Digitale Sicherheit.
Für Mensch & Maschine.

KERN

AWARE7 GmbH

Munscheidstr. 14
Im Wissenschaftspark
45886 Gelsenkirchen

Geschäftsführer

Chris Wojzechowski
Matteo Große-Kampmann

Bankverbindung

Sparkasse Gelsenkirchen
IBAN DE58 4205 0001 0137 0033 66

Gerichtsstand

Amtsgericht Gelsenkirchen
Handelsregister HRB 14935

Über die AWARE7 GmbH

Die AWARE7 GmbH ist ein Cyber Security Unternehmen aus Gelsenkirchen das Technologien und Produkte entwickelt sowie Dienstleistungen anbietet, die zur Förderung, Steigerung und Erhaltung des IT-Sicherheitslevels dienen. Durch die praktische Arbeit und die regelmäßige Veröffentlichung von wissenschaftlichen Artikeln gelingt es uns komplexe Betrugs- und Angriffsmethoden zu erklären um Unternehmen, Behörden und Personen zu schützen.

IT-Sicherheit funktioniert nur, wenn die Technik sicher und die Menschen sensibilisiert sind. Komplexe Angriffe nutzen menschliche Schwachstellen in Kombination mit technischen Sicherheitslücken aus. Betrachten Sie das IT-Sicherheitsniveau in Ihrem Unternehmen ganzheitlich. Auf menschlicher und technischer Ebene.

Portfolio

Live Hacking
& Awareness Shows

Bei einem Live Hacking geht es darum die Risiken kennenzulernen, welche im Umgang mit bewährten und neuen digitalen Medien entstehen. Ein Live Hacking kann sich über unterschiedliche Zeiträume erstrecken. Bei allen Vorträgen geht es darum den Stand der IT-Sicherheit darzustellen, denn wer sich vor Angriffen, Sicherheitslücken und Betrugsmaschen schützen will, muss wissen wie Kriminelle vorgehen. Dabei soll nicht vor der Digitalisierung abgeschreckt werden. Teilnehmer erhalten viel mehr die Möglichkeit sich und andere zu schützen.

Phishing Kampagnen
& Social Engineering Audits

Die meisten Angreifer erhalten über eine Phishing Mail Zutritt zum Unternehmen. Dabei sind es nicht die schlechten Phishing Mails, die für das Unternehmen zur Gefahr werden. Es sind perfektionierte Mails, von denen die Opfer gar nicht merken, dass sie auf eine Phishing Mail hereingefallen sind. Um Ihr Unternehmen vor dem beliebtesten Einfallstor zu schützen, Ihre Mitarbeiter zu trainieren und weiterzubilden, führen wir Phishing Kampagnen auf unterschiedlichen Erkennungsniveaus durch.

Penetrationstest
von Web, iOS und Android Applications

Decken Sie die Sicherheitslücken einer oder mehrerer Anwendungen auf. Wir untersuchen ihre Infrastruktur, Web, iOS oder Android Application auf Sicherheitslücken, dokumentieren diese sorgfältig, fertigen individuelle Handlungsempfehlungen an und präsentieren den Bericht auf Wunsch vor Ort. Dieser Test erfolgt in der Regel auf einem dedizierten Testsystem und wird, um das System widerstandsfähig gegenüber Angreifern zu machen, regelmäßig wiederholt.

RiskRex
Digital Risk Management

Moderne Angriffe nutzen menschliche & technische Sicherheitslücken meist in Kombination. RiskRex hilft Ihnen dabei, das IT-Sicherheitsniveau in Ihrem Unternehmen ganzheitlich zu betrachten und Gegenmaßnahmen einzuleiten. Unsere Plattform unterstützt Sie dabei, das Risiko von Mitarbeiterinnen, Mitarbeitern und der technischen Infrastruktur im Unternehmen zu messen.

AWARE7 GmbH

Munscheidstr. 14
Im Wissenschaftspark
45886 Gelsenkirchen

Geschäftsführer

Chris Wojzechowski
Matteo Große-Kampmann

Bankverbindung

Sparkasse Gelsenkirchen
IBAN DE58 4205 0001 0137 0033 66

Gerichtsstand

Amtsgericht Gelsenkirchen
Handelsregister HRB 14935

Über KERN

Cybersicherheit ist ein multidimensionales Feld. Es gibt jedoch häufig nur eindimensionale Lösungen. Es wird entweder ein technisches Problem gelöst, ein menschliches oder ein organisatorisches.

KERN ist ihr 360° Blick auf das Feld Cybersicherheit. KERN hilft Ihnen dabei IT-Sicherheit auf allen Ebenen zu etablieren und dadurch Mehrwerte zu generieren. Durch die wertschöpfende Verknüpfung von Dienstleistungen und Technologien. Die Leistungen sind dabei modular aufgebaut und können im Rahmen der Mitgliedschaft bei KERN bedarfsgerecht erweitert werden. KERN ist dabei absolut transparent in den enthaltenen Leistungen und der Abrechnung.

