Sicherheit

Security & Forensik
Datensicherheit
Windows & Linux Security
ISO27001

Bildungswege

Seminare & Workshops

Zertifizierungen

EGOS! Entwicklungsgesellschaft für Organisation und Schulung

A-6020 Innsbruck
Eduard Bodem Gasse 1/III
+43 (0)512/364777
+43 (0)512/364779-24
training@egos.co.at

A-5020 Salzburg
Schumacherstraße 14
+43 (0)662/450174
+43 (0)662/450174-24
training@egos.co.at

Stand 08.04.2021

Inhaltsverzeichnis

Inhaltsverzeichnis 2
Seminare und Workshops 4
Datenschutz 5
Betrieblicher Datenschutzbeauftragter 5
DSGVO Update-Workshop 6
Grundlagen 7
Datenschutz in der Cloud 8
Workshop für IT-Pro's 8
HTTP and SSL Communications 9
Mastering { http(s)://deep.dive } 9
Informationssicherheit 10
E-Learning, Clean Desk (Modul 22) 10
E-Learning, Cloud Services (Modul 10) 11
E-Learning, Datenschutz (Modul 18) 12
E-Learning, Dokumentklassifizierung (Modul 19) 13
E-Learning, Grundlagen (Modul 01) 14
E-Learning, Hilfe ich bin gehackt! (Modul 09) 15
E-Learning, Insiderangriff (Modul 12) 16
E-Learning, Kennwort-Sicherheit (Modul 03) 17
E-Learning, Mail & Phishing (Modul 04) 18
E-Learning, Mobile Device Security (Modul 05) 19
E-Learning, Multifunktionsgeräte (Modul 20) 20
E-Learning, Physische Sicherheit (Modul 14) 21
E-Learning, Portable Speichermedien (Modul 21) 22
E-Learning, Remote Arbeitsplätze (Modul 16) 23
E-Learning, Richtiger Umgang mit Daten (Modul 06) 24
E-Learning, Sicherheit auf Reisen (Modul 13) 25
E-Learning, Sicherheit Ihrer Geräte (Modul 15) 26
E-Learning, Sicherheit im Web (Modul 02) 27
E-Learning, Sicherheit im WLAN (Modul 17) 28
E-Learning, Social Engineering (Modul 07) 29
E-Learning, Social Networks (Modul 08) 30
E-Learning, Verschlüsselung (Modul 11) 31
Grundlagen für AnwenderInnen 32
Grundlagen für Führungskräfte 33
Kostentransparenz bei Vorfällen 34
Security Awareness - un:plugged 35
Verlust von Daten behandeln 36
Internet Protocol v6 (IPv6) 37
Architecture and Implementation 37
IT Forensik 38
Rechtliche Grundlagen 38
Tools Workshop 39
IT Security 40
Auditing and Penetration Testing 40
Fundamentals 41
Hacking für System-Administratoren I 42
Hacking für System-Administratoren II 43
Microsoft 365 44
Security Administrator 44
Microsoft Azure 45
Security Technologies 45
Microsoft Intune 46
Modern Device Management mit EndPoint Manager 46
Trend Micro Office Scan, Scan Mail Exchange 47
Workshop 47
Windows 10 48
Client Security Deep Dive 48
Windows Server 49
PKI Design, Implementation and Maintainance 49
Securing 50

Seminare und Workshops

>> Datenschutz

Betrieblicher Datenschutzbeauftragter

Nach dem neuen EU Rechtsrahmen (EU-DSGVO) ist ab 2018 für Datenschutz für bestimmte Organisationen und Unternehmen ein Datenschutzbeauftragter notwendig.

Ihr Nutzen

Nach diesem Seminar kennen Sie die Anforderungen an den Datenschutz in Organisationen und Unternehmen, bezogen auf die neue EU-DSGVO. Sie können die Rolle eines Datenschutzbeauftragten übernehmen und die relevanten Aufgaben sinnvoll steuern. Sie erlernen datenschutzrechtliche Regelungen zu vermitteln und in auf Sie zukommenden Situationen richtig zu handeln.

Preis pro Teilnehmer

EUR 2100,- exklusive der gesetzlichen MwSt.

Seminardauer

3 Tag(e)/Day(s)

Voraussetzungen

Keine

Hinweise

Das Seminar bereitet Sie auf die Zertifizierung der staatlich vom BMWFW anerkannten Organisation CIS-Certification & Information Security Services vor. Die Prüfung kann zum Preis von EUR 345,- exkl. Ust. in Innsbruck oder Wien abgelegt werden.

Version: 1.0

Seminarinhalte

1. Tag
* Grundlagen des Datenschutzgesetzes
- Grundlagen Datenschutzrecht
- Das DSG2000 im Überblick
- Das künftige Datenschutzgesetz

* Rechtmäßigkeit der Datenverarbeitung
- Formeller und materieller Datenschutz
- Ablauf einer Prüfung

* Datentransfers und Cloud-Computing
- EU/US Privacy Shield

* Outsourcing und dessen Auswirkung auf Datenrechtliches
* Haftung, Risiken und Strafen
* Rechte der Betroffenen

* Die Rolle des Datenschutzbeauftragten
- Die Aufgaben des Datenschutzbeauftragten
- Die Stellung im Unternehmen
- Ausübungsformen
- Aufbau einer Datenschutz-Organisation
- Der Datenschutzbeauftragte - ein Tausendsassa?

2. Tag
* Anforderungen an Technik und Organisation
- Management, Organisation und Technik integrieren
- Informations-Sicherheits-Management als Datenschutzaufgabe
- Grundlagen ISO27001 Informationssicherheit

* Kritische Erfolgsfaktoren
* Folgenabschätzung

* Themen aus der Praxis
- E-Mail und Internet am Arbeitsplatz
- Mitarbeiterüberwachung und deren Regelung
- Datengeheimnis und Videoüberwachung
- Data Breach Notification Duty

3. Tag
* Technisch-Organisatorische Maßnahmen
- Welche Maßnahmen sind zuerst zu treffen?
- Nachhaltigkeit bei Mitarbeitern und Vorgesetzen
- Gedanken zu Schulung und Awareness
- Entwicklung eines Datenschutz-Prozesses

* Wo fangen Sie an?
- Konzepte für Datenschutzprojekte
- Aufbau einer internen Datenschutz-Organisation
- Ablauf einer rechtlichen Prüfung in der Praxis
- Verfahrensverzeichnisse
- Standard-Vertragsklauseln
- Dienstleisterverträge
- Zustimmungserklärungen

>> Datenschutz
DSGVO Update-Workshop

Nach dem neuen EU Rechtsrahmen (EU-DSGVO) ist ab 2018 für Datenschutz für bestimmte Organisationen und Unternehmen ein Datenschutzbeauftragter notwendig.

Ihr Nutzen

Ein Jahr nach Einführung der DSGVO. Was haben wir gelernt? Was hat sich entwickelt? - ein aktuelles Update für Sie. Sie erlangen in diesem Workshop Best Practices zur Optimierung der praktischen Umsetzung Ihrer Aufgaben als Datenschutzbeauftragte/r.

Voraussetzungen

Seminar Betrieblicher Datenschutzbeauftragter~9100

oder dem entsprechende Kenntnisse

Preis pro Teilnehmer

EUR 950,- exklusive der gesetzlichen MwSt.

Hinweise

-

Seminardauer

1 Tag(e)/Day(s)

Version: 1.0

Seminarinhalte

* Wiederholung
- Die Eckpunkte der DSGVO

* Wichtige Entscheidungen der Behörde seit Mai 2018
- Muss ich Daten auf Anforderung immer löschen?
- Wie lange darf ich Daten aufbewahren?
- Einsatz von Videokameras
- Welche Informationen muss ich offenlegen?
- u.v.a.m.

*Aufgaben und Pflichten des Datenschutzbeauftragten
- Zuständigkeiten und Verantwortungsbereiche

*Verantwortlicher oder Auftragsverarbeiter
- Was muss ich beachten?
- Wann liegt was vor?
- Konsequenzen

* Umgang mit Datenpannen?
- Wie verhalte ich mich, wenn etwas passiert?
- Notwendige (technisch organisatorische) Maßnahmen
- Praxisfälle aus dem täglichen Leben eines externen Datenschutzbeauftragten

* Nutzung von Cloud-Dienstleistungen
- Welche datenschutzrechtlichen Vorgaben sind zu beachten?
- Wo liegt meine Verantwortung und wo die des Cloud-Providers?

* Umgang mit Betroffenenanfragen
-Was muss ich beantworten?
-Darf ich immer einen Identitätsnachweis fordern?

* Diskussion und Erfahrungsaustasuch

>> Datenschutz
Grundlagen

Die Datenschutzanforderungen in Form von Gesetzen und Verordnungen für Organisationen verlangen nach Wissen über die Rechtslage und klarem Vorgehen. Fundierte Kenntnisse bringen dabei Sicherheit und Verständnis in der ganzen Organisation.

Ihr Nutzen

In diesem Seminar lernen Sie die wichtigsten Datenschutzbestimmungen und wie Sie durch richtigen Umgang mit Daten, richtiges Verhalten und Kommunikation Verständnis und Vertrauen bei Ihren Kunden und Partnern schaffen.

Voraussetzungen

keine

Preis pro Teilnehmer

EUR 750,- exklusive der gesetzlichen MwSt.

Seminardauer

1 Tag(e)/Day(s)

Hinweise

Das Seminar basiert auf der EU Datenschutz-Grundverordnung (EU-DSGVO).

Version: 1.0

Seminarinhalte

* Grundlagen der EU-DSGVO
- Entwicklung und Struktur des Datenschutzrechts
- Entstehung der EU-DSGVO

* Einführung Datenschutzrecht
- Was ist Datenverarbeitung grundsätzlich?
- Räumlicher/sachlicher Anwendungsbereich
- Grundbegriffe und Definitionen der EU-DSGVO

* Rechtmäßigkeit der Datenverarbeitung
- Grundsätze der Datenverarbeitung
- Formeller und materieller Datenschutz
- Datenschutz durch Technik
- Verfahrensverzeichnis
- Datenschutz-Folgenabschätzung

* Rechte der Betroffenen

* Pflichten der Datenverarbeiter
- Auskunft, Berichtigung, Löschung
- Einschränkung, Datenübertragbarkeit, Widerspruch
- Fristen
- Datenportabilität

* Datentransfers und Cloud-Computing

* Innerhalb der EU
- One Stop Shop

* Übermittlung in Drittländer
- EU/US Privacy Shield
- Gleichgestellte Drittländer

* Standardvertragsklauseln
- Binding Corporate Rules
- Ausnahmen

* Datenschutz und Outsourcing

* Haftung, Risiken und Strafen
- Geschäftsführer, Prokuristen, Mitarbeiter
- Sanktionen bei Verstößen und Rechtsbehelfe

* Datenschutzbeauftragter
- Rolle und Aufgaben des Datenschutzbeauftragten
- Stellung im Unternehmen
- Ausübungsformen

* Mitarbeiter
- Meine Verantwortung
- Handlungsempfehlungen
- Datenmissbrauch als zeitliche Herausforderung

* Anforderungen an Technik und Organisation
- Management, Organisation und Technik integrieren
- Informations-Sicherheits-Management als Datenschutzaufgabe

>> Datenschutz in der Cloud

Workshop für IT-Pro's

Die Datenschutzanforderungen in Form von Gesetzen und Verordnungen für Organisationen verlangen nach Wissen über die Rechtslage und klarem Vorgehen. Fundierte Kenntnisse bringen dabei Sicherheit und Verständnis in der ganzen Organisation.

Ihr Nutzen

In diesem Seminar lernen Sie die wichtigsten Datenschutzbestimmungen bezogen auf den Betrieb von Microsoft Cloud Diensten und wie Sie durch die richtigen Vorkehrungen und deren Kommunikation Verständnis und Vertrauen bei Ihren MitarbeiterInnen, Kunden und Partnern schaffen.

Preis pro Teilnehmer

EUR 2100,- exklusive der gesetzlichen MwSt.

Seminardauer

3 Tag(e)/Day(s)

Voraussetzungen

keine

Hinweise

Das Seminar basiert auf der EU Datenschutz-Grundverordnung (EU-DSGVO).

Version: 1.0

Seminarinhalte

1. Tag
* Grundlagen
- Public vs. Private Cloud
- Grundsätze der DSGVO
- Outsourcing
- Mögliche ROI Modelle?
- Meilensteine am Weg in die Cloud

* Rechtliche Aspekte
- Auftrags-Verarbeiter Vereinbarung
- ISO Zertifizierungen, die hier relevant sind (ISO27000, ISO27018)
- Woher bekomme ich die entsprechenden Dokumente?
- Wer/Wo haben wir hier zugestimmt?
- Welche Auswirkungen hat das für die GDPR Konformität?
- Verantwortung für Aufbewahrungszeiträume
- US Cloud Act relevant bei Microsoft?

* Die Cloud Mehrwerte
- Was kann die Cloud besser?
- Sicheres RZ vs. KMU Server Room
- MFA, Condition Access, Access Control, Auditing
- Mehrwert von Azure P1 und Azure P2

* Rollen
- Billing Admin/Rechnungsadressen
- Was behinhaltet eine Lizenz/Subsciption?
- Was steht im SLA oder auch nicht?

2. Tag
* Beleuchtung der M365 Komponenten
- Exchange Online
- SharePoint Online
- Azure
- DLP, eDiscovery, Tracing, ATP, SafeLinks

* Bestehende Infrastruktur
- Was passiert mit meiner Firewall?
- Benötige ich noch einen Malware Schutz?
- Wohin verlagern sich Sicherheits-Komponenten?

* Meine Daten
- Wo liegen meine Daten?
- Was passiert am Ende der Vertragslaufzeit mit meinen Daten?
- Was passiert bei Stilllegung/Pausierung von Konten?
- Welche Wege gibt es von der Cloud zurück?
- Verschlüsselter Datentransport
- Verschlüsselte Datenhaltung

3. Tag
* Erkennen und Aufräumen
- Shadow ITs loswerden
- Sanktionen bei Verstößen und Rechtsbehelfe

* Rolle des Datenschutzbeauftragten
- Rolle und Aufgaben des Datenschutzbeauftragten
- Stellung im Unternehmen
- Ausübungsformen

* Mitarbeiter
- Verantwortung klären
- Handlungsempfehlungen
- Datenmissbrauch als zeitliche Herausforderung

* Anforderungen an Technik und Organisation
- Management, Organisation und Technik integrieren
- Informations-Sicherheits-Management als Datenschutzaufgabe

>> HTTP and SSL Communications

Mastering { http(s)://deep.dive }

EGOS! the education company

HTTP gehört der sogenannten Anwendungsschicht etablierter Netzwerkmodelle an. Die Anwendungsschicht wird von den Anwendungsprogrammen angesprochen, im Fall von HTTP ist das meist ein Webbrowser. Im ISO/OSI-Schichtenmodell entspricht die Anwendungsschicht den Schichten 5-7.

