrete Umsetzung von Maßnahmen gemeinsam mit der ekom21
- Hessisches Cyberabwehrausbildungszentrum HECAAZ (im Aufbau), u. a. mit mobilem IT-Lernlabor
- Beratungsangebote im Bereich Informationssicherheitsmanagementsysteme (ISMS), IT-Krisenmanagement (IT KM) oder Business Continuity Management (BCM)
- Cybersicherheitsgipfel: Sicherheitskongress für Kommunen im Oktober 2022
- Innovationsmanagement Cybersicherheit

Keynotes

Cyber- und IT-Sicherheit in Hessen

Weitere Vorhaben

- Hessisches IT-Sicherheitsgesetz (HITSiG)
- Hessische Cybersicherheitsstrategie
- Ausbau der landesinternen Cyberreserve
- Ausbildung und Awareness-Kampagnen im Bereich Cyber- und IT-Sicherheit, unter anderem mit geförderten Professuren
- Übung von IT-Krisenlagen
- Etablierung einer IT-Sicherheitsdenkkultur

Hinweis
Mehr Informationen über alle Angebote des HMdIS:
https://innen.hessen.de/Sicherheit/Cyber-und-IT-Sicherheit

Ralf Stettner
Hessisches Ministerium des Innern
und für Sport
Abteilung VII Cyber- und IT-Sicherheit,
Verwaltungsdigitalisierung

www.innen.hessen.de

Keynotes

Raus aus den Silos – Sicherheitsanforderungen für smarte Regionen

„Wir können in einer Smart Region sicher leben, kommunizieren und interagieren, vorausgesetzt bestimmte Faktoren und deren Sicherheitsrelevanz werden adressiert."

Von smarten Parksensoren über intelligente Bushaltestellen bis hin zu smarter Straßenbeleuchtung und Luftsensoren – in der vernetzen Stadt/Region funktioniert das Hand in Hand. Diese Interoperabilität setzt jedoch voraus, drei Faktoren und deren Sicherheitsrelevanz zu adressieren: die Visibilität, den Faktor Mensch und die äußeren Bedrohungsszenarien.

Sichere smarte Regionen setzen Visibilität voraus: Man kann nicht schützen, was man nicht sehen kann. Ein Überblick der eigenen IT-Infrastruktur und der einzelnen Smart Devices muss jederzeit sichergestellt werden.

Darüber hinaus gilt es auch stets den Faktor Mensch im Blick zu haben. Zum einen müssen Bürgerinnen und Bürger in den Prozess der Schaffung smarter Regionen einbezogen werden. Nur so kann Sicherheit gelebt und verinnerlicht werden. Zum anderen muss die Ressource Mensch geschaffen werden, damit Sicherheit von Beginn an mit Knowhow und Wissen vorgelebt werden kann.

Darauf aufbauend gilt es immer auch externe Bedrohungen zu berücksichtigen. Dies erfolgt durch die Implementierung geeigneter Methoden, Produkte und Maßnahmen.

Diese drei Faktoren sollten prinzipiell miteinander einhergehen. Denn das beste IT-Securitysystem bietet keinen Schutz, wenn weder klar ist, was geschützt werden muss, noch stringent gehandelt wird.

Werden die Faktoren jedoch berücksichtigt, ermöglicht Security uns, sicher in einer Smart Region zu leben, kommunizieren und interagieren. Sie kann dann dabei helfen, die anfallenden "Informationsknoten" zu erkennen, sammeln und klassifizieren.

Melanie Eschbach
Check Point Software Technologies

www.checkpoint.com

Keynotes

Post-Quantum-Kryptografie für Datenschutz und Sicherheit im Internet

Schwachstellen der derzeit zur Sicherung des Internets genutzten Public-Key-Infrastruktur werden durch die Entwicklung von Quantencomputern verstärkt, mit schwerwiegenden Auswirkungen auf Datenschutz, Sicherheit und Kryptowährungen. Für zukünftige Sicherheitsinfrastrukturen ist die Verteilung von Informationen eine Schlüssellösung. Aufgrund der Entwicklungsplanungen zu Quantencomputern wird für die heute verschlüsselten Daten eine ernsthafte Bedrohung innerhalb von weniger als einem Jahrzehnt prognostiziert. Hier hat man nun die Gelegenheit, die Sicherheit des Internets auf Grundlage der Public-Key-Infrastrukturarchitektur neu zu überdenken.

