

Umfrage bei Kritischer Infrastruktur: Bedeutung durch COVID-19 gestiegen

Seite 2



Sicherheit in Europa und global: Zwei Expert*innen zur Lage

Seite 3



Praxiswirksame Forschungsprojekte zur Infrastruktursicherheit

Seite 3

Qualifikation: Der Blick auf das Wesentliche



Europaweit einzigartige Teststellung für Kameras und Analysesoftware von STYX Sicherheitstechnik in Spielberg im Frühjahr/Sommer 2021

[© Michael Ferlin-Fiedler]

EDITORIAL



[© BMI]

Sylvia Mayer
Bundesministerium für Inneres, Stv. Leiterin der Abteilung BVT/3 – Sicherheit und Schutz

Herausforderungen für Kritische Infrastruktur

Kritische Infrastrukturen werden immer wieder als die Lebensadern unserer Gesellschaft bezeichnet, und tatsächlich wäre ein Leben ohne ihr Funktionieren mittlerweile kaum mehr

vorstellbar. Eine ununterbrochene Stromversorgung, fließendes Trinkwasser, öffentliche Transportmöglichkeiten sowie zuverlässiges Online-Banking sind nur einige der Dienste, auf deren Verfügbarkeit wir uns tagtäglich verlassen, ohne groß darüber nachzudenken. Dass durch spezifische Ereignisse – wie zuletzt die COVID-19-Pandemie – plötzlich das Gesundheitssystem mit seinen Intensivkapazitäten an seine Grenzen stößt, ruft die Verwundbarkeit all dieser Infrastrukturen wieder ins Gedächtnis. Daneben stehen auch klimatische/meteorologische Extremereignisse, Terrorismus, Cyberattacken, Versorgungsstörungen wie ein Blackout sowie eine steigende Vernetzung als Risiken im Fokus von Sicherheitsbeauftragten in Unternehmen.

Doch wie sollte der Staat selbst mit seiner Gewährleistungsverantwortung für eine funktionierende Daseinsvorsorge mit dieser Herausforderung umgehen? Dazu besteht nun seit Dezember 2020 ein Vorschlag der Europäischen Kommission über die Resilienz kritischer Einrichtungen. Die Mitgliedstaaten sollen künftig

ihre Kritische Infrastruktur identifizieren, Risiken bewerten und die Einhaltung von Resilienzmaßnahmen bei Unternehmen überprüfen. Der mittlerweile im Sprachgebrauch sehr gängige Begriff der Resilienz hat hier den bisher verwendeten Terminus der Sicherheit abgelöst und soll einen viel umfassenderen Zugang zur Beherrschung von Risiken gewährleisten.

Die Europäische Kommission versteht darunter unter anderem Maßnahmen zur Katastrophenvorsorge, einen angemessenen physischen Schutz sensibler Bereiche, die Umsetzung von Risiko- und Krisenmanagementverfahren, die Ermittlung alternativer Lieferketten, die Sicherheitsüberprüfung von Personal in kritischen Bereichen sowie die Sensibilisierung von Mitarbeiter*innen.

Das aktuell hoch bewertete Risiko des fehlenden Fachpersonals als maßgebliches Element jedes resilienten Unternehmens wird von der Auflistung im Richtlinienvorschlag nicht erfasst, liegt es doch bereits grundsätzlich im Interesse jeder Organisation, bestens ausge-

bildete und qualifizierte Mitarbeiter*innen zu rekrutieren. Genau hier muss gleichzeitig aber auch der Staat aktiv werden und bestmögliche Rahmenbedingungen schaffen, insbesondere im Bereich der Qualifizierung.

Inhalt

Qualifikation: Der Blick auf das Wesentliche	1
Was braucht die Kritische Infrastruktur?	2
Praxiswirksame Forschung Das Austrian Center for Intelligence, Propaganda and Security Studies 2x3 Fragen und Antworten	3
Personalia D-A-CH-Sicherheitsforum Professionell vernetzt Willkommen im neuen Campusnetzwerk Impressum	4

Was braucht die Kritische Infrastruktur?

Umfrage zeigt: Sicherheit durch COVID-19 wichtiger, steigende Bedrohungen erwartet, qualifiziertes Personal gefragt

Im Rahmen des KIRAS-Projekts AQUUS II wurden insgesamt 440 Sicherheitsverantwortliche in der Kritischen Infrastruktur im Juni 2021 zur Teilnahme an einer anonymen Online-Umfrage eingeladen. 118 vollständig ausgefüllte Fragebögen gingen ein, die Beteiligung lag somit bei 26,8 %. Geantwortet haben Sicherheitsverantwortliche aus Organisationen sämtlicher Sektoren der Kritischen Infrastruktur, allen Bundesländern und Größenklassen. An der Gestaltung und Auswertung der Umfrage war Stefan Rakowsky beteiligt.

