AWARE7
full service awareness agency









Mail hacking@aware7.de
Tel. +49 (0) 209 88306761
Web https://aware7.de

AWARE7 GmbH
Munscheidstr. 14
45886 Gelsenkirchen

Geschäftsführer
Chris Wojzechowski
Matteo Große-Kampmann

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

Wir begeistern Ihr Publikum

Bei einem Live Hacking führen ein oder zwei Hacker vor, wie leicht es für Cyberkriminelle Angriffe durchzuführen. Lernen Sie Risiken kennen und lernen Sie sich effektiv und verhältnismäßig zu schützen. Die Dauer einer Live Hacking Show ist nicht festgelegt. Von 15 bis 180 Minuten lassen sich Vorträge spannend gestalten. Wer sich vor Angriffen, Sicherheitslücken und Betrugsmaschen schützen will, muss wissen wie Kriminelle vorgehen. Dabei soll nicht vor der Digitalisierung abgeschreckt werden. Teilnehmer erhalten die Möglichkeit sich und andere zu schützen.

Seminare, Workshops & E-Learning

Wir geben Wissen weiter

Schulen Sie Mitarbeiter*innen im Umgang mit Technik oder bilden Sie Ihre eigenen Expertinnen und Experten aus. In regelmäßige Workshops und Seminaren schulen wir Ihre Mitarbeiter*innen vor Ort. Unter Anleitungen werden Sicherheitslücken gesucht und ausgenutzt. Im Rahmen unserer Cybersecurity E-Learning Programms, können Sie Ihre Belegschaft gleichzeitig, ohne viel Aufwand, ausbilden.

Penetrationstest

Wir sichern Ihre Infrastruktur vor Cyberkriminellen

Wir untersuchen Ihre Anwendung oder Infrastruktur auf Sicherheitslücken und helfen Ihnen diese im Anschluss zu beseitigen oder das Risiko der Ausnutzung zu minimieren. Sie erhalten eine umfangreiche Dokumentation. Die Untersuchung erfolgt in der Regel auf einem dedizierten Testsystem und wird, um das System widerstandsfähig gegenüber Angreifern zu machen, regelmäßig wiederholt. Wir arbeiten nach gängigen Richtlinien und Best Practices.

RISKREX – Digital Risk Management

Menschliche und technische Sicherheitslücken aufdecken

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

1-Personen Hacking Szenarien

WLAN

Kostenlosen Hotspots

Wer ein Netzwerk betreibt, hat auch erhebliche Möglichkeiten Einfluss auf den Datenverkehr zu nehmen. Die Anzahl der öffentlich verfügbaren Hotspots nimmt stetig zu. Diesen Fortschritt bei der Digitalisierung bringt jedoch auch Risiken mit sich. Wir zeigen welche Risiken das konkret sein können und bringen Tipps zum sicheren Umgang mit öffentlichen Netzwerken direkt mit.

Falsche Portale

Das freie Netzwerk ist gefunden, der Hotspot ausgewählt. Jetzt muss nur noch auf die Maske zum Login gewartet werden. Gerade in Hotels und Fastfood-Restaurants ist diese Methode beliebt, um zu erfassen wer im eigenen Netz surft. Doch diese Captive Portals können auch gefälscht werden. Wir legen für Ihre Veranstaltung ein solches Portal an und zeigen es im Live Hacking Vortrag. Wir helfen Ihnen die falschen Portale zu erkennen.

Verschlüsselung & Profiling

Welche Informationen können Betreiber über mich, mein Handy und Surfverhalten sehen, wenn ich im Netzwerk surfe? Wir zeigen live, was Betreiber eines Hotspots sehen können, ab wann es kritisch wird und wann Sie das Netzwerk auf jeden Fall verlassen sollten. Wir geben Tipps mit, wie der sichere Umgang im digitalen Ausland gelingt – oder in anderen Situationen, wenn sie auf einen Hotspot angewiesen sind.

