

Cyber Experience Center

Erleben Sie Cybersicherheit neu – realistisch, interaktiv und praxisnah

Raum der Theorie verlassen - in echte Szenarien eintauchen

Moderne Bedrohungen erfordern moderne Antworten. In unserem Cyber Experience Center verlassen Sie den Raum der Theorie und tauchen mit uns in echte Szenarien ein. Denn Cybersicherheit muss man nicht nur verstehen, sondern fühlen. Dafür braucht es Erfahrung, Klarheit und entschlossene Reaktionen.

Wir machen die Sicherheit für Sie erlebbar!

Echtes **Verstehen**, aktives **Erleben**, gemeinsame **Diskussionen**

Unsere Kurse bieten **Erlebnis statt Vortrag** und bauen auf Reflektion, Anwenden von Erkenntnissen, kritisches Mitdenken und den Austausch. Erleben Sie auf Wunsch mehrere realistische Szenarien oder kombinieren Sie Ihr Training mit einem Blick hinter die Kulissen unseres **Security Operation Centers (SOC)**. Dort gewinnen Sie **live Einblicke** in den **Arbeitsalltag unserer Cyber Security-Spezialisten**.

Was unsere Kurse ausmacht:

- ✓ **Awareness, die wirkt**
interaktive Trainings und Simulationen – praxisnah und verständlich – um die Nutzer wachzurütteln und zu stärken.
- ✓ **Hands-on statt Hands-up**
Realistische Angriffe, Awareness-Trainings, Echtzeit-Reaktionen und Entscheidungsdruck wie im Ernstfall.
- ✓ **Blick hinter die Firewalls**
Live in unserem Security Operation Center (SOC) – so real, dass Sie den Puls spüren können
- ✓ **Resilienz trainieren**
Aus Datenwissen wird digitale Resilienz mit Notfallübungen und Incident-Response-Szenarien durch unsere Expert:innen
- ✓ **Interaktive Formate**
Cybersicherheit im direkten Handeln erleben – realistisch, aktiv und nachhaltig mit praktischen Übungen und diskussionsbasierten Simulationen

Kursangebot – Verstehen. Erleben. Handeln.

Ob Awareness, Strategie oder technische Tiefe – unser Cyber Experience Center ist Ihr Trainingsfeld. Wir begleiten Sie vom Aha-Moment bis zur Umsetzung. Unser Kursangebot umfasst sowohl Basis- als auch Intensivkurse. Alle Kurse finden im Cyber Experience Center der GISA in Halle (Saale) statt.

Verschaffen Sie sich einen Überblick und melden Sie sich an!

Mehr Informationen unter www.gisa.de/cec

GISA GmbH

Leipziger Chaussee 191 a
06112 Halle (Saale)

T +49 800 7000585

E kontakt@gisa.de

www.gisa.de

GISA[®]
That's IT.

Basiskurse im Überblick

Kurs 1: Phishing live erleben – Interaktive Awareness-Session

Phishing ist der häufigste **Einstiegspunkt für Cyberangriffe**. Erfolgreiche Angriffe starten oft mit nur einem Klick. Mit unserem Kurs werden **Mitarbeitende in die Perspektive von Angreifern und Betroffenen versetzt**. Er zeigt, wie wichtig Aufmerksamkeit, gesunde Skepsis und klare Prozesse im Umgang mit verdächtigen Nachrichten sind. **Damit schärfen Sie das Bewusstsein, stärken die Reaktionsfähigkeit und schaffen konkrete Handlungssicherheit**. Das erwartet Sie:

- Einstieg über ein **realistisches Phishing-Szenario**
- **Analyse echter Mails** und **Webseiten**
- **Erkennen typischer Merkmale**: Absender, Sprache, Timing, Dringlichkeit
- **Interaktiver Test**: Wer klickt? Wer meldet? Wer bleibt skeptisch?
- **Gemeinsame Reflexion**: Wie hätten wir reagiert? Was hilft uns im Alltag?

Auf Wunsch: anonymisierte Auswertung der Live-Testreaktionen und Empfehlungen zur Optimierung der internen Sicherheitskultur.