In der Umfrage ging es primär um Einschätzungen und Erwartungen zum Stellenwert der Sicherheitsorganisation im Unternehmen und von Bedrohungen. Den Schwerpunkt bildeten Einschätzungen zum Bedarf an Qualifikationen für Bewachungsdienstleistungen mit Schwerpunkt auf externe Dienstleistungsunternehmen (Bewachung) und Möglichkeiten der (Mit-)Finanzierung von Mehrqualifikation.

Der Stellenwert der Sicherheitsorganisation in den Organisationen bzw. Unternehmen der Befragten ist im Zuge der COVID-19-Pandemie bei knapp drei Vierteln der Unternehmen (74,6 %) „eher gestiegen“ bis „stark gestiegen“. Weitere 20,3 % gehen von einer gleich gebliebenen Bedeutung aus. (Siehe Abbildung 1)

Etwa die Hälfte gab an, dass ein weiterer Anstieg der Bedeutung erwartet wird (3,4 % „stark“ und 46,6 % „eher“), während weitere

46,6 % für die Zukunft von gleichbleibender Bedeutung ausgehen.

Hinsichtlich der erwarteten Entwicklung einiger wichtiger Bedrohungen bis 2025 zeigte sich ein differenziertes Bild (siehe Abbildung 2):

- Nahezu alle Befragten erwarten einen Anstieg bei IT-Angriffen (44,4 % „stark“ und 48,7 % „eher“); die übrigen 6,8 % gehen von einem Gleichbleiben aus.

- Bei Social Engineering (als Angriffsweg) wird von zwei Dritteln ein Anstieg erwartet (15 % „stark“ und 53,1 % „eher“); weitere 26,5 % erwarten keine Veränderung.

- Eine steigende Bedeutung wird der Bedrohung der Reputation in Folge von Sicherheitsvorfällen zugemessen: 7,1 % erwarten hier einen „starken“ Anstieg, 57,1 % einen „eher steigenden“; weitere 31,3 % sehen diese Bedrohung bis 2025 konstant.

- Weltanschaulich und politisch motivierter Terrorismus wird von 42,2 % der Befragten als steigende Bedrohung erwartet (3,7 % erwarten „starken“ Anstieg, 38,5 % „eher“), während die Mehrheit (52,3 %) von einem Gleichbleiben ausgeht und nur 5,5 % eher eine sinkende Bedrohung annehmen.

- Ein ähnliches Bild zeigt sich bei Spionage – hier überwiegt ebenfalls die Erwartung, dass

die Bedrohung gleich hoch bleibt (61,7 %), während mehr als ein Drittel der Befragten von einem Anstieg ausgeht (0,9 % „stark“ und 35,5 % „eher“).

- Ebenfalls ähnlich konstant und klar sind die Erwartungen hinsichtlich Eigentumskriminalität (72,3 % „gleich bleiben“) und Sabotage (69,4 % „gleich bleiben“).

- Einzig bei (allgemeinen) Gewalthandlungen gibt es einen nennenswerten Anteil von Antworten zu „eher sinken“ (11,8 %) und „stark sinken“ (0,9 %), diese stehen der Erwartung einer „stark steigenden“ (1,8 %) und „eher steigenden“ Entwicklung (16,4 %) gegenüber. Auch hier überwiegt mit 69,1 % die Erwartung einer gleichbleibenden Entwicklung.

Höherqualifikation bei gewerblichen Bewachungsunternehmen und mögliche (Co-)Finanzierung

Die überwiegende Mehrheit der befragten Unternehmen bzw. Organisationen (70,3 %) beauftragt gewerbliche Bewachungsunternehmen. (Siehe Abbildung 3)

Eine relative Mehrheit der Befragten (43,2 %) hält eine allgemeine (nicht objektbezogene) Höherqualifikation des Personals für Sicherheitsdienstleistungen im Bereich der gewerblichen Bewachungsunternehmen für erforderlich; etwa ein Drittel (33,1 %) nicht. (Siehe Abbildung 4)

Fragt man jene 51, die hier eine Höherqualifizierung für erforderlich halten, nach der Ebene, in der diese Notwendigkeit bestehen würde, nennt die überwiegende Mehrheit von 86,3 % der Antwortenden das „dienstverehende Wachpersonal“, außerdem 58,8 % die „mittlere Führungsebene“ und lediglich 13,7 % die „oberste Führungsebene“. (Siehe Abbildung 5)

Die abschließende Frage behandelte die mögliche Mitfinanzierung von Höherqualifizierungsmaßnahmen des eingesetzten Personals von Kundenseite. Hier waren Mehrfachantworten möglich, insgesamt gingen 51 Rückmeldungen ein.