Passwörter

Dictionary-Attack

Wir zeigen an einer bestehenden Sicherheitslücke, wie ein Wörterbuch-Angriff auf ein E-Mail-Postfach aussieht. Der Anbieter dieses Postfachs bietet in Deutschland Millionen von Postfächern an. An diesem Szenario lässt sich gut darstellen, warum es ein Trugschluss ist sich auf den Anbieter zu verlassen. Wir helfen einzuschätzen, wie sicher das eigene Passwort ist. Für dieses Szenario ist **zwingend** Internet notwendig. Siehe Technische Voraussetzungen (Seite 6)

Personalisierte Passwortlisten

Im Durchschnitt besitzt jeder Internetnutzer 100 Accounts. Jeder Account sollte mit einem einzigartigen Passwort versehen werden. Um dieser Anforderung gerecht zu werden, verwenden viele Menschen Passwörter, die sich aus ihrem persönlichen Umfeld herleiten lassen. Name der Mutter, Geburtstag des Vaters, Lieblingskeks des Hundes. Wir zeigen, wie eine professionellere Passwort-Attacke aussieht. Wir empfehlen im Laufe des Vortrages noch über soziale Netzwerke zu sprechen.

Datendiebstahl & Account Hygiene

Mittlerweile wurden über 9.000.000.000 Accounts gestohlen – sind ihre Daten auch dabei? In der breiten Masse der Gesellschaft ist es nicht bekannt, welche Websites und Dienste gehackt worden sind und wie jeder für sich in Erfahrung bringen kann, wann wo seine Daten gestohlen worden sind. Wir stellen vor, welche Dienste kostenfrei in Anspruch genommen werden können und wie sich jeder präventiv davor schützen kann einem Datendiebstahl zum Opfer zu fallen. Denn diese Datendiebstähle sind auch Datenquellen für Kriminelle

Social Engineering

Anonymität im Internet auflösen

eBay Betrüger sowie Betreiber von Fake Accounts sind erfolgreich, da sie sich in der Anonymität des Internets in Sicherheit wiegen. Doch es gibt zahlreiche Möglichkeiten und Ansätze diese Anonymität aufzulösen. Ermittlungsbehörden der ganzen Welt sind mit dieser Herausforderung konfrontiert. Werfen sie mit uns einen Blick in die professionellen Recherchemöglichkeiten des Internets. Lernen sie aus den Fehlern, die die Kriminellen machen, um sich und ihre Privatsphäre zu schützen.

Soziale Netzwerke - Privat

Nicht alles sollte auf sozialen Netzwerken hochgeladen werden. Die Maschinerie, die hinter sozialen Netzwerken wie Facebook, Instagram und Twitter steckt, ist für viele nicht greifbar. Wir nehmen sie mit, zeigen ihnen was professionelle Angreifer mit Schnittstellen und Daten der privaten sozialen Netzwerke anrichten können. Auch wenn das Szenario im ersten Augenblick erschreckend ist, raten wir grundsätzlich davon ab seinen Account im Anschluss zu löschen.

Soziale Netzwerke - Beruflich

Xing und LinkedIn spielen in der heutigen Berufswelt eine große Rolle. Die Vernetzung und das Knüpfen von Kontakten sind wenige, essentielle Aufgaben dieser Netzwerke. Doch die Angabe von Informationen mit beruflichem Kontext und der Registrierung mit der privaten E-Mail ermöglichen Angreifern unterschiedliche Potenziale. Von Fake Accounts- und Anfragen bis hin zur Generierung von beruflichen E-Mail-Adressen ist viel möglich. Wir sensibilisieren und zeigen, was möglich ist und wie Schutzmöglichkeiten aussehen.