Ihr Nutzen

In diesem Workshop lernen die die Arbeitsweise und Funktionen des HTTP Protokolls kennen. Neben Theorieinput werden in vielen Labs die Protokollfunktionen und deren Auswirkungen erlernt.

Voraussetzungen

Grundlegende Netzwerk und IP Kenntnisse

Preis pro Teilnehmer

EUR 1550,- exklusive der gesetzlichen MwSt.

Seminardauer

2 Tag(e)/Day(s)

Hinweise

In diesem Workshop wird in einer klassichen Windows IIS Web Infrastruktur gearbeitet. Neben Bordmitteln werden auch Werkzeuge wie Fiddler, Wfetch, IIS Tracing und Netzwerk-Analysetools verwendet.

Version: 2012

Seminarinhalte

1. Tag
* General HTTP overview
- Anatomy of a HTTP Transaction
- Uniform Resource Identifiers
- Requests & Response
- HTTP Headers & MIME Types

* HTTP request methods (RFC2616)
- GET, HEAD
- POST, PUT, DELETE
- OPTIONS, TRACE, CONNECT

* HTTP Statuscodes
- 1xx - Informational
- 2xx - Successful
- 3xx - Redirection
- 4xx - Client Error
- 5xx - Server Error

* Authentication Protocols (RFC2617)
- Basic Authentication
- Digest Authentication
* Header Field Definitions
- Accept-*
- Content-*
- Cache-*

2. Tag
* HTTP DoS
- File & Pathnames Attacks
- DNS Spoofing
- Location & Header Spoofing

* HTTP Optimization Techniques
- Caching Mechanisms
- HTTP Compression (GZIP, DEFLATE)

* HTTP State Management
- Cookies im http-Header und Client

* General HTTPS overview
- Requirements, Certificates
- Certificate Stores

- TLS Handshake
* SSL Offloading
- Beispiel IIS ARR Proxy
- IIS Certificate Management

* Besondere HTTP Protokoll Spezifikationen
- SPDY & Microsoft S+M
- http 2.0
- http Pipelining & Persistent Connections
* Internet Explorer 11 Enterprise Mode (EMIE)
- Group Policies
- Enterprise Mode Site List Manager

>> Informationssicherheit

E-Learning, Clean Desk (Modul 22)

Organisationen werden heute von unterschiedlichen Seiten angegriffen. Hacker, Viren u.v.a.m. bedrohen Unternehmen von Außen, Social-Engineers und demotivierte MitarbeiterInnen bedeuten eine Gefahr von Innen. Die Einführung eines Security Awareness Programms soll den „Security-Gedanken“ in das tägliche Arbeiten der MitarbeiterInnen bringen, ohne diese zu

Ihr Nutzen

Ein nachhaltiges Security Awareness Programm unterstützen wir mit einem E-Learning Programm. Die Software unterstützt MitarbeiterInnen beim Erlernen und Ausüben von Sicherheitsstandards und Richtlinien. Sie trainieren interaktiv und multimedial ausgewählte Lerninhalte zu Security Awareness-Themen.

Preis pro Teilnehmer

EUR 10,- exklusive der gesetzlichen MwSt.

Seminardauer

0,5 Stunde(n)/Hour(s)

Seminarinhalte

* Was ist Clean Desk Policy?
* Gründe für eine Clean Desk Policy
* Einführung einer Clean Desk Policy
* Clear Screen Policy

Voraussetzungen

keine

Hinweise

Stil: Linear
Dauer: 30 min
Sprachen: Deutsch
Der Preis versteht sich für eine/n BenutzerIn zum sofortigen

Version:

>> Informationssicherheit

E-Learning, Cloud Services (Modul 10)

Organisationen werden heute von unterschiedlichen Seiten angegriffen. Hacker, Viren u.v.a.m. bedrohen Unternehmen von Außen, Social-Engineers und demotivierte MitarbeiterInnen bedeuten eine Gefahr von Innen. Die Einführung eines Security Awareness Programms soll den „Security-Gedanken“ in das tägliche Arbeiten der MitarbeiterInnen bringen, ohne diese zu

Ihr Nutzen

Ein nachhaltiges Security Awareness Programm unterstützen wir mit einem E-Learning Programm. Die Software unterstützt MitarbeiterInnen beim Erlernen und Ausüben von Sicherheitsstandards und Richtlinien. Sie trainieren interaktiv und multimedial ausgewählte Lerninhalte zu Security Awareness-Themen.

Preis pro Teilnehmer

EUR 10,- exklusive der gesetzlichen MwSt.

Seminardauer

0,5 Stunde(n)/Hour(s)

Seminarinhalte

* Cloud Services

- Was sind Cloud Services?

- E-Mail in der Public Cloud

- Cloud Speicher

- Risiken für Privatanwender

- Risiken für Unternehmen

Voraussetzungen

keine

Hinweise

Stil: Linear
Dauer: 30 min
Sprachen: Deutsch
Der Preis versteht sich für eine/n BenutzerIn zum sofortigen

Version:

>> Informationssicherheit

E-Learning, Datenschutz (Modul 18)

Datenschutz ist ein großes Thema – und fängt schon bei den kleinen Fragen des Alltags an: Darf ich dem Anrufer die Handynummer der Kollegin geben? Was passiert mit den Daten früherer Kunden? Und was muss ich beachten, wenn ich mobil auf geschäftliche Daten zugreifen will? Mit unserem standardisierten Datenschutz E-Learning bringen Sie Ihren

Ihr Nutzen

Unser Datenschutz Lernprogramm behandelt die wichtigsten Inhalte und Anwendungsfälle zu Datenschutz in Organisationen und Unternehmen. Der Kurs ermöglicht die optimale Qualifizierung Ihrer Mitarbeiter im richtigen Umgang mit Daten.

Voraussetzungen

Keine

Preis pro Teilnehmer

EUR 10,- exklusive der gesetzlichen MwSt.

Seminardauer

0,5 Stunde(n)/Hour(s)

Hinweise

Stil: Linear
Dauer: 30 min
Sprachen: Deutsch
Der Preis versteht sich für eine/n BenutzerIn zum sofortigen

Version:

Seminarinhalte

* Der Begriff Datenschutz
- Erklärung und Begriffe
- Entwicklung des Datenschutzes

* Entstehung der Datenschutz Grundverordnung
- Was ist neu? Was gab es immer schon?

* Ziele der Datenschutz Grundverordnung
- Was/wer wird geschützt?

* Personenbezogene und sensible Daten
- Definition personenbezogener Daten
- Definition sensibler Daten
- Grundsätze der Verarbeitung

* Aktive und passive Personenrechte
- Welche Rechte sind zu beachten?

* Die Rolle des Datenschutzbeauftragten
- Wer benötigt einen Datenschutzbeauftragten
- Die Aufgaben des Datenschutzbeauftragten

* Meine Verantwortung und Aufgaben

>> Informationssicherheit

E-Learning, Dokumentklassifizierung (Modul 19)

Organisationen werden heute von unterschiedlichen Seiten angegriffen. Hacker, Viren u.v.a.m. bedrohen Unternehmen von Außen, Social-Engineers und demotivierte MitarbeiterInnen bedeuten eine Gefahr von Innen. Die Einführung eines Security Awareness Programms soll den „Security-Gedanken“ in das tägliche Arbeiten der MitarbeiterInnen bringen, ohne diese zu

Ihr Nutzen

Ein nachhaltiges Security Awareness Programm unterstützen wir mit einem E-Learning Programm. Die Software unterstützt MitarbeiterInnen beim Erlernen und Ausüben von Sicherheitsstandards und Richtlinien. Sie trainieren interaktiv und multimedial ausgewählte Lerninhalte zu Security Awareness-Themen.

Preis pro Teilnehmer

EUR 10,- exklusive der gesetzlichen MwSt.

Seminardauer

0,5 Stunde(n)/Hour(s)

Seminarinhalte

* Dokumentklassifizierung

- Was bedeutet Klassifizierung?

- Klassifizierungsstufen

- Warum Klassifizirung?

- Handhabungsrichtlinien im Umgang mit klassifizierten Informationen

Voraussetzungen

keine

Hinweise

Stil: Linear
Dauer: 30 min
Sprachen: Deutsch
Der Preis versteht sich für eine/n BenutzerIn zum sofortigen

Version:

>> Informationssicherheit

E-Learning, Grundlagen (Modul 01)

Organisationen werden heute von unterschiedlichen Seiten angegriffen. Hacker, Viren u.v.a.m. bedrohen Unternehmen von Außen, Social-Engineers und demotivierte MitarbeiterInnen bedeuten eine Gefahr von Innen. Die Einführung eines Security Awareness Programms soll den „Security-Gedanken“ in das tägliche Arbeiten der MitarbeiterInnen bringen, ohne diese zu

Ihr Nutzen

Ein nachhaltiges Security Awareness Programm unterstützen wir mit einem E-Learning Programm. Die Software unterstützt MitarbeiterInnen beim Erlernen und Ausüben von Sicherheitsstandards und Richtlinien. Sie trainieren interaktiv und multimedial ausgewählte Lerninhalte zu Security Awareness-Themen.

Preis pro Teilnehmer

EUR 10,- exklusive der gesetzlichen MwSt.

Seminardauer

0,5 Stunde(n)/Hour(s)

Seminarinhalte

* Grundlagen der Informationssicherheit

- Grundbegriffe der Informationssicherheit

- Wie bewerte ich meine Daten?

- Gemeinsam Sicherheit schaffen

- Sicherheitsvorfälle

- Richtiges Verhalten

- Mögliche Bedrohungen

Voraussetzungen

keine

Hinweise

Stil: Linear
Dauer: 30 min
Sprachen: Deutsch
Der Preis versteht sich für eine/n BenutzerIn zum sofortigen

Version:

>> Informationssicherheit

E-Learning, Hilfe ich bin gehackt! (Modul 09)

Organisationen werden heute von unterschiedlichen Seiten angegriffen. Hacker, Viren u.v.a.m. bedrohen Unternehmen von Außen, Social-Engineers und demotivierte MitarbeiterInnen bedeuten eine Gefahr von Innen. Die Einführung eines Security Awareness Programms soll den „Security-Gedanken“ in das tägliche Arbeiten der MitarbeiterInnen bringen, ohne diese zu

Ihr Nutzen

Ein nachhaltiges Security Awareness Programm unterstützen wir mit einem E-Learning Programm. Die Software unterstützt MitarbeiterInnen beim Erlernen und Ausüben von Sicherheitsstandards und Richtlinien. Sie trainieren interaktiv und multimedial ausgewählte Lerninhalte zu Security Awareness-Themen.

Preis pro Teilnehmer

EUR 10,- exklusive der gesetzlichen MwSt.

Seminardauer

0,5 Stunde(n)/Hour(s)

Seminarinhalte

* Was ist Hacking? Was ist Cracking?

- Wie erkennen Sie, dass Ihr Rechner kompromittiert wurde?

- Richtiges Verhalten im Fall eines kompromittierten Geräts

- Protokollierung von Vorfällen

- Notwendige Meldepflichten

- Was tun, wenn das Smartphone oder der PC zu Hause - gehackt wurde?

Voraussetzungen

keine

Hinweise

Stil: Linear
Dauer: 30 min
Sprachen: Deutsch
Der Preis versteht sich für eine/n BenutzerIn zum sofortigen

Version:

>> Informationssicherheit

E-Learning, Insiderangriff (Modul 12)

Organisationen werden heute von unterschiedlichen Seiten angegriffen. Hacker, Viren u.v.a.m. bedrohen Unternehmen von Außen, Social-Engineers und demotivierte MitarbeiterInnen bedeuten eine Gefahr von Innen. Die Einführung eines Security Awareness Programms soll den „Security-Gedanken“ in das tägliche Arbeiten der MitarbeiterInnen bringen, ohne diese zu

Ihr Nutzen

Ein nachhaltiges Security Awareness Programm unterstützen wir mit einem E-Learning Programm. Die Software unterstützt MitarbeiterInnen beim Erlernen und Ausüben von Sicherheitsstandards und Richtlinien. Sie trainieren interaktiv und multimedial ausgewählte Lerninhalte zu Security Awareness-Themen.

Preis pro Teilnehmer

EUR 10,- exklusive der gesetzlichen MwSt.

Seminardauer

0,5 Stunde(n)/Hour(s)

Seminarinhalte

* Was ist ein Insider Threat?

- Welche Bedrohungen können von Insidern ausgehen?

- Welche Personen sind Insider?

- Typisches Fehlverhalten

- Maßnahmen zur Abwehr von Insiderbedrohungen

Voraussetzungen

keine

Hinweise

Stil: Linear
Dauer: 30 min
Sprachen: Deutsch
Der Preis versteht sich für eine/n BenutzerIn zum sofortigen

Version:

>> Informationssicherheit

E-Learning, Kennwort-Sicherheit (Modul 03)

Organisationen werden heute von unterschiedlichen Seiten angegriffen. Hacker, Viren u.v.a.m. bedrohen Unternehmen von Außen, Social-Engineers und demotivierte MitarbeiterInnen bedeuten eine Gefahr von Innen. Die Einführung eines Security Awareness Programms soll den „Security-Gedanken“ in das tägliche Arbeiten der MitarbeiterInnen bringen, ohne diese zu

Ihr Nutzen

Ein nachhaltiges Security Awareness Programm unterstützen wir mit einem E-Learning Programm. Die Software unterstützt MitarbeiterInnen beim Erlernen und Ausüben von Sicherheitsstandards und Richtlinien. Sie trainieren interaktiv und multimedial ausgewählte Lerninhalte zu Security Awareness-Themen.

Preis pro Teilnehmer

EUR 10,- exklusive der gesetzlichen MwSt.

Seminardauer

0,5 Stunde(n)/Hour(s)

Seminarinhalte

* Sichere Kennwörter

- Warum sind Kennwörter wichtig?

- Was ist ein sicheres Kennwort?

- Die Wahl eines sicheren Kennworts

- Schutz Ihres Kennworts

- Richtiges Verhalten bei Diebstahl

- Wie ändern Sie ihr Kennwort?

Voraussetzungen

keine

Hinweise

Stil: Linear
Dauer: 30 min
Sprachen: Deutsch
Der Preis versteht sich für eine/n BenutzerIn zum sofortigen

Version:

>> Informationssicherheit

E-Learning, Mail & Phishing (Modul 04)

Organisationen werden heute von unterschiedlichen Seiten angegriffen. Hacker, Viren u.v.a.m. bedrohen Unternehmen von Außen, Social-Engineers und demotivierte MitarbeiterInnen bedeuten eine Gefahr von Innen. Die Einführung eines Security Awareness Programms soll den „Security-Gedanken“ in das tägliche Arbeiten der MitarbeiterInnen bringen, ohne diese zu

Ihr Nutzen

Ein nachhaltiges Security Awareness Programm unterstützen wir mit einem E-Learning Programm. Die Software unterstützt MitarbeiterInnen beim Erlernen und Ausüben von Sicherheitsstandards und Richtlinien. Sie trainieren interaktiv und multimedial ausgewählte Lerninhalte zu Security Awareness-Themen.