Folgende Leistungen sind in KERN enthalten und können im Rahmen Ihrer Mitgliedschaft verwendet werden:

Awareness Show

Erleben Sie, wie Hacker arbeiten, denken und vorgehen, um Ihre Daten zu stehlen, Prozesse zu stören und Schaden zu verursachen. Wir zeigen Ihren Mitarbeiter:innen in anschaulichen Szenarien aktuelle Betrugsmaschen und Angriffe. Pro Jahr haben Sie eine Remote Awarenessveranstaltung in Ihrer Mitgliedschaft in KERN. Sie können bei Bedarf weitere Veranstaltungen dazu buchen.

Pentesting

Wir untersuchen Ihre Systeme auf Schwachstellen und helfen Ihnen, diese zu schließen. Im Rahmen von KERN erhalten Sie jährlich ein festes Kontingent an Tagen, die wir in die Sicherheitsüberprüfung Ihrer Systeme stecken. Innerhalb der Laufzeit erhalten Sie jährlich zwei Personentage Pentesting in KERN. Wir stimmen ein Ziel und einen Termin ab und Sie erhalten ein Ergebnisprotokoll am Ende des Tests.

Consulting

Wir beraten Sie im Rahmen einer KERN Mitgliedschaft mit einem festen Kontingent pro Jahr in allen Fragen rund um das Thema IT-Sicherheit. Erarbeiten Sie eine langfristige und nachhaltige Strategie für den Bereich IT-Sicherheit mit unseren Beratern. In Ihrer Mitgliedschaft ist ein Personentag Consulting pro Jahr enthalten.

E-Learning

Erhalten Sie Zugang zu einem unserer E-Learning-Kurse und nutzen Sie die jahrelange IT-Security Erfahrung aus Wirtschaft und Wissenschaft. Bereiten Sie sich mit unseren E-Learning-Kursen auf aktuelle und zukünftige IT-Sicherheitsrisiken vor. In der KERN Mitgliedschaft ist ein eLearning Kurs pro Jahr auf unserem Portal inkludiert.

Phishing Simulation

Wir testen die Awareness Ihrer Mitarbeiter:innen für Sie. Lassen Sie Ihre Organisation den Umgang mit Phishing Attacken trainieren und stärken Sie Ihre menschliche Firewall durch ein Phishing Training. Im Rahmen der KERN Mitgliedschaft erhalten Sie eine Kampagne pro Jahr.

Digital Risk Management

Im Rahmen Ihrer KERN Mitgliedschaft erfassen wir jährlich Ihre externen digitalen Risiken mit unserer Software RISKREX. Erhalten Sie Zugang zu RISKREX Business im Rahmen Ihrer KERN-Mitgliedschaft.

Support

Als IT-Sicherheitsbeauftragter oder -verantwortlicher erhalten Sie nahezu täglich die unterschiedlichen Anfragen rund um das Thema IT-Sicherheit. Leiten Sie diese Fragen einfach weiter, wenn Sie selbst keine Antwort wissen und erhalten Sie innerhalb Ihrer KERN Mitgliedschaft Antworten von unseren Expert:innen. Im Laufe eines Jahres sind zehn solcher Supportanfragen über das KERN Portal inklusive.

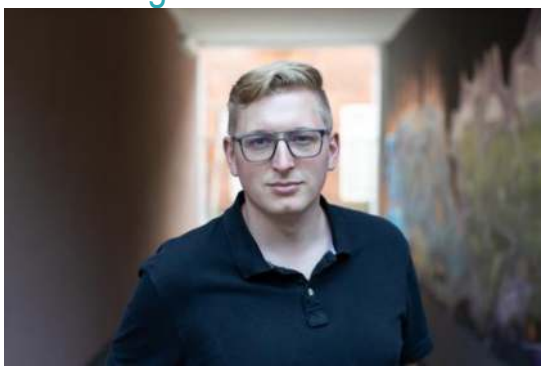
Mitgliedschaft beantragen

Sie wollen IT-Sicherheit ganzheitlich in Ihrem Unternehmen etablieren und nachhaltig Ihre Mitarbeiter:innen einbinden? Dann begrüßen wir Sie gern als neues KERN Mitglied bei uns auf der Plattform.

Eine Mitgliedschaft bei KERN kostet 249 EUR netto im Monat und wird jährlich abgerechnet. Sie zahlen heute Ihre Jahresmitgliedschaft und können dann ein Jahr lang auf KERN zugreifen. Nach Zahlungseingang erhalten Sie von uns ein Willkommenspaket mit weiteren Informationen rund um KERN, Ihre KERN Mitgliedsurkunde und Ihre Zugangsdaten zur KERN-Plattform.

Im Rahmen Ihrer ersten Mitgliedschaft machen wir zusätzlich einen ersten Online-Termin aus, bei dem einer unserer Experten Ihnen die wichtigsten Funktionen der KERN Plattform erklärt und Sie an Bord holt. Im Anschluss können Sie KERN nutzen, um entsprechende Mitgliedsleistungen abzurufen oder bei Bedarf weitere Leistungen modular dazu zu buchen.