Für die Privatsphäre ist es ein großes Risiko, alle Informationen auf einer bestimmten Website zu speichern oder über einen bestimmten Kanal zu senden. Sie stellen Ziele für einen Man-in-the-Middle-, Diensteanbieter- oder Penetrationsangriff dar, der wiederum zu Datenlecks und Ransomware-Angriffen führen kann, wie sie täglich auftreten. Die Informationsverbreitung kann uns heute ineffiziente Lösungen für Daten in Bewegung, aber auch Daten im Ruhezustand liefern. Das Eigentumsrecht an der Information an sich bleibt erhalten, wenn eine Kreditkartennummer, eine Zufallszahl per E-Mail oder per SMS versendet wird, sowie dass das XOR-Gatter die tatsächliche Zahl ist. Mit dem Speichern von Fotos auf Ihrem eigenen Computer/Server riskieren Sie Datenlecks und/oder Ransomware-Angriffe. Beim Speichern in Google Drive und dergleichen setzen Sie Ihr Vertrauen in eine einzelne Entität (und damit allen Arbeitgebern dieser Entität) und Sie setzen sich dem Verlust an Ihrem Eigentum an den Daten aus. Deswegen sollte man eine Multi-Cloud-Lösung, in der jede Cloud die Zufallszahlen speichert, bevorzugen. Blockchain Distributed Trust ergänzt die oben genannten Lösungen und ermöglicht smart contracts.

Fazit

Quantencomputing bietet die Chance, die Sicherheit des Internets neu zu überdenken – ergreifen wir sie!

Prof. Dr. Shlomi Dolev
Ben-Gurion University of the Negev
Be'er Sheva, Israel

www.cs.bgu.ac.il

Keynote

Herausforderungen für sichere Kritische Infrastrukturen

Smarte Regionen und Städte sind extrem abhängig von der Sicherheit ihrer Kritischen Infrastrukturen (KRITIS) – zum Beispiel bei der Digitalisierung und Vernetzung von Kommunikation, Mobilität und Verkehr, Gesundheit und Energie. Und da KRITIS fast immer funktionieren, hat ein möglicher Ausfall umso drastischere Folgen, denn er trifft auf eine unvorbereitete Bevölkerung. Dieser vermeintliche Widerspruch (sichere Infrastrukturen führen zu großen Schäden bei möglichen Ausfällen) wird als „Verletzlichkeitsparadoxon" bezeichnet: „In dem Maße, in dem ein Land in seinen Versorgungsleistungen weniger störanfällig ist, wirkt sich jede Störung umso stärker aus." (BMI – Bundesministerium des Innern und für Heimat)

Für smarte Regionen und Städte ist es deshalb wichtig, Angriffe und Störungen bestmöglich zu vermeiden, sich aber gleichzeitig auf den Umgang mit diesen gut vorzubereiten. Das Risiko- und Krisenmanagement kann dabei folgende Schritte vorsehen:

- Bildung der Gefährdungskategorien
- Festlegung des Schutzniveaus
- Herleitung von Szenarien
- Schwachstellenanalyse
- Definition von Schutzzielen und zugehörigen Maßnahmen
- Bestimmung des Handlungsbedarfs
- Umsetzung und Überprüfung

Zu diesen Themen forscht der Lehrstuhl PEASEC der TU Darmstadt und der Forschungsbereich SecUrban von ATHENE. Weitere Informationen unter www.peasec.de sowie www.securban.athene-center.de.

Prof. Dr. Christian Reuter
ATHENE/TU Darmstadt

www.securban.athene-center.de

Workshops

Die interaktiven Workshops griffen auf Basis eines Vorab-Feedbacks der Teilnehmenden drei sehr spannende Themen und Inhalte auf:

Datenplattformen und andere Digitalisierungsprojekte

Unterstützung durch zivile Hilfskräfte bei Cyber-Großschadenslagen

Governance von Cybersicherheit für Kommunen

Die Teilnehmenden hatten die Gelegenheit, tiefer in die Themen einzusteigen, und auch ihre Herausforderungen und Anforderungen einzubringen.

Workshops

Datenplattformen und andere Digitalisierungsprojekte

Es tut sich etwas im Land: Zu diesem Ergebnis kommt der 3. Smart City Index des Bitkom. Der Index untersucht den Digitalisierungsgrad deutscher Städte ab 100.000 Einwohnern in verschiedenen Kategorien von intermodaler Mobilität und Bürgerbeteiligung über Energie und Umwelt bis zur digitalen Verwaltung. Es zeigen sich viele Dynamiken, insbesondere was die verschiedenen Digitalisierungstrends angeht. Während einige Städte ihren Vorsprung ausbauen, stehen andere noch in den Startlöchern für ihre Smart-City-Strategie. Zu den Spitzenreitern gehören auch in diesem Jahr Hamburg, Köln, Karlsruhe, München und Darmstadt.