37,3 % von diesen können sich eine laufende Beauftragung zu höheren Stundensätzen/Pauschalsätzen vorstellen. 23,5 % würden ggf. Aus- und Weiterbildungskosten von eingesetztem (oder künftig einzusetzendem) Wachpersonal direkt übernehmen, 11,8 % wären zur Finanzierung eines einmaligen oder wiederkehrenden Pauschalbetrags bereit.

Etwa ein Fünftel (19,6 %) würde keine derartigen Mehrkosten abdecken; für ein weiteres Fünftel (19,6 %) ist die Frage nicht relevant.

Die Ergebnisse fließen in den Endbericht zu AQUUS II ein, der im Oktober 2021 bei einer Fachkonferenz an der FH Campus Wien präsentiert wird.

Abbildung 1

Wie haben Sie in Ihrem Unternehmen bzw. Ihrer Organisation die Situation ab Anfang 2020 erlebt? Mit der COVID19-Pandemie ist der Stellenwert der internen Sicherheitsorganisation ...

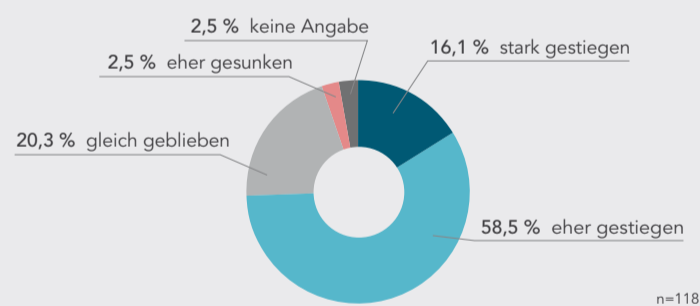


Abbildung 3

Ist Ihre Organisation/Ihr Unternehmen Auftraggeber/in eines gewerblichen Bewachungsunternehmens?

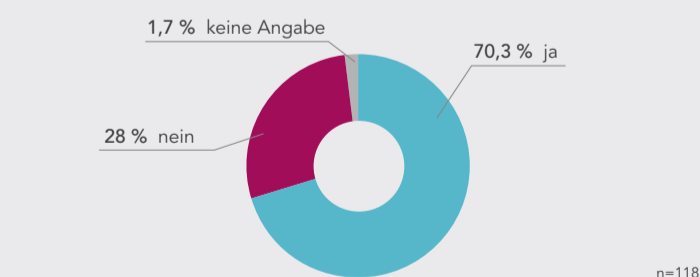


Abbildung 4

Hält Ihre Organisation/Ihr Unternehmen eine allgemeine (nicht objektbezogene) Höherqualifizierung des Personals für Sicherheitsdienstleistungen im Bereich der gewerblichen Bewachungsunternehmen für erforderlich?