Preis pro Teilnehmer

EUR 10,- exklusive der gesetzlichen MwSt.

Seminardauer

0,5 Stunde(n)/Hour(s)

Seminarinhalte

* Sicherer Umgang mit E-Mail

- Benutzerverantwortung

- Begriffsklärungen

- Phishing Mails

- Erkennen von ungewöhnlichen Mails

- Der Umgang mit unerwünschten Mails

- Ausgehende Mails

Voraussetzungen

keine

Hinweise

Stil: Linear
Dauer: 30 min
Sprachen: Deutsch
Der Preis versteht sich für eine/n BenutzerIn zum sofortigen

Version:

>> Informationssicherheit

E-Learning, Mobile Device Security (Modul 05)

Organisationen werden heute von unterschiedlichen Seiten angegriffen. Hacker, Viren u.v.a.m. bedrohen Unternehmen von Außen, Social-Engineers und demotivierte MitarbeiterInnen bedeuten eine Gefahr von Innen. Die Einführung eines Security Awareness Programms soll den „Security-Gedanken“ in das tägliche Arbeiten der MitarbeiterInnen bringen, ohne diese zu

Ihr Nutzen

Ein nachhaltiges Security Awareness Programm unterstützen wir mit einem E-Learning Programm. Die Software unterstützt MitarbeiterInnen beim Erlernen und Ausüben von Sicherheitsstandards und Richtlinien. Sie trainieren interaktiv und multimedial ausgewählte Lerninhalte zu Security Awareness-Themen.

Preis pro Teilnehmer

EUR 10,- exklusive der gesetzlichen MwSt.

Seminardauer

0,5 Stunde(n)/Hour(s)

Seminarinhalte

* Mobile Device Security

- Einführung in die Welt mobiler Geräte

- Risiken beim Einsatz mobiler Geräte

- Maßnahmen zur Sicherung mobiler Geräte

- Verhalten bei Verlust oder Dienstahl

Voraussetzungen

keine

Hinweise

Stil: Linear
Dauer: 30 min
Sprachen: Deutsch
Der Preis versteht sich für eine/n BenutzerIn zum sofortigen

Version:

>> Informationssicherheit

E-Learning, Multifunktionsgeräte (Modul 20)

Organisationen werden heute von unterschiedlichen Seiten angegriffen. Hacker, Viren u.v.a.m. bedrohen Unternehmen von Außen, Social-Engineers und demotivierte MitarbeiterInnen bedeuten eine Gefahr von Innen. Die Einführung eines Security Awareness Programms soll den „Security-Gedanken“ in das tägliche Arbeiten der MitarbeiterInnen bringen, ohne diese zu

Ihr Nutzen

Ein nachhaltiges Security Awareness Programm unterstützen wir mit einem E-Learning Programm. Die Software unterstützt MitarbeiterInnen beim Erlernen und Ausüben von Sicherheitsstandards und Richtlinien. Sie trainieren interaktiv und multimedial ausgewählte Lerninhalte zu Security Awareness-Themen.

Preis pro Teilnehmer

EUR 10,- exklusive der gesetzlichen MwSt.

Seminardauer

0,5 Stunde(n)/Hour(s)

Seminarinhalte

* Sicherer Umgang mit Multifunktionsgeräten

- Was sind Multifunktionsgeräte?

- Mögliche Gefahrenquellen bei Multifunktionsgeräten

- Der Umweltgedanke

- Taschen von Ersatzteilen

Voraussetzungen

keine

Hinweise

Stil: Linear
Dauer: 30 min
Sprachen: Deutsch
Der Preis versteht sich für eine/n BenutzerIn zum sofortigen

Version:

>> Informationssicherheit

E-Learning, Physische Sicherheit (Modul 14)

Organisationen werden heute von unterschiedlichen Seiten angegriffen. Hacker, Viren u.v.a.m. bedrohen Unternehmen von Außen, Social-Engineers und demotivierte MitarbeiterInnen bedeuten eine Gefahr von Innen. Die Einführung eines Security Awareness Programms soll den „Security-Gedanken“ in das tägliche Arbeiten der MitarbeiterInnen bringen, ohne diese zu

Ihr Nutzen

Ein nachhaltiges Security Awareness Programm unterstützen wir mit einem E-Learning Programm. Die Software unterstützt MitarbeiterInnen beim Erlernen und Ausüben von Sicherheitsstandards und Richtlinien. Sie trainieren interaktiv und multimedial ausgewählte Lerninhalte zu Security Awareness-Themen.

Preis pro Teilnehmer

EUR 10,- exklusive der gesetzlichen MwSt.

Seminardauer

0,5 Stunde(n)/Hour(s)

Seminarinhalte

* Bauliche und infrastrukturelle Maßnahmen

- Organisatorische Maßnahmen

- Sicherheitmaßnahmen innerhalb eines Gebäudes

- Sicherheitsmaßnahmen außerhalb eines Gebäudes

Voraussetzungen

keine

Hinweise

Stil: Linear
Dauer: 30 min
Sprachen: Deutsch
Der Preis versteht sich für eine/n BenutzerIn zum sofortigen

Version:

>> Informationssicherheit

E-Learning, Portable Speichermedien (Modul 21)

Organisationen werden heute von unterschiedlichen Seiten angegriffen. Hacker, Viren u.v.a.m. bedrohen Unternehmen von Außen, Social-Engineers und demotivierte MitarbeiterInnen bedeuten eine Gefahr von Innen. Die Einführung eines Security Awareness Programms soll den „Security-Gedanken“ in das tägliche Arbeiten der MitarbeiterInnen bringen, ohne diese zu

Ihr Nutzen

Ein nachhaltiges Security Awareness Programm unterstützen wir mit einem E-Learning Programm. Die Software unterstützt MitarbeiterInnen beim Erlernen und Ausüben von Sicherheitsstandards und Richtlinien. Sie trainieren interaktiv und multimedial ausgewählte Lerninhalte zu Security Awareness-Themen.

Preis pro Teilnehmer

EUR 10,- exklusive der gesetzlichen MwSt.

Seminardauer

0,5 Stunde(n)/Hour(s)

Seminarinhalte

* Überblick über portable Speichermedien

- Einsatzbereiche portabler Speichermedien

- Risiken bei der Verwendung

- Richtlinien zur Verwendung

- Verschlüsselung auf einem portablen Speichermedium

- Verhalten bei Verlust oder Diebstahl

Voraussetzungen

keine

Hinweise

Stil: Linear
Dauer: 30 min
Sprachen: Deutsch
Der Preis versteht sich für eine/n BenutzerIn zum sofortigen

Version:

>> Informationssicherheit

E-Learning, Remote Arbeitsplätze (Modul 16)

Organisationen werden heute von unterschiedlichen Seiten angegriffen. Hacker, Viren u.v.a.m. bedrohen Unternehmen von Außen, Social-Engineers und demotivierte MitarbeiterInnen bedeuten eine Gefahr von Innen. Die Einführung eines Security Awareness Programms soll den „Security-Gedanken“ in das tägliche Arbeiten der MitarbeiterInnen bringen, ohne diese zu

Ihr Nutzen

Ein nachhaltiges Security Awareness Programm unterstützen wir mit einem E-Learning Programm. Die Software unterstützt MitarbeiterInnen beim Erlernen und Ausüben von Sicherheitsstandards und Richtlinien. Sie trainieren interaktiv und multimedial ausgewählte Lerninhalte zu Security Awareness-Themen.

Preis pro Teilnehmer

EUR 10,- exklusive der gesetzlichen MwSt.

Seminardauer

0,5 Stunde(n)/Hour(s)

Seminarinhalte

* Remote Arbeitsplätze
- Was ist ein Remote Arbeitsplatz?
- Besonderheiten der Remote Arbeit

* Einrichtung eines Remote Arbeitplatzes
- Regelungen für Remote Arbeit
- Organisatorische Vorkehrungen
- Technische Vorkeherungen

* 12 goldene Regeln
- Empfehlungen für mich
- Empfehlungen für Teamarbeit

Voraussetzungen

keine

Hinweise

Stil: Linear
Dauer: 30 min
Sprachen: Deutsch
Der Preis versteht sich für eine/n BenutzerIn zum sofortigen

Version:

>> Informationssicherheit

E-Learning, Richtiger Umgang mit Daten (Modul 06)

Organisationen werden heute von unterschiedlichen Seiten angegriffen. Hacker, Viren u.v.a.m. bedrohen Unternehmen von Außen, Social-Engineers und demotivierte MitarbeiterInnen bedeuten eine Gefahr von Innen. Die Einführung eines Security Awareness Programms soll den „Security-Gedanken“ in das tägliche Arbeiten der MitarbeiterInnen bringen, ohne diese zu

Ihr Nutzen

Ein nachhaltiges Security Awareness Programm unterstützen wir mit einem E-Learning Programm. Die Software unterstützt MitarbeiterInnen beim Erlernen und Ausüben von Sicherheitsstandards und Richtlinien. Sie trainieren interaktiv und multimedial ausgewählte Lerninhalte zu Security Awareness-Themen.

Preis pro Teilnehmer

EUR 10,- exklusive der gesetzlichen MwSt.

Seminardauer

0,5 Stunde(n)/Hour(s)

Seminarinhalte

* Richtiger Umgang mit Daten

- Was sind Daten?

- Typische Fehler im Umgang mit Daten

- Verarbeitung personenbezogener Daten

- Datenwiederherstellung

- Richtiges Löschen von Daten

- Daten auf Papier

Voraussetzungen

keine

Hinweise

Stil: Linear
Dauer: 30 min
Sprachen: Deutsch
Der Preis versteht sich für eine/n BenutzerIn zum sofortigen

Version:

>> Informationssicherheit

E-Learning, Sicherheit auf Reisen (Modul 13)

Organisationen werden heute von unterschiedlichen Seiten angegriffen. Hacker, Viren u.v.a.m. bedrohen Unternehmen von Außen, Social-Engineers und demotivierte MitarbeiterInnen bedeuten eine Gefahr von Innen. Die Einführung eines Security Awareness Programms soll den „Security-Gedanken“ in das tägliche Arbeiten der MitarbeiterInnen bringen, ohne diese zu

Ihr Nutzen

Ein nachhaltiges Security Awareness Programm unterstützen wir mit einem E-Learning Programm. Die Software unterstützt MitarbeiterInnen beim Erlernen und Ausüben von Sicherheitsstandards und Richtlinien. Sie trainieren interaktiv und multimedial ausgewählte Lerninhalte zu Security Awareness-Themen.

Preis pro Teilnehmer

EUR 10,- exklusive der gesetzlichen MwSt.

Seminardauer

0,5 Stunde(n)/Hour(s)

Seminarinhalte

* Sicherheit auf Reisen

- Einführung in die Welt der Dienstreisen

- Planung einer Dienstreise

- Sicherheitsaspekte

- Zusätzliche Tipps

Voraussetzungen

keine

Hinweise

Stil: Linear
Dauer: 30 min
Sprachen: Deutsch
Der Preis versteht sich für eine/n BenutzerIn zum sofortigen

Version:

>> Informationssicherheit

E-Learning, Sicherheit Ihrer Geräte (Modul 15)

EGOS! the education company

Organisationen werden heute von unterschiedlichen Seiten angegriffen. Hacker, Viren u.v.a.m. bedrohen Unternehmen von Außen, Social-Engineers und demotivierte MitarbeiterInnen bedeuten eine Gefahr von Innen. Die Einführung eines Security Awareness Programms soll den „Security-Gedanken“ in das tägliche Arbeiten der MitarbeiterInnen bringen, ohne diese zu

Ihr Nutzen

Ein nachhaltiges Security Awareness Programm unterstützen wir mit einem E-Learning Programm. Die Software unterstützt MitarbeiterInnen beim Erlernen und Ausüben von Sicherheitsstandards und Richtlinien. Sie trainieren interaktiv und multimedial ausgewählte Lerninhalte zu Security Awareness-Themen.

Preis pro Teilnehmer

EUR 10,- exklusive der gesetzlichen MwSt.

Seminardauer

0,5 Stunde(n)/Hour(s)

Seminarinhalte

* Sicherheit Ihrer Geräte

- Überblick IT-Geräte

- Benutzungsrichtlinen

- Stationäre und mobile Geräte

- Internet of Things (IoT)

Voraussetzungen

keine

Hinweise

Stil: Linear
Dauer: 30 min
Sprachen: Deutsch
Der Preis versteht sich für eine/n BenutzerIn zum sofortigen

Version:

>> Informationssicherheit

E-Learning, Sicherheit im Web (Modul 02)

Organisationen werden heute von unterschiedlichen Seiten angegriffen. Hacker, Viren u.v.a.m. bedrohen Unternehmen von Außen, Social-Engineers und demotivierte MitarbeiterInnen bedeuten eine Gefahr von Innen. Die Einführung eines Security Awareness Programms soll den „Security-Gedanken“ in das tägliche Arbeiten der MitarbeiterInnen bringen, ohne diese zu

Ihr Nutzen

Ein nachhaltiges Security Awareness Programm unterstützen wir mit einem E-Learning Programm. Die Software unterstützt MitarbeiterInnen beim Erlernen und Ausüben von Sicherheitsstandards und Richtlinien. Sie trainieren interaktiv und multimedial ausgewählte Lerninhalte zu Security Awareness-Themen.

Preis pro Teilnehmer

EUR 10,- exklusive der gesetzlichen MwSt.

Seminardauer

0,5 Stunde(n)/Hour(s)

Seminarinhalte

* Sicheres Surfen im Internet

- Gefahren im Internet

- Erkennen von Gefahren

- Technische Schutzmaßnahmen

- Konfiguration Ihres Browsers

- Digitale Zertifikate

- Surfen in öffentlichen Netzen

Voraussetzungen

keine

Hinweise

Stil: Linear
Dauer: 30 min
Sprachen: Deutsch
Der Preis versteht sich für eine/n BenutzerIn zum sofortigen

Version:

>> Informationssicherheit

E-Learning, Sicherheit im WLAN (Modul 17)

Organisationen werden heute von unterschiedlichen Seiten angegriffen. Hacker, Viren u.v.a.m. bedrohen Unternehmen von Außen, Social-Engineers und demotivierte MitarbeiterInnen bedeuten eine Gefahr von Innen. Die Einführung eines Security Awareness Programms soll den „Security-Gedanken“ in das tägliche Arbeiten der MitarbeiterInnen bringen, ohne diese zu

Ihr Nutzen

Ein nachhaltiges Security Awareness Programm unterstützen wir mit einem E-Learning Programm. Die Software unterstützt MitarbeiterInnen beim Erlernen und Ausüben von Sicherheitsstandards und Richtlinien. Sie trainieren interaktiv und multimedial ausgewählte Lerninhalte zu Security Awareness-Themen.