Die Bestplatzierten haben sich in den vergangenen Monaten im Besonderen der Einführung von Smart-City-Datenplattformen gewidmet, die das technische Herz der digitalen Stadt bilden. Darmstadt ist mit seiner Datenplattform im Februar 2019 produktiv gegangen. Sie bündelt und visualisiert verschiedene Sensordaten der Stadt in Echtzeit und sorgt damit für Transparenz über das Stadtgeschehen. Durch Datenanalysen und Herstellung von Kausalitäten zwischen den Daten werden nicht nur neue Erkenntnisse gewonnen, sondern auch Verbesserungen ermöglicht. Ein Beispiel hierfür ist die Verbindung von Verkehrsdaten mit Umweltdaten und Veranstaltungen im Stadtgebiet. Hier bietet die Datenplattform die Basis, um über Verkehrsvorausberechnungen mit intelligenter Verkehrssteuerung zur Verbesserung des Verkehrsflusses und der Luftqualität beizutragen. Ein echter Gewinn für alle!

Fazit

Datenplattformen bilden das Herzstück einer Smart City. Durch die Verfügbarkeit und Auswertung vernetzter Daten ist es möglich, notwendige urbane Entscheidungs- und Planungsprozesse zu unterstützen und zu beschleunigen – ein echter Gewinn für alle!

Simone Schlosser
Digitalstadt Darmstadt

www.digitalstadt-darmstadt.de

Michael Pfefferle
Bitkom e.V.

www.bitkom.org

Workshops

Unterstützung durch zivile Hilfskräfte bei Cyber-Großschadenslagen

Tritt eine Cyber-Großschadenslage ein, ist schnelles Handeln gefragt. Mit den Cyber Emergency Response Teams (CERTs) und Mobile Incidence Response Teams (MIRTs) gibt es bereits staatliche Notfalleinheiten für Cybervorfälle. Doch was, wenn die vorhandenen Kapazitäten nicht mehr ausreichen?

Eine zusätzliche Unterstützung könnte durch ausgebildete Freiwillige erfolgen. Für kleinere Fälle besteht in Deutschland bereits das Cyber-Sicherheitsnetzwerk, das KMUs telefonische Hilfe durch digitale Ersthelfer anbietet. Für große Schadenslagen gibt es das noch nicht. Eine Freiwilligenorganisation könnte analog zu bereits existierenden Hilfsorganisationen schnelle Hilfe zur Wiederherstellung leisten. Das Expertennetzwerk AG KRITIS hat dafür bereits Anregungen ausgearbeitet, und der Koalitionsvertrag der neuen Regierung sieht eine Ausweitung der Cyberkapazitäten innerhalb des Technischen Hilfswerks vor.

Dass die Einbindung Freiwilliger gelingen kann, zeigt die Cyber Unit der Estonian Defence League. Die Freiwilligenorganisation wurde als Reaktion auf die großflächigen Cyberangriffe von 2007 aus unterstützenden Unternehmen sowie Expertinnen und Experten ins Leben gerufen.

Hinweis

Um kritische Infrastrukturen auch in Deutschland auf Krisen vorzubereiten, forscht der Lehrstuhl PEASEC der TU Darmstadt zu den Anforderungen der Kommunen und Infrastrukturbetriebe im Hinblick auf Cyber-Großschadenslagen. Personen in diesem Tätigkeitsfeld sind herzlich eingeladen, als Interview- oder Diskussionspartner zu unterstützen. Interessierte können sich unter diesem Link registrieren.

Jasmin Haunschild
ATHENE/TU Darmstadt

www.securban.athene-center.de

Workshops

Governance von Cybersicherheit für Kommunen

Kirstin Scheel und Michael Kreutzer von ATHENE präsentieren das Ergebnis eines vom Hessischen Ministerium des Innern und für Sport geförderten Projektes. Im Projekt wurden fünf Präventivmaßnahmen identifiziert, die dazu beitragen können, das Risiko von Cybervorfällen im Prozess der Entwicklung in Richtung smarter Communities abzuschwächen. Diese basieren auf den in Abbildung 1 dargestellten Grundsätzen:

Verankerung,

Verantwortlichkeiten,

Vereinheitlichung,

Vereinigung und

Verbesserung.

Die Cybersicherheit muss auf höchster Ebene in der Organisation verankert werden. Die oberste Führungsebene muss sich der Notwendigkeit von Sicherheit als Eckpfeiler aller Digitalisierungsprojekte bewusst sein.

Es müssen klare Verantwortlichkeiten zugewiesen werden. Darüber hinaus sind angemessene Ressourcen für die Wahrnehmung dieser Zuständigkeiten erforderlich.

Ein weiterer zentraler Gedanke ist die Vereinheitlichung von Systemen und Prozessen über Organisationseinheiten hinweg. Viele Fälle von Malware-Befall können sich zum Beispiel über Systeme ausbreiten, die nicht richtig segmentiert sind.

Wichtig sind auch die betriebliche Vereinigung und bereichsübergreifende Kooperation, um Ressourcen effizient und effektiv einzusetzen.

Sich dynamisch verändernde Umgebungen erfordern eine kontinuierliche Verbesserung. Das Lernen aus internen und externen Fehlern ist unerlässlich, um mit diesen Entwicklungen Schritt zu halten.