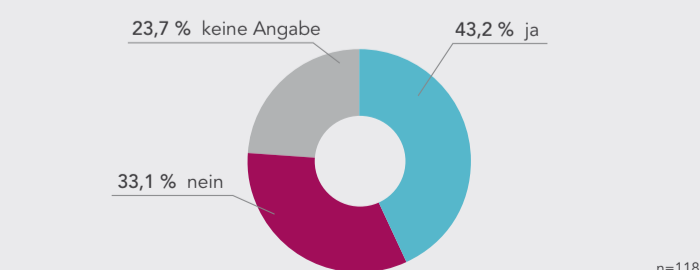
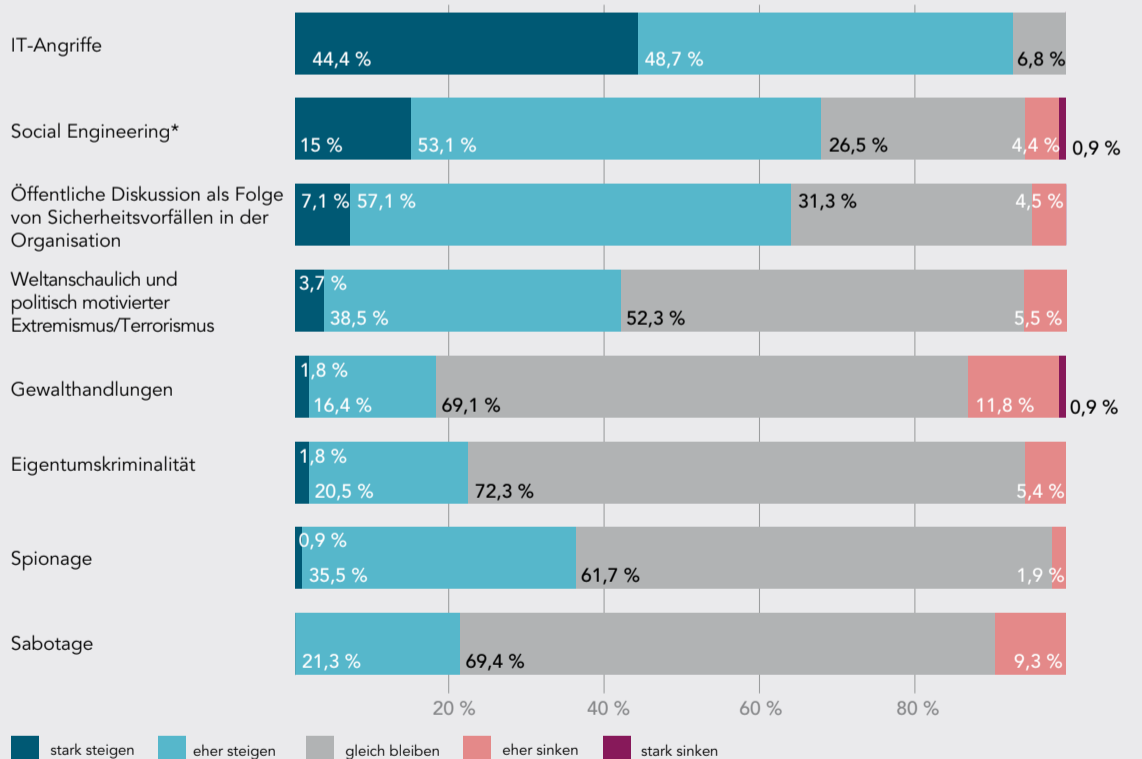


Abbildung 2

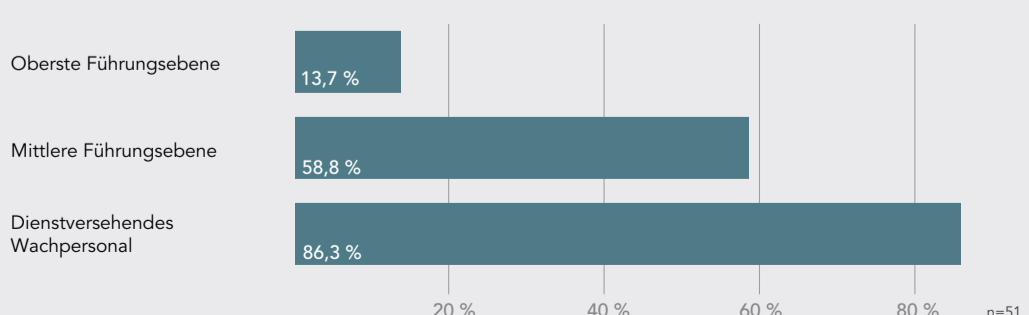
Was sind für den Zeitraum bis 2025 Ihre Erwartungen in Bezug auf folgende Bedrohungen für Ihr Unternehmen bzw. Ihre Organisation?



* als Angriffsweg im Sinn von „zwischenmenschliche Beeinflussungen, um Vertrauen von Mitarbeiter*innen zur Herausgabe von Unterlagen, Informationen oder Vornahme anderer Handlungen zu erreichen (z. B. CEO-Fraud ...)“

Abbildung 5

In welcher Organisationsebene der gewerblichen Bewachungsunternehmen erkennen Sie diese Notwendigkeit?



Innovation in Forschung und Lehre



Überreichung des Preisgelds zum Projekt für die Wiener Stadtwerke im Juni [© FH Campus Wien/Schedl]

IRM Fallstudie Wiener Stadtwerke

Gefahren für Unternehmen frühzeitig zu erkennen und zu verhindern: Das ist die Aufgabe des Risikomanagements. Wie effektiv und qualitativ dieses arbeitet, wird wiederum von der Internen Revision objektiv überprüft. Spielen beide Abteilungen optimal zusammen, kann dies Unternehmen vor wirtschaftlichen sowie Image-Schäden bewahren und nachhaltig sicher für die Zukunft aufstellen. Das Institut für Interne Revision (IIA Austria) und der Fachbereich Risiko- und Sicherheitsmanagement haben daher eine Kooperation gestartet, um Studierenden die Relevanz dieses „Dreamteams“ und praxisrelevantes Know-how zu vermitteln.

