Berufsakademie Gera
Themen für die Projektarbeit

Themenvorschlag 1:

Passen Sie die vom BSI vorgegebenen Definitionen der Schutzbedarfskategorien an Ihre Behörde/Ihr Unternehmen an.
Beschreiben Sie Ihre Vorgehensweise. Zeigen und begründen Sie an zwei Beispielen, wie Sie den Schutzbedarf aufgrund dieser Definitionen festgestellt haben.

Die Projektarbeit sollte die folgenden Aspekte enthalten:

- Aufzeigen der behandelten Schutzbedarfskategorien
- Anpassen der Formulierung an die Belange der Behörde
- Befragen von weiteren für die Informationssicherheit Zuständigen, Abstimmen mit der Leitung, den Fachabteilungen und IT-Referaten.
- Vorstellung der zwei ausgewählten Beispiele (mit unterschiedlichem Schutzbedarf)
- schlüssige, an den eigenen Definitionen orientierte Begründung der Schutzbedarfsfeststellungen

Themenvorschlag 2:

Stellen Sie für Ihre Behörde/Ihr Unternehmen ein Sensibilisierungs- und Schulungsprogramm zusammen.

Die Projektarbeit sollte die folgenden Aspekte berücksichtigen:

- Welche Zielgruppen müssen sensibilisiert werden?
- Welche Schulungen sind für welche Zielgruppe notwendig (sowohl Sicherheitsschulungen als auch Anwenderschulungen)?
- Welche Schulungen sind für wen in welchem Zeitraum verpflichtend?
- Wie soll die Sensibilisierung geschehen (Vorträge, Web-based Training, Intranet-Inhalte, Sensibilisierungskampagnen)? Beschreiben Sie das Vorgehen in Ihrer Behörde.
- Wie wird Sensibilisierung aufgefrischt (Intranet)?
- Welche (möglichen) Sicherheitsvorfälle sollen behandelt werden?
- Wie und von wem (extern, intern) soll die Schulung durchgeführt werden?

Themenvorschlag 3:

Stellen Sie die organisatorischen, technischen und personellen Voraussetzungen für den Einsatz eines Intrusion Detection Systems aus der Sicht des IT-Sicherheitsbeauftragten zusammen.

Die Lösung sollte folgende Aspekte umfassen:

- Da beim Einsatz von neuen technischen Sicherheitssystemen auch die IT-Sicherheitsbeauftragten einbezogen werden sollen, müssen sie sich für eine solche Aufgabe zunächst einmal kundig machen, wie ein IDS arbeitet, welche Arten von IDS es gibt und wofür (wogegen) sie sinnvoll eingesetzt werden können.
- Als nächstes sind die Anwendungen und IT-Systeme zu identifizieren, die mit einem IDS überwacht werden sollen. Begründen Sie die Auswahl.
- Allerdings ist es nicht ausreichend, ein IDS zu implementieren, es muss auch das Wissen vorhanden sein, um die notwendigen Einstellungen vorzunehmen (Schulung, Einbindung von Externen).
- Außerdem fällt zusätzliche Arbeit für die IT-Gruppe an, um die Logfiles und mögliche Sicherheitsvorfälle zu untersuchen.
- Datenschutzrechtliche Aspekte, die eine Beratung mit dem Datenschutzbeauftragten und dem Personalrat/Betriebsrat erfordern.

Themenvorschlag 4:

Welche Maßnahmen sind einzuplanen, wenn in Ihrer Behörde/Ihrem Unternehmen Verschlüsselung und elektronische Signatur eingesetzt werden sollen?

Die Erarbeitung eines vollständigen Konzepts würde den Rahmen der Arbeit sprengen. Daher soll hier nur dargelegt werden, welche Vorgehensweise und Maßnahmen erforderlich sind.

Folgende Themen müssten bearbeitet werden:

- Welche Daten (E-Mails, Dokumente) sollen verschlüsselt bzw. signiert werden?
- Wo werden die öffentlichen Schlüssel gespeichert?
- Verfügbarkeitsanforderungen an den Schlüsselserver
- Wie wird der Schlüsselserver vor Missbrauch geschützt?
- Kriterien für die Auswahl eines Produkts
- Ablaufprozedur, wie die Schlüsselpaare generiert und den einzelnen Personen zugewiesen werden
- Ein Schlüsselpaar oder zwei (eines für Verschlüsselung und eines für elektronische Signatur)?
- Benennung von Verantwortlichen
- Schulungskonzept
- Wann müssen die Schlüssel gewechselt werden?