Dr. Michael Kreutzer
ATHENE/Fraunhofer SIT

www.athene-center.de

Best Practices

Wie können sichere smarte Städte und Regionen gelingen? Welche Voraussetzungen müssen dafür vorab geschaffen werden? Wie wichtig ist Security by Design für sichere smarte Städte und Regionen? Welche spannenden Forschungsprojekte und Unternehmensgründungen gibt es in diesem Bereich? Welchen Einfluss hat Partizipation beim Aufbau smarter Städte und Regionen? Und was können wir dabei von Israel lernen?

Diese und weitere Fragen wurden in den Best Practice Sessions aufgegriffen und beantwortet. Auf den folgenden Seiten finden Sie die kurzen und spannenden Zusammenfassungen dazu.

Living Labs und innovative Ökosysteme

Die Sicherheit von Bürgerinnen und Bürgern sowie die Widerstandsfähigkeit von smarten Städten und Regionen verbessern

Die digitale Kommune – smart UND sicher!

Cyber-Sicherheit in smarten Regionen – auch eine Frage verständlicher Zahlen!

Partizipation als zentrales Element der Smart Region

Gemeinsam zu einer nachhaltigen Sicherheitskultur

Protecting the IoT – Lösungen für vernetzte Systeme

Sichere 5G-basierte Lösung zur smarten Verkehrssteuerung

Erhöhte Sicherheit durch autonomes Verkehrsmanagement

Anwendungorientierte Forschungsförderung in Hessen

Best Practices

Living Labs und innovative Ökosysteme

Je smarter man ist, umso verletzlicher wird man. Smart Regions zielen darauf ab, Umgebungen zu schaffen, die sowohl für Mensch und Umwelt als auch für den Datenschutz sicherer sind, und müssen daher Infrastruktur und Daten schützen. Dazu müssen innovative neue Lösungen gefunden und eingesetzt werden. Zwei Dinge haben sich hierbei als Best Practice erwiesen:

Erstens ist es für Gemeinden von Vorteil, neue und innovative Lösungen in Living Labs zu testen. Solche Living Labs gibt es in Tel Aviv, aber auch vielen anderen Städten. Die Idee dahinter ist, Anwendungen in einer geschützten, aber realen Live-Umgebung zu pilotieren.

Zweitens ist es sinnvoll, Innovations-/Start-up-Communities entweder zu initiieren oder zu nutzen. In einigen Fällen kann es sogar ein guter Weg sein, dediziert aufzurufen, Lösungen zu entwickeln. In Tel Aviv wird dies durch wirkungsvolle Start-up-Programme wie das des in Tel Aviv ansässigen Accelerators CityZone unterstützt.

Das Programm von CityZone nutzt eines der produktivsten und innovativsten Start-up-Ökosysteme der Welt – es verbindet Start-ups, Städte und Branchenführer, um gemeinsame Herausforderungen zu meistern. Es bietet Zugang zu Sandboxing, Finanzierung und Austausch, zum Beispiel mit dem „City Corporate Start-up" - Roundtable.

Empfehlung:

- Living Labs und Acceleratoren nutzen, um Anwendungen in einer geschützten, aber realen Live-Umgebung zu pilotieren
- Innovations-/Start-up-Communities entweder initiieren oder bereits vorhandene nutzen

Gaby Kaminsky
CityZone

www.city-zone.co

Best Practices

Die Sicherheit von Bürgerinnen und Bürgern sowie die Widerstandsfähigkeit von smarten Städten und Regionen verbessern

„Wie schützen Sie nicht nur die Sicherheit Ihrer Bürgerinnen und Bürger, sondern sorgen auch für Nachhaltigkeit und Widerstandsfähigkeit Ihrer Smart City/Smart Region?"

Menschen und Infrastrukturen in Smart Regions und Smart Cities sind einer Vielzahl von Bedrohungen ausgesetzt. Zum einen besteht die ständige Gefahr von Cyberangriffen auf die Infrastruktur. Zum anderen gibt es ökologische Faktoren wie Luft- und Wasserverschmutzung, Hitzewellen, Stürme, Überschwemmungen oder sogar Waldbrände. Für smarte Regionen ist somit die Kernfrage, wie nicht nur die Sicherheit der Bürgerinnen und Bürger, sondern auch die Nachhaltigkeit und Widerstandsfähigkeit der Regionen und Städte verbessert werden können.

Jede Gemeinde sollte auf der organisatorischen Ebene eine Nofallmanagerin/einen Notfallmanager und ein C&C-Zentrum einrichten. In dieser Funktion werden Visualisierung und Warnungen sowie ein dauerhafter Zugriff auf alle relevanten Informationen benötigt. Die Aufgabe umfasst Erkennung und Vorhersage sowie die Reaktion. Das Notfallmanagement sollte automatisiert werden, mit der Möglichkeit, manuell eingreifen zu können.