Die insgesamt 20 Teilnehmer*innen mussten im „Parallel Engineering“ ein realistisches Szenario lösen: Als breit diversifizierter Konzern sind die Wiener Stadtwerke mit stark divergierenden rechtlichen und ökonomischen Rahmenbedingungen konfrontiert. Die Studie-

renden sollten zeigen, wie in dem breit aufgestellten Konzern zusammenwirkende Risiken strukturiert identifiziert und dargestellt werden können. Die beste Lösung für das Problem fanden schließlich Florian Kysela, Riad Laske, Marie-Theres Leikam, Rainer Lindorfer und Claudia Loksik.

Bundesamt für Verfassungsschutz und Terrorismusbekämpfung – Metriken für den Schutz im Bereich Energieversorgung

Der ISM-Studierende Peter Kaderabek entwickelte im Rahmen seiner Bachelorarbeit eine neue Metrik zum Schutz Kritischer Infrastruktur im Sektor Energie: das innovative Konzept der Goal-Question-Metrik. Im Juni stellte er seine Ergebnisse Vertreter*innen des Bundesamts für Verfassungsschutz und Terrorismusbekämpfung, Betreiber*innen Kritischer Infrastrukturen und ausgewählten Security-Expert*innen vor. Fazit: ein interessanter Ansatz, um Evaluierungen zu objektivieren.

Sicherheitsuntersuchungsstelle des Bundes – Eisenbahnunfälle

Im Rahmen von drei Bachelorarbeiten wurden aktuelle Unfalluntersuchungsmethoden hinsichtlich ihrer Nutzung bei der Untersuchung von Eisenbahnunfällen evaluiert. Anhand des Unfalls vom 29. November 2016 in Hütteldorf wurden die Methoden AcciMap, Cast und FRAM von Ivana Vukasovic, Manuel Seidl und Daniel Hinteregger auf ihre Eignung getestet und die Ergebnisse anschließend bei einem

Online-Workshop präsentiert. Die Studierenden diskutierten mit Vertreter*innen der Sicherheitsuntersuchungsstelle des Bundes, der ÖBB, Steffen Müller (Behördenleiter der deutschen Bundesstelle für Eisenbahnunfalluntersuchung) und Christoph Kupper (Bereichsleiter Unfalluntersuchung Bahnen und Schiffe) aus der Schweiz. Die Ergebnisse der drei Bachelorarbeiten liefern einen wichtigen Beitrag für die zukünftigen Methoden im Bereich der Eisenbahnunfalluntersuchung.



Die Referent*innen bei der 31. ACIPSS-Arbeitstagung (v. l. n. r.): Reinhard Raml (IFES), Lukas Wank (Shabka-Gründer), Sandra Goldberger (VASBÖ-Vorstand, Bundesministerium für Inneres), Profiler Milos Rakic und Thomas Goiser (ACIPSS-Repräsentant in Wien, Lektor; Absolvent Risk Management & Corporate Security 2021). [© ACIPSS]

Das Austrian Center for Intelligence, Propaganda and Security Studies (ACIPSS) lud zum Start des Semesters gemeinsam mit dem Fachbereich Risiko- und Sicherheitsmanagement und dem VASBÖ (Verband akademischer

Sicherheitsberater Österreichs) zur Arbeitstagung. Die rund 25 Gäste aus Unternehmen, Behörden, Institutionen und Medien erlebten einen abwechslungsreichen Vormittag an der FH Campus Wien.

2 x 3 Fragen und Antworten



[© Luiza Putu]

Florence Gaub, stellvertretende Direktorin des EUISS (European Union Institute for Security Studies) und eine von fünf Vizepräsidentinnen des Europäischen Forums Alpbach

1 Was halten Sie für die größte Sicherheitsherausforderung für Europa in den nächsten 12 Monaten? (Stand Anfang September 2021)

1 Viele haben gedacht, dass die Problematik mit dem Terrorismus nicht mehr existiert, aber das wird uns leider auch weiterhin begleiten und das hängt auch nicht mit der derzeitigen Situation in Afghanistan zusammen. Einzelfälle lassen sich nur sehr schwer verhindern.