Ein Auszug der Menschen hinter KERN



Chris Wojzechowski

Geschäftsführer und Gründer

Chris Wojzechowski ist Geschäftsführer der AWARE7 GmbH und war von 2014 - 2018 Mitarbeiter am Institut für Internet-Sicherheit an der Westfälischen Hochschule in Gelsenkirchen. Dort war er bis zur Gründung der AWARE7 verantwortlich für die Live Hacking und Awareness Abteilung. Er zeigt Mitarbeitern, Privatpersonen und Firmenchefs wie Kriminelle vorgehen. Schutzmöglichkeiten und Sofortmaßnahmen zählen, neben eindrucksvollen live Vorführungen, zu seinen Vorträgen. Zu aktuellen Themen der IT-Sicherheit und Informationstechnik steht er regelmäßig Rede und Antwort vor Mikrofon und Kamera.

Berufserfahrung	> 6 Jahre
Verantwortungsbereich	• Geschäftsführung • Live Hacking, Social Engineering Audits, Phishing Simulation
Qualifikation	B. Sc. Wirtschaftsinformatik M.Sc. Internet-Sicherheit BSI-Grundschutz Praktiker
Fachliche Spezialisierung	• Organisation, Planung und Durchführung von Live Hacking & Awareness Veranstaltung • Entwicklung von Workshop und Seminarinhalten sowie deren Durchführung • Erstellung von technischen Reports, Repräsentation und Unterstützung bei der Durchführung bei technischen Sicherheitsanalysen
Publikationen	Kompass IT-Verschlüsselung Orientierungs- und Entscheidungshilfen für kleine und mittlere Unternehmen (Bundesministerium für Wirtschaft und Energie) Security and Privacy in Blockchain Environments (dotmagazine) Internet of Things – Herausforderungen für die IT-Sicherheit (IT-SICHERHEIT)
Sprachen	Deutsch, Englisch

Matteo Große-Kampmann

Geschäftsführer und Gründer

Matteo Große-Kampmann ist technischer Geschäftsführer der AWARE7 GmbH, kooperativer Doktorand am Institut für Internet-Sicherheit und der Ruhr Universität Bochum und forscht interdisziplinär in den Bereichen IT-Sicherheit, Datenschutz und Medizintechnik. Er veröffentlicht zudem diverse wissenschaftliche Papiere, sowie massentaugliche Artikel und Blogbeiträge. Bundesweit wird er für Live Hacking und Awareness Veranstaltungen gebucht. Als Experte steht er im (über)regionalen Funk und Fernsehen gelegentlich vor der Kamera.

Berufserfahrung	> 6 Jahre
Verantwortungsbereich	• Geschäftsführung • Penetrationstest, Research & Development
Qualifikationen	B. Sc. Medizintechnik M. Sc. Internet-Sicherheit Promotionskandidat Ruhr Universität Bochum (Dr.Ing.) ISO 27001 Lead Auditor
Fachliche Spezialisierung	• Leitung und Organisation der Technology, Research & Development • Analyse und Bewertung von IT-Sicherheitsaspekten technischer Geräte, Prozesse und Architekturen
Publikationen	Where is my mind?! Assessing Security & Privacy in Mental Health Applications, to be published. GDPiRate – Stealing Your Personal Information on and Offline, ESORICS 2019, Luxembourg. Threat Modeling for Mobile Health Systems, 2018 IEEE Wireless Communications and Networking Conference Workshops: IoT Health 2018, Barcelona. Verwendung von Geolokationsdaten als Angriffsvektor für Social Engineering (DACH Security Konferenz 2018) Wie gehen Angreifer vor: Einführung und Grundlagen in angriffsszentriertes Risikomanagement und Intelligence Driven Risk Awareness. An Usable Application for Authentication, Communication and Access Management in the Internet of Things (Springer International Publishing, ICIST 2016, Druskininkai, Lithuania Netzwerksicherheit - Dozentenbuch (Handwerkskammer Rheinhessen)
Sprachen	Deutsch, Englisch

Jonas Poenicke

Referent für Cybersecurity

Jonas Poenicke ist nach zwei Jahren Tätigkeit am Institut für Internet-Sicherheit in Gelsenkirchen für die AWARE7 GmbH als Live-Hacking-Referent tätig geworden und seit Gründung der AWARE7 GmbH verantwortlich für Ausbau und Wartung der Live-Hacking-Infrastruktur. Er koordiniert deutschlandweit die Referent*innen für diverse Awareness Kampagnen. Darüber hinaus schreibt er regelmäßig Blogbeiträge zu aktuellen Themen der IT-Sicherheit.