Preis pro Teilnehmer

EUR 10,- exklusive der gesetzlichen MwSt.

Seminardauer

0,5 Stunde(n)/Hour(s)

Seminarinhalte

* Sicherheit im WLAN

- Was ist WLAN und Wi-Fi?

- Offene und verschlüsselte WLANs

- Verhalten in offenen WLANs

- WLAN im Unternehmen

- WLAN-Sicherheit zu Hause

Voraussetzungen

keine

Hinweise

Stil: Linear
Dauer: 30 min
Sprachen: Deutsch
Der Preis versteht sich für eine/n BenutzerIn zum sofortigen

Version:

>> Informationssicherheit

E-Learning, Social Engineering (Modul 07)

Organisationen werden heute von unterschiedlichen Seiten angegriffen. Hacker, Viren u.v.a.m. bedrohen Unternehmen von Außen, Social-Engineers und demotivierte MitarbeiterInnen bedeuten eine Gefahr von Innen. Die Einführung eines Security Awareness Programms soll den „Security-Gedanken“ in das tägliche Arbeiten der MitarbeiterInnen bringen, ohne diese zu

Ihr Nutzen

Ein nachhaltiges Security Awareness Programm unterstützen wir mit einem E-Learning Programm. Die Software unterstützt MitarbeiterInnen beim Erlernen und Ausüben von Sicherheitsstandards und Richtlinien. Sie trainieren interaktiv und multimedial ausgewählte Lerninhalte zu Security Awareness-Themen.

Preis pro Teilnehmer

EUR 10,- exklusive der gesetzlichen MwSt.

Seminardauer

0,5 Stunde(n)/Hour(s)

Seminarinhalte

* Social Engineering

- Begriffsdefinition

- Die Stufen des Social Engineering

- Besonders gefährdete Personen

- Schutzkonzepte

Voraussetzungen

keine

Hinweise

Stil: Linear
Dauer: 30 min
Sprachen: Deutsch
Der Preis versteht sich für eine/n BenutzerIn zum sofortigen

Version:

>> Informationssicherheit

E-Learning, Social Networks (Modul 08)

Organisationen werden heute von unterschiedlichen Seiten angegriffen. Hacker, Viren u.v.a.m. bedrohen Unternehmen von Außen, Social-Engineers und demotivierte MitarbeiterInnen bedeuten eine Gefahr von Innen. Die Einführung eines Security Awareness Programms soll den „Security-Gedanken“ in das tägliche Arbeiten der MitarbeiterInnen bringen, ohne diese zu

Ihr Nutzen

Ein nachhaltiges Security Awareness Programm unterstützen wir mit einem E-Learning Programm. Die Software unterstützt MitarbeiterInnen beim Erlernen und Ausüben von Sicherheitsstandards und Richtlinien. Sie trainieren interaktiv und multimedial ausgewählte Lerninhalte zu Security Awareness-Themen.

Preis pro Teilnehmer

EUR 10,- exklusive der gesetzlichen MwSt.

Seminardauer

0,5 Stunde(n)/Hour(s)

Seminarinhalte

* Social Networks

- Einführung in Social Networks

- Gefahren bei der Nutzung

- Grundregeln

- Sicherheitseinstellungen

- Wie schützen Sie sich?

Voraussetzungen

keine

Hinweise

Stil: Linear
Dauer: 30 min
Sprachen: Deutsch
Der Preis versteht sich für eine/n BenutzerIn zum sofortigen

Version:

>> Informationssicherheit

E-Learning, Verschlüsselung (Modul 11)

Organisationen werden heute von unterschiedlichen Seiten angegriffen. Hacker, Viren u.v.a.m. bedrohen Unternehmen von Außen, Social-Engineers und demotivierte MitarbeiterInnen bedeuten eine Gefahr von Innen. Die Einführung eines Security Awareness Programms soll den „Security-Gedanken“ in das tägliche Arbeiten der MitarbeiterInnen bringen, ohne diese zu

Ihr Nutzen

Ein nachhaltiges Security Awareness Programm unterstützen wir mit einem E-Learning Programm. Die Software unterstützt MitarbeiterInnen beim Erlernen und Ausüben von Sicherheitsstandards und Richtlinien. Sie trainieren interaktiv und multimedial ausgewählte Lerninhalte zu Security Awareness-Themen.

Preis pro Teilnehmer

EUR 10,- exklusive der gesetzlichen MwSt.

Seminardauer

0,5 Stunde(n)/Hour(s)

Seminarinhalte

* Einführung in die Welt der Verschlüsselung

- Symmetrische und asymmetrische Verschlüsselung

- Wo wird Verschlüsselung eingesetzt?

- Digitale Zertifikate

- Digitale Signatur

Voraussetzungen

keine

Hinweise

Stil: Linear
Dauer: 30 min
Sprachen: Deutsch
Der Preis versteht sich für eine/n BenutzerIn zum sofortigen

Version:

>> Informationssicherheit

Grundlagen für AnwenderInnen

Da die stetig wechselnden und komplexer werdenden Gefahren von Sicherheitslecks in Software und Netzwerken zu einer zunehmenden Unsicherheit führen, ist eine Sensibilisierung bezüglich der aktuellen Sicherheitsproblematik vonnöten, die in diesem Security Seminar für Anwender vermittelt wird.

Ihr Nutzen

Nach diesem Seminar sind Sie in der Lage, aktuelle Sicherheitsprobleme zu erkennen und sich unter Verwendung neuer Technologien des Informationsschutzes entsprechend zu verhalten. Neben Wissen zu Technologien stärken Sie in diesem Seminar auch Ihr Selbstvertrauen im Umgang mit Bedrohungen sowohl in als auch außerhalb Ihrer Organisation.

Preis pro Teilnehmer

EUR 450,- exklusive der gesetzlichen MwSt.

Seminardauer

1 Tag(e)/Day(s)

Voraussetzungen

Windows und Office Anwenderkenntnisse

Hinweise

Die Inhalte dieses Workshops können individuell an Rahmenbedingungen und Richtlinien in Ihrer Organisation angepasst werden.

Version:

Seminarinhalte

* Übersicht über potentielle Sicherheitsprobleme
- Was ist die Bedrohung?
- Typische Vorfälle aus der Vergangenheit
- Was ist meine Verantwortung als Anwender?

* IT-Sicherheit-Grundbegriffe
- Daten und Informationen
- Ziele der IT-Sicherheit
- IT-Sicherheitsmanagement

* Cybercrime
- Überblick über Gefahren
- Bin ich wirklich betroffen?

* Social Engineering und Phishing
- Methoden und Muster
- Erkennen von Angriffen
- Vorbeugende Maßnahmen

* Zugang zu meinen Daten
- Kennwörter
- Verschlüsselung
- Handlungsempfehlungen

* Verhaltensregeln für den PC Arbeitsplatz
- Clean Desk Policy
- Clear Screen
- Dumpster Diver
- USB-Port
- Vorbeugende Maßnahmen
- Umgang mit Angriffen

* Umgang mit Informationen
- Umgang mit Unternehmensdaten
- Dokumentklassifizierung
- Dokumenteigenschaften
- Schutz von Dokumenten

* Malware und Ransomware
- Begriffsklärung
- Arten von Malware
- Schutz meiner Geräte
- Zertifikate & Digitale Unterschrift
- Vorbeugende Maßnahmen
- Umgang mit Angriffen

* Das Internet
- Internet Downloads
- Cookies und meine Spuren im Internet
- Meine persönliche Daten
- Einkäufe im Internet
- Social Networks

* Mobiles Arbeiten
- WLAN und HotSpots
- SmartPhones und Tablets
- Verwenden von App's
- Nutzen von Cloud Diensten
- Offline Files & Synchronisierung

* Management der Datensicherheit
- Datensicherung
- Datenvernichtung

* Mein Beitrag zur Informationssicherheit
- Zusammenfassung

* Optional:
- Gesetz zum Schutz von personenbezogenen Daten (Privacy-Gesetz) – Grundlagen und Konsequenzen

>> Informationssicherheit

Grundlagen für Führungskräfte

Da die stetig wechselnden und komplexer werdenden Gefahren von Sicherheitslecks in Software und Netzwerken zu einer zunehmenden Unsicherheit führen, ist eine Sensibilisierung bezüglich der aktuellen Sicherheitsproblematik vonnöten, die in diesem Security Seminar für Führungskräfte vermittelt wird.

Ihr Nutzen

Nach diesem Seminar sind Sie in der Lage, aktuelle Sicherheitsprobleme zu erkennen und sich unter Verwendung neuer Technologien des Informationsschutzes entsprechend selbst zu verhalten und Ihre MitarbeiterInnen zu führen. Neben Wissen zu Technologien erhalten Sie Empfehlungen im Umgang mit Bedrohungen sowohl in als auch außerhalb Ihrer Organisation.

Preis pro Teilnehmer

EUR 550,- exklusive der gesetzlichen MwSt.

Seminardauer

1 Tag(e)/Day(s)

Seminarinhalte

* Gesetzliche Rahmenbedingungen
- Das Datenschutzgesetz
- Die Verantwortung von Führungskräften

* IT-Sicherheit in Organisationen
- Regeln und Richtlinien
- Schutz durch Infrastruktur

* Übersicht über potentielle Sicherheitsprobleme
- Was ist die Bedrohung?
- Typische Vorfälle aus der Vergangenheit
- Was ist meine Verantwortung als Anwender?

* IT-Sicherheit-Grundbegriffe
- Daten und Informationen
- Ziele der IT-Sicherheit
- IT-Sicherheitsmanagement

* Cybercrime
- Überblick über Gefahren
- Bin ich wirklich betroffen?

* Überblick über Bedrohungen
- Social Engineering und Phishing
- Zugang zu meinen Daten / Kennwörter
- Verhaltensregeln für den PC Arbeitsplatz
- Umgang mit Informationen
- Malware und Ransomware
- Das Internet
- Mobiles Arbeiten

* Management der Datensicherheit
- Datensicherung
- Datenvernichtung

* Schadens-Minimierung im Ernstfall
- Forensik
- Kommunikation

* Vorbeugende Maßnahmen
- Security Awareness Projekte

Die Inhalte dieses Workshops können individuell an Rahmenbedingungen und Richtlinien in Ihrer Organistaion angepasst werden.

Voraussetzungen

keine

Hinweise

Im Zuge der Digitalisierungsoffensive führt das BFI Salzburg diesen Kurs in Kooperation mit EGOS! durch.

Version:

Ihr Nutzen

Im Seminar lernen die Teilnehmer, Sicherheitsvorfälle unvoreingenommen zu bewerten und die verschiedenen Varianten der Bewertung praktisch einzusetzen. Durch einen Vergleich mit Vorfällen aus der Wirklichkeit (Case Studies) werden die Handlungsspielräume des eigenen Unternehmens erfahrbar.

Preis pro Teilnehmer

EUR 1450,- exklusive der gesetzlichen MwSt.

Seminardauer

2 Tag(e)/Day(s)

Seminarinhalte

Motivation:
CIOs, CISOs, CSOs, CFOs und CEOs erfahren Druck von zwei Seiten: einer Security-Branche, die die Kosten von Sicherheitsvorfällen gerne maßlos übertreibt, um dadurch Produkte zu verkaufen und der tatsächlichen Bedrohung durch einen Sicherheitsvorfall im eigenen Haus und der Schwierigkeit, Investitionen zu rechtfertigen oder ROIs für Security-Investitionen seriös zu bilden.

Ebenso steht die Frage der tatsächlich entstandenen Kosten eines Sicherheitsvorfalls im Zentrum jeder Form der juristischen Aufarbeitung nach einem real aufgetretenen Vorfall und wird über Wohl und Wehe der anschließenden Verfahren (sei es als Klagender oder Beklagter) entscheiden.

Inhalt und Themenblöcke
* Berechnungsmodelle für die Kosten von Sicherheitsvorfällen

* Fallbeispiele zur Berechnung

* Reale Case Studies zu Sicherheitsvorfällen
- Fallverlauf
- Schaden
- Folgekosten und Aufarbeitung

Voraussetzungen

Keine

Hinweise

Version: N/A

>> Informationssicherheit

Security Awareness - un:plugged

Da die stetig wechselnden und komplexer werdenden Gefahren von Sicherheitslecks in Software und Netzwerken zu einer zunehmenden Unsicherheit führen, ist eine Sensibilisierung bezüglich der aktuellen Sicherheitsproblematik vonnöten.

Ihr Nutzen

In diesem spannenden Vortrag erfahren Sie aktuelle Trends bei Angriffen und Bedrohungen und erhalten Tipps wie Sie sich und Ihre Geräte und Daten vor Angriffen effizient schützen können.

Voraussetzungen

Windows und Office Anwenderkenntnisse

Preis pro Teilnehmer

EUR 250,- exklusive der gesetzlichen MwSt.

Seminardauer

0,5 Tag(e)/Day(s)

Hinweise

Die Inhalte dieses Workshops können individuell an Rahmenbedingungen und Richtlinien in Ihrer Organisation angepasst werden.

Version:

Seminarinhalte

* Übersicht über potentielle Sicherheitsprobleme
- Was ist die Bedrohung?
- Warum steigt das Bedrohungspotential?
- Die neue EU-DSGVO
- Was ist meine Verantwortung als Anwender?
- Typische Vorfälle aus der Vergangenheit

* Die wichtigsten Bedrohungen - eine Begriffsklärung
- Mein PC-Arbeitsplatz (Kennwörter, Clear Desk)
- Sonstige IT-Geräte (Smartphone, Festplatten, USB,…)
- Mobiles Arbeiten (Home Office, VPN, WIFI)
- Meine persönlichen Daten (personenbezogene Daten und Preisgabe)
- Umgang mit Daten und Dokumenten (Sicherheitsstufen und Dokumentklassifizierung)
- Phishing und andere Angriffe (z.B. Smartphone Hacking)
- Das Internet
- Clouddienste (Richtlinie)
- Social Networks
- Social Engineering

* Wie kann ich mich schützen?
- 3 heiße Tipps
- Was tun im Ernstfall?

>> Informationssicherheit

Verlust von Daten behandeln

Als Datenpanne oder Datenleck bezeichnet man einen Vorfall, bei dem Unberechtigte Zugriff auf eine Datensammlung erhalten. Wird der Begriff weit ausgelegt, so schließt er auch das unerwünschte Löschen von Daten (Datenverlust) ein.

Ihr Nutzen

In diesem Seminar lernen Sie aktuelle Real-Life-Vorfälle kennen und wie diese behandelt worden sind. Außerdem werden Methoden zur Behandlung von Sicherheitsvorfällen vorgestellt und bearbeitet.