AWARE7 GmbH

Munscheidstr. 14
Im Wissenschaftspark
45886 Gelsenkirchen

Geschäftsführer

Chris Wojzechowski
Matteo Große-Kampmann

Phishing, Vhishing & Domain Squatting

E-Mail Betrug und Fälschung

Was an einer E-Mail lässt sich fälschen, wie lässt es sich kontrollieren und erkennen? Wir zeigen anhand unterschiedlicher Spam- und Phishingmails, wie die echten E-Mails von unechten unterschieden werden können. Eine E-Mail ist das häufigste Einfallstor für Kriminelle. Links und Anhänge lassen sich verschicken – und wenn sich der Kriminelle die Arbeit gemacht hat, sehen die Mails zusätzlich noch seriös aus.

Mit der falschen Nummer anrufen

Die Polizei ruft nicht mit der 110 an! Wir zeigen es aus Sensibilisierungsgründen trotzdem – und geben Tipps, wie sie die Betrugsmaschen entlarven können. Denn was viele nicht wissen: Die Kriminellen müssen nicht die Telefonnummer von der Polizei nehmen. Sie können auch jede andere verwenden. So kann es auch ein falscher Anruf vom Wasserversorger, Telekommunikationsanbieter, dem Nachbarn oder der eigenen Mutter sein.

Eine SMS fälschen

Der Großteil der Kommunikation findet mittlerweile über Instant Messenger statt. Es werden kaum noch Kurznachrichten versendet. Die SMS wird aber noch aktiv von Unternehmen genutzt, um Ihren Account abzusichern. Jahrelang war auch die Überweisung von Geld, mit der Hilfe des SMS TAN Verfahrens, aus dem online Banking Bereich möglich. Wir zeigen die Schwachstellen der SMS und warum sie sich auf andere Technologien verlassen sollten.

So fälschen Kriminelle Webseiten

Wir zeigen Ihnen wie Kriminelle Internetseiten fälschen und Ihnen den Eindruck vermitteln, dass Sie sich auf der originalen Website befinden. Am Ende zielt alles darauf ab Ihre Daten zu stehlen. Schützen Sie sich und Ihre Mitarbeiter/innen vor Daten- und Identitätsdiebstahl.

Phishing in sozialen Netzwerken

Eine Handvoll Phishing-Kampagnen in sozialen Netzwerken hat es bereits in die Tagesnachrichten gebracht. Sie sind auf der einen Seite gut gemacht, teilweise individualisiert und werden meist mit einem Schneeballartigen Effekt angetrieben. Wir zeigen Ihnen aktuelle Kampagnen und geben Tipps, wie man sich schützt.

Whatsapp als Phishingplattform

Der Instant Messenger erfreut sich größter Beliebtheit – weltweit. Doch die Plattform wird auch von Kriminellen verwendet. Die Ende-zu-Ende Verschlüsselung verhindert weitere Analysen. Stets ist der Anwender, die Anwenderin gefragt. Doch was gibt es zu beachten bei Links von Freunden und Bekannten? Wir zeigen die Masche und die Schutzmöglichkeiten!

USB-Geräte, Ladekabel und Zerstörungssticks

USB-Geräte, die keine sind

Schnell eine Datei auf einen Stick ziehen, zur Kollegin rüberreichen und ihn dann vergessen. Doch welche potenziellen Gefahren können USB-Sticks mit sich bringen, die von Externen ins Unternehmen gebracht werden? Wir stellen Ihnen unser Repertoire vor und zeigen die Gefahren, die daraus entstehen. Die Tipps, wie Sie mit diesem Risiko umgehen, behalten wir nicht für uns. Schaffen Sie Awareness für fremde Geräte und vermeiden Sie so Sicherheitsvorfälle im Unternehmen

Ladekabel, Geräte und der Akku

Mal schnell das Handy aufladen. Wir zeigen Ihnen Ladekabel, die in der Lage sind Ihre Infrastruktur zu kompromittieren. Auf Geschenke dieser Form sollte deshalb verzichtet werden. Erstrecht wenn Sie medizinische Geräte in der Verwendung haben, ist die Erhöhung der Aufmerksamkeit für solche Attacken ratsam. Sichtbare Chancen, unsichtbare Gefahren – gerade bei der Digitalisierung spielt die richtige Einschätzung des Risikos eine größere Rolle als bisher.

