FOX Group

THINK IT – WE MAKE IT!

Serviceleistungen

www.foxgroup.de

FOX Group
THINK IT - WE MAKE IT!

DIE FOXGROUP

WER WIR SIND.

Die **FOXGroup** ist ein Verbund von hochspezialisierten Firmen in den Bereichen **Datenschutz & Informationssicherheit**, **IT- Security** und **Managed Services**, die im intelligenten und modernen Austausch alle Synergien der Digitalisierung nutzen, um einen erfolgreichen Projektabschluss für ihre Kunden zu erzielen.

Um maximale Sicherheit und Qualität bieten zu können, ist die **FOXGroup** nach den Normen **ISO 9001** und **ISO 27001** zertifiziert.

Unser Versprechen - Ihre Vorteile

Mehr als 30 Jahre Erfahrung

Wir haben langjähriges Know-how bei kleinen und mittelständischen, sowie großen Unternehmen und Konzernen.

Alles aus einer Hand

Wir bieten Ihnen individuelle Einzellösungen oder Komplett-betreuung Ihrer IT.

Expertenteam

Stetige Weiterbildungen halten unser zertifiziertes Experten-team immer auf dem neuesten Wissensstand.

Synergie

Sie profitieren von unserer breitgefächerten Erfahrung aus unseren Geschäfts-bereichen.

Zukunftsorientierung

Unsere Produkte, Dienstleistungen und unser Wissen unterstützen Sie bei Ihrem Erfolg, heute und morgen.

FOX Group

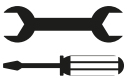
DATENSCHUTZ & INFORMATIONS-SICHERHEIT

- DATEN-SCHUTZ
- INFORMATIONS-SICHERHEIT
- BERATUNG
- AUDITIERUNG

IT-SECURITY

- SECURITY ASSESSMENTS
- MANAGED SOC
- INCIDENT HANDLING & RESPONSE

MANAGED SERVICES



- SERVER
- VIRTUALISIERUNG
- CLIENT/ ENDGERÄTE
- NETZWERK
- CLOUD

SCHULUNGS-ANGEBOTE

- INFORMATIONS-SICHERHEITS-BEAUFTRAGTER
- IT-GRUNDSCHUTZ-PRAKTIKER
- IT-GRUNDSCHUTZ-BERATER
- DATENSCHUTZ-BEAUFTRAGTER
- WEITERE SCHULUNGEN AUF ANFRAGE

1. Datenschutz & Informationssicherheit

1. DATENSCHUTZ & INFORMATIONSSICHERHEIT

1.1 DATENSCHUTZ

1.1.1 Inhouse Schulungen beim Kunden

Wir schulen Ihre Belegschaft in allen Belangen des Datenschutzes, von den Grundlagen bis zu spezifischen Einzelfällen und dabei insbesondere:

- dessen Zweck und weshalb er eine wichtige Rolle im Unternehmen spielt
- Gesetzliche Grundlagen und wie man diese praxisnah umsetzt
- Pflichtenverteilung im Unternehmen, der Mitarbeiter, des Datenschutzbeauftragten
- Verstöße gegen den Datenschutz werden an Beispielen erklärt

Inhouse Schulungen werden als Workshop in Ihren eigenen Räumlichkeiten durchgeführt.
Dabei entfallen Ihnen natürlich alle Reisekosten und die Praxisnähe zu Ihrem Untenehmen kann an, individuell auf Sie zugeschnittenen, Beispielen aufgezeigt werden.

1.1.2 Unterstützung des internen DSB

Bei der Auswahl eines internen Datenschutzbeauftragten sollten die ausschlagebenden Kriterien stets die notwendige berufliche Qualifikation, insbesondere das Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis sein.
Je nach Unternehmensgröße und Anforderungen wird ein Teilzeit- oder Vollzeit-DSB bestellt.
Vorteile eines internen DSB sind vor allem:

- Aufbau einer internen Expertise
- hohe Flexibilität und
- schnelle Erreichbarkeit

Wir unterstützen Ihren internen Datenschutzbeauftragten jederzeit effizient und effektiv.
Zudem stehen wir bei Fragestellungen, zum Einholen einer Zweitmeinung oder zur allgemeinen Unterstützung, jederzeit mit unserem Fachwissen als Experte zur Verfügung.

1.1.3 Stellung des externen DSB

Der externe Datenschutzbeauftragte übernimmt, nach Absprache mit der Geschäftsführung, die laufende Beratung in allen Fragen, die den Datenschutz gem. DSGVO betreffen.
Hierzu gehören insbesondere:

- **Unterstützung** in den Belangen des Datenschutzes, auch im Fall der Kontrolle durch Aufsichtsbehörden.
- Durchführung von **Schulungen** und **Schaffung von Transparenz** im Bereich Datenverarbeitung.
- **Datenschutzfolgeabschätzung** bei automatisierter Datenverarbeitung (z.B. bei neuen IT-Systemen/Anwendungen).
- **Prüfung** der Zulässigkeit der Verarbeitung von Daten.
- **Unterstützung bei Benachrichtigungspflichten** von Betroffenen (z.B. bei datenschutzrelevanten Vorfällen).
- **Support** bei Anfragen durch das Unternehmen oder von Betroffenen (Mitarbeiter, Kunden, Drittparteien).
- Erarbeitung bzw. Zurverfügungstellung von **Vorschriften und Musterdokumenten**.
- Mitwirkung bei Entwicklungen von **datenschutzrelevanten Richtlinien** und **Betriebsvereinbarungen**.
- **Kontaktaufnahme zu Behörden und Verbänden** (bei datenschutzrechtlichen Problemstellungen), anonym oder mit Einverständnis des Auftraggebers.
- **Information** des Auftraggebers über die aktuelle Gesetzeslage.
- **Beratung** über technische und organisatorische Maßnahmen zur Datensicherheit.
- **Pflege** der Datenschutzleitlinie bzw. des Datenschutzkonzepts.
- **Berichtspflicht** gegenüber der Geschäftsführung (Tätigkeitsbericht).

Kompetenzen unserer Datenschutzbeauftragten, die Sie beziehen können:

- Fachwissen auf dem Gebiet des Datenschutzrechts
- Fachwissen im Bereich IT bzw. der Sicherheit der Verarbeitungen
- Praktisches Fachwissen
- Weiterbildungspflicht
- Diskretion
- Konfliktfreiheit und Weisungsfreiheit (direkt der Geschäftsleitung unterstellt)
- Zuverlässigkeit

1.2 INFORMATIONSSICHERHEIT

1.2.1 Beratung

Unsere zertifizierten Berater begleiten Sie bei der Umsetzung der Informationssicherheit in Ihrem Unternehmen. Wir unterstützen Sie bei der Implementierung und Optimierung Ihres **Informationssicherheits-Managementsystems (ISMS)** und machen Ihr Unternehmen fit für eine Zertifizierung nach **ISO 27001** oder dem **IT-Grundschutz**. Informationssicherheit bedeutet Schutz vor Kapitalschäden jeglicher Art, wie:

Datenverlust

Produktivitäts-ausfall, wie:
-Hardwaredefekt
-Virenbefall
-Softwareausfall

Spionage
Ideenraub

Bruch der obersten Schutzziele, wie:
-Vertrauen
-Verfügbarkeit
-Integrität

Diebstahl
Zerstörung
Vandalismus
natürliche Vorfälle
Unfälle
Katastrophen

Abmahnungen
Bußgelder
Anzeigen

Image- und Vertrauensverlust

1.2.1.1 Inhouse Schulungen beim Kunden

Wir schulen Ihre Belegschaft zu allen Belangen der Informationssicherheit.
Durch zahlreiche Beispiele , werden die Teilnehmer dafür sensibilisiert, die Informationssicherheit im Unternehmen zu erhöhen.
Inhouse Schulungen werden als Workshop in Ihren eigenen Räumlichkeiten durchgeführt.
Dabei entfallen Ihnen natürlich alle Reisekosten und die Praxisnähe zu Ihrem Unternehmen kann an, individuell auf Sie zugeschnittenen, Beispielen aufgezeigt werden.