Berufserfahrung	2 Jahre
Verantwortungsbereich	• Reliability Technician Live-Hacking und Awareness • Organisation, Planung und Durchführung von Live Hacking & Awareness Kampagnen
Qualifikationen	Student der Informatik an der Freien Universität Berlin Certified Ethical Hacker (CEH)
Fachliche Spezialisierung	• Ausbau und Wartung der Live-Hacking-Infrastruktur • Durchführung von Live-Hacking-Vorträgen unterschiedlicher Form
Sprachen	Deutsch, Englisch

Moritz Gruber

Referent für Cybersecurity

Moritz Gruber ist Penetrationstester, Softwareentwickler und Cybersecurity Referent bei der AWARE7 GmbH. Er arbeitet seit 2014 in der IT-Sicherheitsbranche. Er war bis zu seinem Wechsel zu der AWARE7 Projektmitarbeiter und zuständig für die Durchführung von Penetrationstests, Awareness Schulungen sowie der Beratung bei der Einführung von Informationssicherheits-Managementsystemen. Dabei zählen gerade die Analyse von Webanwendungen, Webservices sowie die Analyse von Systemen von KRITIS-Betreibern zu seinen Stärken.

Berufserfahrung	> 5 Jahre
Verantwortungsbereich	• Pentrationstesting • Softwareentwicklung • Referententätigkeit
Qualifikation	M. Sc. IT-Sicherheit/Informationstechnik OSSTMM Professional Security Tester (OPST) Cyber Security Practitioner (CSP)
Fachliche Spezialisierung	• Schwachstellenanalyse und Penetrationstests von Webanwendungen & Webservices • Organisation, Planung und Durchführung von Awareness Schulungen • Entwicklung von Backend-Systemen • Beratung bei der Umsetzung und Planung von ISM-Systemen • Umsetzung von individuellen Awareness Kampagnen
Publikationen	Systematic Analysis and Classification of XSLT Attacks Security Evaluation and Classification of Vulnerabilites found in REST API Management Frameworks
Sprachen	Deutsch, Englisch

Jan Hörnemann

Referent für Cybersecurity

Jan Hörnemann ist Softwareentwickler und Cybersecurity Referent bei der AWARE7 GmbH. Er arbeitet seit 2018 als Projektmitarbeiter und ist zuständig für die Entwicklung von Anwendungen und die Durchführung von Awareness Schulungen. Er ist zudem aktiver Autor auf dem IT-Sicherheitsblog. Das Entdecken von neuen Betrugsmaschen im Internet zählt ebenfalls zu seinem Aufgabengebiet. Die anschließende Erstellung von Inhalten, um die Bevölkerung zu sensibilisieren, ist für Ihn obligatorisch.

Berufserfahrung	2 Jahre
Verantwortungsbereich	• Softwareentwicklung • Referententätigkeit • Blog Autor
Qualifikation	B.Sc. Informatik.Softwaresysteme Certified Ethical Hacker (CEH)
Fachliche Spezialisierung	• Durchführung von Awareness Schulungen • Entwicklung von Frontend-Systemen • Umsetzung von individuellen Awareness Kampagnen
Publikationen	Konzeptionierung und prototypische Entwicklung einer Visualisierung von Daten, die innerhalb einer Threat-Intelligence-Plattform erfasst werden.
Sprachen	Deutsch, Englisch

Referenzen

Munich RE	Projekttyp	**Diverse Security Awareness Days, Awareness Kampagnen und Sensibilisierungsveranstaltungen**
Münchener Rückversicherungs-Gesellschaft Aktiengesellschaft in München	Projektbeschreibung	Die MunichRE ist führender Experte für globale & lokale Risikolösungen: Erst- & Rückversicherungen, Gesundheitsgeschäft und vieles mehr. Im Rahmen der Security Awareness Days wird laufend auf die Cyber Gefahren aufmerksam gemacht. Im Kontext des Berufs- wie auch Privatlebens der Mitarbeiterinnen und Mitarbeiter, wurde gemeinsam mit der AWARE7 GmbH ein Vortragsformat speziell für den Konzern entworfen, konzipiert, entwickelt und durchgeführt.
Branche: Versicherung/ Finanzen Zielgruppe: Vorstand, Führungskräfte, Mitarbeiter Einsatzort: München	Arbeitspakete	- Vorbereitung und Individualisierung von Szenarien angepasst auf das Bedrohungspotenzial des Kunden - Bühnen Performance für 150+ Teilnehmer mit Live Aspekten und Vorführungen - Individualisierung von Live Szenarien - Umfangreiche Q&A Sessions nach Vorträgen

MEAG	Projekttyp	**Awareness & Live Hacking Training In Nord- West & Süddeutschland**
MEAG MUNICH ERGO AssetManagement GmbH	Projektbeschreibung	Die MEAG Munich Ergo Assetmanagement GmbH ist der Vermögensverwalter der Munich Re und der ERGO Group. Sie setzt neben der Verwaltung der konzerneigenen Gelder auf das Geschäft mit Partnern außerhalb des Munich-Re-Konzerns. Im Rahmen der Awareness & Live Hacking Vorträge wurde den MA dargestellt, wie schnell ein Hacking Angriff erfolgreich sein kann und welche Informationen dafür verwendet werden. Im Anschluss wurden hilfreiche Handlungsempfehlungen für den privaten und beruflichen Bereich gegeben.
Branche: Versicherung/ Finanzen Zielgruppe: Führungskräfte, Mitarbeiter Einsatzort: München, Düsseldorf, Hamburg	Arbeitspakete	- Vorbereitung, Anpassung und Erstellung individueller Live Hacking Szenarien - Vortragsperfomance im Duett für ca. 30 – 50 MA an unterschiedlichen Standorten - Ausführliche Beantwortung von Fragen in der anschließenden Q&A Session