- Wie werden die persönlichen Schlüssel gespeichert?
- Datensicherung der Schlüssel und verschlüsselten Daten
- Regelungen für den Umgang mit Verschlüsselung und Signatur, zum Beispiel Vertretungsregelung, Schlüsselhinterlegung und Vorsorge für unvorsehbare Ereignisse (Krankheit, Verlust des Schlüssels)

Themenvorschlag 5:

Erstellen Sie ein Datensicherungskonzept für Ihre Behörde/Ihr Unternehmen.

Festzulegen sind:

- Welche Daten müssen gesichert werden?
- Art der Datensicherung
- Wo werden zu sichernde Daten hinterlegt (Server)?
- Zeitpunkt und Häufigkeit
- Vorgehensweise und Speichermedium (z.B. Band, Ausweichserver in anderem RZ)
- Aufbewahrung der Datensicherungsmedien (inkl. Schutz)
- Fristen für die Aufbewahrung und Anzahl der Generationen
- Festlegen der Verantwortlichkeiten
- Übungen zur Datenrekonstruktion
- Verpflichtung der Mitarbeiter zur Datensicherung

Themenvorschlag 6:

Erarbeiten Sie eine Dienstanweisung, in der Mitarbeiter, denen ein Gerät zur mobilen Kommunikation, z.B. ein Laptop anvertraut wird, auf einen angemessenen Umgang mit diesen Geräten hingewiesen werden. Skizzieren Sie ferner technische Maßnahmen für die Sicherheit der auf den mobilen Geräten gespeicherten Daten.

Festzulegen sind:

- Konfiguration der Laptops
- Umgang mit dem Laptop unterwegs (Diebstahlsicherung)
- Schutz des Laptops (Passwort, Bios Passwort, biometrische Sicherung)
- Einwahl ins behördeninterne Netz
- Einwahl ins Internet von unterwegs oder zu Hause
- Anschluss ins Netz in der Behörde
- Virenschutzregelungen
- Verschlüsselung

Themenvorschlag 7:

Erarbeiten Sie ein Konzept (Dienstanweisung) für den Umgang mit dem Internet in der Behörde/dem Unternehmen.
Das Konzept sollte enthalten:

- Sinn dieser Regelung
- Ist privates Surfen erlaubt: Wenn ja, in welchem Umfang, wenn nein, welche Kontrollen und Maßnahmen bei Zuwiderhandlung sind möglich.
- Regelungen für Downloads
- Erlaubte Plugins
- Erlaubte aktive Inhalte
- Umgang mit Cookies
- Proxy-Einstellungen, Filter (Welche Seiten sind gesperrt)
- Unterschiedliche Sicherheitseinstellungen im Internet und Intranet und bei den verwendeten Browsern?

Themenvorschlag 8:

Prüfen Sie die Maßnahmen, mit denen die Serverräume Ihrer Behörde/ Ihres Unternehmens physisch gesichert sind. Dokumentieren Sie Ihre Prüfergebnisse und zeigen Sie ggf. Möglichkeiten auf, mit denen die Sicherheit der dort untergebrachten IT-Systeme den Anforderungen entsprechend angepasst werden können.

Für diese Aufgabe müssen sich IT-Sicherheitsbeauftragte zunächst mit den Maßnahmen des IT-Grundschutzes für den Serverraum beschäftigen und diese verstehen. Anschließend müssen Sie den IT-Administrator interviewen und ggf. zumindest stichprobenartig die Maßnahmen überprüfen.
In der Ausarbeitung sollten zu allen im IT-Grundschutz angegebenen Maßnahmen Erläuterungen enthalten sein.

Themenvorschlag 9:

Erstellen Sie einen Netzplan über die logische Struktur des Netzes Ihrer Behörde/ Ihres Unternehmens.
Gruppieren Sie dabei die IT-Systeme soweit wie dies sinnvoll möglich ist. Begründen Sie die vorgenommenen Gruppierungen. Stellen Sie außerdem fest, welche Kommunikationsverbindungen besonders abgesichert werden sollten.
Die Einschränkung auf einen Teilbereich ist möglich.
Diese Aufgaben müssen IT-Sicherheitsbeauftragte zu Beginn der IT-Strukturanalyse und bei der Schutzbedarfsfeststellung vornehmen.