Voraussetzungen

Grundkenntnisse der Prozesse einer IT Infrastruktur

Preis pro Teilnehmer

EUR 950,- exklusive der gesetzlichen MwSt.

Seminardauer

1 Tag(e)/Day(s)

Hinweise

Im Zuge der Digitalisierungsoffensive führt das BFI Salzburg diesen Kurs in Kooperation mit EGOS! durch.

Version: 1.0

Seminarinhalte

1. Tag
* Ein Sicherheitsvorfall - Was tun?
- Allgemeine Vorgehensweisen

* Vorfallstypen und deren Behandlung
- Datendiebstahl
* Interne und externe Behandlung
- Kommunikation
- PR Communication

* Case Studies - Session 1
- Fall Datendiebstahl 1 mit nationalem Täter
- Fall Datendiebstahl 2 mit internationalem Täter

* Case Studies - Session 2
- Der verschwundene Dienstvertrag
- IT-Forensik spart 850.000.- Euro

- Umsatzeinbruch um 2Mio Euro durch internen Täter

* Auf einen beispielhaften Vorfall reagieren
- Alarmierung
- Strategische Entscheidungsgrundlagen
- Richtlinien zur Abwicklung mit Internen und Externen
- Dokumentation zur internen oder gerichtlichen Verwendung

>> Internet Protocol v6 (IPv6)

Architecture and Implementation

Das Internet Protocol Version 6 (IPv6) (auch IPnG, Internet Protocol Next Generation) ist der Nachfolger des gegenwärtig im Internet noch überwiegend verwendeten Internet Protocol in der Version 4. Beide Protokolle sind Standards für die Netzwerkschicht des OSI-Modells und regeln die Adressierung und das Routing von Datenpaketen durch ein Netzwerk.

Ihr Nutzen

In diesem Seminar erlernen Sie die Grundlagen und Architektur von IPv6 und können IPv6 implementieren und dessen Kommunikationswege analysieren. Sie stellen damit alle Aspekte einer effektiven Einführung von IPv6 in ihrer IT-Umgebung sicher.

Voraussetzungen

Networking Technologies~6231

oder dem entsprechende Kenntnisse

Preis pro Teilnehmer

EUR 1750,- exklusive der gesetzlichen MwSt.

Seminardauer

3 Tag(e)/Day(s)

Hinweise

Version: 6

Seminarinhalte

1. Tag
* Einführung in IPv6
* Aufbau des IPv6 Headers
* Aufbau des IPv6 Adressbereichs
* Neighbour Discovery (ND)
* Autoconfiguration
* Path MTU and Fragmentation
* IPv6 DNS
- IPv6 DNS Records
* DHCPv6

2. Tag
* Renumbering with IPv6
* Routing mit IPv6
- RIPng
- OSPFv3
- MP-BGP
* IPv6 in Backbone Networks
* IPv4/IPv6 Transitions und Integration
- Manuelle Tunnel
- Tunnel Broker
- Implementierung von ISATAP

3. Tag
- Implementierung von 6to4
- Implementierung von NAT-PT
* IPv6 Security
- IPSec in IPv6 Umgebungen
- IPv6 ACLs
* Multicasting mit IPv6
* QoS

>> IT Forensik

Rechtliche Grundlagen

Unter IT Forensik versteht man die Verfolgung von Spuren auf einem System. Sei es die Nachverfolgung eines Einbruchversuchs in ein Netzwerk oder die Beweissicherung in strittigen Fällen.

Ihr Nutzen

In diesem Seminar erhalten Sie einen Überblick über die Aktionen, die in einem Notfall (Einbruch, Diebstahl, DOS Attacke) durchzuführen sind, insbesondere den rechtlichen Grundlagen.

Voraussetzungen

Grundkenntnisse der PC und Netzwerksicherheit.

Preis pro Teilnehmer

EUR 750,- exklusive der gesetzlichen MwSt.

Seminardauer

1 Tag(e)/Day(s)

Hinweise

Im Zuge der Digitalisierungsoffensive führt das BFI Salzburg diesen Kurs in Kooperation mit EGOS! durch.

Version:

Seminarinhalte

1. Tag
* Einführung in Computer-Forensik
- Unterscheidung Netzwerk/System-Forensik

* Ansatzpunkte für forensische Untersuchungen im Netzwerk

* Strukturierung einer forensischen Untersuchung

* Beweissicherung für gerichtliche Zwecke

* Netzwerkforensik
- Sammeln von relevanten Daten
- Datenauswertung
- Datenarchivierung

* Forensische Untersuchungen
- Ablaufpläne
- Checklisten

>> IT Forensik
Tools Workshop

Unter IT Forensik versteht man die Verfolgung von Spuren auf einem System. Sei es die Nachverfolgung eines Einbruchversuchs in ein Netzwerk oder die Beweissicherung in strittigen Fällen.

Ihr Nutzen

Dieses Seminar gibt Ihnen einen Überblick über die Konzepte der Forensik und Aktionen die in einem Notfall (Einbruch, Diebstahl, DOS Attacke) durchzuführen sind. Nach dem Seminar können Sie mit Forensic Case Tools umgehen und Beweise und Vorgänge auf Windows Systemen entsprechend sichern.

Voraussetzungen

Grundkenntnisse der PC und Netzwerksicherheit.

Preis pro Teilnehmer

EUR 2100,- exklusive der gesetzlichen MwSt.

Seminardauer

3 Tag(e)/Day(s)

Hinweise

Im Zuge der Digitalisierungsoffensive führt das BFI Salzburg diesen Kurs in Kooperation mit EGOS! durch.

Version:

Seminarinhalte

1. Tag
* Zulassungsprüfung: Rechtliche Grundlagen
* Wiederholung
- Was ist IT Forensik?
- Wissenschaftliche Methoden (Tools, Dokumentation)
- Vorbereitung der Organisation
- Forensische Ermittler und die Judikative
* Konzepte in der IT Forensik
- Kodierung
- Dateierweiterungen und Header
- Speicher und Hauptspeicher
- Flüchtige / Nicht flüchtige Speicher
- Computer / Netzwerke / Mainframe / Cloud
- Arten von Daten
- Dateisystem
- Belegter / Freier Speicher
- File Carving
* Das Forensische Labor einrichten
* Auswahl von Tools
- Sichern der Daten
- Dokumentation

2. Tag
* Methoden in der Forensik
- Dokumentieren der Umgebung
- Spurensicherung
- Forensisches Clonen der Datenträger
- Live System versus Dead System
- Hashing
- Berichterstellung
* Windows System Artifakte
- Gelöschte Daten
- Hibernate/Page-Files
- Die Registry
- Print Spooler
- Metadaten
- Prefetch,Link Files,Shadow Copies, Recent Files
* Interessante Spuren
- Eventlogs
- Applikations-Installationen erkennen
- Seltsame Services erkennen
- Database Mystery (ESE, Thumbs.DB, Index)
- USB/BYOD Forensik auf Windows Systemen

3. Tag
* Antiforensik
- Das Konzept der Antiforensik
- Daten verstecken
- Daten vernichten
* Internet Explorer und E-Mail
- Cookies
- Web Cache
- History
- E-Mail Spuren
* Übersicht über Forensik im Netzwerk
* Übersicht über Mobile Device Forensik
* Ausblick
- Trends in der Computerkriminalität
- Moderne Tools

Security Auditing und Vulnerability Scanner ermöglichen Ihnen den Sicherheits-Level ihrer Server und Netzwerke zu überprüfen und zu dokumentieren.

Ihr Nutzen

Sie lernen Sie wie ein Auditprozess implementiert werden kann und wie der darin enthaltene Penetration Test durchgeführt wird. Sie lernen spezielle Tools kennen und erfahren wie die Ergebnisse dokumentiert werden.

Voraussetzungen

Grundkenntnisse des TCP/IP Protokolls und von Netzwerkdiensten. Besuch des Seminars Hacking für System-Administratoren oder entsprechende Kenntnisse.

Preis pro Teilnehmer

EUR 1400,- exklusive der gesetzlichen MwSt.

Seminardauer

2 Tag(e)/Day(s)

Hinweise

Im Zuge der Digitalisierungsoffensive führt das BFI Salzburg diesen Kurs in Kooperation mit EGOS! durch.

Version:

Seminarinhalte

1. Tag
* Der Auditprozess
- Ablauf des Auditprozesses
- Tools für die Steuerung des Auditprozesses
- Vorbereitung und Absicherung

* Der Penetration Test
- Abgrenzung zum Auditprozess
- Abgrenzung zum Hacking

* Test-Bereiche definieren (Scoping)

* Arten des Penetration Tests
- Der Black Box Penetration Test
- Der White Box Penetration Test

* Ablauf des Penetration Test
- Stufen des Penetration Test
- Risiken der jeweiligen Stufen

2. Tag
* Beispielhafte Tools
- Netzwerk/Penetrationtest: Nessus
- Web Applications: Burp
* Dokumentation und Berichterstellung
- Vorlagen / Tools für die Dokumentation
- Berichterstellung
- Empfehlungen dokumentieren
- Handlungsanweisungen geben

* Gruppenarbeit: Mein erster PenTest

* Überprüfung auf Umsetzung der Empfehlungen

>> IT Security
Fundamentals

Das Verständnis für Sicherheitsebenen und Sicherheitsaspekten ist eine notwendige Voraussetzung für die erfolgreiche Absicherung von PC Netzwerken.

Ihr Nutzen

Nach dem Seminar verstehen Sie die relevanten Sicherheitsebenen, Sicherheit des Betriebssystems, Grundlagen der Netzwerksicherheit und Sicherheits-Software.

Voraussetzungen

Networking Technologies~6231

oder dem entsprechende Kenntnisse

Preis pro Teilnehmer

EUR 1550,- exklusive der gesetzlichen MwSt.

Seminardauer

3 Tag(e)/Day(s)

Hinweise

MOC40367, Dieses Seminar dient zur Vorbereitung zur MTA Zertifizierung. Examen: 98-367
Im Zuge der Digitalisierungsoffensive führt das BFI Salzburg diesen Kurs in Kooperation mit EGOS! durch.

Version: N/A

Seminarinhalte

Tag 1:
* Verständnis für Sicherheitsebenen
- Grundprizipien von IT-Sicherheit
- Physische Sicherheit

* Authentifizierung, Autorisierung und Kontoführung
- Authentifizierung
- Vergleich Rechte und Berechtigungen
- Authentifizierung für Sicherheit nutzen
- Verschlüsselung für Datenschutz nutzen

Tag 2:
* Security Policies
- Passwortrichtlinien zur Erweiterung der Sicherheit

* Grundlegendes Netzwerk-Sicherheit
- Firewalls verwenden
- Network Access Protection (NAP)
- Isolation zum Netzwerkschutz
- Datenschutz mit Protokollsicherheit
- Wireless Networks absichern

Tag 3:
* Schutz von Server und Client
- Client Computer schützen
- Malwareschutz
- E-Mailschutz
- Server schützen
- Internet Explorer schützen

* Security Fundamentals Exam
- Prüfungsvorbereitung

>> IT Security

Hacking für System-Administratoren I

Angriffe auf Netzwerke stellen eine ernstzunehmende Bedrohung für IT Netzwerke und damit das ganze Unternehmen dar. Systemadministratoren können ein Netzwerk nur mit fundierten Kenntnissen des "Hacking" sinnvoll schützen.

Ihr Nutzen

In diesem Seminar lernen Sie aktuelle Angriffsvektoren auf Netzwerke kennen. Nach dem Seminar sind Sie in der Lage diese zu erkennen und Gegenmaßnahmen zu ergreifen. In zahlreichen praktischen Übungen werden typische Angriffs-Szenarien erarbeitet.

Voraussetzungen

Kenntnisse von TCP/IP und Administrationskenntnisse von Windows oder Linux.

Preis pro Teilnehmer

EUR 2100,- exklusive der gesetzlichen MwSt.

Seminardauer

3 Tag(e)/Day(s)

Hinweise

Dieses Seminar dient zur Vorbereitung auf die Zertifizierung Certified Ethical Hacker 312-50.
Prüfungsgebühren: Euro 1.200,-

Version:

Seminarinhalte

1. Tag
* Einführung „Ethisches Hacken“
- Bedrohungen, Angriffsvektoren
- Informationssicherheit
- Konzepte
- Phasen eines Hacks

* Footprinting und Reconnaissance
- Informationsbeschaffung

* Scannen von Netzwerken

2. Tag
* Enumeration

* System Hacking
- Methoden
- Passwörter knacken
- Steganographie

* Social Engineering

3. Tag
* Denial of Service
* Session Hijacking
* Webserver hacken
* Hacking von Webapplikationen
* SQL Injektion

>> IT Security

Hacking für System-Administratoren II

Angriffe auf Netzwerke stellen eine ernstzunehmende Bedrohung für IT Netzwerke und damit das ganze Unternehmen dar. Systemadministratoren können ein Netzwerk nur mit fundierten Kenntnissen des "Hacking" sinnvoll schützen.

Ihr Nutzen

Vertiefen Sie Ihre Kenntnisse, wie Sie Ihre IT-Umgebung vor Hacker-Angriffen schützen können. Dieses Seminar dient zusätzlich zur Vorbereitung zur Ethical Hacking Zertifizierung.

Voraussetzungen

Seminar Hacking für Systemadministratoren~5029

oder entsprechende Kenntnisse

Preis pro Teilnehmer

EUR 1550,- exklusive der gesetzlichen MwSt.

Seminardauer

2 Tag(e)/Day(s)

Hinweise

Dieses Seminar dient zur Vorbereitung auf die Zertifizierung Certified Ethical Hacker 312-50.
Prüfungsgebühren: Euro 1.200,-

Version:

Seminarinhalte

1. Tag
* Wiederholung der Grundlagen
* Schwachstellenanalyse
* Bedrohungen durch Malware
* Sniffing
* IDS, Firewall und Honeypots umgehen
* Drahtlosnetzwerke hacken

2. Tag
* Mobile Plattformen
* Internet of Things
* Cloud
* Kryptographie

>> Microsoft 365
Security Administrator

EGOS! the education company

Microsoft 365 vereint Funktionen aus verschiedensten Microsoft-Produkten in einer zentralen Lösung, die auf kleine und mittlere Unternehmen zugeschnitten ist. Und im Hintergrund sorgen Office 365 und Windows 10 mit umfassender Geräteverwaltung und Sicherheit für den Schutz Ihrer Unternehmensdaten.

Ihr Nutzen

Nach diesem Seminar können Sie die Security Funktionen von Microsoft 365 identifizieren, konfigurieren, ausrollen und verwalten. Schwerpunkts sind Identity Management, Threat Protection und Information Protection.

Voraussetzungen

Microsoft 365, Identity and Services~9868

Windows Server und Active Directory Administrations-Kenntnisse von Vorteil

Preis pro Teilnehmer

EUR 2250,- exklusive der gesetzlichen MwSt.