BG3000 smart camps	Projekttyp	**Live Hacking & Awareness Shows im gesamten Bundesgebiet, Europa und der Schweiz**
BG3000 Service GmbH	Projektbeschreibung	Die BG3000 ist ein Social Impact Start Up, das aus einer regionalen Initiative aus Bonn-Bad Godesberg hervorgegangen ist und sich mit digitalen Bildungs- und Gesellschaftsthemen auseinandersetzt. Darüber hinaus organisieren wir Technologietalks, Thinktanks und gezielte Projekte zur digitalen Wirtschafts- und Kommunalentwicklung. Im wiss. Beirat des Unternehmens sitzen u.a. Axel Voss (MdEP) Im Rahmen unterschiedlicher Formate werden von der AWARE7 GmbH zielgruppenspezifische Awareness Vorträge mit Live Hacking Aspekten konzipiert, entwickelt und durchgeführt. Zu den Zielgruppen stehen Schüler/innen, Lehrer/innen sowie Schulleiter/innen. Bisher wurden international durch diese Kooperation 25.000 Menschen geschult, wobei kein Vortrag mehr als 100 Zuschauer/innen hat.
Branche: Weiterbildung/ Erwachsenenbildung Zielgruppe: Schüler*innen, Lehrer*innen, Schulleiter*innen Einsatzorte: Europa, Schweiz	Arbeitspakete	- Laufende Anpassung von Vortrags- und Live Elementen eines Vortrages - Branchenspezifische Anpassung von Vortragsunterlagen

GELSENWASSER GAS. STROM. NATÜRLICH WASSER.	Projekttyp	Unternehmensweite Awareness Kampagne mit Live Hacking und Demonstrationselementen
GELSENWASSER AG Branche: KRITIS/ Strom-/ Wasser & Gasversorgung Einsatzorte: NRW Zielgruppe: Vorstand, Führungskräfte, Mitarbeiter	Projektbeschreibung	Die GELSENWASSER AG mit Sitz in Gelsenkirchen ist eines der größten Trinkwasserversorgungsunternehmen Deutschlands. Neben dem Geschäftsbereich Wasserversorgung engagiert sich die Gelsenwasser AG auch in den Bereichen Abwasser und Strom- und Gasversorgung. Im Rahmen wiederkehrender Awareness und Sensibilisierungsmaßnahmen wurde gemeinsam mit der AWARE7 ein individuelles Programm ausgearbeitet, dass die Mitarbeiter*innen auf bekannte und neuartige Betrugs- und Bedrohungsmaschen aus und mit dem Internet vorbereitet.
	Arbeitspakete	- Individualisierung und Erstellung von Vortragsinhalten und Demonstrationen - Beantwortung von Fragen persönlich und beruflicher Natur - Durchführung von mehr als 70 Vorträgen

	Projekttyp	Vorträge und Live Hacking Sessions für unterschiedliche Zielgruppen und angepasster Länge in 2018 und 2019
Ministerium für • Wirtschaft, Innovation, Digitalisierung und Energie (NRW) • Klimaschutz, Umwelt, Landwirtschaft, Natur und Verbraucherschutz (NRW) • Kultur und Wissenschaft (NRW) • Kinder, Familie, Flüchtlinge und Integration (NRW) • Heimat, Kommunales, Bau und Gleichstellung (NRW)	Projektbeschreibung	Nordrhein-Westfalen ist ein Land und eine parlamentarische Republik im Westen der Bundesrepublik Deutschland und grenzt im Norden und Nordosten an Niedersachsen. Die Landeshauptstadt ist Düsseldorf. Mit ca. 18 Millionen Einwohnern ist das Land NRW das bevölkerungsreichste deutsche Land. Im Rahmen wiederkehrender Awareness Maßnahmen hat die AWARE7 GmbH gemeinsam mit Verantwortlichen der Ministerien unterschiedliche Vortrags- und Live Hacking Demonstrationen entwickelt.
Branche: Regierung Einsatzorte: NRW Zielgruppe: Mitarbeiter	Arbeitspakete	- Individualisierung und Erstellung von Vortragsinhalten und Demonstrationen - Beantwortung von Fragen persönlich und beruflicher Natur - Durchführung von mehreren unterschiedlichen Vorträgen und Awareness Demonstrationen