Der Kurs richtet sich an:
alle Mitarbeitenden einer Institution/eines Unternehmens

Kursdauer
90 Minuten

Preis
250 EUR zzgl. MwSt.
pro Teilnehmenden

Kurs 2: Threat Briefing – Aktuelle Cyberbedrohungen & Trends

Ein **fundiertes Lageverständnis** ist der Schlüssel zur Priorisierung und Vorbereitung. In Zeiten wachsender Vernetzung und immer kürzerer Reaktionszeiten müssen Management und IT-Verantwortliche auf derselben Wissensbasis arbeiten. Dieser Kurs **schafft Klarheit in der Lageeinschätzung, Verständnis für Risiken und die Grundlage für strategische Entscheidungen**.

Unsere Expert:innen bringen Sie auf den neuesten Stand zu aktuell relevanten Bedrohungen sowie neuen Angriffswegen der Cyberkriminellen und zeigen Handlungsoptionen auf. Das erwartet Sie:

- **Die Top 5 Bedrohungen**: Von Deepfakes bis Ransomware-as-a-Service
- **Supply Chain Attacks**: Wie Drittanbieter zur Schwachstelle werden
- **Live-Demo**: So sieht ein Deepfake-Angriff im Kontext CEO Fraud aus
- Diskussion **aktueller Fallstudien** und **konkreter Schutzmaßnahmen**

Jede Session wird tagesaktuell angepasst – auf Wunsch auch branchenspezifisch.

Der Kurs richtet sich insbesondere an:

- Mitarbeitende aus der IT
- Management
- Risiko- und Sicherheitsbeauftragte

Kursdauer
90 Minuten

Preis
220 EUR zzgl. MwSt.
pro Teilnehmenden

Kurs 3: CEO Fraud & Fake President – Taktiken, Schutz und Sofortmaßnahmen

Diese **Angriffsmethoden** setzen nicht auf Technik, sondern auf Vertrauen und Zeitdruck. Die Täter nutzen gezielt menschliche Schwächen und unklare Prozesse. Wer diese Mechanismen versteht, kann Angriffe frühzeitig enttarnen – und mit klarem Kopf richtig reagieren. Werden Sie zu souveränen Entscheidern, indem sie **Täuschungsversuche erkennen, Sicherheit in Entscheidungen stärken** und **Schutzmechanismen etablieren**.

Wir sensibilisieren gezielt die Personen, die besonders im Fokus von Täuschungsversuchen stehen. Das erwartet Sie:

- **Analyse echter Betrugsversuche** – inklusive Originalkommunikation
- **Psychologische Tricks**: Vertrauen, Druck, Isolation
- **Kommunikationsregeln & technische Schutzmaßnahmen**
- **Notfallplan**: Was tun, wenn es passiert ist?
- **Optional**: Integration unternehmensspezifischer Prozesse und Kommunikationswege in das Training

Der Kurs richtet sich insbesondere an:

- Geschäftsleitung
- Assistenz
- Finance-Mitarbeitende

Kursdauer
2 Stunden

Preis
270 EUR zzgl. MwSt.
pro Teilnehmenden

Kurs 4: Cyber Security Basics für Nicht-Techniker

Dieser Kurs schafft das nötige Grundverständnis, um Sicherheit nicht als Bürde, sondern als Teil des **beruflichen Selbstverständnisses eines jeden Mitarbeitenden** zu sehen. Wer versteht, warum etwas sicher oder unsicher ist, wird automatisch achtsamer und verantwortungsbewusster im digitalen Raum. Im lebendigen, alltagsnahen und interaktiven Kurs **bauen wir ein Grundverständnis auf, bauen Berührungspunkte ab und fördern so die Sicherheitskultur**. Das erwartet Sie:

- Verständlicher Einstieg in die Welt der Cybersicherheit inklusive **Erklärung zentraler Begriffe anhand alltagsnaher Beispiele mit Quizfragen und Gruppenübungen**
 - Was ist ein **Cyberangriff**? Wie entstehen **Sicherheitslücken**?
 - **Grundbegriffe**: Von Firewalls bis Social Engineering
 - **Gefahrenquellen** im Alltag: E-Mails, Geräte, Passwörter
 - Wie erkenne ich ein verdächtiges Verhalten oder System?
- Tipps für mehr **Sicherheit im eigenen Arbeitsumfeld**