Lösungen wie IPgallery nutzen die vernetzte Infrastruktur und erweitern sie um KI-basierte Dienste. Kleinere Vorfälle können tagtäglich von ihnen eingesehen werden, außerdem bieten sie auch den vollen Technologieumfang für den Umgang mit größeren Notfallsituationen.

Avihai Degani
IPgallery

www.ipgallery.com

Best Practices

Die digitale Kommune – smart UND sicher!

Die Stabsstelle Digitalisierung der Stadt Offenbach hat zwei Aufgaben: die Smart-City-Transformation Offenbachs sowie die digitale Transformation der Verwaltung gemeinsam mit den IT-Abteilungen von Stadt und Stadtwerken voranzutreiben. Zentrale IT-Sec-Herausforderungen dabei sind:

Open-Source-Software als Baustein der digital souveränen Smart City: Die sicherheitsorientierte (Weiter-)Entwicklung der Software muss zentral gewährleistet werden (ZenDis - Zentrum für Digitale Souveränität der Öffentlichen Verwaltung).

Verschlüsselung: Durch Vereinfachung und Zentralisierung – zum Beispiel eine Landes CA (Certification Authority) – können die Kommunen entlastet werden.

Wachsende „Geschäftsmodelle" wie Ransomware-as-a-Service und unzureichende Digital Security Awareness: Mehr zentrale, niedrigschwellige Lernangebote und entsprechende finanzielle Ausstattung sind nötig.

Empfehlung:

Als Best Practice-Beispiele für das Thema Datenschutz in der Smart City stehen Kollaborationstools wie der OS-Messenger der Bundeswehr und das Projekt Open Diffix, das eine einfache Anonymisierung von Datensätzen verspricht.

Anne Schwarz
Stadt Offenbach

www.offenbach.de

Best Practices

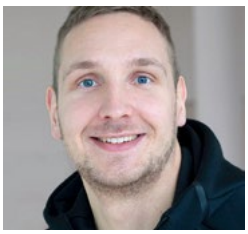
Cybersicherheit in smarten Regionen – auch eine Frage verständlicher Zahlen!

Viele IT-Infrastrukturen sind über Jahre mehr oder weniger strukturiert gewachsen. Das Resultat: Trotz steigender Awareness für IT-Sicherheit haben Unternehmen, Organisationen und auch Gemeinden vielfach keinen vollständigen Überblick über die Gesamtheit ihrer IT-Systeme, zum Beispiel Webseiten, Netzwerk oder Software. Die Verantwortlichen wissen so oft nicht, wie sicher ihre Systeme sind und wie gut sie gegen Attacken geschützt sind.

Um den Überblick über die eigene IT-Infrastruktur und die eigene IT-Sicherheitslage zu erhalten, können Lösungen eingesetzt werden, die automatisch alle IT-Assets einer Organisation scannen und – samt Sicherheitsstatus – dokumentieren. Dadurch ist wiederum eine Priorisierung erforderlicher Sicherheitsaktivitäten möglich.

In Hessen bietet das Start-up LocateRisk eine solche Lösung an: Mit ihr werden IT-Infrastrukturen aus externer Perspektive erfasst, bewertet und in einem Bericht mit priorisierten Handlungsempfehlungen zusammengefasst. Kommunen können unter www.locaterisk.com unverbindlich eine Erstanalyse mit darauf aufbauendem kostenfreien Beratungsgespräch vereinbaren.

Fazit:
Verschaffen Sie sich einen Überblick über die Gesamtheit Ihrer IT-Systeme. Nur so können Sie gezielte Maßnahmen zu deren Schutz einleiten!



Lukas Baumann
LocateRisk

www.locaterisk.com

Best Practices

Partizipation als zentrales Element der Smart Region

In der Digitalisierung von Beteiligung in Smart Cities, Communities und Regions steckt das Potenzial, die Art und Weise, wie Entscheidungen getroffen werden, zu verändern. Konkret: Smart Regions bedeutet für uns, Politik und Verwaltung nutzen das Wissen von Bürgerinnen und Bürgern sowie anderen Stakeholdern. Durch die konstruktive Einbeziehung der Bürgerinnen und Bürger in einer Region entstehen bessere Entscheidungen, mehr Akzeptanz und ein Gemeinschaftsgefühl. Das ist Smart Region. Wir begleiten Regionen auf dem Weg zur Smart Region mit unserer Methode Insights-Prozess und Software CrowdInsights-Plattform. Mehr Informationen unter diesem Link.

Empfehlung:

Bürgerinnen und Bürger stellen als Nutzer und Bewohner einer Stadt das zentrale Element einer Smart City dar. Binden Sie sie ein und nutzen Sie die Partizipation als zentrales Element der smarten Stadtentwicklung!

Dominik Wörner
CrowdInsights

www.crowdinsights.de

Best Practices

Gemeinsam zu einer nachhaltigen Sicherheitskultur

„Wir wollen helfen, das digitale Deutschland schrittweise sicherer zu machen, und fangen in Darmstadt damit an."

