

Digitale Selbstverteidigung – Mit Know-how Cyberattacken vorbeugen

Produktnummer
2025-45507K

Termin
06.10.2025
09:00-16:45

Gebühren pro Teilnehmer/-in
296,00 EUR

Die VWA geht davon aus, dass der Arbeitgeber die Teilnahmegebühr sowie Reisekosten übernimmt.

Einleitung

In den letzten zwei Jahren haben die Cyber-Angriffe um über 300 % zugenommen – Tendenz stark steigend! Unternehmen ist es peinlich, wenn Daten oder Angriffe an die Öffentlichkeit gelangen. Ein Angriff kann schnell existenzbedrohend werden! Wer den Feind kennt, kann sich besser verteidigen. Schützen Sie sich und Ihre Mitarbeitenden durch eine Sensibilisierung. Dieses Seminar zeigt nicht nur die Gefahren und Wege auf, die Kriminelle für ihre Machenschaften nutzen, sondern auch Maßnahmen, damit es erst gar nicht so weit kommt. Schreiten Sie zur digitalen Selbstverteidigung! Erklärt an konkreten Beispielen aus der Praxis – direkt zum Nachvollziehen.

Inhalte

- Cyber-Welt entmystifiziert: Angriffsvektoren verstehen, Täuschungen enttarnen - von Phishing-Mails bis E-Mail-Links
- Mobiler Phishing-Schutz: Tücken der Phishing-Erkennung auf mobilen Geräten – Besonderheiten und Gefahrenabwehr am Smartphone
- Social-Engineering entgegenwirken: Psychologische Tricks und versteckte Gefahren durchschauen.
- Zum Cyber-Verteidiger werden: mit Expertenwissen zur effektiven digitale Selbstverteidigung.

Grundsätzliches:

- Vorfälle und Notwendigkeiten - warum Informationssicherheit wichtig ist
- Abgrenzung Informationssicherheit - IT-Sicherheit - Datenschutz
- Privat vs Unternehmen
- Die Währung für "Gratis-Information"
- CIA (vertraulich - verfügbar)
- Risiken 2.0

Faktor Mensch:

- Die häufigsten Angriffspfade - CEO Fraud & Co

Ort

VWA Karlsruhe
Kaiserallee 12E
76133 Karlsruhe

Kontakt

Information

Ursula Deck
0721/985 50 14
ursula.deck@vwa-baden.de

Konzeption und Beratung

Tabea Adams
0721/985 50 18
tabea.adams@vwa-baden.de

[Anmelde- und
Teilnahmebedingungen](#)

[Impressum](#)

[Datenschutzhinweise](#)

- Innere Kündigung, inneres Mindset, Unternehmenskultur
- Mensch unterwegs (abhören, abfilmen, beobachten, VPN, Hacken, Klauen, WLAN-Betrug, Verschlüsselung)
- Riskante Hilfsbereitschaft

Faktor Technik:

- Schwachstellen: Trojaner, Viren, Botnet, Abhören
- IT-Schnittstellen (USB-Sticks, vernetzte Systeme, E-Mails)
- KI und AI

Die IT-Abteilung – Helfer oder Bremser?

- Wie kommuniziert – interner Software-Shop – Komplexität der internen Systeme
- Notfalladresse
- Passworte

Mensch im Unternehmen

Mein Gerät

- Updates und Patches – was kann ich mindestens tun?
- Primärschutz: Virenschutz, Firewall & Co

Meine Arbeit

- Phishing – Absender, Anlagen, Absichten
- Human Firewall
- (k)eine eigene Hardware & Software
- HomeOffice und Unterwegs

Erste Hilfe - Wichtigste Maßnahmen

- Browser (an/abmelden, Passworte & Co)
- Software-Nutzung
- Speichermedien – (wo, was und wie lange)
- Kollaboration – MS Teams mit OneNote und Dateien / SharePoint
- Kommunikation – E-Mail, intern / extern
- Datensparsamkeit und Transparenz

Sicheres Verhalten am Arbeitsplatz - digitale Selbstverteidigung

- Cyberabwehr: Die goldenen Regeln der Informationssicherheit

Dozent

Kerstin Armbrust

Digital Working Coach, Informationssicherheitsbeauftragte (zertifiziert nach ISO 27001), IT-Grundschutz-Praktiker, Datenschutz-Auditorin

Lernziele

Die Teilnehmenden lernen

- Sicherheitsbedrohungen zu erkennen und einzuschätzen,
- Gefährdungspotentiale im täglichen Arbeiten zu identifizieren und
- Schutzmaßnahmen zu treffen / zu agieren, statt zu reagieren.

Veranstalter

VWA Karlsruhe