USB-Sticks mit Überspannung

Vandalismus. Nicht erst seit gestern ein Problem. Kaum ein elektronisches Gerät – außer es ist darauf ausgelegt – ist vor einem Überspannungsschutz gefeit. Wir zeigen Ihnen USB-Sticks, mit denen Sie innerhalb von Minuten Dutzend elektronische Geräte zerstören könnten. Ein Schutz vor diesen Sticks ist schwierig umzusetzen. Wir geben Ihnen trotzdem hilfreiche Tipps und Empfehlungen mit, wie mit diesen USB-Sticks umgegangen werden sollte.

Google Hacking, Darknet & Alternativen

Erleben Sie, was Google kann!

Die beliebteste Suchmaschine in Deutschland ist Google. Die ausgereifte Technologie hinter der Suchmaschine serviert den Suchenden die Informationen, die er zu suchen scheint. Doch die Suchmaschine indexiert noch viel mehr. Vom Drucker bis hin zu geheimen Dokumenten und Gutscheinen lässt sich nicht nur bei Google suchen – es lassen sich auch viele der Punkte

Das Darknet

Sie wollen anonymer surfen als sonst? Sind im Hotel und wissen nicht, ob das Netzwerk vertrauenswürdig ist? Sie sind an einem öffentlichen Computer und wollen keine Daten hinterlassen? In solchen – und vielen anderen Fällen – kann Ihnen das Darknet behilflich sein. Wir ziehen das anonyme Netzwerk für Sie aus dem Schatten und zeigen, dass es nicht viel schlimmer ist, als das normale Internet ebenfalls.

Alternativen

Die ganze Welt verlässt sich auf Google, Windows und Chrome? Von wegen! Es gibt zahlreiche, vielversprechender Alternativen. Wir zeigen Ihnen gerne ausgewählte Alternativen, die Ihnen vielleicht mehr zusagen, als die Branchenriesen es im Augenblick tun. So erfreut sich DuckDuckGo z.B. steigender Beliebtheit. Doch die Suchmaschine macht mehr als nur Ihre Privatsphäre schützen. Wir zeigen Ihnen was genau!

AWARE7 GmbH

Munscheidstr. 14
Im Wissenschaftspark
45886 Gelsenkirchen

Geschäftsführer

Chris Wojzechowski
Matteo Große-Kampmann

2-Personen Hacking Szenarien

Flugdrohnen

Daten einsehen, stehlen und ersetzen

Drohnen sind in der Lage gestochen scharfe Fotos zu schießen – sogar aus einer Entfernung von mehreren Metern zum Objekt. Doch wie sicher sind die Daten auf der Drohne gesichert? Wir zeigen Ihnen am Beispiel einer Consumer-Drohne (ca. 200 EUR), dass an Sicherheit nicht immer gedacht worden ist und sie lieber darauf verzichten Bilder mit Ihrer Drohne zu schießen, die zu viel über Sie verraten.

Verbindungen stören und Drohnen stehlen

Drohnen in Deutschland müssen mit einer Kennzeichnung versehen sein, wem die Drohne gehört bzw. wer verantwortlich ist. Die Verbindung zwischen Drohne und Steuerungseinheit kann auf unterschiedliche Arten und Weisen stattfinden. Anhand unserer Consumer Drohne zeigen wir Ihnen, wie leicht es ist die Kontrolle über die Drohne zu gewinnen. Für das was danach passiert, ist der Inhaber verantwortlich

Hochprofessionelle Phishing Attacken

Knacken der Zwei-Faktor-Authentifizierung

Sie haben in Ihrem Unternehmen nicht nur Benutzernamen und Passwörter – sondern auch einen zweiten Faktor, der bei der Authentifizierung angegeben werden muss? Beliebte Softwarelösungen sind z.B. der Google oder Microsoft Authenticator. Wir zeigen Ihnen, warum auch diese Lösungen keine 100%ige Sicherheit versprechen – und wie man die Sicherheitsmechanismen umgehen kann.