Die meisten erfolgreichen Cyberattacken starten mit dem Faktor Mensch, zum Beispiel mit Phishing. Wer sich davor erfolgreich schützen will, setzt nicht nur auf Technologie, sondern insbesondere auf eine gute Sicherheitskultur. Organisationen schulen und sensibilisieren ihre Mitarbeiterinnen und Mitarbeiter deshalb idealerweise in Awareness-Trainings.

Mit der kostenlosen Kampagne „Bleib wachsam, Darmstadt!" hat die Stadt Darmstadt diesen Gedanken zusammen mit IT-Seal weiterentwickelt. Sie hat die erste lokale Cybersicherheits-Kampagne gestartet und ein Sicherheitstraining für ihre Bürgerinnen und Bürger angeboten. Das Ziel: eine nachhaltige Sicherheitskultur, die in die Breite geht. Der Gedanke: je mehr Menschen gut trainiert sind, desto besser der Schutz der Gesellschaft.

Unter dem Motto „Du bist die Firewall" setzt die Kampagne auf Multiplikationseffekte. Die Inhalte sind für alle konzipiert und sensibilisieren für den Umgang mit der eigenen IT, Social Engineering, E-Mail-Sicherheit/Phishing, Social Media und den eigenen Passwörtern.

„Bleib wachsam, Darmstadt!" wurde von IT-Seal entwickelt, einem führenden Awareness-Spezialisten im Security Valley Darmstadt. Mehr Infos unter www.darmstadt.bleib-wachsam.de.

Alex Wyllie
IT-Seal

www.it-seal.de

Best Practices

Protecting the IoT – Lösungen für vernetzte Systeme

Supply-Chain-Software-Angriffe werden zum bevorzugten Angriffsvektor für die organisierte Kriminalität. SolarWinds, Microsoft und einige andere wurden von organisierten Kriminellen genutzt, um Kundinnen und Kunden dieser Unternehmen anzugreifen. Dazu nutzen sie entdeckte und in einigen Fällen sogar böswillig und aktiv eingeführte Software-Schwachstellen aus. Andere Schwachstellen wurden nicht absichtlich eingeführt. Sie entstanden durch Entwicklungsfehler und durch die verworrene Lieferkette vieler Softwareanbieter, die die Identifizierung von 3rd-Party-Komponenten und deren Aktualisierung bei Entdeckung einer Schwachstelle erschwert.

Smart Cities müssen die auf Lieferketten bezogenen Cybersicherheitsmaßnahmen verschärfen. Eine wichtige Komponente dabei ist die Identifizierung kommerzieller Softwarekomponenten und der damit verbundenen Schwachstellen. IoT-Anbieter müssen Software-Images auf bekannte Schwachstellen, Konfigurationsrisiken, unsichere Binärdateien, fehlerhafte Passwörter und mehr scannen.

Fazit:
Supply-Chain-Software-Angriffe häufen sich. Kommunen müssen deshalb auf besonderen Schutz ihrer IoT achten.

Gregor Knappik
Karamba Security

www.karambasecurity.com

Best Practices

Sichere 5G-basierte Lösung zur smarten Verkehrssteuerung

„Mit sicherer und smarter Verkehrssteuerung zu mehr Effizienz, Umweltschutz und Lebensqualität, ohne die Bürgerinnen und Bürger in ihrer Mobilität einzuschränken!“

25 Kilometer pro Stunde war die durchschnittliche Reisegeschwindigkeit des Pferdes. In Berlin liegt sie derzeit bei 17 Kilometern. Die Gründe: mehr Autos und eine Infrastruktur, die nicht für das aktuelle Verkehrsaufkommen gebaut wurde. Das überlastete System führt zu Staus, Produktivitätsverlusten und übermäßiger Umweltverschmutzung. Um diese Probleme anzugehen, sind Smart Cities gut beraten, effektive, intelligente Verkehrsmanagementsysteme zu implementieren. Intelligent eingesetzt, reduzieren diese Systeme nicht nur Staus, sondern ermöglichen Gemeinden auch andere Verkehrsarten, zum Beispiel Verkehrmittel einzubinden und entsprechend zu priorisieren.

Ein Beispiel für ein solches System ist die KI-basierte Software des israelischen Start-ups ITC. Die Software lässt sich in vorhandene Straßenkameras integrieren und ermöglicht so den Zugriff auf eine Vielzahl von Daten, um die Clusterbildung von Verkehrsmustern zu identifizieren. Auf diese Weise können Staumuster vorhergesagt und durch einen maßgeschneiderten Verkehrsplan direkt entschärft werden – lange bevor es zu Staus kommt. Gleichzeitig bereiten intelligente Verkehrslösungen Smart Cities auf zukünftige technologische Entwicklungen wie Connected Vehicle und den vollständigen Einsatz von 5G-Netzen vor.

