Fortbildungskampagne
öffentliches Recht.

INTENSIV-PRAXISSEMINAR

02.04.2025
online

jetzt anmelden

Cyberangriffe verstehen und abwehren

Angriffsmethoden und -Instrumente | Belastbarkeit ermitteln | Richtlinien und Standards der Informationssicherheit

Heiko Behrendt

ISO 27001 Auditor
Datenschutz- und IT-Sicherheitsexperte
einer Landes-Prüfbehörde

In einer zunehmend digitalisierten Welt stehen Behörden, Kommunen und öffentliche Einrichtungen vor einer stetig wachsenden Bedrohung: Cyberangriffe nehmen nicht nur an Häufigkeit, sondern auch an Komplexität zu. Ob Phishing-Mails, Ransomware oder gezielte DDoS-Attacken – die Methoden der Angreifer werden immer raffinierter. Solche Angriffe können nicht nur vertrauliche Daten kompromittieren, sondern auch den gesamten Betrieb lahmlegen und erhebliche finanzielle wie reputative Schäden verursachen. Besonders betroffen sind Organisationen, die Schwachstellen in ihrer IT-Infrastruktur oder keine klar definierte Informationssicherheitsstrategie haben.

Dieses Seminar vermittelt Ihnen ein tiefgreifendes Verständnis für die Mechanismen und Auswirkungen von Cyberangriffen. Sie erfahren, welche Angriffstechniken aktuell besonders häufig eingesetzt werden und wie Sie den Status Quo der IT-Sicherheit in Ihrer Organisation ermitteln können. Durch praxisnahe Ansätze und verständlich aufbereitete Methodiken lernen Sie, wie Schwachstellen erkannt und gezielt behoben werden können – sowohl auf technischer als auch auf organisatorischer Ebene.

Ein besonderer Schwerpunkt liegt auf der Anwendung anerkannter Standards der Informationssicherheit. Ob IT-Grundschutz, ISO 27001 oder VdS 10000: Sie erfahren, wie Sie die passende Grundlage für Ihre Organisation auswählen und diese pragmatisch umsetzen können. Mit Hilfe von praxisnahen Hilfsmitteln wie Checklisten und einem kostenfreien Tool für die Dokumentation der Sicherheitsmaßnahmen erhalten Sie konkrete Werkzeuge, um die Abwehr von Cyberbedrohungen nachhaltig zu stärken.

Schützen Sie Ihre Organisation vor den Risiken des digitalen Zeitalters und machen Sie sich fit für die Herausforderungen der Cybersicherheit – damit Ihre „Kronjuwelen“ auch in Zukunft sicher bleiben.

Inhaltsübersicht

- Cyberangriffe I + II
- Ziele und Auswirkungen
- Angriffsmethoden und Angriffsinstrumente
- Phishing, Viren und Ransomware, Künstliche Intelligenz (KI),
- Brute-Force-Angriffe, Distributed-Denial-of-Service (DDoS) Attack, Man-in-the-Middle, SQL-Injection
- Wie belastbar ist die Informationssicherheit meiner Organisation?
- Habe ich Schwachstellen und bin angreifbar?
- Status Quo ermitteln
- Methodik und Durchführung eines Sicherheitschecks
- Technische und organisatorische Datenverarbeitung auf Schwachstellen analysieren
- Das Sicherheitsniveau mit elementaren Sicherheitsmaßnahmen schnell und einfach erhöhen
- Anerkannte Standards zur Informationssicherheit anwenden!
- Orientierung an anerkannten Richtlinien und Standards der Informationssicherheit
- Welcher Standard passt zu meiner Organisation?
- VdS 10000, CISIS12, IT-Grundschutz oder ISO 27001
- Gegenüberstellung der Standards
- Sicherheitsmaßnahmen mit einem (kostenlosen) Tool (Verinice) verwalten und den Umsetzungsstand dokumentieren
- Weg in die Basisabsicherung (WiBA) des IT-Grundschutzstandards mit Hilfe von Checklisten (toolbasierend)
- Tool-Datenbank (Verinice) mit allen Sicherheitsmaßnahmen zur Cyberabwehr zum Mitnehmen und Anwenden

08:45 **Login**

09:00 **Begrüßung und Vorstellungsrunde**

- Vorstellung des Referenten und der Teilnehmenden

09:15 **Cyberangriffe I**

- Ziele und Auswirkungen
- Angriffsmethoden und Angriffsinstrumente

10:15 **Kaffeepause**

10:45 **Cyberangriffe II**

- Phishing, Viren und Ransomware, Künstliche Intelligenz (KI),
- Brute-Force-Angriffe, Distributed-Denial-of-Service (DDoS) Attack, Man-in-the-Middle, SQL-Injection

12:30 **Mittagspause**

13:30 **Wie belastbar ist die Informationssicherheit meiner Organisation?**

- Habe ich Schwachstellen und bin angreifbar? Status Quo ermitteln
- Methodik und Durchführung eines Sicherheitschecks
- Technische und organisatorische Datenverarbeitung auf Schwachstellen analysieren
- Das Sicherheitsniveau mit elementaren Sicherheitsmaßnahmen schnell und einfach erhöhen

15:15 **Kaffeepause**

15:45 **Anerkannte Standards zur Informationssicherheit anwenden**

- Orientierung an anerkannten Richtlinien und Standards der Informationssicherheit
- Welcher Standard passt zu meiner Organisation?
- VdS 10000, CISIS12, IT-Grundschutz oder ISO 27001
- Gegenüberstellung der Standards
- Sicherheitsmaßnahmen mit einem (kostenlosen) Tool (Verinice) verwalten und den Umsetzungsstand dokumentieren
- Weg in die Basisabsicherung (WiBA) des IT-Grundschutzstandards mit Hilfe von Checklisten (toolbasierend)
- Tool-Datenbank (Verinice) mit allen Sicherheitsmaßnahmen zur Cyberabwehr zum Mitnehmen und Anwenden

16:45 **Ende des Seminars**

Fortbildungskampagne
öffentliches Recht.