2 Ich bin überzeugt davon, dass Cyber-Attacks das ganz große Problem der Zukunft werden. Gerade im letzten Jahr haben wir gesehen, dass etwa China massiv die EU ins Visier nimmt und Mail-Accounts hackt. Der Vorfall mit dem Cyberhack eines belgischen Krankenhauses während COVID hat gezeigt, wie wenig wir

2 Wie wird sich das auf die Sicherheitslage von Unternehmen in Europa auswirken?

darauf vorbereitet sind. Das Bewusstsein für die Thematik ist zwar da, aber es wird noch zu defensiv auf diese Form der Attacks reagiert. Manche EU-Mitgliedsstaaten, wie etwa Frankreich, haben sehr offensive Cyber Capabilities, die können sich gut wehren. Aber davon bekommt man zum Beispiel selten etwas mit und in der Bevölkerung erweckt das bis zu einem gewissen Grad auch das Gefühl, dass wir nichts tun. Cyber-Attacks werden zunehmen und wir haben keine Methode, uns davor zu schützen, und keine offensive Antwort darauf. Und das wird für Unternehmen ein echtes Problem, denn die staatlichen Kapazitäten sind nicht da.

3 Sollten Ausbildungseinrichtungen darauf aktuell reagieren? Wenn ja, wie?

3 Die müssen auf alle Fälle reagieren, aber hier müssen wir länger vorausschauen – bis 2030 oder 2050. Wir müssen uns die Frage stellen, welche Kapazitäten Kinder, die heute eingeschult werden, in 20 Jahren auf dem Arbeitsmarkt benötigen. Da wird es weniger darum gehen, ob sie die Hauptstädte aller europäischen Länder kennen, sondern es wird viel mehr darum gehen, ob sie komplexe Informationen verarbeiten können, wissen, wo und wie sie zu richtigen Informationen kommen und wie sie innovativ mit Problemen umgehen können. Ich befürchte, nichts davon wird derzeit unterrichtet.



[© foto-prudio]

Gerald Höller, Absolvent Integriertes Sicherheitsmanagement, Leiter Krisen- und Sicherheitsmanagement bei Boehringer Ingelheim RCV GmbH & Co KG

1 Die Situation in Afghanistan ist allgegenwärtig und womöglich werden die Zahlen der schutzsuchenden Personen in Europa steigen, aber das ist nicht „die“ Herausforderung. Sicherheitspolitisch betrachtet blockiert die vorhandene Uneinigkeit in vielen Bereichen die Entscheidungsfindung der EU massiv und ist für den weiteren Zusammenhalt kontraproduktiv. Aus meiner Sicht ist die größte sicherheitsrelevante Herausforderung die Situation in Nordafrika und in den Sahel-Staaten. Diese Region wird derzeit in Europa kaum wahrgenommen, die Ausbildungsmissionen der EU zeigen kaum Wirkung und selbst Frankreich beginnt langsam damit, sich aus einzelnen Staaten zurückzuziehen.

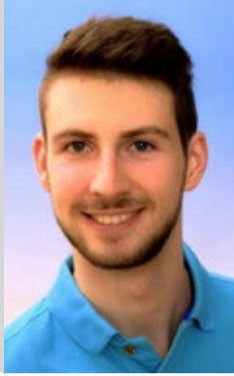
2 Der mögliche Wachstumsmarkt Afrika muss sehr differenziert betrachtet werden und es gibt Bedarf eines erhöhten Planungsaufwandes, um vor Ort tätig zu werden. Nur mit Partner*innen zu arbeiten, ist eine Möglichkeit, aber in Zusammenhang mit Korruption und der oftmaligen Nichteinhaltung von Grundrechten ist dies für jedes global tätige Unternehmen ein heikles Thema.

Für produzierende Unternehmen ist aber die langfristige Rohstoffversorgung die größte Herausforderung für die nächsten Jahre. Dies ist einerseits der COVID-Situation geschuldet und andererseits wird dies durch bestehende Konflikt- und Krisenräume verstärkt.

3 Ausbildungseinrichtungen sollten sich in regelmäßigen Abständen selbst die Frage stellen, ob ihre Ausbildung den Anforderungen des Marktes gerecht wird. Aus meiner Sicht wäre es zweckmäßig, Ausbildungen, die die Bereiche Datenerhebung sowie Analysemethoden abbilden, zu forcieren. Unternehmen benötigen zukünftig Mitarbeiter*innen, die Länder, Märkte und Region möglichst umfassend aufbereiten können und dadurch in der Lage sind, Zusammenhänge zu erkennen. Eine Risikoanalyse ist einfach, aber die Aufbereitung der Rahmenbedingungen und das Identifizieren von Chancen und Risiken ist die tatsächliche Herausforderung.