Dvir Kenig
ITC - Intelligent Traffic Control

www.itc-israel.co.il

Best Practices

Erhöhte Sicherheit durch autonomes Verkehrsmanagement

Autonomes Verkehrsmanagement ist in einer smarten Region eine Maßnahme, die eine unmittelbare Wirkung zeigt. Gemeinden müssen zunächst digitale Netze schaffen, die Daten und Informationen austauschen, um Staus deutlich zu reduzieren und Verkehr intelligent zu managen.

Für viele Städte ist dies jedoch eine Herausforderung, da ihre Kreuzungen oft manuell und unvernetzt sind. Um dies zu überwinden, haben Unternehmen wie NoTraffic Plattformen geschaffen, die schnell bereitgestellt werden und die von Sensoren gesammelten Netzdaten mithilfe von vernetztem Edge-Computing und Cloud-basiertem Management wirksam einsetzen können. Diese Daten können durch zusätzliche Datenquellen ergänzt werden, um so ein vollautomatisiertes Verkehrsmanagement zu ermöglichen, beispielsweise um bestmögliche Entscheidungen treffen zu können, eine Ampel zu schalten oder den Rettungskräften bei Unfällen Vorrang zu geben. Dies führt zu weniger Verzögerungen, deutlich weniger Emissionen und eröffnet Möglichkeiten für neue vernetzte Dienste. Man gewinnt an Sicherheit und hat einen klaren finanziellen Vorteil.

Empfehlung:

Nutzen Sie bereits vorhandene Ressourcen und setzen Sie diese wirksam ein, um einen wertvollen Beitrag in den Bereichen Sicherheit, Verkehrsmanagement und Navigation zu schaffen!

Matan Nir
NoTraffic

www.notraffic.tech

Best Practices

Anwendungsorientierte Forschungsförderung in Hessen

Das Referat Innovationsmanagement Cybersicherheit im Hessischen Ministerium des Innern und für Sport verfolgt zwei große Ziele: Zum einen verbindet es anwendungsorientiert – also möglichst direkt nutzbar – fachliche Bedarfe und Forschung miteinander, und zwar in überschaubaren, konkreten, projektierten Vorhaben. Zum anderen geht es um Wissenstransfer, Vernetzung und den Ausbau eines engen Ökosystems. Die Angebote richten sich an die hessischen Sicherheitsbehörden und Kommunen.

Die vier Säulen des Innovationsmanagements Cybersicherheit sind:

1. Strategische Steuerung, unter anderem mit dem Beirat Cybersicherheit
2. Forschung im Ökosystem mit einer eigenen Förderrichtlinie, Förderaufrufen und einem Rahmenvertrag Forschung
3. Veranstaltungsformate wie Ringvorlesungen, Podcast-Reihe, Kommunal-Tag Cybersicherheit oder Workshops mit Markterkundungen
4. Bundes- und europaweite Kontakte und Vernetzung, zum Beispiel mit der länderübergreifenden Plattform Cybersicherheitsforschung unter hessischer Federführung, der Vernetzung mit dem EU-Kompetenzzentrum Bukarest, der Agentur für Innovation in der Cybersicherheit etc.

Mehr Informationen unter:
https://innen.hessen.de/Sicherheit/Cyber-und-IT-Sicherheit/Innovationsmanagement-Cybersicherheit

Dirk Dohn
Hessisches Ministerium des
Innern und für Sport
Referat Innovationsmanagement
Cybersicherheit

www.innen.hessen.de

Panel

Im Abschlusspanel ging es insbesondere um die praktische Umsetzung von sicheren smarten Maßnahmen für smarte Regionen und Städte sowie deren Voraussetzungen. Die Panelisten aus Israel und Deutschland berichteten über ihre direkten und indirekten Erfahrungen. Dabei waren:

Johannes Rothmund
Bürgermeister Gemeinde Eichenzell

www.smartcity-eichenzell.de
www.eichenzell.de

Dr. Steven Arzt
ATHENE/Fraunhofer SIT

www.athene-center.de

Jochanan Sommerfeld
7CI

www.sevenci.com

Rami Efrati
MSF Partners Innovation

www.msfpartners.com

Panel

Statements

» Johannes Rothmund

„Smarte Angebote sind für die Attraktivität und die Effizienz unserer Gemeinde extrem wichtig. Dabei wollen wir die Daten unserer Bürgerinnen und Bürger schützen und den höchsten Standard im Bereich Datensicherheit, des Datenschutzes und der Datenhoheit bieten. So nutzen wir beispielsweise ein vielfach zertifiziertes Rechenzentrum vor Ort.