Extras: Mini-Glossar zum Mitnehmen + Quiz-Auswertung zur Selbsteinschätzung

Der Kurs richtet sich insbesondere an:

- Fachabteilungen
- Assistenzen
- Projektleitungen
- HR-Abteilungen

Kursdauer
90 Minuten

Preis
200 EUR zzgl. MwSt.
pro Teilnehmenden

Kurs 5: Identitäten, Passwörter & MFA – So schützen Sie sich wirklich

Identitätsmissbrauch zählt zu den häufigsten und gleichzeitig folgenreichsten Cyberangriffen. **Dieses Training vermittelt nicht nur Wissen, sondern macht Sicherheit zur Gewohnheit.** Denn wer seine digitalen Schlüssel versteht und schützt, kann die Tür für Angreifer dauerhaft schließen. Mit dem Kurs erzielen Sie **sofort anwendbare Sicherheit im Berufs- und Privatleben und schaffen nachhaltige Awareness.**

Wir zeigen, anhand von Praxisbeispielen, wie Identitätsdiebstahl funktioniert und Sie sich effektiv schützen. Das erwartet Sie:

- Wie funktionieren **Passwortdiebstahl & Credential Stuffing?**
- Was bringt **Mehrfaktor-Authentifizierung** und wo sind Grenzen?
- Tipps für **starke Passwörter** und **sichere Logins** (auch privat)
- Tools & Tricks für **Passwort-Management**
- **Checkliste & persönlichen Security-Tipps** zum Mitnehmen

Der Kurs richtet sich an Mitarbeitende aus allen Bereichen.

Kursdauer
90 Minuten

Preis
220 EUR zzgl. MwSt
pro Teilnehmenden

Intensivkurse im Überblick

Kurs 1: Crisis Simulation—Der Ernstfall live

Krisenmanagement ist keine Theorie. Nur wenn Entscheidungsträger:innen und Krisenteams unter realitätsnahen Bedingungen üben, entstehen Routinen, Vertrauen und Handlungssicherheit.

Diese Simulation ist der Härtestest für jede Organisation – im geschützten Raum, aber mit realem Puls. Die Teilnehmenden erleben eine **realitätsnahe Krisensimulation**, bei der nichts vorhersehbar ist. Die Ereignisse entwickeln sich dynamisch, Entscheidungen müssen ad hoc getroffen, kommuniziert und dokumentiert werden. Das erwartet Sie:

- **Realistische Live-Simulation eines großflächigen Cyberangriffs** – inklusive Eskalationsstufen, Medienreaktionen, Stakeholder-Kommunikation und forensischer Indizien.
- **Echtzeitentscheidungen im interdisziplinären Team:** Wann wird kommuniziert, wann eskaliert, wann extern involviert?
- **Reflexion zu kritischen Erfolgsfaktoren:** Informationsfluss, Führungsverhalten, technische Reaktionsfähigkeit, interne Kommunikation
- **Auswertung** inkl. konkreter Optimierungspotenziale

Der Kurs richtet sich insbesondere an:

- Geschäftsleitung
- IT-Leitung
- Krisenstäbe
- Kommunikationsverantwortliche

Kursdauer
4 Stunden

Preis
590 EUR zzgl. MwSt.
pro Teilnehmenden

Kurs 2: Incident Response Bootcamp – Hands-on unter Hochdruck

Im Ernstfall zählt jede Sekunde und jeder Klick muss sitzen. Das Bootcamp schult technisches Können, systematisches Vorgehen, Prioritätensetzung und Zusammenarbeit unter Druck. Mit der forensischen Praxis in Live-Umgebungen **professionalisieren Sie Ihre technische Reaktionsfähigkeit, verstehen Bedrohungen und verankern strukturierte Incident Response**. Angriffe werden durchgespielt, jeder Schritt nachvollzogen. Das erwartet Sie:

- **Technischer Deep-Dive in reale Angriffsverläufe** – mit Fokus auf Analyse und Reaktion sowie Forensik
- **Arbeiten mit echten Fallbeispielen:** Loganalyse, Endpoint-Isolation, Speicheranalysen, Netzwerk-Traffic-Untersuchungen
- **Schulung in Tools** wie Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), Netzwerk- und Prozessmonitoring
- **Realitätsnahe Use-Cases:** Vom initialen Zugriff über Privilege Escalation bis Persistenz u. Exfiltration von Daten zum Angreifer
- **Intensives Coaching** durch erfahrene Incident-Responder

Der Kurs richtet sich insbesondere an:

- IT-Security-Teams
- SOC-Analysten
- Blue-Teams

Kursdauer

1 Tag (8 Stunden)

Preis

720 EUR zzgl. MwSt.
pro Teilnehmenden

Kurs 3: Awareness & Social Engineering Training – der Mensch im Visier

Technik schützt, Menschen entscheiden. Erfolgreiche Angriffe erfolgen häufig über **Social Engineering** als Einstiegspunkt. Dieses **Training macht Mitarbeitende zu souveränen Sicherheitsfaktoren – nicht zu Angriffsflächen**. Im Kurs werden **reale Angriffssituationen** simuliert: Deepfake-Videos, manipulierte Telefonanrufe, überzeugende Phishing-Nachrichten. Die Teilnehmenden lernen in Echtzeit, wie sich menschliche Schwächen gezielt ausnutzen lassen und wie man ihnen begegnet. Das erwartet Sie:

- **Realistische Simulationen** und Beispiele für Phishing, Pretexting, Fake Calls und Deepfakes
- **Aufklärung über die psychologischen Prinzipien hinter Social Engineering:** Vertrauen, Druck, Neugier, Autorität
- **Übungen zur Erkennung von Täuschungsversuchen** am Telefon, per E-Mail oder in persönlichen Gesprächen
- **Checklisten und Tools** zur sicheren Verifizierung und internen Weitergabe verdächtiger Vorgänge
- **Gruppendynamische Elemente** zur Stärkung der kollektiven Awareness und Risikowahrnehmung

Der Kurs richtet sich insbesondere an:

- Mitarbeitende Human Resources
- Mitarbeitende Vertrieb
- Führungskräfte
- Assistenzen

Kursdauer

4 Stunden

Preis

390 EUR zzgl. MwSt.
pro Teilnehmenden

Kurs 4: Regulatorische Resilienz & DSGVO in der Krise

Juristische Klarheit ist besonders unter Zeitdruck eine Notwendigkeit. Dieses Training bereitet Teams darauf vor, **regulatorisch sicher, rechtlich nachvollziehbar und datenschutzkonform** zu agieren, wenn es wirklich darauf ankommt. Anhand eines **simulierten Datenschutzvorfalls** erleben die Teilnehmenden, welche Fragen, Erwartungen und rechtlichen Anforderungen im Krisenfall auf sie zukommen. Juristische Deadlines, Dokumentationspflichten, Meldelogik werden live durchgespielt. Das erwartet Sie:

- Praxistaugliches Wissen über **regulatorischen Anforderungen im Cybervorfall** – speziell für BDSG, KRITIS, DSGVO & Co.
- **Überblick über typische Fehler:** Meldeverzug, Kommunikationsspannen, fehlende Dokumentation
- **Rechtssichere Kommunikation** mit Behörden, Betroffenen und Öffentlichkeit
- **Vorbereitung auf Audits** und **forensische Anforderungen** – inkl. Datenintegrität und Beweissicherung
- **Klare Definitionen:** Was ist eine meldepflichtige Datenschutzverletzung? Wer muss wann informiert werden?
- **Einbindung des Datenschutzes** in Krisenreaktion und Business Continuity Planning

Der Kurs richtet sich insbesondere an Mitarbeitende:

- Bereich Legal
- Bereich Compliance
- Bereich Datenschutz
- Audit-Verantwortliche