1.2.1.2 Einführung ISMS

Der Aufbau eines **Informationssicherheitsmanagementsystems (ISMS)** und die Vorbereitung auf die Zertifizierung nach **ISO 27001** stellen Organisationen vor große Herausforderungen. Hierbei muss man stets - neben der technischen Infrastruktur - auch die rechtlichen Aspekte und die organisatorischen Maßnahmen in das ISMS mit einbeziehen. Die Maßnahmen im Bereich der Informationssicherheit müssen zudem kontinuierlich auf ihre Wirksamkeit und Angemessenheit geprüft werden und einen ständigen Verbesserungszyklus unterlaufen. Das ISMS muss effizient, zielorientiert und professionell während des laufenden Betriebs geplant und nachhaltig umgesetzt werden. Das Managementsystem ist sowohl in die Gesamtstrategie des Unternehmens als auch in den kontinuierlichen Unternehmensalltag voll zu integrieren, um zu funktionieren. Unsere zertifizierten Berater begleiten Sie hier mit einer klaren und zielorientierten Vorgehensweise bis hin zum weltweit höchsten Zertifikat der Informationssicherheit, dem **ISO 27001-Zertifikat**. Mit einem mehrstufigen Fahrplan und den darin definierten, einzelnen Phasen und Meilensteinen bis zur Zertifizierung auf Basis **ISO 27001** werden Sie von unseren Fachexperten zielgerichtet in die vielen Themen und Anforderungen der Norm eingearbeitet.

1.2.1.3 Unterstützung des internen ISB

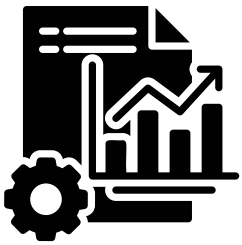
Bei der Auswahl eines internen ISB sollten die ausschlagebenden Kriterien stets die notwendige berufliche Qualifikation, insbesondere das Fachwissen auf dem Gebiet der Informationssicherheit sein.
Je nach Unternehmensgröße und Anforderungen wird ein Teilzeit- oder Vollzeit-ISB bestellt.
Vorteile eines internen ISB sind vor allem:

- Aufbau einer internen Expertise
- hohe Flexibilität und
- schnelle Erreichbarkeit

Wir unterstützen Ihren internen Informationsschutzbeauftragten jederzeit effizient und effektiv.
Zudem stehen wir bei Fragestellungen, zum Einholen einer Zweitmeinung oder zur allgemeinen Unterstützung, jederzeit mit unserem Fachwissen als Experte zur Verfügung.

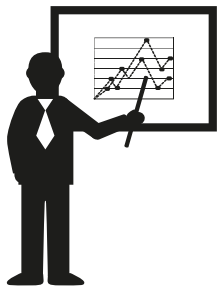
1.2.1.4 Stellung des externen ISB

Die Aufgaben des externen **ISB** lassen sich im Wesentlichen in drei große Teilbereiche untergliedern.
Diese bestehen aus **Analytik**, **Consulting** und **Koordination**.



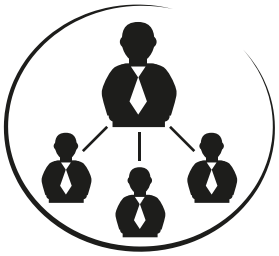
Analytik

- Aufbau und fortlaufende Aktualisierung des ISMS (Informationssicherheitsmanagementsystem)
- Betreuung der IT-Sicherheitsleitrichtlinien
- Aktualisierung der Betriebshandbücher zur permanenten Aufrechterhaltung des ISMS-Prozesses
- Strukturanalyse
- Risikomanagement
- Schutzbedarfsfeststellung
- Erstellung der Informationssicherheitsmaßnahmen und Realisierungsfortschrittskontrolle
- Erstellung von Richtlinien und Regelungen in Bezug auf Informationssicherheit
- Feststellung und Untersuchung auftretender sicherheitsrelevanter Zwischenfälle (Forensik)



Consulting

- Implementierung, Steuerung und Kontrolle sowie innerbetriebliche Schulungen zum ISMS
- Zentraler Ansprechpartner in allen Fragen zur Informationssicherheit
- Mitwirkung im gesamten ISMS-Prozess und als zentraler Ansprechpartner zu allen Fragen hinsichtlich der Informationssicherheit
- Initiierung bzw. Durchführung von internen Audits und Begleitung von externen Audits
- Organisation / Koordination von Informationsveranstaltungen und Schulungen zur Informationssicherheit
- Regelmäßiger Managementreview
- Regelmäßige Abstimmung mit den Abteilungsleitern bzw. den relevanten Führungsebenen



Koordination

- Koordination und Erstellung des IT-Sicherheitskonzeptes sowie Vorgaben einheitlicher Informationssicherheitsstandards
- Ansprechpartner für die externen Unternehmensparteien, wie Kunden und Lieferanten bzgl. der Informationssicherheit
- die Möglichkeit, bei Bedarf Erfüllungsgehilfen einzusetzen
- Zusammenarbeit mit dem Datenschutzbeauftragten und weiteren wichtigen Ansprechpartnern für aufsichtsrechtliche und regulatorische Themenstellungen
- Mitwirkung bei der Etablierung eines Prüfsystems (Auditsystem), mit dem die der Verfahrensregelungen und die Wirksamkeit der Maßnahmen überprüft werden kann

1.2.2 Auditierung

Neben der beratenden Tätigkeit ist die **complimant AG** auch auditierend für verschiedene Zertifizierungsgesellschaften tätig. Die Erfahrungen unserer Lead-Auditoren ermöglichen den Kunden maßgeschneiderte Lösungen für ihr Unternehmen zu erlangen.