Heiko Behrendt

Als zertifizierter ISO 27001 Auditor für Informationssicherheit begleitet Heiko Behrendt Behörden und Firmen bei der Einführung und Sicherstellung von IT-Grundschutz- und Datenschutzstandards. Darüber hinaus führt er in seiner Funktion als Datenschutz- und IT-Sicherheitsexperte einer Aufsichtsbehörde Datenschutz-Audits sowie datenschutzrechtliche und sicherheitstechnische Kontrollen der Einhaltung der Datenschutzgrundverordnung durch.

Zielgruppe – An wen richtet sich dieses Seminar?

Dieses Seminar richtet sich an IT-Verantwortliche, Datenschutz- und Informationssicherheitsbeauftragte sowie Fachabteilungsleiterinnen und -leiter in öffentlichen Einrichtungen, die aktiv an der Sicherung ihrer Organisation gegen Cyberbedrohungen arbeiten möchten. Auch Mitarbeitende aus anderen Bereichen, die ein grundlegendes Verständnis für die Funktionsweise von Cyberangriffen und geeignete Schutzmaßnahmen gewinnen möchten, sind angesprochen. Egal, ob Sie bereits Vorkenntnisse mitbringen oder sich erstmals mit dem Thema befassen – dieses Seminar bietet wertvolle Einblicke und praxisnahe Ansätze für alle, die die Informationssicherheit in ihrer Organisation stärken wollen.

Fortbildungskampagne
öffentliches Recht.

jetzt anmelden

Termin:

02.04.2025

online

TEILNAHMEGEBÜHR:

Online-Teilnahme: 427,- Euro zzgl. MwSt.

DIE TEILNAHMEGEBÜHR BEINHALTET:

- Schulungsunterlagen (digital)
- Teilnahmezertifikat

ANMELDUNG:

Bitte verwenden Sie zur Anmeldung unser Online-Anmeldeformular unter: www.fortbildungskampagne.de/anmeldung

KONTAKT FÜR RESERVIERUNGEN UND BUCHUNGEN:

Haben Sie Fragen zum Seminar oder zu Reservierungen und Buchungen?
Schreiben Sie uns einfach eine Email oder rufen Sie uns unter der folgenden Rufnummer an:
Email: team@fortbildungskampagne.de | Telefon: +49 (0) 30 89 56 27 16

TEILNAHME- UND STORNIERUNGSKONDITION (AUSZUG):

Die verbindliche Anmeldung erfolgt über unser Online-Anmeldeformular und wird durch Zusendung einer Anmeldebestätigung sowie der Rechnung bestätigt. Stornierungen sind bis vier Wochen vor Veranstaltungsbeginn kostenfrei, bereits gezahlte Beträge werden erstattet. Bei kurzfristiger Stornierung oder beispielsweise krankheitsbedingter Abwesenheit ist die Benennung eines Ersatzteilnehmers jederzeit möglich. Sofern sich kein Ersatzteilnehmer findet, kann nach Absprache ein Gutschein ausgestellt werden, der zur Teilnahme an einem Nachfolgetermin oder einem ähnlichen Seminar berechtigt. Bitte beachten Sie unsere AGB, die unter dem folgenden Link aufgerufen werden können: www.fortbildungskampagne.de/agb

DATENSCHUTZHINWEISE:

Wir weisen darauf hin, dass Sie die Verwendung Ihrer Daten gemäß unserer Datenschutzbestimmungen durch eine Nachricht an datenschutz@fortbildungskampagne.de selbstverständlich jederzeit widerrufen können. Bitte beachten Sie unsere Datenschutzbestimmungen, die unter dem folgenden Link aufgerufen werden können: www.fortbildungskampagne.de/privacy

HINWEISE ZUM DATENSCHUTZ BEI ONLINE-TEILNAHME:

Details zur technischen Umsetzung der Online-Teilnahme erhalten Sie im Anschluss an Ihre Anmeldung. Ein wirksamer Auftragsverarbeitungsvertrag mit dem technischen Dienstleister liegt vor. Durch die Fortbildungskampagne als Veranstalter erfolgt während der Online-Teilnahme keine Speicherung von schriftlichen, akustischen oder visuellen Daten der Teilnehmenden. Eine temporäre Protokollierung des Chat-Verlaufes einer Online-Veranstaltung wird binnen zwei Arbeitstagen nach der Veranstaltung gelöscht. Bitte beachten Sie, dass Sie im Rahmen Ihrer Online-Teilnahme möglicherweise unfreiwillig Daten und Informationen übertragen, etwa durch weitere Personen in Ihrem Raum. Eine mögliche Übertragung derartiger Informationen liegt in Ihrem Verantwortungsbereich.