Themenvorschlag 10:

Entwerfen Sie eine Leitlinie zur Informationssicherheit für Ihre Behörde/ Ihr Unternehmen, die alle gemäß IT-Grundschutzmethodik vorgegebenen Inhalte enthält. Gehen Sie in Ihrer Skizze insbesondere auch auf die Struktur der Verantwortlichkeiten im Infomationssicherheitsprozess ein.

In der Projektarbeit sollten folgende Aspekte erläutert werden:

- Stellen Sie ein Modell des Informationssicherheitsprozesses vor, an dem die Bedeutung der Leitlinie zur Informationssicherheit für weitere Maßnahmen des Sicherheitsmanagements erklärt wird
- Unterscheiden Sie die Verantwortlichkeiten für Informationssicherheit in Ihrer Behörde/Ihrem Unternehmen
- Erläutern Sie an Hand einer Grafik die für Informationssicherheit zuständigen Instanzen, Gremien und ihre Zuordnung zur Leitung
- Zeigen Sie in Schritten auf, wie Ihre Behörde/Ihr Unternehmen zu einer wirksamen IT- Sicherheitsleitlinie kommt
- Erläutern Sie im Entwurf der Leitlinie zur Informationssicherheit Ihre Formulierung für die Bedeutung der IT für Ihre Behörde/Ihr Unternehmen, wie wichtig die IT für die Geschäftsvorgänge/IT-Anwendungen ist und welches Sicherheitsniveau erreicht werden sollte.
  Nennen Sie die wichtigsten Sicherheitsziele und was Sie als grobe Sicherheitsmaßnahmen und als organisatorische Regelungen vorschlagen, um diese Ziele zu erreichen:
- Erklären Sie, wie die Beschäftigten über diese Leitlinie informiert werden sollten

Themenvorschlag 11:

Entwerfen Sie ein Virenschutzkonzept für Ihre Behörde/Ihr Unternehmen.
Auch die Konzepterstellung für eine Ergänzung, Aktualisierung oder Migration eines bestehenden Virenschutzkonzeptes ist möglich.
Berücksichtigen Sie dabei sowohl die zentralen als auch die dezentralen Möglichkeiten zum Schutz vor Schadsoftware oder Spam.

Es sollten zu allen im IT-Grundschutz Baustein Computer-Virenschutzkonzept enthaltenen Maßnahmen Aussagen zu Ihrer Behörde/Ihrem Unternehmen getroffen werden.

Themenvorschlag 12:

Erarbeiten Sie eine Vorlage zur Entscheidung für die Behördenleitung, in der Sie verschiedene Firewallkonzepte sowie deren Vor- und Nachteile skizzieren und begründen Sie, welches das geeignete Konzept für Ihre Behörde/Ihr Unternehmen ist.

Sinn dieser Aufgabe ist, die verschiedenen Firewallkonzepte zu verstehen und eine Auswahl und ihren Einsatz in der Behörde/dem Unternehmen zu begründen.

Themenvorschlag 13:

Entwerfen Sie einen Fragebogen, mit dessen Hilfe Sie die Akzeptanz verschiedener einschränkender Sicherheitsmaßnahmen bei den Benutzern testen:

a) der Verschluss von Laufwerken an den Clients,
b) das Verbot, eigenmächtig Programme zu installieren
c) Internetfilter
d) Passwortregelungen (Anforderung an die Güte und Länge der Passwörter, regelmäßiger Passwortwechsel, Umgang mit dem Passwort)
e) das Verbot, Brandschutztüren offen zu halten
f) Sperrung des APC bei Verlassen des Raumes, Einsatz von Bildschirmschonern

Entwerfen Sie ferner kurze Erläuterungstexte, in denen Sie den Benutzern den Sinn der jeweiligen Maßnahmen begründen.

Themenvorschlag 14:

Angenommen, es wird von Ihrer Behörden- bzw. Firmenleitung erwogen, die beiden Aufgaben Administration der Firewall und Durchführung der Datensicherung für einen Standort der Behörde an ein externes Dienstleistungsunternehmen zu vergeben.
Erstellen Sie eine Präsentation, in der Sie der Behördenleitung die Vor- und Nachteile einer solchen Lösung darstellen und Anforderungen formulieren, die ein Dienstleistungsunternehmen für diese Aufgaben erfüllen muss.