SAP	Projekttyp	Security Awareness Day
SAP SE Branche: Software Einsatzorte: Walldorf Zielgruppe: Belegschaft	Projektbeschreibung	Die SAP SE mit Sitz in Walldorf ist ein börsennotierter Softwarekonzern. Nach Umsatz ist SAP das größte europäische (und außeramerikanische) sowie das weltweit drittgrößte börsennotierte Softwareunternehmen. Tätigkeitsschwerpunkt ist die Entwicklung von Software zur Abwicklung sämtlicher Geschäftsprozesse eines Unternehmens. Auf dem Security Awareness Day 2019 hat die AWARE7 GmbH moderne Angriffsattacken im Duett vorgestellt. Zusätzlich wurden im Vortrag Schutzmöglichkeiten dargestellt.
	Arbeitspakete	- Individualisierung und Erstellung von Vortragsinhalten und Demonstrationen - Durchführung des Vortrages in englischer Sprache - Vortrag vor ca. 300 Personen

Weitere Referenzen finden Sie im Anhang. Auf Nachfrage erhalten Sie unsere Branchenreferenzen.

Sie möchten Kontakt mit uns aufnehmen?

Chris Wojzechowski

Tel. +49 (0) 209 / 88 30 676 – 1
Mobil +49 (0) 0170 / 411 3255
Mail chris@aware7.de

Matteo Große-Kampmann

Tel. +49 (0) 209 / 88 30 676 – 2
Mobil +49 (0) 170 / 229 6288
Mail matteo@aware7.de

KERN

- Live Hacking & Awareness Kampagnen
- Schulungsformate & Workshops
- Phishing Kampagnen & Simulationen
- Social Engineering Audits
- Penetrationstest Web, iOS & Android
- Sicherheitsuntersuchungen & Sicherheitsanalysen
- RiskRex – Digital Risk Management

Anhang

Mitgliedschaft in Verbänden

Um die Rolle der AWARE7 GmbH im IT-Sicherheitsbereich weiter zu verstärken, stehen wir im ständigen Austausch mit relevanten Unternehmen, Organisationen und Forschungseinrichtungen. Darüber hinaus engagiert sich die AWARE7 GmbH in Vereinen und Verbänden, die sich der Weiterentwicklung von IT-Sicherheitslösungen und Konzepten widmen. Außerdem unterstützen wir Verbände mit reduzierten, teilweise kostenfreien Vorträgen und Shows, um die Sensibilisierung in der Allgemeinheit zu erhöhen.

eco - Verband der Internetwirtschaft e.V.	Mit der Digitalisierung erleben wir eine Phase des Strukturwandels und des Umbruchs, in der sich traditionelle Industrie- und Wirtschaftsbereiche verändern, täglich neue Geschäftsmodelle entstehen und bestehende digitale Anwendungen optimiert werden. Das Internet verändert unser Kommunikationsverhalten, unsere Arbeitsweise, unseren gesamten Alltag. Es verändert auch die Wirtschaft fundmental – und damit jedes einzelne Unternehmen. Das eco Hauptstadtbüro versteht sich als Sprachrohr der Internetbranche im politischen Berlin und in Brüssel. Dafür bringt unser interdisziplinäres Team aus Juristen, Politikwissenschaftlern und PR-Fachleuten seine gesamte Kompetenz ein.
eurobits Europäisches Kompetenzzentrum für IT-Sicherheit	Mit eurobits e. V. hat sich seit 1999 erfolgreich eine Dachmarke etabliert, unter der sich führende Forschungsinstitute, engagierte Unternehmen der Branche sowie junge Wachstumsunternehmen vereint haben. Jedes Mitglied bringt einen enormen Schatz an wertvollem Spezialwissen aus dem Bereich der IT-Sicherheit und Informationssicherheit mit. Damit ist eurobits der kompetente Ansprechpartner für Anfragen zu aktuellen IT-Sicherheitsthemen mit technologischem, wirtschaftlichem und wissenschaftlichem Bezug. Eurobits hat auch ein vielgefächertes Angebot an wissenschaftlichen Studiengängen und zertifizierten Weiterbildungsangeboten, welches in seiner Breite einzigartig in Deutschland ist. Die eurobits Mitglieder bieten u.a. die folgenden Studien- und Weiterbildungsmöglichkeiten an.
ASW Allianz für Sicherheit in der Wirtschaft Nordrhein-Westfalen e.V.	Die Allianz für Sicherheit in der Wirtschaft e.V. versteht sich als eine branchenübergreifende Plattform für einen Informationsaustausch zu sicherheitsrelevanten Herausforderungen der Privatwirtschaft. Durch ein umfangreiches Portfolio an Leistungen fördert der Verband die Kriminalprävention. Zu unseren Mitgliedern zählen Großkonzerne, kleine und mittelständische Unternehmen sowie Unternehmen der Sicherheitswirtschaft. Der Verband ist Mitglied der Public-Private Partnership „Sicherheitspartnerschaft NRW gegen Wirtschaftsspionage und Wirtschaftskriminalität“, zusammen mit den Landesministerien des Inneren und der Wirtschaft sowie der IHK NRW. Dabei verfolgt die ASW West - Allianz für Sicherheit in der Wirtschaft West e.V. ausschließlich und unmittelbar gemeinnützige Zwecke.
Ruhrvalley Cluster e.V.	Um der strategischen Innovationspartnerschaft ruhrvalley eine dauerhafte Struktur zu geben, wurde am 11. Januar 2019 der ruhrvalley Cluster e.V. gegründet. Ziel des Vereins ist es, die Durchführung von Forschungs-, Entwicklungs- und Innovationsaufgaben sowie den Wissenstransfer zwischen Wissenschaft und Wirtschaft zu fördern und zu unterstützen. Der ruhrvalley Cluster e.V. führt verschiedene Fach- und Netzwerkveranstaltungen durch, um Mitgliedern untereinander und im Austausch mit Experten und Entscheidern ein Forum für den gegenseitigen Austausch, die Formierung gemeinsamer Projekte und Initiativen zu bieten.
Bundesverband mittelständische Wirtschaft	Digitalisierung und Globalisierung stellen den Mittelstand vor neue gewaltige Herausforderungen. Der BVMW ist der Partner für die Unternehmen auf ihrem erfolgreichen Weg in die Zukunft. Denn der Unternehmer als Einzelkämpfer hat keine Chance mehr, gefragt sind Vernetzung und ganzheitliches Denken. Als wichtigster Mittelstandsverband Deutschlands vertritt er machtvoll die Interessen der mehr als drei Millionen Klein- und Mittelbetriebe in unserem Land. Der BVMW ist Kritiker und Partner der Politik zugleich.