Copytrap

Wie oft kopieren Sie Texte aus dem Internet? Kaum taucht ein Problem auf, sucht man im Internet nach einer Lösung. Die ist in der Regel auch schnell gefunden. Doch wieso sollte man den Text abtippen – wenn auch kopieren reicht? Wir zeigen Ihnen, warum Sie von fremden Websites nur mit Bedacht etwas kopieren sollten.

Cutting-Edge Watering-Hole-Angriff Methoden

In regelmäßigen Abständen tauchen neue, ausgefeilte Phishing Methoden auf, die nicht nur für den Laien, sondern auch für den erfahrenen Nutzer sehr schwierig zu erkennen sind. Dazu zählen z.B. Social Login HTML Inline Formulare oder der Chrome Browser Scrolling Tab Injection Angriff zu. Dieses Szenario empfehlen wir ausschließlich für technisch versiertes Publikum.

Live Social Engineering

Im Rahmen Ihrer Veranstaltung führen wir zu Beginn eine Live Social Engineering Attacke durch. Hierzu wird ein freiwilliger aus dem Publikum gewählt, der anschließend Fragen beantworten muss. Was wir mit den gewonnenen Informationen machen? Das zeigen wir Ihnen im Anschluss.

AWARE7 GmbH

Munscheidstr. 14
Im Wissenschaftspark
45886 Gelsenkirchen

Geschäftsführer

Chris Wojzechowski
Matteo Große-Kampmann

Technische Voraussetzungen

Bitte beachten Sie das unsere Referenten stets mit ihren eigenen Laptops arbeiten – unabhängig davon ob der Vortrag durch einen oder zwei Referenten durchgeführt wird. Es ist eine zwingende Voraussetzung für die Durchführung der Veranstaltung, dass die entsprechenden Geräte auf der Bühne verwendet werden können. Es ist leider nicht möglich für die Live Hacker auf einen stationären Laptop/ Vortragsnotebook zurückzugreifen.

All unsere Referenten arbeiten mit aktueller Hard- und Software aus dem Hause Apples. Auf vor Ort installierte Apple TVs greifen wir gerne zurück. Eine Projektion mit Hilfe von Microsoft Wireless Display können wir nicht verwenden.

Anforderungen für einen Referenten

Sitz/Stehgelegenheit

1x Sitzplatz inkl. Tisch und/**oder**
Stehpult alt. Stehtisch

Stromversorgung

Mindestens 1x Stromanschluss
Im besten Fall 4x Anschlüsse

Darstellung & Projektion

1x Leinwand/Projektionsfläche und
1x Beamer und/**oder**
1x ausreichend großer Bildschirm (60“+)

Mögliche Anschlüsse sind HDMI, DVI und VGA
Alle relevanten Adapter werden mitgebracht. Denken Sie beim Einsatz eines HDMI-Splitters bitte an einen HDCP-Unterdrücker

Internetanschluss

Optimal:	LAN Anschluss Falls ein Whitelisting der MAC-Adresse nötig ist, melden Sie sich bitte vorher.
Optional:	WLAN-Zugang
Notfall:	Mobilfunk Falls kein (W)LAN verfügbar ist, melden Sie sich bitte vorher.