1.2.2.1 ISO 27001

Die Standardnorm **ISO 27001** ist gegenwärtig der höchste international anerkannte Sicherheitsstandard im Bereich der Informationssicherheit. Eine erfolgreiche Zertifizierung bescheinigt dem Unternehmen, dass die gesamte IT-Struktur und Informationsverarbeitung auf Basis einer Sicherheits- und Risikoanalyse ordnungsgemäß, wirksam, kontinuierlich und zuverlässig entlang des ISO-Standards umgesetzt ist.
Die aktuellste, internationale Norm **ISO/IEC 27001:2022** spezifiziert die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung eines dokumentierten Informationssicherheit-Management-systems unter Berücksichtigung der IT-Risiken innerhalb der gesamten Organisation, insbesondere:

- Formulierung von Anforderungen und Zielsetzungen zur Informationssicherheit sowie kosteneffizientes Management von Sicherheitsrisiken
- Sicherstellung der Konformität mit Gesetzen und Regulatorien
- Implementierung und Management von Maßnahmen zur Sicherstellung von spezifischen Zielen zur Informationssicherheit
- Identifikation und Definition von bestehenden und neuen Informationssicherheits-Managementprozessen und -tätigkeiten

Eine koordinierte Umstellung auf die aktuelle **ISO 27001:2022** kann mit unserer Unterstützung und unserem Fachwissen auch in ihrem Untenehmen durchgeführt werden

1.2.2.2 IT-Grundschutz

ISO 27001-Zertifizierungen auf der Basis von **IT-Grundschutz** geben Institutionen die Möglichkeit, ihre Bemühungen um Informationssicherheit und die erfolgreiche Umsetzung internationaler Normen, unter Anwendung der **IT-Grundschutz-Methodik**, nach innen und außen zu dokumentieren.
Mit der Vergabe eines Zertifikats wird der Institution bescheinigt, dass

- Informationssicherheit ein anerkannter Wert ist,
- ein funktionierendes IS-Management vorhanden ist
- zu einem bestimmten Zeitpunkt ein definiertes Sicherheitsniveau besteht.

Prüfgrundlage des Verfahrens sind:

DIN ISO/ IEC 27001 „Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme–Anforderungen“

BSI-Standard 200-1 „Managementsystem für Informationssicherheit ISMS“

BSI-Standard 200-2 „IT-Grundschutz-Methodik“

BSI-Standard 200-3 „Risikoanalyse auf Basis von IT-Grundschutz“, IT-Grundschutz-Kompendium

Erst nach erfolgreicher Initialisierung des Zertifizierungsprozesses durch die Stellung eines Zertifizierungsantrags und Prüfung der Unabhängigkeitserklärungen aller Mitglieder des Auditteams, kann ein Audit begonnen und durchgeführt werden.

1.2.2.3. TISAX (Trusted Information Security Assessment Exchange) Informationssicherheit für die Automobilbranche

TISAX ist ein **unternehmensübergreifendes Prüf- und Austauschverfahren für Informationssicherheit in der Automobilindustrie**.
Dabei geht es um den Schutz Ihrer Daten, Ihrer Integrität und Verfügbarkeit im Herstellungsprozess sowie im Betrieb von Fahrzeugen.

Dies erfolgt über ein **Informationssicherheits-Managementsystem (ISMS)** analog zur Norm **ISO 27001**.

1.2.2.4. C5

Wir prüfen das **Cloud Computing C5** anhand des dafür vorgesehenen BSI-Kriterienkatalogs.
Ein akkreditierter **ISO 27001**-Lead-Auditor oder Auditor auf Basis **IT-Grundschutz** führt die Prüfung durch.
Hierfür müssen dem Prüfer entweder

- die entsprechenden Dokumentationen zur Verfügung gestellt werden mit einem reduzierten persönlichen Einbezug in Form von Interviews oder
- die Dokumentationen gänzlich in Interviewform vorgestellt werden.
  In dieser Form müssen dem Prüfer keine Dokumentationen übersandt bzw. zur Einsicht bereitgestellt werden, der Kunde muss jedoch 100% der Prüfungszeit anwesend sein.

Prüfungen zum Nachweis der Konformität mit diesem Kriterienkatalog C5 haben nach Auffassung des BSI mit hinreichender Sicherheit zu erfolgen.
Ferner wird zwischen der **Prüfung einer Erklärung** und einer **direkten Prüfung** unterschieden.
Grundsätzlich eignen sich beide Prüfungsarten für die Beurteilung des Nachweises der Konformität mit diesem Kriterienkatalog. Zudem können Prüfungen in der Form einer **Angemessenheitsprüfung** oder einer **Wirksamkeitsprüfung** durchgeführt werden. Prüfungen der Angemessenheit des dienstleistungsbezogenen internen Kontrollsystems sollten dabei jedoch nur im Falle der Erstprüfung eines Cloud-Dienstes nach diesem Kriterienkatalog erfolgen und keinesfalls mehrmals hintereinander in Betracht gezogen werden.

1.2.2.5 SOC 2

Bei diesen Reports geht es um **interne Kontrollen in Bezug auf Sicherheit, Verfügbarkeit, Integrität bzw. Vertraulichkeit (Datenschutz)** im Hinblick auf IT-Rechenzentren.

Anhand der **SOC 2**-Zertifizierung wissen Unternehmen, dass ein Cloud-Anbieter diese nachweisbar erfüllt. Konkret gibt dies Sicherheit, dass Informationen und Systeme gegen unbefugten Zugriff, unbefugte Offenlegung von Informationen und Schäden an den Systemen geschützt sind.

SOC 2 ist insbesondere geeignet für Unternehmen, die Nutzerdaten in Clouds speichern sowie für Unternehmen aus dem Finanz- und Gesundheitswesen.

Beim **SOC 2**-Audit werden die Informationssicherheitslevel einer Organisation auf Basis der TSCs und Prinzipien bewertet und eingestuft. Dementsprechend erhält ein Unternehmen eine Bewertung und den aktuellen Status der Informationssicherheit.

Erwähnenswert ist an dieser Stelle die Tatsache, dass durch die Einführung der SOC-Reports nun erstmalig die Möglichkeit besteht, Dienstleister miteinander zu vergleichen. Dies wird dadurch gewährleistet, dass sich der Kontrollbezug auf vordefinierte Kriterien bezieht und vor allem auch der Kontrollzeitpunkt festgelegt wird. Es findet eine Beurteilung und Berichterstattung zum Kontrolldesign im Hinblick auf die Angemessenheit der Definition der Ziele und der zugehörigen Kontrollen (Typ I) statt. Eine Prüfung nach Typ II prüft darüber hinaus auch noch die Wirksamkeit der eingerichteten Kontrollen und beinhaltet die Testszenarien sowie die Testergebnisse im Bericht.

Folgende Kriterien und Richtlinien für diese Vereinbarungen sind in den Vertragsrahmenbedingungen festzuhalten:

Sicherheit

Dass das System gegen den nicht autorisierten Zugang geschützt ist.

Verfügbarkeit

Dass das System wie vertraglich vereinbart zur Verfügung steht.

Daten-verarbeitung

Die Verarbeitung von Daten ist vollständig, exakt, rechtzeitig und entsprechend autorisiert.

Vertraulichkeit

Dass die von einer Organisation gehaltenen, vertraulichen Informationen sicher geschützt sind.

Datenschutz

Dass personenbezogene Daten spezifisch geschützt sind.

1.2.2.6 KRITIS

Laut einer neuen Bestimmung des Bundesamtes für Sicherheit in der Informationstechnik brauchen **KRITIS**-Betriebe ab **1. Mai 2023** eine Angriffs-Früherkennung.