Accelerator & Inkubator Programme

Die AWARE7 GmbH ist ein Unternehmen am IT-Sicherheitsmarkt und hat in der jungen Unternehmensgeschichte bereits zahlreiche Unternehmen, Organisationen, Behörden, Ministerien und Vereine von der eigenen Kompetenz überzeugen können. Für die ständige Weiterentwicklung von Sicherheitslösungen haben wir bereits an zahlreichen Accelerator & Inkubator Programmen teilgenommen.

TECHBOOST STARTUP Ein Programm der T · · · **Deutsche Telekom AG**	TechBoost, das Startup-Programm der Deutschen Telekom, unterstützt ausgewählte Technologie-Startups mit Guthaben für das Public-Cloud- Angebot der Telekom, die Open Telekom Cloud, sowie Kontakten zu potentiellen Kunden und gemeinsamen Aktivitäten im Bereich Vertrieb und Marketing. Startups mit einer digitalen Geschäftsidee auf Cloud-Basis können sich für TechBoost bewerben. Dabei spielt es zunächst keine Rolle, in welchem Entwicklungsstadium sich die Startups befinden. Denn es gibt unterschiedliche TechBoost-Programme für die verschiedenen Entwicklungsstufen.

pwc **PricewaterhouseCoopers GmbH**	Scale | FinTech ist ein Programm für wachstumsstarke europäische Start-ups u. a. aus den Bereichen Banking, Financial Solutions, Kreditvergabe, digitale Vermögensverwaltung und Kryptowährung und viele weitere Themen. Wir helfen Euch über einen Zeitraum von zwei Monaten eure Skalierungshürden zu überwinden und bringen Euch mit einflussreichen Unternehmen und Investoren zusammen. Potenzielle Unternehmenskooperationen und der Austausch von wertvollem Wissen mit Branchenexperten sind nur einige der vielen Chancen, die die Teilnahme an unserem Programm bietet. Das Programm beinhaltet mehrere Bausteine, die Euer Geschäft schnell auf das nächste Level bringen. Während der Events habt Ihr als Gründer die Möglichkeit, ein großes Netzwerk aus Führungskräften und Entscheidungsträgern der Industrie kennenzulernen und Euer Business den ausgewählten PwC Kunden vorzustellen. In unseren Masterclasses bekommt Ihr von PwC und Industrieexperten essenzielles Wissen vermittelt und profitiert von individueller Hilfestellung, die auf die Bedürfnisse Eures Start-ups zugeschnitten ist.

Cube 5 / Ruhr-Universität Bochum	Das Liftoff ist ein intensives Trainingsprogramm für early stage Cybersecurity Startups. Bei dem Programm geht es um mehr als finanzielle Unterstützung. Wichtiger ist, dass jedes Startup einen kraftvollen Schub für das Geschäftsmodell erhält. Coaches und Mentoren unterstützen die Startups bei der Entwicklung ihrer Go-To-Market-Strategie und schulen sie in effektiven Kommunikationsfähigkeiten. Auf der ITS.Connect, Deutschlands größter Jobmesse für Studierende der IT-Sicherheit, bekommen unsere Liftoff-Teams die Möglichkeit, ihr Unternehmen und offene Stellen zu präsentieren. Die Startups vernetzen sich und rekrutieren ihre zukünftigen Angestellten an ihrem eigenen Messestand. In den letzten Wochen des Liftoff-Programms werden Pitch-Fähigkeiten mithilfe der Experten erlernt. Daraufhin präsentiert ihr euch bei unserem Investoren-Pitch.