Themenvorschlag 15:

Entwerfen Sie ein Konzept für die Reaktion auf Sicherheitsvorfälle (einschließlich Zuständigkeiten und Meldewegen, Nachbereitung etc.).
Berücksichtigen Sie dabei unterschiedliche Arten von Vorfällen (z.B. Virenbefall, Hackereinbruch, Systemzusammenbruch durch technisches Verfahren).
Allgemein beschrieben sind die Maßnahmen bei Sicherheitsvorfällen im IT-Grundschutz M 6.60.
Diese und insbesondere die Meldewege sind auf die Behörde angepasst in der Ausarbeitung zu spezifizieren.

Themenvorschlag 16:

Stellen Sie die wesentlichen Anwendungen zusammen, die in Ihrer Einrichtung eingesetzt werden. Bestimmen Sie für jede Anwendung anhand zuvor festgelegter Kriterien, welchen Bedarf an Verfügbarkeit sie hat, und beschreiben Sie für zwei bis drei Anwendungen mit höheren Verfügbarkeitsanforderungen, mit welchen Maßnahmen Sie diese Anforderungen gewährleisten wollen.

Die Ausarbeitung sollte enthalten:

- Spezifikation für normale, hohe und sehr hohe Verfügbarkeit
- Begründung für die Verfügbarkeitsanforderungen von ca. 10 Anwendungen
- Maßnahmen für zwei bis drei Anwendungen, die zu einer hohen Verfügbarkeit der Anwendungen beitragen

Themenvorschlag 17:

Ihre IT-Administration schlägt den Einsatz von Security Scannern vor. Informieren Sie sich über Arten und Leistungen von Security Scannern auf dem Markt.

Beschreiben Sie die wesentlichen Aufgaben dieser Produkte und stellen Sie Kriterien zusammen, die ein solches Werkzeug erfüllen sollte, damit es in Ihrer Einrichtung eingesetzt werden kann. Begründen Sie mit Hilfe dieser Kriterien, welches dieser Programme ausgewählt werden sollte.

Themenvorschlag 18:

Entwerfen Sie eine Struktur (Gliederung) mit allen wesentlichen Inhalten zur Informationssicherheit, die von unterschiedlichen Benutzergruppen aus Ihrem Intranet abgerufen werden können.
Schlagen Sie eine sinnvolle Struktur vor und ordnen Sie Themen zu und erläutern Sie das Informationsangebot (inklusive Aktualisierung).

Themenvorschlag 19:

Ihre Einrichtung plant die Einführung eines chipkartengestützten Zeiterfassungssystems. Eine wesentliche Komponente soll ein zentraler Server sein, auf dem die Zeitdaten aller Beschäftigten gespeichert sind, zusammen mit allen anderen Daten, die für die Lohn- und Gehaltsabrechnung bedeutsam sind.
Stellen Sie die wichtigen Sicherheitsanforderungen an die Anwendung und an den Server zusammen.

Themenvorschlag 20:

In einer Behörde ist ein homogenes Windows XP-Netz mit entsprechenden Clients und Servern eingerichtet.
Entwerfen Sie eine Sicherheitsrichtlinie für die Clients, die ausschließlich für übliche Büroanwendungen und E-Mail benutzt werden.
Begründen Sie Ihre Entscheidungen.

Themenvorschlag 21:

In Ihrer Einrichtung ergibt sich die Notwendigkeit funkgebundener Kommunikation, z.B. weil Kabel nicht über ein dazwischen liegendes Gebiet gezogen werden können.
Entwickeln Sie für Ihre Behörden-/Ihre Unternehmensleitung eine Entscheidungsgrundlage für den Einsatz eines WLAN Konzeptes.
Erarbeiten Sie die dafür notwendigen Sicherheitsmaßnahmen.
Stellen Sie sichere Zugangsmöglichkeiten dar. Betrachten und beachten Sie bei der Integration und Nutzung der WLAN - Technik die organisatorischen und technischen Randbedingungen ihrer Behörde.