KRITIS steht für kritische Infrastrukturen. Das sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, zum Beispiel die Energie- und Wasserversorgung, der Verkehr und auch sämtliche medizinische Versorgungseinrichtungen.

Seit 2023 müssen **KRITIS**-Unternehmen dem BSI Nachweise vorlegen, dass sie Angriffserkennungssysteme nutzen. Danach erfolgt eine Nachweispflicht alle zwei Jahre.
Wir bieten Ihnen hierfür die optimale Lösung an:

Unser FOX Managed SOC (Security Operations Center) ist ihr System zur Angriffserkennung:

Unser Team aus hochqualifizierten Spezialisten im Bereich IT-Sicherheit kümmert sich darum, bei unseren Kunden Hacker-Angriffe frühzeitig zu erkennen und Gegenmaßnahmen einzuleiten. So können mögliche Schäden erst gar nicht entstehen oder, im Falle eines Angriffes, verringert werden.

Mehr Informationen zu unserem **FOX Managed SOC** erfahren Sie unter 2.2.4

1.2.2.7 weitere Auditierungen

Auditiert wird unter anderem auch noch:

- SMGWA
- ISO 22301
- EN50600

2.IT-SECURITY

Unter dem Begriff **IT-Security** verbergen sich Maßnahmen zum Schutz von IT-Systemen und der darauf befindlichen Daten. Durch IT-Security soll die Manipulation von Systemen und Daten durch unautorisierte Drittpersonen verhindert werden. Sozio-technische Systeme, also Mensch und Technologie, innerhalb von Unternehmen / Organisationen und deren Daten sollen und müssen gegen Schäden und Bedrohungen geschützt werden.

Hierbei ist nicht nur die Rede von Informationen und Systemen, sondern auch Cloud-Dienste und Rechenzentren.

Um ihr Unternehmen bestens zu schützen erarbeitet die **FOXGroup** maßgeschneiderte Lösungen im Bereich der drei wichtigsten Eckpfeiler der IT-Security: **Security Assessments, Managed SOC** und **Incident Handling & Response**.

Security Assessments sind spezifisch anwendbare Schwachstellenanalysen, die je nach Bedarf, Unternehmensressourcen auf etwaige Sicherheitslücken prüfen. Durch speziell entwickelte Analysen werden Identitäten, sowie Anwendungen, Geräte und Infrastrukturen untersucht.

Managed SOC ist ein auf verschiedenen Komponenten basierender Security Service, der mit Sicherheitsanalysten besetzt, eine Erweiterung Ihres eigenen IT-Teams darstellt.

Unter Verwendung führender Technologien soll im Falle eines Angriffs frühzeitig reagiert und geeignete Gegenmaßnahmen umgehend eingeleitet werden können.

Incident Handling & Response ist der Prozess eines Unternehmens, bei dem auf bereits erfolgte IT-Bedrohungen wie Cyberangriffe, Sicherheitsverletzungen und Serverausfälle reagiert wird.

2.1 SECURITY ASSESSMENTS

2.1.1 Cyber Security Check

In dem Cyber Security Check wird das Unternehmen auf den aktuellen Stand des IT-Sicherheitsniveaus geprüft. Ein besonderer Fokus liegt dabei auf der Ermittlung der größten Risiken. Die Ergebnisse werden in einem Bericht dokumentiert und Handlungsempfehlungen werden je nach Dringlichkeit daraus abgeleitet. Dieser Check bietet einen roten Faden, welche konkreten Maßnahmen umzusetzen sind. Bei der Umsetzung und der Abarbeitung dieser Handlungsempfehlungen kann die **FOXGroup** im Anschluss unterstützen und den gesamten Prozess begleiten.

2.1.2 PenTest

Ein **IS-Penetrationstest** ist ein erprobtes und geeignetes Verfahren, um das Angriffspotenzial auf einen Informationsverbund, ein einzelnes informationsverarbeitendes System oder eine IT-Anwendung zu überprüfen. Ziel ist es, die Erfolgsaussichten eines tatsächlichen vorsätzlichen Angriffs einzuschätzen und die Wirksamkeit der bereits bestehenden Sicherheitsmaßnahmen zu überprüfen. Aus den Testergebnissen werden darauffolgend ergänzende Sicherheitsmaßnahmen abgeleitet.

Um die Planung und Durchführung von Penetrationstests kümmert sich innerhalb der **FOXGroup** das Expertenteam der **pen.sec AG**.

Für ihre maximale Sicherheit und Qualität ist die **pen.sec AG** nach den Normen **ISO 9001** und **ISO 27001** zertifiziert.

2.1.3 Red Teaming

Beim **Red Teaming** wird die Sicherheit Ihrer Systeme getestet, indem versucht wird, diese zu hacken. Es geht darum, einen Angriff zu simulieren und zu versuchen, in Ihr System einzudringen.

Diese Art von Tests bringen ein realistischeres Bild der Sicherheitslage als andere Übungen, Rollenspiele oder anders angekündigte Tests. Je nach Testergebnis werden dann entsprechende Gegenmaßnahmen empfohlen und ergriffen.

Der Unterschied zwischen **Penetrationstest** und **Red Teaming** liegt hauptsächlich in der Zielgestaltung der Projekte und damit einhergehend in deren zeitlichem Umfang und Realitätsgrades. Bei Penetrationstests wird vorab festgelegt, welche Sicherheitsaspekte konkret getestet werden sollen. Sie zielen eher auf das grundsätzliche Vorhandensein bestimmter Sicherheitskomponenten ab und testen diese in der Breite.

2.1.4 Threat Intelligence

Die zertifizierten **Threat – Intelligence - Module** analysieren externe, interne sowie menschliche Faktoren, die ein Sicherheitsrisiko darstellen können und schaffen so eine ganzheitliche Betrachtung Ihrer IT-Sicherheitslandschaft.

Durch automatisierte Analysen, Tests und Hacking-Simulationen spüren sie mit ihren Software-Lösungen "**Threat Intelligence**" in Ihrem Unternehmen Bedrohungen für Cyberangriffe auf und stellen aktuelle Informationen über die Bedrohungslage der jeweiligen IT-Landschaft in aufbereiteter Form zur Verfügung.

Die **Vulidity GmbH** bietet auf ihrem Portal, neben den **Threat Intelligence** Modulen, auch das **Security Rating**, das **Schwachstellenmanagement** und einen **Überblick zum Datenschutzniveau** an.