TV, Radio & Interviews

TV

Titel	Veröffentlicht
Statement zum Datendiebstahl zahlreicher Prominenter und Politiker	Taff, Prosieben
Digitale Sicherheit betrifft am Ende uns alle!	WDR, Aktuelle Stunde
Live Interview zum Thema: Open Data & Sicherheit	WDR, Lokalzeit Duisburg
Live Interview zum Thema: Breitbandausbei in Essen	WDR, Lokalzeit Ruhr
Neues Facebook-Löschzentrum in Essen vorgestellt	WDR, Aktuelle Stunde
Betrug mit der 110	WDR, Lokalzeit Ruhr
Freie Ausfahrt – WannaCry betrifft Parkhäuser!	WDR, Lokalzeit Ruhr
Erpressung ála Hollywood in Essen	Frühstücksfernsehen, Sat.1
Live Interview zum Thema: Fehlinformationen im Internet	WDR, Lokalzeit Ruhr
Wie schütze ich meinen Router?	Sat. 1 NRW

Radio

Titel	Veröffentlicht
Die unsichere Kommunikation mit anonymen Quellen	Deutschlandfunk
Hackerangriff: Experten diskutieren Stromausfall im Ruhrgebiet	WDR
Services im Darknet	Radio Emscher Lippe
Hacker-Angriffe: Droht uns der totale Stromausfall?	Radio Essen
Spionageschutz	TopFM 106,4
Der ThyssenKrupp Hack	Deutschlandfunk
Payback Punkte weg, warum?	Radio Oberhausen
Anstieg von Spam in Deutschland stark gestiegen.	Antenne 1 Stuttgart

Interviews

Titel	Veröffentlicht
48 Stunden Stromausfall – Mülheim hätte ein ernstes Problem	WAZ plus
Browser synchronisieren: Wie es geht, was Sie beachten müssen	Techbook.de, hna.de
Firefox blockiert Ton und Videos Standardmäßig	Insuedthueringen.de
Wenn der eigene Körper zum Passwort wird	Saarbrücker Zeitung
Schüler lernen sich und das Netz beherrschen	Stuttgarter Nachrichten
Beim „Live Hacking“ wird’s still	Techbote
Für wen taugt Linux?	Wiesbadener Kurier
Sind Apple-Rechner sicherer als Windows-PCs?	Welt.de
NetzDG: Weniger Hass oder weniger Meinungsfreiheit?	NRW
Ist das heimische WLAN mittlerweile sicher?	Welt.de
Fingerabdruck, Iris- und Gesichtserkennung – Was kann Biometrie?	wired
Bluetooth Sicherheitslücke – Fünf Milliarden Geräte gefährdet	tagesschau
Gastkommentar: Facebook will Gedanken lesen!	Weser Kurier
Passwörter: So schützen Sie ihre Online-Accounts	Gmx.at
So ist das Bankkonto vor Hacker-Angriffen sicher!	Aachener Nachrichten
Das digitale Klassenzimmer	WAZ
Umsicht oder Virenscanner – Androiden angemessen schützen!	Gelnhäuser Tageblatt
Navigation ohne Internet, offline zum Ziel	Süddeutsche Zeitung
Die Gefahr durch Bloat- und Crapware!	Welt.de, Handelsblatt.de
Die größetn Bedrohungen im Netz	DPA
Passwörter sind sicherer als biometrische Verfahren	DPA

Fachartikel, Paper & Studien

Titel	Veröffentlicht
Plenty Of Phish in the Sea – Analyzing PreAttack Surfaces	ESORICS 2020, Surrey, GB.
GDPiRate – Stealing Your Personal Information on and Offline	ESORICS 2019, Luxembourg.
Verwendung von Geolokationsdaten als Angriffsvektor für Social Engineering	DACH Security Konferenz 2018, syssec Verlag 2018
MENSCHpunktNULL - Gestaltungsansätze für die digitale Gesellschaft	Self-publishing
Kompass IT-Verschlüsselung Orientierungs- und Entscheidungshilfen für kleine und mittlere Unternehmen	Bundesministerium für Wirtschaft und Energie
Security and Privacy in Blockchain Environments	Dotmagazine
3D-Druck in der Entwicklung, Revolution des Druckens	IT-SICHERHEIT
Cybersicherheit für vernetzte Anwendungen In der Industrie 4.0	Vogel Fachverlag
Internet of Things - Herausforderungen für die IT-Sicherheit	IT-Sicherheit
Interconnected, Secured and Authenticated Medical Devices	Springer International Publishing SSIC17, Jaipur, India
Monitoring des Wohlergehens von alleinlebenden Senioren auf Basis von dezentral gemessenen Energieverbrauchswerten	VDE Kongress
Effiziente und sichere Behördenkommunikation	DATAKONTEXT-Fachverlag
Sicherheitsarchitektur von Windows 10: Sicherheitsanalyse von Windows 10 gegenüber Windows 8.1 und Windows 7	Springer Verlag
Prototyping a Minimally Invasive, Privacy-Compliant, Distributed AAL-System	IEEE Wireless Communications and Networking Conference Workshops