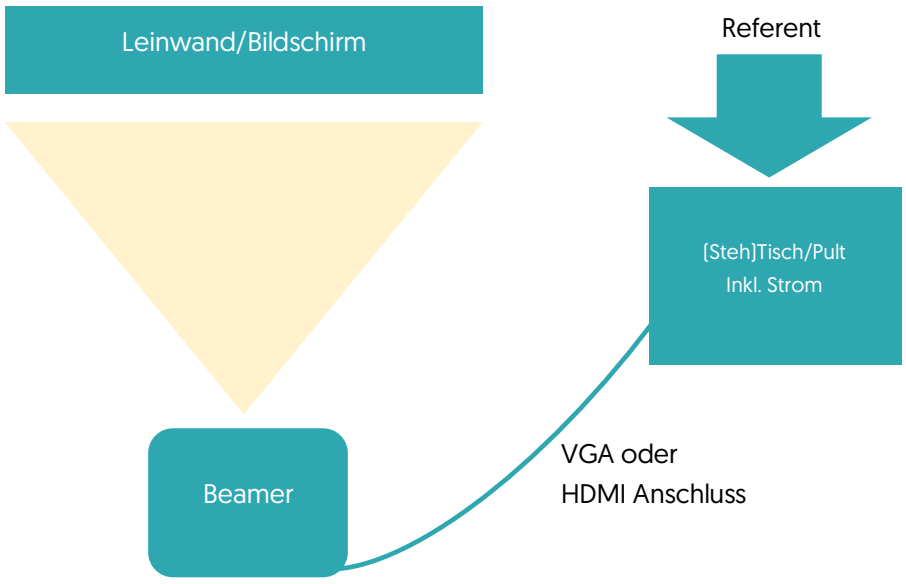
Akustik

Ab ca. 50 Personen (nach Raumgestaltung) sind Mikrofone als Headsets geeignet
Ein Klinkenstecker o.ä. für den Laptop ist nicht nötig

Wünschenswert

Stilles Wasser und/oder Kaffee für den Referenten.

Schematischer Aufbau für einen Referenten



AWARE7 GmbH

Munscheidstr. 14
Im Wissenschaftspark
45886 Gelsenkirchen

Geschäftsführer

Chris Wojzechowski
Matteo Große-Kampmann

Anforderungen für zwei Referenten

Sitz/Stehgelegenheit

2x Sitzplatz inkl. Tisch und/**oder**
2x Stehpult alt. 2x Stehtisch

Stromversorgung

Mindestens 2x Stromanschlüsse
Im besten Fall 5x Anschlüsse

Darstellung & Projektion

2x Leinwände/Projektionsflächen und 2x Beamer und/**oder**
2x ausreichend große Bildschirme (i.d.R. 60“+)
Auf einer Projektionsfläche/Bildschirm wird jeweils ein Laptop dargestellt

Mögliche Anschlüsse sind HDMI, DVI und VGA
Alle relevanten Adapter werden mitgebracht. Denken Sie beim Einsatz eines HDMI-Splitters bitte an einen HDCP-Unterdrücker

Internetanschluss

Optimal: LAN Anschlüsse
Falls ein Whitelisting der MAC-Adresse nötig ist melden Sie sich bitte vorher.

Optional: WLAN-Zugänge

Notfall: Mobilfunk
Falls kein (W)LAN verfügbar ist, melden Sie sich bitte vorher.