Seminardauer

4 Tag(e)/Day(s)

Hinweise

MS-500, Diese Seminar bereitet Sie auf die Zertifizierung zum Microsoft Security Administrator vor.

Version: N/A

Seminarinhalte

1. Tag: MS-500T01: Managing Microsoft 365 Identity and Access
* User und Group Security
- User Accounts in Microsoft 365
- Roles und Security Groups
- Password Management
- Azure Identity Protection und MFA

* Identity Synchronization
- Planung von Azure AD Connect
- Einrichten von Azure AD Connect
- Verwalten von snychronisierten Identities

* Federated Identities
- Einführung in Federation
- Planung von ADFS
- ADFS einrichten und konfigurieren
- Web Application Proxy für ADFS
- Hochverfügbarkeit
- Konfiguration von ADFS mit AADConnect

* Access Management
- Conditional Access
- Verwaltung von Device Access
- Role Based Access Control (RBAC)
- Lösungen für externen Zugriff

2. Tag:
* MS-500T02: Implementing Microsoft 365 Threat Protection
* Security on Microsoft 365
- Threat Vectors und Data Breaches
- Überblick über Security Lösungen on M365
- Microsoft Secure Score

* Advanced Threat Protection (ATP)
- Exchange Online Protection (EOP)
- Office 365 ATP
- Safe Attachments und Safe Links
- Azure ATP
- Windows Defender ATP

* Threat Intelligence
- Das Security Dashboard
- Was ist Advanced Threat Analytics?
- Einrichten des ATA Centers
- Nutzen des Microsoft Intelligent Security Graph
- Threat Explorer

* Mobility
- Planung von Mobile Application Management
- Planung von Mobile Device Management
- Verwendung von Intune
- MDM für Office 365 vs. Intune
- Device Security and Enrollment Policies

3. Tag: MS-500T03: Implementing Microsoft 365 Information Protection
* Information Protection
- Information Rights Management
- SMIME
- Office 365 Message Encryption
- Azure Information Protection
- Windows Information Protection

* Data Loss Prevention (DLP)
- Was ist DLP?
- DLP Policies
- Policy Tips
- Managed Properties

* Cloud Application Security
- Cloud App Security verstehen
- Cloud App Security einrichten
- Policies für Cloud Apps
- Der Cloud App Catalog einrichten
- Das Cloud Discovery Dashboard
- Cloud App Berechtigungen

4. Tag: MS-500T04: Administering Microsoft 365 Built-In Compliance
* Archivierung und Aufbewahrung
- Archivierung in M365
- Retention in M365
- Retention Policies im Security und Compliance Center
- Archivierung in Exchange
- Records Management in SharePoint

* Datenschutz und Microsoft 365
- Planung von Security und Compliance
- Ethical Walls in Exchange Online
- DSGVO/GDPR mit Microsoft 365
- Analytics und Telemetrie

* Informationssuche und Beweissicherung
- Contentsuche im Security Center

Azure ist Microsofts Cloud-Computing-Plattform mit dem Cloud-Betriebssystem Windows Azure und anderen Diensten wie SQL Azure oder AppFabric.

Ihr Nutzen

Im diesem Seminar erlernen Teilnehmer die Kenntnisse um Security Policies zu implementieren, Schwachstellen zu identifizieren und zu beheben. Das Seminar beinhaltet Scripting-Technologien for Automatisierung, Virtualisierung und Cloud N-Tier Architekturen.

Voraussetzungen

Azure Administering~9656

oder dem entsprechende Kenntnisse

Preis pro Teilnehmer

EUR 2450,- exklusive der gesetzlichen MwSt.

Seminardauer

4 Tag(e)/Day(s)

Hinweise

AZ-500T00,

Version: N/A

Seminarinhalte

1. Tag
* Identity and Access
- Understand the Zero Trust Model
- Configure Azure AD PIM
- Configure Azure AD for Azure Workloads
- Security for an Azure Subscription

2. Tag
* Implement Platform Protection
- Understanding Cloud Security
- Azure networking
- Secure the network
- Implementing host security
- Implement platform security
- Implement subscription security

3. Tag
* Secure Data and Applications
- Configure security policies to manage data
- Configure security for data infrastructure
- Configure encryption for data at rest
- Understand application security
- Implement security for application lifecycle
- Secure applications

4. Tag
* Manage Security Operations
- Configure Security Services
- Configure security policies using Azure Security Center
- Manage security alerts
- Respond to and remediate security issues
- Create security baselines

>> Microsoft Intune

Modern Device Management mit EndPoint Manager

Microsoft Endpoint Manager ist die Cloud-Lösung von Microsoft zur Verwaltung von Endgeräten wie Windows 10, IOS und Android Geräten.

Ihr Nutzen

Nach dem Seminar können Sie Endgeräte registrieren und verwalten. Im Workshop wird Applikations-Management, Conditional Access, Compliance Policies, Co-Management und Autopilot behandelt.

Voraussetzungen

Kenntnisse von Active Directory und Azure AD von Vorteil.

Preis pro Teilnehmer

EUR 1550,- exklusive der gesetzlichen MwSt.

Seminardauer

3 Tag(e)/Day(s)

Hinweise

MS-101, basierend auf Original Microsoft Training.

Version: 2020

Seminarinhalte

1. Tag
* Überlick Endpoint Management
- Funktionen und Architektur
- MDM vs. MAM Funktionalität

* Device-Enrollment
- Windows Enrollment
- Unternehmens-Portal
- Konfiguration von Hybrid-Join
- Intune Connector für Active Directory
- Lokales Management (CmdLine, EventLog)
- IOS und Android Enrollment
- Geräte-Management und Remote-Aktionen

* Geräte-Gruppen erstellen
- Statische und dynamische Gruppen

* Device Compliance
- Compliance Policies erstellen und zuweisen
- Monitoring von Device Compliance

* Configuration Profiles
- CSPs verstehen
- VPN, Wi-Fi,
- Zertifikate und NDES Connector
- Administrative Templates
- Überblick Endpoint Protection

2. Tag
* PowerShell Scripts in Endpoint Manager

* Endpoint Security
- Windows Defender Antivirus
- Bitlocker verwalten
- Bitlocker Self-Service Portal
- Firewall-Konfiguration

* Conditional Access
- Zuweisung
- Conditions
- Access Controls

* Enterprise Apps
- Platform Apps bereitstellen
- Store Apps bereitstellen
- Integration in Windows Store for Business
- Required vs Assigned
- App Configuration Policies
- Office Policies
- App Protection Policies

3. Tag
* Co-Management
- Einrichtung in MECM/SCCM
- Registrierung von CM Devices
- Registrierung von Intune Devices in CM
- Der MECM Cloud Management Gateway

* Windows Autopilot
- Autopilot Profiles erstellen
- Device Import und Zuweisung
- White Glove Deployment
- SCCM Autopilot Task Sequences

* Monitoring und Reporting
- Trends
- Überblick Log Analytics

* Advanced Topics
- Cloud App Security einrichten und konfigurieren
- Advanced Threat Analytics
- Windows ATP Konfiguration

>> Trend Micro Office Scan, Scan Mail Exchan

Workshop

Trend Micro Office Scan und Scanmail für Exchange ist die Office-Anti-Virus/Anti Malware Lösung von Trend Micro.

Ihr Nutzen

Die Teilnehmer werden mit den Kenntnissen und Fertigkeiten vertraut, die für die Installation, Konfiguration und Administration der Trend Micro-Produkte benötigt werden.

Voraussetzungen

Grundkenntnisse von Betriebssystem und Netzwerken.

Preis pro Teilnehmer

EUR 1250,- exklusive der gesetzlichen MwSt.

Seminardauer

2 Tag(e)/Day(s)

Hinweise

Dieses Seminar wird zusammen mit einem zertifizieten Trend-Micro Trainingspartner durchgeführt.

Version: N/A

Seminarinhalte

1. Tag
* OfficeScan
- Produkt-Architektur
- Installation und Konfiguration
- Verwalten von OfficeScan
- Scan Resultate und Log Files
- Fehlerbehebung

2. Tag
* ScanMail für Exchange
- Produkt-Architektur
- Installation und Konfiguration
- Verwaltung
- Fehlerbehebung

* Trend Micro Control Manager
- Installation und Konfiguration
- Produkt-Architektur
- Verwaltung
- Log Files
- Fehlerbehebung

>> Windows 10
Client Security Deep Dive

Windows 10 hat sehr viele Sicherheitsfunktionen im Betriebssystem eingebaut. Nutzen Sie diese um Ihre Client Infrastrukturen sicherer gegenüber modernen Angriffsvektoren zu machen.

Ihr Nutzen

In diesem Workshop erfahren Sie alles über die Konfiguration der Windows 10 Sicherheitsfunktionen. In vielen praktischen Übungen erlernen Sie den Umgang und die Best-Practices der Windows 10 Security Features.

Voraussetzungen

Windows 10 Implementing & Managing~8522

oder dem entsprechende Kenntnisse

Preis pro Teilnehmer

EUR 1150,- exklusive der gesetzlichen MwSt.

Seminardauer

2 Tag(e)/Day(s)

Hinweise

MOC40554,

Version: N/A

Seminarinhalte

1. Tag
* Security Thread Landscape
* Übersicht Schutz-Optionen

* Device Protection
- Windows Defender SmartScreen
- Windows Defender Sandbox
- SRP and Applocker
- Virtualization Based Security (VBS)
- Hypervisor Code Integrity (HVCI)
- Windows Defender Application Control (WDAC)
- Device Guard

* Hardware Assisted Protection
- UEFI Secure Boot
- Early Launch Antimalware
- Device Health Attestation (DHA)
- Control Flow Guard (CFG)
- Windows Event Forwarding (WEF)

* Memory Attacks
- Data Execution Prevention (DEP)
- Structured Exception Handling Overwrite Protection (SEHOP)
- Address Space Layout Randomization (ASLR)
- Process Migitation Options via GPO
- Process Migitation PowerShell Module

* Identity Protection
- Credential Guard

2. Tag
* Information Protection
- Enterprise Certificate Pinning
- Windows Defender Antivirus
- Font Blocking

* Build into the Kernel
- Kernel Pool Protections
- Protected Processes
- UWP Applications Protection
- Heap Protection

* Network List Manager Policies

* Security Policies
- Account Policies
- User Rights Assignment
- Auditing and Advanced Auditing

* Security Compliance Manager
* Security Compliance Toolkit Baselines

* AlwaysOnVPN Konfiguration
- Network Design
- CSP Konfiguration
- PowerShell Konfiguration

>> Windows Server

PKI Design, Implementation and Maintainance

Unternehmensnetzwerke benötigen in vielfältigen Anwendungen (EFS, SmartCard-Logon, VPN, Lync, SSL, IPSec) Zertifikate und eine Infrastruktur um diese sicher im Unternehmen zu verwalten.

Ihr Nutzen

Sie können eine Public Key Infrastructure planen und erstellen. Ebenso wissen Sie um die Vorteile einer "Certification Authority" Bescheid und können etwaig auftretende Probleme beseitigen. Die Verteilung, Planung, Revokation von Schlüsseln in Unternehmens-umgebungung ist ein Schwerpunkt des Seminars. Praktische Tips aus Projekten runden das Thema ab.

Preis pro Teilnehmer

EUR 2450,- exklusive der gesetzlichen MwSt.

Seminardauer

4 Tag(e)/Day(s)

Voraussetzungen

Windows Server Administration (2012/2016)~8779

oder dem entsprechende Kenntnisse

Hinweise

Version: 2019

Seminarinhalte

1. Tag
* Einführung in Kryptographie
- Methoden und Techologien
- Algorythmen und Keys
- Encryption und Signing
- Public Key Infrastructures
- Begiffe CRL, CRT, AIA
- Zertifikate und "Certification Authorities"
* Entwerfen einer "Certification Authority" Hierarchie
- Identifizieren notwendiger CA Entwurfselemente
- Analysieren von Entwurfsbedingungen

2. Tag
* Erstellen einer "Certification Authority" Hierarchie
- Erstellen einer Offline-CA
- Überprüfen von Zertifikaten
- Planen einer untergeordneten/subordinate CA
- Multi-Tier CAs
* Verwalten der Windows PKI Komponenten
- Verwalten von Zertifikaten (Revoke, Renew, etc.)
* Verwalten von CA's
- Certification Practice Statement (CSP)
- CRL und AIA Distribution via LDAP/AD/HTTP
- Role Separation
- CAPolicy.inf und erweiterte CA Einstellungen
* Erstellen und Verwalten von Zertifikatsvorlagen

3. Tag
* Online Certificate Status Protocol (OCSP)
* Zertifikats-Verteilung
- Manuelle Verteilung
- Automatische Zuweisung (AutoEnrollment)
- Web-Enrollment
- Online Responder Service
- Webservices für Enrollment und Policy Enrollment
- Network Device Enrollment Service (NDES)
- Verteilung von Smart Card Zertifikaten
- Inside X509 Certificates

4. Tag
* Key Archiv
- Erstellen und Verwalten des Archivs
- Wiederherstellung
* Command-Line Werkzeuge
- certutil und certreq
- PowerShell Cmd-Lets für CA-Management
- PowerShell cert: Drive
* Erstellen von Trusts zwischen Organisationen
- Erweiterte PKI Hierarchien
- Trusts mit Einschränkungen: Qualified Subordination
* Unterstützung von Smart Cards
- Authentication against AD, VPN, 802.1x
* Sicherer Webzugang mit SSL
- Aktivieren von SSL auf einem Web Server
- Zertifikat basierte Authentifizierung
* Konfiguration der Sicherheit für E-Mails
- Wiederherstellen von privaten Schlüsseln für E-Mail
* Entwerfen einer Wiederherstellungsstrategie
* Disaster Recovery

Windows Server 2016 ist die On-Premise und Cloud Betriebssystem des Microsoft Ecosystems.

Ihr Nutzen

Nach diesem Seminar sind Sie in der Lage Windows Server 2016 Umgebungen nach Security-Aspekten zu konfigurieren. Sie erkennen Angriffs-vektoren und können Maßnahmen zum Schutz der Infrastruktur ableiten und konfigurieren.

Voraussetzungen

Gute Administrationskenntnisse inkl. Netzwerk und Active Directory in Windows Server 2016

Preis pro Teilnehmer

EUR 2550,- exklusive der gesetzlichen MwSt.