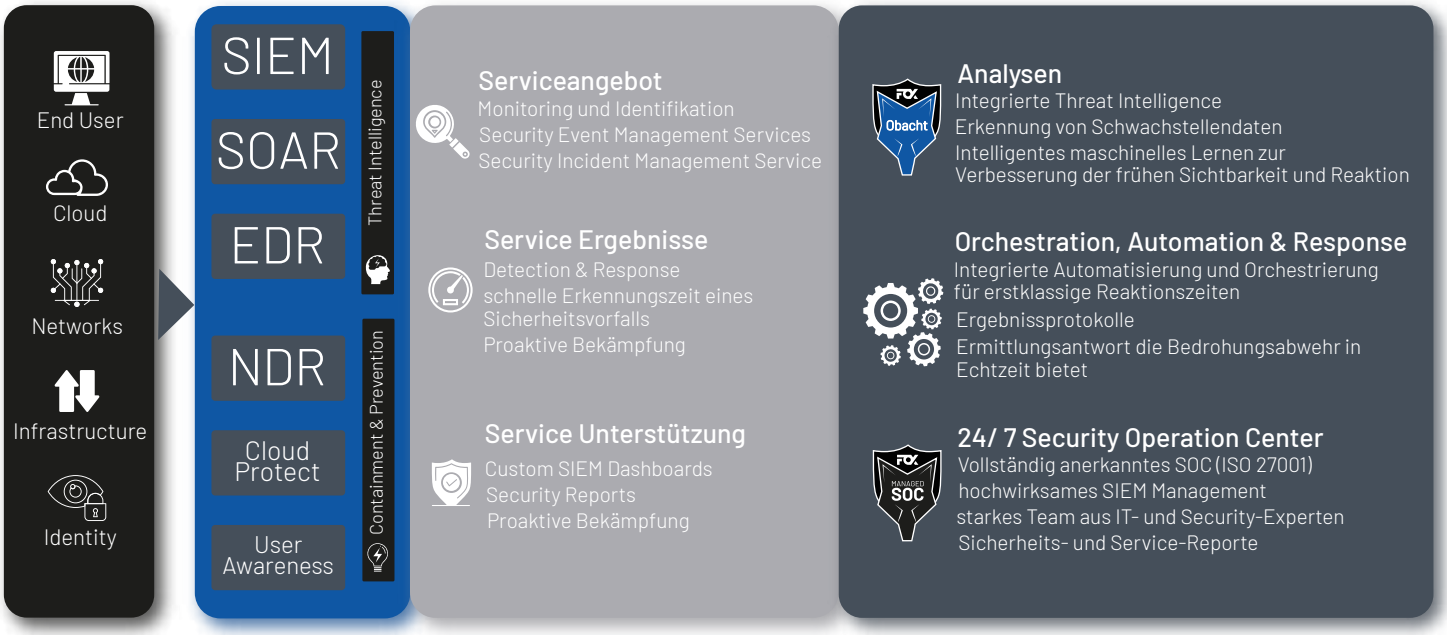
Unternehmen bekommen hier auch ein Abbild der **ISO 27001**.

2.2 MANAGED SOC

FOX Managed SOC ist ein auf verschiedenen Komponenten basierender Security Service, der eine Erweiterung des IT-Teams Ihres Unternehmens darstellt.
Security Operations Centers (SOC) sind mit Sicherheitsanalysten und IT-Experten besetzt. Ein **SOC** dreht sich um ein **Security Incident and Event Management System (SIEM)**, das Protokolldaten von verschiedenen Endpunkten aufnimmt und bei verdächtigen Aktivitäten warnt.
FOX Managed SOC bietet **Detection and Response** Services, unter Verwendung führender Technologien.

Durch unser **Security Operations Center** sind wir in der Lage, ausgefeilte Cyber-Bedrohungen zu erkennen und mit Gegenmaßnahmen zu reagieren. Somit stellen wir sicher, dass Ihr Unternehmen optimal geschützt ist.

Warum sollten Sie **FOX Managed SOC** verwenden?
In unserer vernetzten Welt wird es immer schwieriger, Daten von Unternehmen zu schützen. Technologien entwickeln sich schnell – Arbeitsweisen von Unternehmen ändern sich. Reaktionen wie der Schutz der Netzwerkinfrastruktur sind selbstverständlich. Trotzdem werden Unternehmen Opfer von Cyber-Attacken. **FOXManaged SOC** schafft Transparenz und Sicherheit - vor allem in Bezug auf Verfügbarkeit und Fachwissen. Es empfiehlt sich insbesondere für Unternehmen mit begrenzten Ressourcen, **FOX Managed SOC** zur Erkennung und Verwaltung von Vorfällen zu verwenden. Alternativ kann nach Bedarf mit fundiertem Fachwissen und Service unterstützt werden



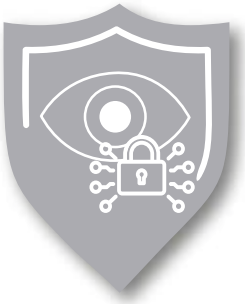
2.2.1 FOX Obacht

Durch automatisierte Analysen, Tests, Hacking- und Phishing-Simulationen spürt **FOX Obacht** Bedrohungen für Cyberangriffe auf, indem Angriffe simuliert und Systeme geprüft werden.

Besonders wichtig ist in diesem Zusammenhang der Faktor Mensch:

Schulungen alleine bilden kein Sicherheitsbewusstsein. Unser Social Engineering Modul baut langfristig ein solides Bewusstsein gegen Phishing und anderen Social Engineering Angriffen auf. Individuell erstellte Awarenesspläne schaffen ein optimales Bewusstsein über die möglichen Gefahren bei allen AnwenderInnen und senken somit effektiv das Risiko von Phishing Attacken.

2.2.2 SIEM & SOAR



SIEM kommt aus dem Englischen und nennt sich „**Security Information and Event Management**". In einer **SIEM**-Lösung werden alle LogFile Daten, die in einer Unternehmens-IT vorkommen, in ein zentrales Datensystem gespielt. Unsere **SOC**-Mitarbeiter analysieren diese LogFile Daten rund um die Uhr und erhalten so Ergebnisse über mögliche Anomalien, also Unregelmäßigkeiten, die auf Hacker-Angriffe hinweisen können.

Die **SOAR**-Lösung, „**Security Orchestration, Automation and Responses**", unterstützt das Team mittels Playbooks bei der schnellen Erledigung ihrer Aufgaben. Wenn es zu einer Attacke kommt, muss unmittelbar und fehlerfrei agiert werden.

SIEM & SOAR unterstützen dabei, dass **SOC**-Mitarbeiter nicht nur reagieren, sondern auch richtig und zeitnah agieren können.

2.2.3 Vulnerability Management

Ein modernes **Schwachstellenmanagement** gehört zu den wichtigsten Maßnahmen, um IT-Infrastrukturen vor Angriffen zu schützen, indem **Schwachstellen** in IT-Anwendungen &- Systemen schnell erkannt und zeitnah behoben werden können.

Mit unserem **Schwachstellenmanagement** stellen wir den technologischen Marktführer. Wir bieten Planung und Etablierung von regelmäßig automatisieren sowie manuellen Schwachstellenscans an. Außerdem führen wir Penetrationstests durch, um exponierte und besonders gefährdete Teile der IT-Infrastruktur umfassend zu überprüfen und zu überwachen.

Bei einem **nicht invasiven Schwachstellenscan** werden Systeme mittels eines **Schwachstellenscanners (SW-Tool)** auf bekannte Unregelmäßigkeiten überprüft.