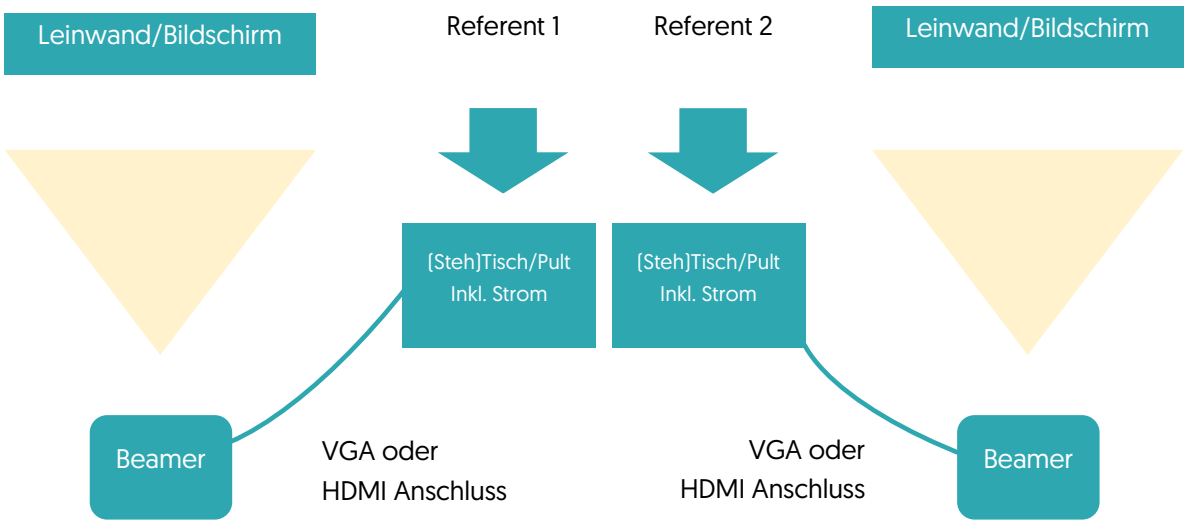
Akustik

Ab ca. 40 – 50 Personen (je nach Raumgestaltung) sind Mikrofone als Headsets geeignet
Ein Klinkenstecker o.ä. für den Laptop ist nicht nötig

Wünschenswert

Wasser und/oder Kaffee für die Referent

Schematischer Aufbau für zwei Referenten



AWARE7 GmbH

Munscheidstr. 14
Im Wissenschaftspark
45886 Gelsenkirchen

Geschäftsführer

Chris Wojzechowski
Matteo Große-Kampmann

Sie möchten Kontakt mit uns aufnehmen?

➔kontakt@aware7.de

Chris Wojzechowski

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

- Live Hacking & Awareness Kampagnen
- Schulungsformate & Workshops
- Phishing Kampagnen & Simulationen
- Social Engineering Audits

Matteo Große-Kampmann

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

- Penetrationstest Web, iOS & Android
- Sicherheitsuntersuchungen & Sicherheitsanalysen
- RiskRex – Digital Risk Management

AWARE7 GmbH

Munscheidstr. 14
Im Wissenschaftspark
45886 Gelsenkirchen

Geschäftsführer

Chris Wojzechowski
Matteo Große-Kampmann

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 **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 • Bochum **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 Nordrhein-Westfalen **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.
ruhr valley **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.
BVMW Bundesverband mittelständische Wirtschaft **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	TechBoost, das Startup-Programm der Deutschen Telekom, unterstutzt ausgewahlte Technologie-Startups mit Guthaben fur das Public-Cloud- Angebot der Telekom, die Open Telekom Cloud, sowie Kontakten zu potentiellen Kunden und gemeinsamen Aktivitaten im Bereich Vertrieb und Marketing. Startups mit einer digitalen Geschaftsidee auf Cloud-Basis konnen sich fur TechBoost bewerben. Dabei spielt es zunachst keine Rolle, in welchem Entwicklungsstadium sich die Startups befinden. Denn es gibt unterschiedliche TechBoost-Programme fur die verschiedenen Entwicklungsstufen.
Deutsche Telekom AG	

pwc	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.
PricewaterhouseCoopers GmbH	

CUBE 5 LIFTOFF PARTICIPANT	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.
Cube 5 / Ruhr-Universität Bochum	

AWARE7 GmbH

Munscheidstr. 14
Im Wissenschaftspark
45886 Gelsenkirchen

Geschäftsführer

Chris Wojzechowski
Matteo Große-Kampmann

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
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

AWARE7 GmbH

Munscheidstr. 14
Im Wissenschaftspark
45886 Gelsenkirchen

Geschäftsführer

Chris Wojzechowski
Matteo Große-Kampmann