Seminardauer

5 Tag(e)/Day(s)

Hinweise

MOC20744,

Version: 2019

Seminarinhalte

1. Tag
* Einbrüche, Attacken und Vektoren erkennen
- Angriffstypen, Cybercrime und Vektoren
- Verwenden der Sysinternals Tools

* Benutzer-Rechte, Security Optionen und Service Accounts
- Verstehen von Benutzer-Rechten
- Computer und Service-Accounts
- Priviledged Access Workstations und Jump Server
- Local Admin Password Solutions (LAPS)
- Restricted Groups, GMSAs
- Credential Guard konfigurieren

2. Tag
* Beschränkung von Administrations-Rechten
- Verstehen von Just-Enough-Administration (JEA)
- Konfiguration von JEA
- Role und Session Configuration Files
- JEA Endpoints erstellen
- Verteilen von JEA mit DSC

* Priviledged Access Management und Admin-Forests
- Enhanced Security Administrative Environment (ESEA)
- Microsoft Identity Manager (MIM)
- Just In Time (JIT) Administration
- Layered Security Approach

3. Tag
* Schutz vor Malware und anderen Threats
- Windows Defender konfigurieren
- Software-Restriction Polices und AppLocker
- Device Guard verwenden

* Analyse von Aktivitäten
- Überblick über Windows Server Auditing
- PowerShell Auditing und Logging
- Advanced Audit Policies

4. Tag
* Microsoft Advanced Thread Analytics
- Überblick über ATA
- Verstehen der Operations Management Suite (OMS)
- Konfiguration von ATA und OMS

* Virtuelle Umgebungen und Infrastrukturen schützen
- Guarded Fabric VMs mit Administrator-Trusted Attestation
- Shielded und Encryption-Supported VMs

* Schützen von Developer und Server-Workloads
- Security Compliance Manager
- Nano-Server und Container nutzen

* Datenschutz durch Verschlüsselung
- Deployment von EFS und BitLocker

5. Tag
* Schutz von Files und Foldern
- File Server Resource Manager (FSRM)
- DFS nutzen, File Screening
- Dynamic Access Control einsetzen

* Konfiguration der Windows Firewall
- Inbound/Outbound Rules konfigurieren
- SD Distributed Firewalls

* Netzwerk-Traffic absichern
- Connection Security Rules
- Advanced DNS Settings
- Verwenden des Message Analyzers
- SMB traffic absichern
- DNSSEC konfigurieren

* Patching von Windows Server
- WSUS Konfiguration

>> Security & Risk Control

EGOS! the education company

Informationstechnologie

Sie möchten den aktuellen Sicherheitszustand Ihres Unternehmens überprüfen und verbessern, sowie nach Sicherheitsvorfällen schnell und richtig reagieren?

Die Informationssicherheit eines Unternehmens erfordert immer die unabhängige Prüfung von außen. Nur so können Sie Fehler die durch Betriebsblindheit entstehen vermeiden beziehungsweise aufdecken.

Mit unseren Dienstleistungen können Sie Leistungen in den Bereichen

- Security Check / Penetration Test
- ISO 27001 Etablierung
- Security Awareness Programme
- Server Hardening
- Code Hardening
- Firewall Rule Check
- Press Communication
- IT Forensics

Kostengünstig und modular vergeben.

Damit können Sie nur Teile oder auch Ihr gesammtes Unternehmen inklusive aller Abläufe auf Sicherheitsmängel überprüfen.

Wir stellen Ihnen ausgewiesene Information Security Experten zur Seite die mit Ihnen gemeinsam ein passgenaues Angebot an Security Dienstleistungen zusammenstellen.

Am Ende jeder unserer Security Dienstleistungen steht ein Dokument mit expliziten Handlungsempfehlungen. Selbstverständlich werden alle während der Sicherheitsdienstleistungen in Erfahrung gebrachten Informationen höchst vertraulich behandelt.

Ihr Nutzen

Information

Sie erhalten klare Informationen über Ablauf, dauer und Endprodukt Ihres Security Dienstleistungs Pakets.

Transparenz

Unsere Security Fachleute sind auf dem aktuellsten Stand der Technik, was Sie durch adequate Sicherheitszertifizierungen nachweisen können.

Ganzheitlich

Für uns endet Security nicht bei der Überprüfung Ihrer Website. Auf Wunsch wird die gesamte Informationssichereit vom Prozessor bis zum Unternehmensprozess überprüft.

Erfahrung

Viele Kunden unterschiedlichster Unternehmensgrößen die von uns betreut wurden sprechen für die Erfahrung unserer Security Berater

Unabhängigkeit

Nur wer unabhängig von Betriebsblindheit und eigenem Nutzen agiert ist wirklich in der Lage Ihre Informationssicherheit zu bewerten.

5 Gründe für eine Partnerschaft mit uns:

Wir weisen nicht nur über zehn Jahre Erfahrung im IT-Consulting auf, sondern vermitteln Ihnen auch fundiertes Basiswissen.

Wir geben Ihnen nicht nur konkrete Vorschläge für die Umsetzung, sondern erarbeiten gemeinsam mit Ihnen die optimale Lösung und begleiten Sie auch bei Implementierung und Betrieb des Systems.

Die Zusammenarbeit verschiedener Teams erhöht die Akzeptanz einzuführender IT Lösungen.

Ihr Projektrisiko wird durch objektive externe Betrachtung minimiert.

Der sichere Umgang mit neuen Technologien ermöglicht die schnelle Reaktion auf neue Geschäftsanforderungen. Dafür garantieren unsere vom Hersteller zertifizierten Berater.

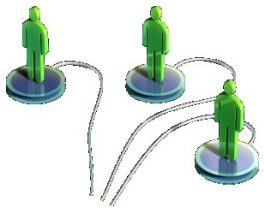
Dabei können wir Sie unterstützen:

	Management	IT-Administratoren	Entwickler	Anwender	Pressesprecher
Preventative Controls – Vorbeugende Maßnahmen ergreifen					
Code Hardening			■		
Server Hardening		■			
Awareness Programme	■			■	■
Detective Controls – Sicherheitsrisiken erkennen					
ISO 27001 Einführung	■				
Penetration Test		■	■		
Awareness Test	■			■	■
Firewall Rule Check		■			
Process Audit	■	■	■	■	■
Corrective Controls – Regeneration nach Sicherheitsvorfällen					
IT Forensics	■	■	■		■
Press Communication	■				■

>>Security Awareness Programme

EGOS! the education company

Organisationen werden heute von unterschiedlichen Seiten angegriffen. Hacker, Viren und Würmer bedrohen Unternehmens-Assets von außen, Sozial Engineers und demotivierte MitarbeiterInnen bedeuten eine Gefahr von Innen. Die Einführung eines Security Awareness Programms soll den Security Gedanken in das tägliche Arbeiten der MitarbeiterInnen bringen, ohne Diese zu behindern.



Social Engineering	Social Networking	Security Policies		Physical Security		Helpdesk	PC Security	Backup
E-Mail, Instant Messaging	Mobile Devices	Data Security	Security Awareness	Home-Office	Incidents	IT Team	User	Social Media
Internet	Passwords	Data Destruction	Encryption	Insider	WI-FI	Home-Office	Cloud	Document Classif.

Möglicher Ablauf zur Einführung

Analyse
- Ziele
- Bedrohungen
- Rahmen-bedingungen
- Umfang & Zeitplan
- Angriffe

Akzeptanz
- MitarbeiterInnen
- Führungskräfte
- Bezug zu Strategien
- Kultur
- Widerstände

Umsetzung
- Seminare
- E-Learning
- WebCasts
- Materialien
- ....

Transfer
- Angriffe
- Evaluierung
- Hotine
- Coaching
- ...

1. **Risikoanalyse (Initial Workshop):** Es werden mögliche Bedrohungen erhoben, Zeitrahmen, Methoden sowie budgetäre Mittel festgelegt. Die Unternehmenskultur ist bei der Auswahl der Aktivitäten zu beachten.
2. **Simulation von Social Engineering Angriffen:** Mögliche Aktivitäten könnten illegales Betreten der Organisation, Anrufe, Mails, Platzierung von Fremdgeräten etc. sein. Zusätzlich werden die Security Policies sowie sonstige relevante Richtlinien und Dokumente geprüft.
3. **Umsetzung Security Awareness Programm:** Die Ergebnisse der Angriffe werden ausgewertet. Basierend auf den Erkenntnissen wird ein passendes Programm erstellt:
4. **Transfersicherung:** Einige Zeit nach Durchführung der Aktivitäten werden erneut ähnliche *Angriffe* wie am Beginn durchge-

Richtlinien	Training	Kommunikation	Marketing
•Policies	•Seminare/Workshops	•Veranstaltungen	•POI's nutzen
•Compliance	•Webinare/Web-Cast's	•Videos	•Broschüren
•Datenklassifizierung	•E-Learning	•Infoportale	•Give Aways
•Rollenbeschreibungen	•IT-Team	•Intranet/Foren	•Screensaver
•Arbeitsverträge	•Datenschutzbeauftr.	•Wiki's / Blogs	•Firmenzeitungen
•Anweisungen	•Sicherheitsbeauftr.	•Mobile App's	•Infoscreens
	•Führungskräfte	•Mails/Umfragen	•Poster

führt. Die Ergebnisse der Angriffe werden korreliert und die entsprechenden Schritte für ein *nachhaltiges Programm* gesetzt.

Training der MitarbeiterInnen in Seminaren

- Informationssicherheit für Anwender, Grundlagen: http://www.egos.co.at/go/agenda/4238
- Datenschutz I: Grundlagen: http://www.egos.co.at/go/agenda/8079
- Datenschutz II: Praxisumsetzung in Organisationen: http://www.egos.co.at/go/agenda/8080
- Datenpannen: Bedrohung und Handling: http://www.egos.co.at/go/agenda/7462
- Betrug und kriminelle Aktivitäten in der IT: http://www.egos.co.at/go/agenda/7461

Training der MitarbeiterInnen mit E-Learning

Ein nachhaltiges Security Awareness Programm unterstützen wir mit der Lernsoftware Virtual Training Company. Die 3D-Software unterstützt MitarbeiterInnen beim Erlernen und Ausüben von Sicherheitsstandards und Richtlinien. Sie trainieren interaktiv und multimedial ausgewählte Lerninhalte zu Security Awareness-Themen. Dabei navigieren die Mitarbeiterinnen nachweislich durch ein virtuelles Unternehmen, in welchem kontextbezogen verschiedene Inhalte mit Hintergrundinformationen, Beispielen und Trainingsszenarien untergebracht sind.

Schauplätze sowie die Lerninhalte der Virtual Training Company sind auf Wunsch an die Optik und Corporate Identity des Unternehmens anpassbar und voll konfigurierbar. Die 3D-Software ist die derzeit innovativste Lösung, um Security Awareness nachhaltig zu vermitteln und das Sicherheitsbewusstsein der MitarbeiterInnen entscheidend zu stärken.

Mögliche Intensität eines Programms

② Schwerpunkt Compliance	③ Awareness & Change	④ Nachhaltigkeit
Das geplante Programm konzentriert sich auf Anforderungen für Compliance oder Zertifizierungs-Audits. Trainings werden sporadisch angeboten. Die Wichtigkeit von Sicherheitsrichtlinien für den Schutz von Unternehmensdaten ist Mitarbeitern zwar bekannt, wird aber nur wenig umgesetzt.	Das Programm hat große Auswirkungen auf die Unternehmensziele und fokussiert die Trainingsmaßnahmen darauf. Neben regelmäßigen Trainingsmaßnahmen werden laufen Maßnahmen zur Festigung der Richtlinien durchgeführt. Die Inhalte werden in unterschiedlichen Kanälen kommuniziert sodass das Verhalten von Mitarbeitern am Arbeitsplatz, zu Hause und auf Reisen positiv beeinflusst wird. Als Ergebnis verstehen Mitarbeiter die Sicherheits-Richtlinien, befolgen diese und tragen aktiv zur Umsetzung bei.	Das Programm definiert Prozesse im Rahmen einer langfristigen Umsetzung. Als Minimum werden ein jährliches Review und eine Aktualisierung der Inhalte und der Kommunikationskanäle durchgeführt. Sicherheits-Richtlinien sind Teil der Unternehmenskultur und sind auf dem aktuellen Stand.
• Welche Standards muss das Unternehmen erfüllen? • Welche Anforderung an Security Awareness fordert der Standard? • Entwicklung oder Anschaffung von Trainingsinhalten (Online oder Classroom) • Messung der Trainingsergebnisse (Wer hat das Training besucht?)	• Definition der Projektbeteiligten • Erhebung des IST-Zustandes (siehe Messkriterien) • Erstellen eines Projektplans mit den Verantwortlichen: Kostenrahmen, Anwendungsbereiche (Geschäftsbereiche, Abteilungen), Meilensteinen und Annahmen • Freigabe des Projektplans durch das Management • WER ist die Zielgruppe des Programms? z.B.: MitarbeiterInnen, Service-Desk, IT Administratoren, Entwickler, Führungskräfte • WELCHE Inhalte sind für welche Zielgruppe relevant? Erstellen Risikomatrix / Priorisierung Themenbereiche • WIE wird der Inhalt kommuniziert? Wesentlich ist die Unterscheidung in Vermittlung von Inhalten und Transfermethoden. Inhaltsvermittlung können Präsenztraining oder Webinare sein. Zur Transfersicherung sind Newsletters, Poster, PodCasts, Assessments und Blogs denkbar. • Erstellen eines Durchführungsplans mit Zeitplan. • Vorstellung des Zeitplans im Management	• Definition der Zeitpunkte an denen eine Überarbeitung erfolgt • Auflistung von neuen oder geänderten Technologien, Bedrohungen, Geschäftsanforderungen oder geänderten Standards • Erhebung der Kennzahlen aus Phase 3 • Umfrage bei Mitarbeitern, welche Inhalte am besten angekommen sind und wo Änderungsbedarf besteht • Prüfung aller Dokumente und Inhalte die kommuniziert werden. • Aktualisierung der zu ändernden Inhalte und Dokumente • Aktualisierung der Projektplans • Kommunikation der geänderten Inhalte
• Trainings-Inhalte • Teilnahme-Dokumentation	• IST Zustand samt KPIs • Projektplan • Inhalts-Matrix • Zielgruppen-Matrix • Management-Präsentation	• Änderungsprotokoll (Was wurde von wem wann geändert?)

Mögliche Messbarkeit eines Programms

Das Programm setzt auf Kennzahlen, die laufend kontrolliert werden:

- Definition der Kennzahlen, die gemessen werden sollen
- Dokumentation wie und wann die Messwerte erhoben werden.
- Wer wird über die Messwerte informiert? Wo werden Diese dargestellt?
- Anzahl Personen mit Phishing Attacken
- Anzahl der gemeldeten Security Incidents
- Anzahl der infizierten Systeme
- Anzahl Personen, die das Awareness Training absolviert haben
- Anzahl unsichere Kennwörter u.v.a.m.