Themenvorschlag 22:

Ihre Behörde/Ihr Unternehmen plant eine Zertifizierung nach ISO 27001 auf Basis von IT Grundschutz. Erstellen Sie hierfür einen Projektplan.
Berücksichtigen Sie dabei maßgebliche Komponenten, wie

- Initiierung des Informationssicherheitsprozesses
  - Definition des betrachteten IT-Verbundes, der Leitlinie zur Informationssicherheit und die Einrichtung des Sicherheitsmanagements.
- Durchführung einer IT-Strukturanalyse
  - Erfassung Komponenten des IT Verbundes IT-Anwendung, IT-System, Raum und Kommunikationsverbindung
- Durchführung einer Schutzbedarfsfeststellung
  - Festlegen mit einer auf den IT-Verbund angepassten Definition der Schutzbedarfskategorien, die in der Institution abgestimmt ist.
- Modellierung nach IT-Grundschutz
  - Modellierung nach IT-Grundschutz (Phase 4) unter Zuhilfenahme des GSTOOL
- Durchführung des Basis-Sicherheitsscheck
  - Durchführung des Basis-Sicherheitsscheck unter Verwendung des GSTOOL

Themenvorschlag 23:

In Ihrer Einrichtung fallen Daten an, die bezüglich der Grundwerte Vertraulichkeit, Integrität und Authentizität einen höheren Schutzbedarf benötigen. Zum Schutz der genannten Grundwerte sollen kryptographische Verfahren eingesetzt werden.
Entwickeln Sie zum Schutz dieser Daten ein Kryptokonzept unter Berücksichtigung des BSI Kryptoleitfadens und der BSI-Arbeitshilfe zur Erstellung von Kryptokonzepten.

Themenvorschlag 24a:

In Ihrer Behörde steht eine Migration von Clients an. Evaluieren Sie aus Sicht des IT-Sicherheitsbeauftragten, welche Auswirkungen diese geplante Migration auf Sicherheitsaspekte hat. Entwickeln Sie eine Entscheidungsvorlage für ihre Behördenleitung zur Migration der Clients. Begründen Sie ihre Entscheidung, indem Sie auf technische und organisatorische Maßnahmen eingehen.

Themenvorschlag 24b:

In Ihrer Behörde steht eine Migration der Serverumgebung an. Evaluieren Sie aus Sicht des IT-Sicherheitsbeauftragten, welche Auswirkungen diese geplante Migration auf Sicherheitsaspekte hat. Entwickeln Sie eine Entscheidungsvorlage für Ihre Behörden-/Ihre Unternehmensleitung zur Migration der Umgebung. Begründen Sie ihre Entscheidung, indem Sie auf technische und organisatorische Maßnahmen eingehen.

Anm.: Themen 24a und 24b können auch zusammengelegt werden. Hier ist jedoch der Aufwand zu beachten

Themenvorschlag 25:

In Ihrem IT-Umfeld wird bei der Schutzbedarfsanalyse ein höherer Schutzbedarf identifiziert. Im Rahmen der IT-Grundschutz-Vorgehensweise wird zunächst in einer ergänzenden Sicherheitsanalyse untersucht, welche Zielobjekte mit Hilfe einer Risikoanalyse genauer betrachtet werden müssen.
Berücksichtigen Sie dabei maßgebliche Komponenten, wie

- Erstellung einer Gefährdungsübersicht
- Ermittlung zusätzlicher Gefährdungen
- Bewertung der Gefährdungen
- Behandlung der Risiken und Maßnahmenauswahl
- Konsolidierung des Sicherheitskonzepts

Themenvorschlag 26:

In Ihrer Einrichtung ist ein Geschäftsprozess besonders wichtig. Analysieren Sie die Verfügbarkeitsanforderungen dieses Prozesses und die Auswirkungen, die der Ausfall dieses Prozesses auf Ihre Behörde/Ihr Unternehmen hätte.
Entwerfen Sie Maßnahmen, bezogen auf

- Infrastruktur
- Organisation
- Personal
- Technik
- Kommunikation

die für die Aufrechterhaltung (und den Wiederanlauf) des Prozesses notwendig sind. Beachten Sie auch sog. Sofortmaßnahmen.

Themenvorschlag 27:

In Ihrem Hause steht mittelfristig eine Informationssicherheitsrevision auf Basis von IT-Grundschutz an. Entwickeln Sie einen Maßnahmenplan oder Projektplan, um sich einen Überblick über das Thema „IS-Revision“ zu verschaffen. Machen Sie sich durch Ihren Maßnahmenplan mit den Voraussetzungen und dem Ablauf einer IS-Revision vertraut.