Personalia

Studierender
Integriertes
Sicherheits-
management



[Foto: privat]

Absolventin
Integriertes
Sicherheits-
management



[© Foto Hartlauer]

Lektor Integriertes
Sicherheits-
management



[© Helene Steiner]

Absolvent
Integriertes
Sicherheits-
management



[Foto: privat]

Risiken umfassend verbessern

Manuel Lechner (*1997) ist seit August als Risk Consultant/Risk Engineer beim Wiener Beratungsunternehmen Risk Experts beschäftigt. Bei Begehungen (Surveying) erhebt er Risiken für Kund*innen aus Industrie und Gewerbe und erarbeitet Verbesserungsvorschläge. Weitere Aufgabengebiete sind Schadenmanagement sowie Schulungstätigkeiten für die Risk Experts Academy. Davor war er ab 2018 bei EGSTON im Qualitätsmanagement tätig. Lechner hat die HTL Mechatronik und Automatisierungstechnik in Karlstein abgeschlossen. Aktuell befindet er sich im 5. Semester des Bachelorstudiums und beschäftigt sich für seine Bachelorarbeit mit dem Themenfeld Social Engineering.

Museen professionell schützen

Lena Schwarz (*1996) hat mit Juni die stellvertretende Leitung des Sicherheitsmanagements der Österreichischen Galerie Belvedere übernommen. In dieser Funktion ist sie für die drei Standorte Oberes und Unteres Belvedere sowie Belvedere 21 tätig. Im Studium konnte sie relevante Zusatzqualifikationen und Zertifikate erwerben; ihre Bachelorarbeit verfasste sie über „Wahrnehmung kriminalpräventiver Maßnahmen in der Seestadt Aspern“. Nach facheinschlägigen Praktika bei der Gas Connect Austria und der UNIQA war sie ab Februar 2021 einige Monate als Koordinatorin für Gesundheitsschutz und Arbeitssicherheit tätig.

Immer den Überblick behalten

René Steinkellner (*1982), Gründer und CEO der STYX Sicherheitstechnik GmbH, ist seit dem Sommersemester 2021 als Lektor für Perimeter-schutz im Bachelorstudiengang ISM tätig. Steinkellner verfügt über zwei Jahrzehnte unternehmerische Projekterfahrung in unterschiedlichen Technikbereichen. Zu seinen Kund*innen zählen die Kritische Infrastruktur, darunter Industriebetriebe, Forschungseinrichtungen, Logistikunternehmen, Behörden und Energieversorger sowie private Ressorts. Mit der Marke AVASUN ist er europaweit im Perimeterschutz für Solar-kraftwerke aktiv. Darüber hinaus engagiert sich Steinkellner im Verband akademischer Sicherheitsberater Österreich (VASBÖ).

Informationssicheres Gesundheitswesen

Alexander Zauner (*1984) ist seit Frühjahr 2021 als Informationssicherheits-Koordinator der Or-densprovinz der Barmherzigen Brüder Öster-reich tätig. Von Eisenstadt aus ist er als CISO für die Information Security sämtlicher Kran-kenhäuser und Pflegeeinrichtungen provin-zweit verantwortlich. Frühere Karrierestationen umfassten die thyssenkrupp Presta AG in Liech-tenstein (BMC), die Infraprotect GmbH (Leitung Business Continuity Management) sowie die Logwin AG (Qualität, Sicherheit und Umwelt). Vor und nach dem Bachelorstudium ISM (2007-2010) führten ihn Auslandseinsätze für das Ös-terreichische Bundesheer nach Tuzla in Bosnien und Herzegowina. Zauner hat auch Communi-cation Management an der FH Wien der WKW absolviert.

Sicherheitsforum am Ersatztermin

Das 8. D-A-CH-Sicherheitsforum beim Stanglwirt in Going der SIMEDIA Akademie macht pandemiebedingt am Ersatztermin 16. und 17. November einen 3. Anlauf. Auch diesmal wird es wieder eine exklusive Plattform für Fach- und Führungskräfte aus dem Sicherheitsbereich zur Vernetzung und zum Erfahrungs- und Informationsaustausch auf hohem Niveau werden. Der Fachbereich Risiko- und Sicherheitsmanagement ist wieder Lead-Partner der Fachkonferenz.