Wir erleben dabei, dass Datenschützerinnen und Datenschützer neue, smarte Angebote oftmals kritisch sehen – auch weil Erfahrungen mit diesen fehlen. So sind wir oft langsamer als wir sein wollen. Deshalb verfolgen wir bei Pilotprojekten einen agileren Ansatz: wir planen diese natürlich unter Berücksichtigung aller Aspekte des Datenschutzes, gehen dann in deren Umsetzung und prüfen währenddessen, in Zusammenarbeit mit dem Hessischen Datenschutzbeauftragten, wo wir noch nachbessern müssen. So können wir gemeinsam frühzeitig sicherstellen, auf dem richtigen Weg zu sein."

» Jochanan Sommerfeld

„Sicherheit ist keine Funktion, sondern ein Merkmal eines jeden Systems, jeder Umgebung und jeder gesamten Lösung. Daher sollte Sicherheit ähnlich wie Qualität betrachtet und in allen Phasen eines Lebenszyklus berücksichtigt werden, von der Ideenfindung über die Bereitstellung bis hin zur Wartung. Da es jedoch eine Vielzahl an Sektoren und Branchen sowie an Technologien gibt, die an der Reise zu einer smarten Region beteiligt sind, ist es wichtig, die Komplexität so weit wie möglich zu vereinfachen. Eine Reise, die mit Komplexität beladen ist, ist unweigerlich zum Scheitern verurteilt. Meiner Ansicht nach sind insbesondere diese Prinzipien zu beherzigen:

- Standardisierung und Best Practices
- Befolgen von YAGNI (You Ain't Gonna Need It) führt zu schlankeren und fokussierteren Apps
- Design for Scale
- Sicherheit als Merkmal und nicht als Funktion betrachten
- Identitätsmanagement vereinheitlichen"

Panel

Statements

» Dr. Steven Arzt

„Bei neuen IT-Projekten sollte von Anfang an ein konfigurierbares Framework zur systematischen Risikobewertung genutzt werden. Hierbei gibt es etablierte Konzepte, um die erwarteten Angreifer, deren Angriffsziele, Motivationen, Bedingungen, usw. abzuschätzen. Auf dieser Basis können Gegenmaßnahmen geplant, bewertet und entschieden werden. Leitfragen sind: Was muss abgesichert werden und welche Maßnahme ist bzgl. Kosten und Nutzen angemessen? Für die Gegenmaßnahmen sind wiederverwendbare Prozesse und Bausteine für Sicherheit und Datenschutz essenziell. Hierdurch wird vermieden, das Rad immer wieder neu zu erfinden.

Software ist bei fast allen öffentlichen IT-Projekten ein Thema. Hier stehen SecDevOps-Prozesse im Vordergrund, mit beispielsweise automatischen Codescannern als eine Maßnahme zur Sicherstellung eines Mindestniveaus bezüglich der Qualität des Softwarecodes."

» Rami Efrati

„Als Land genießen wir den Ruf, sehr stark im Improvisieren zu sein, was oft sehr vorteilhaft ist. Aber bei Cyber improvisieren wir nicht: Cyber ist Teil unserer Kultur. Das heißt, wir sehen dies nicht nur auf der Grundlage eines einzelnen Problems. Es ist eingebettet in unser Bewusstsein, unsere Resilienz und andere Überlegungen. Es basiert auf Erfahrungen und Best Practices. Wir leben Cyber und Privacy by Design und sobald Sie an diesem Punkt angekommen sind, können Sie viel beschleunigen. Meine drei Best Practices sind also:

1. Cyber sollte Ihre oberste Priorität sein: Wenn Sie sich nicht vor Cyberangriffen schützen, schützen Sie auch nicht Ihre Privatsphäre.
2. Verfolgen Sie einen strategischen Ansatz und priorisieren Sie, was für Sie am wichtigsten ist, um damit zu beginnen.
3. Lernen Sie, sich schnell auf effektive Lösungen zu konzentrieren."

Impressum

Geschäftsstelle Smarte Region:

Hessische Staatskanzlei
Hessische Ministerin für Digitale Strategie und Entwicklung
info@smarte-region-hessen.de
www.smarte-region-hessen.de

Impressum

Herausgeber
Hessische Staatskanzlei,
Ministerin für Digitale Strategie und Entwicklung
Georg-August-Zinn-Straße 1
65183 Wiesbaden

Der Herausgeber übernimmt keine Gewähr für die Richtigkeit, die Genauigkeit und die Vollständigkeit der Angaben sowie für die Beachtung privater Rechte Dritter. Die in der Veröffentlichung geäußerten Ansichten und Meinungen müssen nicht mit der Meinung des Herausgebers übereinstimmen.

Redaktion:
Ute Richter, Lena Kress
ATHENE Projekt Digital Hub Cybersecurity

Lektorat:
Transline Deutschland GmbH

Gestaltung:
Fraunhofer-Institut für Sichere Informationstechnologie SIT
www.sit.fraunhofer.de

Bildnachweise:
Umschlag: istockphoto/metamorworks
Bilder der Mitwirkenden wurden uns zur Verfügung gestellt.