Investitionsparameter

Maßnahme	Kosten pro Maßnahme	Multiplikator	Grund-lagen	Nach-haltigkeit
Initial-Workshop - Festlegen Themenbereiche - Auswahl Kommunikation und Terminplan/Häufigkeit - Bereitstellung von Werkzeugen - Festlegen der Kennzahlen	€ 1.600,-	pro Tag	X	
Simulation von Social Engineering Angriffen (20 Angriffe)	€ 2.500,-	pro Simulation	X	
Erarbeiten Security Richtlinien (ca. 1,5 Tage)	€ 1.200,-	pro Tag	X	
Erarbeiten Dokumentklassifizierung (ca. 1,5 Tage)	€ 1.200,-	pro Tag	X	
Vorstellung des Programms in Veranstaltung (bis ca. 100 Personen)	€ 1.200,-	pro Tag	x	
Vorstellung des Programms bei Führungskräften (ca. 0,5 Tage)	€ 1.200,-	pro Tag	X	
Security Awareness Seminar für AnwenderInnen (ca. 1 Tag)	€ 1.200,-	pro Tag	X	
Security Awareness Seminar für IT MitarbeiterInnen (Ca. 3 Tage)	1.600,-	pro Tag	X	
Security Awareness E-Learning Lizenz	ca. € 50,-	pro Mitarbeiter	X	
Erstellen Broschüre, Aufsteller, 2xA4 Seite (2 Varianten / 1 Review)	€ 350,-	pro Dokument	X	X
Druck-Kosten Broschüre, Aufsteller	ca. € 10,-	pro Broschüre		
Erstellen Poster in A1/HD oder Rollup (2 Varianten / 1 Review) Input Auftraggeber: Themenbereich, 3-5 Stichworte, Basis-Design/Corporate Design	€ 350,-	pro Poster		x
Druck-Kosten Poster Größe A1 ohne Rahmen	ca. € 50,-	pro Poster		X
Produktions-Kosten Rollup	ca. € 150,-	pro Rollup		X
Erstellen Awareness Video	n. Aufwand	pro Video		
Vorschlag und Auswahl eines Giveaways (2-3 Vorschläge)	€ 350,-	pro Giveaway		X
Produktions-Kosten Giveaway	n. Aufwand	pro Giveaway		X
Erstellen Artikel für Firmenzeitung (Größe ca. ½ Seite) Input Auftraggeber: Themenbereich, 3-5 Stichworte, Basis-Design/Corporate Design	€ 400,-	pro Ausgabe		X
Wartung Informations-Portal mit gelieferten Inhalten (2 Inhalte pro Monat) Input Auftraggeber: Themenbereich, 3-5 Stichworte	€ 800,-	pro Monat		x
Gestaltung, Wording und Versand Newsletter Input Auftraggeber: Themenbereich, 3-5 Stichworte SMTP Zugang erforderlich	€ 400,-	pro Newsletter		X
Erstellen Blog-Eintrag Input Auftraggeber: Themenbereich, 3-5 Stichworte Remote-Zugang zu Blog erforderlich	€ 400,-	pro Artikel		X
Weitere Workshops für: • Abstimmung mit Auftraggeber • Redaktionssitzungen für Kommunikation • Update von Content • Qualitätssicherung • Weiterentwicklung etc.	€ 1.600,-	pro Tag	x	x

Alle Preise verstehen sich als Richtwerte exkl. USt. und evtl. anfallender Reisekosten von TrainerInnen / BeraterInnen

>>EGOS! Comprehensive Security & Functionality Check

*Wenn die Fähigkeit einer Organisation **Informations- oder IT-Sicherheit** zu implementieren, Dritten gegenüber bewiesen werden muss (z.B. Kunden, internen oder externen Auditoren) oder intern auf Basis eines pragmatischen Ansatzes getestet werden soll, ist es empfehlenswert einen **Sicherheitstest** anzuwenden, der generisch genug ist, dass er an die Bedürfnisse der Organisation und des Audits angepasst werden kann.*

Die hier im Weiteren dargelegte Vorgangsweise kann auch unter dem Aspekt der **Funktionalitätsüberprüfung** (Validierung oder Audit) einer IT-Landschaft angewendet werden, sodass diese Aspekte vorrangig vor reinen Informations- oder IT-Sicherheitsaspekten behandelt werden. Ein generischer Sicherheitstest behandelt alle wesentlichen Aspekte von Informations- und **IT-Sicherheit in Hinblick auf die Informationswerte** der betrachteten Organisation.

Wir bieten dazu den Comprehensive Security & Functionality Check an, der aus ISO27001, anderen relevanten Standards des Risiko- und Continuity Managements sowie einem Schichtenmodell zusammengesetzt wurde.

Der Comprehensive Security & Functionality Check ist ein Ergebnis kontinuierlicher Forschung nach verbesserten Test- und Auditmethoden und kombiniert technische und organisatorische Zugänge aus internationalen, generischen und branchenspezifischen Standards und Best Practice. Zur Implementierungsreife gelangt im Jahr 2002 wurde der Comprehensive Security & Functionality Check seither in zahlreichen Organisationen und Unternehmen von 100 bis 2000 Mitarbeitern eingesetzt.

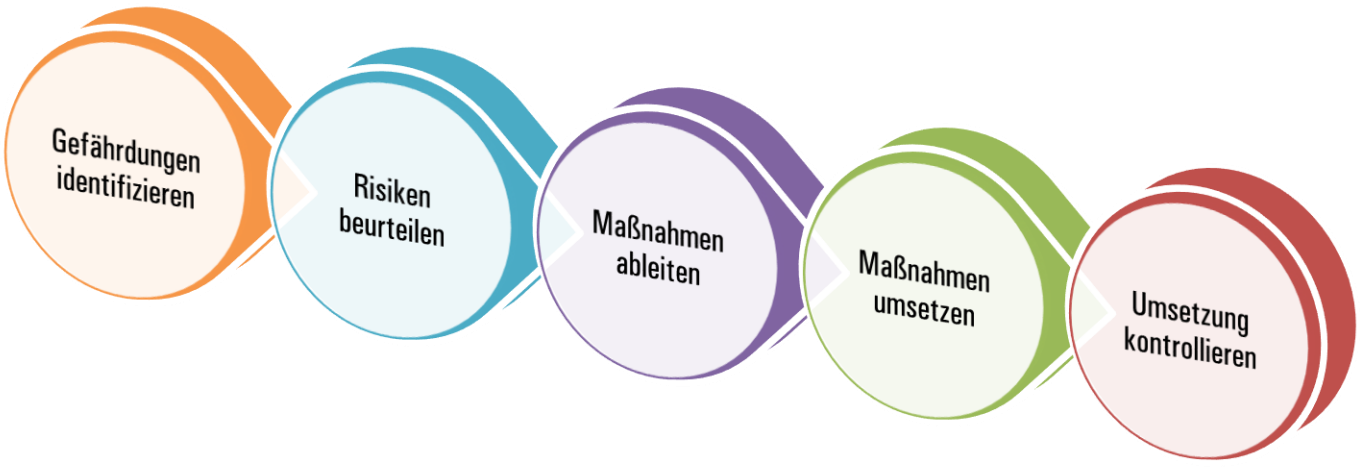
Ein CSFC kann wirkungsvoll eingesetzt werden, wenn

- die **Funktionalität** von IT-Abläufen Bezug nehmend auf IT-Betriebsabläufe oder Geschäftsprozesse geprüft werden sollen.
- die **Informationssicherheit** eines Unternehmens ganzheitlich betrachtet werden soll.
- punktgenau **Verbesserungspotential** auf den funktionellen Ebenen des CFSC festgestellt werden soll.

Tipp

Der CSFC ist als Baustein auf dem Weg zu einer ISO27001 Zertifizierung verwendbar. Der Ergebnisreport kann als Nachweis der Basis-Sicherheitschecks verwendet werden.

Version 14-06.08.15



>>EGOS! Comprehensive Security & Functionality Check

EGOS! the education company

Der EGOS! Comprehensive Security & Functionality Check (CSFC)

Im Rahmen eines CSFC wird das Unternehmen in funktionelle Schichten „geteilt“, auf denen sich jeweils sehr spezifische Funktionalitäts- und Sicherheitsfragen stellen, die im Rahmen einer **ganzheitlichen Betrachtung** berücksichtigt werden müssen, um sicherzustellen, dass **Betriebsabläufe oder Geschäftsprozesse** effektiv, effizient und ihrer definierten Funktionalität entsprechend ablaufen können.

Funktionelle Schichten des CSFC

Im Zuge des Testes werden diese fünf Schichten nunmehr ausgehend von einer Definition des Betriebsablaufs oder Geschäftsprozesses vertikal durchlaufen, sodass in jeder Schicht die Tragfähigkeit der bereits existierenden Maßnahmen gegenüber definierten Anforderungen überprüft werden kann.

Layer	Schicht	Teilbereiche (Auszug)	Testing
 **5**	Prozesse	Geschäfts- und IT-Prozesse	internal
		Security Management	internal
		Backup- und Notfall-Strategien	internal
		ITIL-Konformität	internal
 **4**	Applikationen	Web-Seiten und Web-Applikationen	internal/external
		E-Commerce Lösungen	internal/external
		Communication & Collaboration	Internal/external
		ERP/CRM	internal
 **3**	Hardware Betriebssysteme	Servers (Betriebssysteme, Applikationsserver,..)	internal/external
		Clients (PC’s, Mobile Devices, Antivirus,…)	internal/external
		Large Scale Systems	internal/external
		Cloud Security	internal/external
 **2**	Networking	Network Devices (Routers, Switches, Firewalls, Access Points,…)	internal/external
		Network Infrastructure (DMZ, WAN, Internet,…)	internal/external
 **1**	Physical Security	Zutritt zu Räumen & Zutritts-Kontrollen	external
		Überwachung und Monitoring (Loging, Brand, Wasser, Notfallpläne,..)	internal
		Benutzerverhalten, Benutzerrichtlinien	internal/external

>>EGOS! Comprehensive Security & Functionality Check

Worin liegt der Nutzen eines CFSC?

Nutzen auf organisatorischer Ebene	Nutzen auf technischer Ebene
▪ Eine klare strategische Übersicht über Möglichkeiten, Geschäftsprozesse in Hinblick auf Informationssicherheit oder Funktionalität zu verbessern. ▪ Identifizierung organisatorischer Risiko und Bedrohungsfaktoren bzw. Rückkopplungsaussage über den Einfluss von technischen oder sicherheitstechnischen Störungen auf die untersuchten Geschäftsprozesse oder Betriebsabläufe.	▪ Bestimmung des Grades physikalischer Sicherheit für Informationswerte. ▪ Detaillierte Sicherheitsstudie über Sicherheitsrisiken, Bedrohungen und technische Schwachstellen (Vulnerabilities) sowie organisatorische Sicherheitsprobleme. ▪ Genaue Dokumentation der IT Umgebung auf OSI-Schichten 2, 3 und 7 (falls notwendig) ▪ Dokumentierte Bestimmung von Abhängigkeiten in der IT Landschaft, die in kritischen Situationen reduzierter Verfügbarkeit, Vertraulichkeit oder Integrität unterstützend zur Problemlösung verwendet werden kann. ▪ Bei Rückkopplungstests: Bestimmung der Funktionsfähigkeit von technischen Betriebsabläufen und deren genaues Auswirkungspotential im Störungsfall in Hinblick auf die vorgelagerten Geschäftsprozesse.

Ablauf eines Comprehensive Security & Functionality Checks

Ein CSFC wird in den folgenden Schritten ausgeführt

Aufwände für einen CSFC

Basierend auf unserer Implementierungserfahrung können die folgenden Werte angenommen werden:

Service Modul	Dauer (Personentage)		
	Minimum	Maximum	Multiplikator
Bestimmung Organisatorischer Umfang	0,5 Tage	2 Tage	Anzahl Standorte & Prozesse
Bestimmung Technischer Umfang	0,5 Tage	2 Tage	Anzahl Systeme
Risikoanalyse – und bewertung (optional)	0,5 Tage	2 Tage	Branche, Risiken
Durchführen der organisatorischen Tests	1 Tag	3 Tage	Anzahl Systeme
Durchführen der technischen Tests	1 Tag	5 Tage	Anzahl Systeme
IT System Abhängigkeitstest (optional)	1 Tag	5 Tage	Anzahl Systeme
Berichterstellung und Präsentation	1 Tag	2 Tage	Anzahl Findings
Erneute Tests nach Umsetzung der Maßnahmen (optional)	1 Tag	3 Tage	Anzahl Findings
Gesamtdauer	**5 Tage**	**24 Tage**	

Alle Service Module können unabhängig voneinander bestellt und ausgeführt werden mit Ausnahme des Moduls zur Umfangsbestimmung, das vor allen anderen ausgeführt werden muss.

Die maximale Dauer zur Ausführung eines einzelnen Moduls hängt von den genauen inneren, zuvor erfassten, Gegebenheiten ab und muss, abhängig vom Umfang, mit den jeweiligen Multiplikatoren multipliziert werden, um die Gesamtdauer zu erhalten. Die im Rahmen von Angebotsgesprächen oder bei besonders komplexen Projekten im Rahmen des allerersten Projektschritts durchgeführte genaue Umfangsuntersuchung liefert typischerweise die genauen anzuwendenden Maximalwerte.

Anwendungsbeispiel

Eine Organisation mit einem Standort, 3 kritischen Geschäftsprozessen und 5 Systemen benötigt Dienstleistungen zwischen 7,5 und 10 Personentagen; inklusive Dokumentation und Abhängigkeitsanalyse werden zwischen 10 und 20 Personentage benötigt. Der tatsächliche Wert wird durch den Projektteil Umfangsbestimmung festgelegt.

Auf Grund seiner modularen Struktur und seines ganzheitlichen Ansatzes liefert der Comprehensive Security & Functionality Check zügige Ergebnisse in unübertroffener Genauigkeit, die den Kunden in die Lage versetzen, einen klaren Einblick in die Situation der eigenen Sicherheitsmanagement-Organisation und IT-Infrastruktur zu gewinnen. Daraus können gezielte Maßnahmen abgeleitet werden, die zu einer nachhaltigen, langfristigen Verbesserung der unternehmensweiten Informations- oder IT Sicherheit beitragen oder die Gestaltung und Abstimmung von Geschäftsprozessen und technischen Betriebsabläufen wesentlich erleichtern und optimieren.

Sicherheitshinweis

Ein Comprehensive Security & Functionality Check kann innerhalb des EGOS! Sicherheitsmodells in 3 verschiedenen Geheimhaltungsstufen ausgeführt werden, die an die Sicherheitsbedürfnisse der Organisation angepasst werden:

- Grundstufe (Industriestandard)
- Aufbaustufe (Erhöhter Industriestandard)
- Regierungsstandard

In besonders sensiblen Situationen ist die Ausführung aller Arbeiten vor Ort auf Geräten des Kunden empfehlenswert.

Besuchen Sie uns auch auf Facebook:

facebook.com/egos.education

EGOS! Entwicklungsgesellschaft für Organisation und Schulung

A-6020 Innsbruck
Eduard Bodem Gasse 1/III
+43 (0)512/364777
+43 (0)512/364779-24
training@egos.co.at

A-5020 Salzburg
Schumacherstraße 14
+43 (0)662/450174
+43 (0)662/450174-24
training@egos.co.at