Ein **nicht invasiver Schwachstellenscan** erreicht im Vergleich zu einem manuell durchgeführten **Penetrationstests** eine zwar nur geringe Testtiefe, hat aber den Vorteil, dass er automatisiert und damit kostengünstig sowie in engen Zeitabständen durchgeführt werden kann.

Durch den Einsatz eines hoch qualifizierten Schwachstellenscanners kann sichergestellt werden, das bekannte Abweichungen erkannt und beseitigt werden, was einen wichtigen Bestandteil von sicheren Systemen darstellt.

Kunden profitieren durch:

Erkennung von Schwachstellen in IT-Anwendungen &- Systemen

Schnelle Reaktionsfähigkeit durch tägliche Durchführung

Übersichtliches Dashboard

Unterstützung durch Pen-Test-Experten

Unterstützung bei der Definition, Umsetzung und Dokumentation eines modernen Schwachstellenmanagements, inklusive Prozess

2.3 INCIDENT HANDLING & RESPONSE (REAKTIV)

Vorfallbehandlung und Reaktion

Benötigt Ihr Unternehmen sofortige Unterstützung bei der Reaktion auf einen Vorfall?

- Haben Sie anomale oder verdächtige Aktivitäten in Ihrem Netzwerk festgestellt?
- Sind Sie von einem Ransomware-Angriff betroffen?
- Haben Sie den Verdacht, dass eine Sicherheitslücke vorliegt, oder haben Sie eine Benachrichtigung über eine Sicherheitslücke erhalten?
- Haben Sie eine verdächtige Email erhalten?

Unser Team aus Sicherheitsexperten unterstützt Sie im Vorfeld, um hohe Schäden zu verhindern, aber wir sind auch im Notfall sofort für Sie zur Stelle.

3.MANAGED SERVICES

Bei unseren Managed Services handelt es sich um IT-Dienstleistungen, die im Auftrag eines Unternehmens durch uns als Managed Services Provider (MSP) erbracht werden.

Managed Services umfassen eine Vielzahl von IT-Leistungen, die überwiegend remote ausgeführt werden. Zu **Managed Services** zählen proaktive IT-Dienstleistungen, die sich mit den Bereichen **Server, Virtualisierung, Client, Netzwerk und Cloud** beschäftigen.

Wir stellen demnach mit unseren Services vor allem den laufenden Betrieb von IT-Systemen sicher und übernehmen die IT-Überwachung, meistens per Fernzugriff. Potentielle Störfälle sollen frühzeitig erkannt und verhindert werden.

Bei unseren **Managed Services** werden Verantwortlichkeiten, die auch unternehmenskritische und sicherheitsrelevante Anwendungen betreffen können, zwar an uns abgegeben, die Daten- und Finanzhoheit verbleibt aber beim Auftraggeber bzw. dem Unternehmen. Es geht darum, unternehmenseigene IT-Abteilungen zu entlasten oder die IT für Unternehmen zu übernehmen, die über keine eigene Abteilung verfügen.

3.1 SERVER

Ein professioneller Serverbetrieb, ob in der Cloud oder im eigenen Rechenzentrum, stellt sicher, dass Ihr Unternehmen wie gewohnt funktioniert.

Wir überwachen Ihre Server auf ihren Zustand und patchen diese regelmäßig, um Sicherheitslücken gar nicht erst entstehen zu lassen. Regelmäßige Updates und Benutzerrechte zu administrieren gehört ebenso zum Leistungsumfang wie die richtige Lizenzierung und Hardwarewartung.

3.1.1 Backup

Wir bieten **Backup-/Recovery-Software** an, um Ihre Daten sicher zu speichern und im Notfall auch wiederherstellen zu können z. B. im Falle von **Datenverlust** oder **Datenbeschädigung**.

3.1.2 Monitoring

Die **FOXiT GmbH** übernimmt die **Betreuung und Wartung von IT-Infrastrukturen** im Rahmen von Managed Services Verträgen. Sie etabliert Maßnahmen – wie Monitoring und proaktive Services – zur Aufrechterhaltung der **technischen Funktionsfähigkeit** und erhöht damit die **Systemverfügbarkeit**.

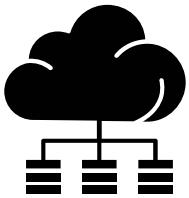
Im Fehlerfalle schützen **Service Levels** für Clients, Server und Netzwerk vor längeren Ausfallzeiten und sorgen für eine Wiederherstellung innerhalb vereinbarter Reaktionszeiten. Auf diese Weise werden unproduktive Zeiten minimiert und schaffen mehr Anwenderzufriedenheit.

3.2 VIRTUALISIERUNG

Virtualisierung ist ein Prozess zur Erstellung softwarebasierter oder virtueller Nachbildungen eines Objekts, z.B. virtuelle Anwendungen, Server, Storage-Ressourcen und Netzwerke.

3.2.1 VM-Ware und MS Hyper V

mit diesen beiden Sortwareprogrammen können Sie **mehrere verschiedene Betriebssysteme gleichzeitig** auf einem einzelnen Computer ausführen.



Server Virtualisierung

Serverkonsolidierung durch Virtualisierung bietet einen hervorragenden Ansatz, **Kosten** für den Betrieb dieser Systeme erheblich zu r**eduzieren**, da sie die **Administration vereinfacht** sowie gleichzeitig ihre **IT-Systeme besser auslastet** und die **Verfügbarkeit erhöht**.

Desktop Virtualisierung

Client-Virtualisierung – oder **Server Based Computing** – eröffnet **enorme Einsparpotentiale** durch den Einsatz von Thin Clients (z.B. IGEL). VMware View und Citrix XenApp/XenDesktop bieten sich hier als optimale Basis an. Wenn bereits eine **Server-Virtualisierung** im Einsatz ist, kann ohne große Zusatzinvestition eine **Desktop-Virtualisierung** aufgebaut werden.

Folgende Vorteile sprechen für die Desktop-Virtualisierung:

- Flexible und schnelle Bereitstellung von Desktop-Systemen
- Niedrige Investitions- und Betriebskosten
- Mehr Sicherheit durch geschlossene Systeme
- Kostenreduzierung durch Zentralisierung der gesamten Desktop-Administration

3.3 CLIENT/ENDGERÄTE

Als „**Allgemeiner Client**“ wird ein **IT-System mit einem beliebigen Betriebssystem bezeichnet**, das die Trennung von Benutzern zulässt und nicht dazu dient, auf Server-Dienste zuzugreifen.
Auf einem Client sollten mindestens eine Administrator- und eine Benutzer-Umgebung eingerichtet werden können. Das IT-System verfügt in der Regel über Laufwerke und Anschlussmöglichkeiten für externe bzw. wechselbare Datenträger, weitere Schnittstellen für den Datenaustausch sowie andere Peripheriegeräte.

Typischerweise ist ein solches IT-System in ein **Client-Server-Netz** eingebunden. Bei dem IT-System kann es sich beispielsweise um einen **PC mit oder ohne Festplatte**, um ein **mobiles oder stationäres Gerät**, aber auch um eine **Linux-Workstation** oder einen **Apple Mac** handeln. Ziel dieses Bausteins ist der **Schutz von Informationen**, die auf jeglicher Art von Clients, unabhängig vom verwendeten Betriebssystem, erstellt, gelesen, bearbeitet, gespeichert oder versendet werden.