Kursdauer

4 Stunden

Preis

450 EUR zzgl. MwSt.
pro Teilnehmenden

Kurs 5: Cyberstrategie & Resilienz-Check für Führungskräfte

Der Kurs befähigt Entscheider:innen, das Thema Cybersicherheit **strategisch, strukturiert und zielgerichtet zu steuern** um Risiken zu erkennen und Resilienz nachhaltig zu verankern. In moderierten **Simulationen** erleben Sie strategische Entscheidungsprozesse unter Unsicherheit, bewerten konkrete Lagebilder, analysieren Schwachstellen u. priorisieren Maßnahmen. Das erwartet Sie:

- **Fundiertes Lagebild** zu aktuellen **Bedrohungsszenarien** und **Trends**
- Einführung in **Modelle zur Bewertung der Cyber-Resilienz:** u.a. Maturity Level, Schutzbedarfsanalysen, Business-Impact
- **Analyse bestehender Strategien:** Sind Governance, Prozesse, Reportinglinien und Budgets stimmig?
- **Benchmarking** gegenüber Best Practices der Branche – auch im internationalen Kontext
- **Praxisnahe Tools** zur Ableitung strategischer Maßnahmen
- **Diskussion realistischer Planszenarien** – inklusive Entscheidungssimulationen und Lessons Learned

Der Kurs richtet sich insbesondere an:

- Geschäftsleitung
- IT-Verantwortliche mit strategischer Verantwortung

Kursdauer

4 Stunden

Preis

520 EUR zzgl. MwSt.
pro Teilnehmenden

Kurs 6: Informationssicherheit—Verantwortung liegt bei allen

Informationssicherheit geht Alle an! Im Kurs erleben die Teilnehmenden interaktiv, wie Informationssicherheit im Alltag konkret aussieht und wie leicht sie durch Unachtsamkeit gefährdet werden kann. Anhand praxisnaher Beispiele und kleiner Simulationen werden die Teilnehmenden für **Informationssicherheit sensibilisiert, sicherheitsbewusstes Verhalten gefördert und die individuelle Verantwortung gestärkt**. Das erwartet Sie:

- **Fundiertes Verständnis für Informationssicherheit**
- Konkrete Einblicke in **typische Bedrohungen wie Phishing, Social Engineering, schwache Passwörter, unsichere Datenübertragungen**
- **Alltagstaugliche Verhaltensregeln** für den sicheren Umgang mit E-Mails, Passwörtern, mobilen Geräten und sensiblen Informationen
- **Interaktive Übungen und Fallbeispiele**, die zeigen, wie leicht Fehler passieren und wie man sie vermeidet
- **Antworten auf häufige Fragen**, wie: Was tun bei einem Verdacht? Wer ist Ansprechpartner? Welche Verantwortung trage ich als Mitarbeitender?

Der Kurs richtet sich an alle Mitarbeitenden (Enduser).

Kursdauer

3 Stunden

Preis

320 EUR zzgl. MwSt.
pro Teilnehmenden

Kurs 7: Verantwortung gemäß NIS-2 und §38 BSIG

Die Verantwortung für Informationssicherheit beginnt bei der Geschäftsleitung! Der Kurs vermittelt ein fundiertes Verständnis der gesetzlichen Anforderungen aus **§38 BSIG und NIS-2-Richtlinie**. Er schafft **Klarheit über die Pflichten, Sicherheit im Umgang mit Risiken und Handlungsstärke für Ihre Organisation**. Das erwartet Sie:

- **Risiken frühzeitig erkennen und bewerten:** anhand realistischer Szenarien wie Ransomware, CEO-Fraud, Supply-Chain-Attacken oder Missbrauch von Cloud-Diensten, (optional OT/ICS-Angriffe)
- **Dokumentation und Nachweisführung** über die Wahrnehmung der Verantwortung: Best Practices aus der ISO 27001 und praxisnahe Tipps zur Audit-Readiness und aktiven Minimierung von Haftungsrisiken
- **Aufklärung zu Pflichten der Geschäftsleitung:** von der Umsetzung und Überwachung von Risikomanagementmaßnahmen bis zur regelmäßigen Schulungspflicht.

Der Kurs richtet sich insbesondere an:

- Geschäftsleitung besonders wichtiger und wichtiger Einrichtungen gemäß BSIG (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik) und NIS-2-Umsetzungsgesetz

Kursdauer

2 Stunden

Preis

550 EUR zzgl. MwSt.
pro Teilnehmenden