Unter anderem erwarten folgende Fach-vorträge die Gäste: „Desinformation als Waffe: Fake News als Herausforderung für die Unternehmenssicherheit“, „Sicherheit im 21. Jahrhundert: Wie die Digitalisierung in einer offenen Gesellschaft Sicherheit und

Frieden und Freiheit herausfordert“, „Tatort Text – Überführung anonymer Täter auf dem sprachwissenschaftlichen Seziertisch“ sowie „Zwischen VUCA-World und Informationszeit-alter – Ist die Sicherheitswirtschaft auf die Zukunft vorbereitet?“

Professionell vernetzt

Seit dem Frühjahr existiert eine (interne) Gruppe auf der digitalen Business- und Kar-riereplattform LinkedIn, die für Studierende, Alumni und Lehrende des Fachbereichs aller Jahrgänge offensteht. Darin werden derzeit überwiegend Hinweise zu Veranstaltungen und Jobausschreibungen ausgetauscht. Fünf Personen sind derzeit als Administrator*innen/ Manager*innen tätig: Isabel Kopezky, Thomas Goiser, Florian Polt, Joachim Pöttinger und Markus Schwaiger, sie können persönliche Kontakte mit Fachbereichsbezug einladen.



[© Rawpixel/shutterstock.com]

Willkommen im neuen Campusnetzwerk

Die Netzwerkplattform der FH Campus Wien wurde Anfang des Jahres einem Relaunch unterzogen und steht nun in neuem Glanz und mit zusätzlichen Funktionen für Studierende, Absolvent*innen, Lehrende, Mitarbeiter*innen und Partner*innen bereit.

Eine Plattform, viele Möglichkeiten

Ziel des campusweiten Netzwerks ist es, den aktiven Austausch zwischen den Mit-

gliedern zu fördern und Studierende sowie Absolvent*innen im beruflichen Leben zu unterstützen. Eine eigene Job- und Praktikum-börse soll den Berufsein- und -umstieg erleichtern. Persönliche Profile ermöglichen die Darstellung der bisherigen Erfahrungen sowie Ausbildungen und laden zur direkten Kontaktaufnahme ein. Der Newsfeed dient als schwarzes Brett, im Eventbereich wird auf Kar-riere- und Fachveranstaltungen aufmerksam

gemacht. Kooperationspartner*innen nutzen zudem das Unternehmensverzeichnis, um sich als attraktive Arbeitgeber*innen zu präsentieren.

Beziehungen schaffen und einander helfen

Mitglieder können ab sofort unkompliziert Unterstützung anfragen und/oder selbst anbieten. Bereits bei der Registrierung wird abgefragt, wonach Nutzer*innen suchen und in welchen Bereichen sie sich engagieren möchten. Mit-hilfe von Mentoring soll die persönliche und berufliche Weiterentwicklung von Studie-renden und Absolvent*innen, insbesondere Berufseinsteiger*innen, gefördert werden. Ob beim Bewerbungsprozess, bei der Unter-nehmensgründung oder beim Aufbau eines beruflichen Netzwerks – in (virtuellen) Mee-tings können Absolvent*innen, Lehrende,

Mitarbeiter*innen und Partner*innen ihre per-sönlichen Erfahrungen an Hilfesuchende wei-tergeben.

Jetzt Mitglied werden

Registrieren Sie sich auf campusnetzwerk.ac.at und werden Sie Teil unserer Commu-nity. Für Studierende, Absolvent*innen, Mitarbeiter*innen sowie Lehrende der FH Cam-pus Wien ist der Zugang kostenlos. Unterneh-men und Organisationen testen die Plattform bis Ende 2021 kostenlos und unverbindlich.

Weiterführende Informationen

Absolvent*innen:

www.fh-campuswien.ac.at/absolventinnen

Unternehmen/Organisationen:

www.fh-campuswien.ac.at/kooperationen

Anfragen:

campusnetzwerk@fh-campuswien.ac.at

Impressum

Medieninhaber: FH Campus Wien – Verein zur Förderung des Fachhochschul-, Entwicklungs- und Forschungszent-rums im Süden Wiens > ZVR-Zahl 625976320, DVR-Zahl: 2111102 > Diese Zeitung wurde vom Fachbereich Risiko- und Sicherheitsmanagement der FH Campus Wien erstellt. > Für den Inhalt verantwortlich: Martin Langer > Projektteam und Redaktion: Thomas Goiser, Isabel Kopezky > Druck: Gerin > Die Texte und Daten wurden sorgfältig ausgearbei-tet, dennoch können wir keine Haftung für die Richtigkeit der Angaben übernehmen. > Wien, im September 2021 > Kontakt für Feedback: risikomanagement@fh-campuswien.ac.at