Clients sind besonders anfällig für Schadsoftware. Sie werden direkt von den Benutzern bedient und sind somit oft das Einfallstor für schädliche Inhalte jeglicher Art. Besuchen die Benutzer bösartige Webseiten, öffnen E-Mails mit schädlichem Inhalt von privaten Konten oder kopieren Schadsoftware über lokale Datenträger auf den Client, kann sich so die Schadsoftware über die Clients in das Netz der Institution verbreiten. Zentrale Schutzmechanismen, wie z. B. ein Virenschutz auf dem Datei- oder E-Mail-Server, können so oft umgangen werden.

Wir können Sie bei den richtigen Schutzmaßnahmen beraten und diese auch für Sie umsetzen.

3.4 NETZWERK

3.4.1 Router und Firewall

Eine Firewall ist ein Sicherheitssystem, welches den Datenverkehr über eine bestimmte Schnittstelle kontrolliert. Bei einem Internet-Router ist das die Schnittstelle von Ihrem Netzwerk zum Internet. Ziel ist es, nur Datenverkehr zuzulassen, welcher von einem Ihrer Geräte initiiert wurde bzw. von Ihnen gewollt ist. Ungewollte, bzw. unerlaubte Datenströme sollen gefiltert werden.

Wir beraten Sie jederzeit gerne, wie Sie die Router-Firewall richtig konfigurieren, um den maximalen Schutz zu erhalten.

3.4.2 Switches/W-Lan

Wir planen, installieren und unterstützen **Daten-/Kommunikationsnetze** und **WLANs (systemgestützte Ausleuchtung)**. Hochwertige Komponenten und professionelle Dokumentation gewährleisten die erforderliche Stabilität von Netzwerklösungen.

Wir verfügen über umfangreiche Erfahrungen mit sämtlichen gängigen Netzwerktechnologien und sichern eine schnelle Auffindung von Störungsquellen durch modernste Werkzeuge zu.

Die Datensicherheit und die Leistungsfähigkeit Ihres Netzes ist grundlegender Bestandteil der Konzeption von **VLANs**.

3.5 CLOUD

Daten in einer **Cloud** zu sichern, gewährt einfachen Zugriff auf Daten, die dort gespeichert sind. Einfacher **Zugriff zu jeder Zeit von jedem Ort** ist möglich. Hierfür gibt es jedoch auch Sicherheitsbedenken, die beachtet werden müssen.
Es ist auch essenziell, stets die neueste Technik zu verwenden. Somit kann eine möglichst hohe Sicherheit garantiert werden.

Unser Team unterstützt Sie bei der Umstellung auf eine Datensicherung in einer Cloud.

3.5.1 Microsoft 365

Gerne stellen wir Ihnen die neue Microsoft-Version 365 zur Verfügung. Wir kümmern uns um ihre Microsoft Landschaft, von der Migration und Lizensierung bis zum Support.
Mit MS 365 erhalten Sie Folgendes: Die neuesten Produktivitäts-Apps wie Microsoft Teams, Word, Excel, PowerPoint, Outlook, OneDrive und vieles mehr.

Office 365 ist die im Juni 2011 veröffentlichte, Cloud-gestützte Weiterentwicklung des ursprünglichen Office-Pakets für die lokale Installation (z. B. „Office 2016", „Office 2019" etc.).
Der wesentliche Unterschied ist die **schier grenzenlose Rechenleistung und Speichergröße der Cloud** (= die Microsoft Rechenzentren) im Hintergrund, was zahlreiche komplett neue Möglichkeiten eröffnet.

Im Unterschied zum ursprünglichen Office (welches im Wesentlichen aus Excel, Word, Outlook und PowerPoint besteht) ermöglicht die Cloud-Unterstützung dem 365-Ökosystem zum Beispiel deutlich mehr und leistungsstärkere Dienste, Services, Anwendungen und auch Ressourcen (Rechenkapazitäten und Online-Speicherplatz).
Diese helfen dabei, die **Produktivität und Effizienz in Unternehmen** zu **verbessern** sowie bei der **digitalen Zusammenarbeit** zu **unterstützen**.
Ebenfalls können wir Sie bei der **Migration** von **Exchange on Premis** auf **Exchange Online** unterstützen, sowie die **Einrichtung** Ihres **MDM System Intune** übernehmen.

3.5.2 Private Cloud

Die **Private Cloud** steht für **Cloud-Computing-Dienste**, die **nicht für die Allgemeinheit**, sondern nur für ausgewählte Benutzer über das Internet oder ein privates internes Netzwerk bereitgestellt werden. Wir richten Ihnen gerne eine Private-Cloud-Computing Umgebung in einem unserer Rechenzentren ein. Dies bietet Unternehmen viele Vorteile einer Public Cloud wie z. B. **Self-Service, Skalierbarkeit und Elastizität**.

Gleichzeitig werden zusätzliche Steuerungs- und Anpassungsoptionen unterstützt, die mithilfe dedizierter Ressourcen über eine lokal gehostete Computing-Infrastruktur bereitgestellt werden. Darüber hinaus bieten Private Clouds Sicherheit und Datenschutz auf einem höheren Niveau durch Unternehmensfirewalls und internes Hosting. So wird sichergestellt, dass Drittanbieter keinen Zugriff auf Vorgänge und vertrauliche Daten erhalten.

3.5.3 Public Cloud

Wir stellen Ihnen gerne eine **Public Cloud** zur Verfügung. Als Ihr Clouddienstanbieter kümmern wir uns um die gesamte Verwaltung und Wartung des Systems.

Alle Mitarbeitenden Ihres Unternehmens können vom Gerät ihrer Wahl und von jedem Büro und jeder Filiale aus, die gleichen Anwendungen nutzen, solange sie Zugang zum Internet haben. Auch wenn es Sicherheitsbedenken bezüglich Public-Cloud-Umgebungen gibt, kann eine Public Cloud bei richtiger Implementierung genauso sicher sein, wie eine besonders effektiv verwaltete Private-Cloud-Implementierung. A**ngemessene Sicherheitsmaßnahmen** sind hier der Schlüssel zum Erfolg.

4. SCHULUNGS-ANGEBOTE

Wir können Sie, unabhängig von unseren aktuellen Angeboten, in jedem Bereich der IT und des Datenschutzes schulen. Kommen Sie einfach auf uns zu und wir ermöglichen Ihnen eine passende, auf Sie individuell abgestimmte Schulung. Anbei finden Sie eine kleine Schulungsauswahl:

4.1 Informationssicherheitsbeauftragter (ISB)

Ziel ist es, die **gesetzlichen Vorschriften** zum **Datenschutz** und zur **Informationssicherheit** zu kennen und Wege aufzuzeigen, wie diese in der Praxis im Unternehmen erfüllt werden können. Zudem werden Ihre eigenen Kenntnisse im Datenschutz systematisch ergänzt und auf den neuesten Stand gebracht.

Zielgruppe:

Alle Mitarbeitenden, die sich mit dem Thema Informationssicherheit auseinandersetzen, wie: (angehende) Informationssicherheitsbeauftragte, IT-Security-Beauftragte, Management-systembeauftragte allgemein (z.B. nach ISO9001), EDV-Leiter, IT-Verantwortliche, IT-(Projekt)Manager bzw. IT-Verantwortliche innerhalb von Projektteams, Sachverständige, Datenschutzbeauftragte, Berater.
Es werden keine Vorkenntnisse benötigt, jedoch ist ein grundlegendes IT-Verständnis von Vorteil.

Inhalt:

- Rechtliche Grundlagen
- IT-Sicherheitsgesetz
- EU-DS-GVO & BDSG
- Überblick zu den Normen & Standards
- IT-Grundschutz
- ISO 27000-Reihe
- Aufbau einer Sicherheitsorganisation in den Grundzügen (ISMS)
- KVP und KPI´s
- Awareness & Kommunikationsmanagement
- Der Audit-Prozess in den Grundzügen
- Notfallmanagement nach BSI-Standard 100-4

4.2 IT-Grundschutz-Praktiker

Ziel ist es, einen **fundierten Überblick** über die Inhalte und die Umsetzung der **IT-Grundschutz-Methodik** des **Bundesamtes für Sicherheit in der Informationstechnik (BSI)** zu erhalten.

Der Schwerpunkt unserer Schulung liegt auf der Vermittlung von Fachbegriffen aus dem Bereich der Informationssicherheit. Sie erwerben das erforderliche Fachwissen für die Planung, den Aufbau, den Betrieb sowie die Aufrechterhaltung und Verbesserung eines **ISMS** gemäß BSI IT-Grundschutz bis hin zur erforderlichen Zertifizierungsreife.

Nach erfolgreichem Schulungsabschluss erhalten Sie das **IT-Grundschutz-Zertifikat auf Basis der ISO 27001**.

Zielgruppe:

Alle Personen, die in der Informationssicherheit Verantwortung tragen, wie Informationssicherheitsbeauftragte, Datenschutzbeauftragte, Berater und Führungskräfte.

Ein grundlegendes Verständnis zur IT-Grundschutz-Methodik ist sinnvoll, darüber hinaus werden keine besonderen Vorkenntnisse benötigt.

Inhalt:

- Einführung und Grundlagen der IT-Sicherheit und rechtlicher Rahmenbedingungen
- Normen und Standards zur Informationssicherheit
- Einführung IT-Grundschutz
- IT-Grundschutz-Vorgehensweise (Überblick)
- IT-Grundschutz-Kompendium (Überblick)
- Praxisübung/Praxisbeispiel zur IT-Grundschutz-Vorgehensweise
- IT-Grundschutz-Check
- Risikoanalyse
- Umsetzungsplan
- Aufrechterhaltung und kontinuierliche Verbesserung
- Zertifizierung und Erwerb des IT-Grundschutz-Zertifikats auf Basis der ISO 27001
- IT-Grundschutz-Profile
- Vorbereitung auf ein Audit
- Notfallmanagement
- Zusammenfassung und Prüfungsvorbereitung

4.3 IT-Grundschutz-Berater

Ziel dieser Schulung ist es, dass Sie danach Behörden und Unternehmen bei der **Entwicklung von Sicherheitskonzepten** sowie bei der **Vorbereitung auf eine Zertifizierung** gemäß ISO 27001 auf Basis von IT-Grundschutz unterstützen zu können. Darüber hinaus werden Sie die Kenntnisse zur **Einführung eines Managementsystems für Informationssicherheit (ISMS)** begleiten können.

Der Schwerpunkt unserer Schulung liegt auf der Vermittlung des erforderlichen Know-hows, um Organisationen bei der praktischen Umsetzung eines ISMS gemäß **ISO 27001** auf Basis des BSI IT-Grundschutzes zu beraten.

Zielgruppe:

Hauptverantwortliche der Informationssicherheit, die eine Zertifizierung beim BSI anstreben und eine Schulung zum IT-Grundschutz-Praktiker erfolgreich abgeschlossen haben, wie Informationssicherheitsbeauftragter (ISB), Information Security Manager (ISM) oder IT-Sicherheitsbeauftragter (IT-SiBe).

Inhalt:

- Normen und Standards zur Informationssicherheit
- BSI IT-Grundschutz Vorgehensweise
- BSI IT-Grundschutz-Kompendium
- BSI IT-Grundschutz-Check
- BSI-IT-Grundschutz-Profile
- Vorbereitung auf ein Audit
- Notfallmanagement

4.4 Datenschutzbeauftragter (DSB)

Schulungsziel ist es, dass Sie die **gesetzlichen Vorschriften** zum Datenschutz kennenlernen und Wege aufzeigen können, wie diese in Unternehmen zu erfüllen sind. Darüber hinaus werden Ihre eigenen Kenntnisse im Datenschutz systematisch ergänzt und auf den neuesten Stand gebracht.

Zielgruppe:

Zukünftige Datenschutzbeauftragte, sowie alle Interessierten zum Thema Datenschutz, Betriebsräte und Führungskräfte. Es werden keine gesonderten Vorkenntnisse benötigt.

Inhalt:

- Grundlagen des Datenschutzes
- Aufgaben des DSB
- Mitarbeiterdatenschutz
- IT-Sicherheitsmaßnahmen
- Übermittlung personenbezogener Daten ins Ausland
- Zusammenarbeit mit dem Betriebsrat
- Datenschutz im Marketing
- Auftragsverarbeitung & gemeinsame Verantwortung
- Praktische Umsetzung des Datenschutzes

Sehr geehrte Leserinnen und Leser

Mit unserem **IT-Servicekatalog** beschreiben wir unsere Produkte und Dienstleistungen umfassend und schaffen somit einen größtmöglichen Überblick.
Wir dokumentieren die stetige Entwicklung unserer Serviceleistungen, in Anpassung an sich fortlaufend verändernde Rahmenbedingungen. Damit stellen wir sicher, dass Sie immer auf dem neuesten Stand sind.
Die **aktuellste Version** unseres **Servicekatalogs** finden Sie unter:

www.foxgroup.de/news/

Sämtliche Services funktionieren wie ein Baukastensystem und können einzeln oder kombiniert gewählt und in die bestehende IT-Architektur integriert werden.

Alle aktuellen Schulungsangebote finden sie unter:

www.events.foxgroup.de

Weitere Schulungen können gerne angefragt werden.

Transparenz bringt Vertrauen und Vertrauen schafft Partnerschaften.
Somit legen wir mit unserem IT-Servicekatalog eine wichtige Grundlage für eine erfolgreiche Zusammenarbeit.

FOX Group

Pillerfeld 4
D-84529 Tittmoning
Tel. +49 86 83 / 99 39 0 - 0

info@foxgroup.de
www.foxgroup.de

FOX Group

Pillerfeld 4

D-84529 Tittmoning

Tel. +49 86 83 / 99 39 0 - 0

info@foxgroup.de

www.foxgroup.de

FOXiT GmbH
Pillerfeld 4
84529 Tittmoning

Vertreten durch
Geschäftsführer: Franz Obermayer