

[[TOC]]

Modul 263 - LBV 3

Beruf

- ICT-Fachfrau/Fachmann EFZ

Bezug zur Modulversion

-

Institut (Bezug zum Autor, mehrere Institutionen möglich)

gibb Berufsfachschule Bern

Verfasser (Wird nicht im MBK publiziert)

Susanne Annen

Übersicht

Beschreibung

Zweiteilige LB mit einer Fallanalyse und einer praktischen Umsetzung in einer Gruppe

Anzahl LBV-Elemente

2

Richtzeit Total (über alle Elemente)

14

Ergänzung (Wird nicht im MBK publiziert)

Element 1

Prüfungs - und Sozialform

- Methode: schriftlich
- Prüfungsform: Fallanalyse

Gewichtung

- 50%

Richtzeit (Empfehlung)

- 2

Hilfsmittel

Gemäss Vorgabe der Schule

Element Beschreibung

Die schriftliche Fallanalyse umfasst folgende Themen:

- Fallanalyse (ein Benutzerendgerät in einem Firmennetzwerk) gemäss Strukturanalyse IT-Grundschutz (Netzplan, Applikationen, Systeme) analysieren.
- Bedrohungen gemäss Fallbeschreibung mittels IT-Grundschutz bestimmen und Fragen des Kunden zu Bedrohungen beantworten.
- Zu konkreten Bedrohungen des Falls Massnahmen definieren.
- An einer virtuellen Maschine mit technischen Hilfsmittel die ordnungsgemässe Funktion überprüfen und die Wirksamkeit des Schutz überprüfen.

Zu überprüfende Handlungsziele 1 IT-Sicherheitsbegriffe erläutern (Schutzobjekte, Schwachstellen, Bedrohungen, Gefahr, Datenschutz, Datensicherheit, Schutzmassnahmen) und Zusammenhänge verstehen. 2 ICT-Endgeräte gemäss Vorgabe auf eine entsprechende Sicherheits-Konfiguration hin überprüfen.

Bewertung

HZ1 50%

HZ2 50%

Praxisbezug

ICT-Fachleute müssen Bedrohungen systematisch analysieren, Schutzmassnahmen definieren und Kunden entsprechend beraten können.

Element 2

Prüfungs - und Sozialform

- Methode: praktisch am Objekt
- Form: Gruppenarbeit

Gewichtung

- 50%

Richtzeit (Empfehlung)

12

Hilfsmittel

Unterlagen, Internet, Literatur, usw.

Element Beschreibung

In Gruppen wird ein Benutzerendgerät (z.B Windows 11 Client, Android-Handy, usw) ausgewählt. Im Bewertungsraster befinden sich je nach Gruppengrösse Anforderungen die nach BSI umgesetzt werden müssen. Die Gruppenmitglieder setzen folgendes um:

- Zu den vorgegebenen Anforderungen nach BSI(Basis und/oder Standard) geeignete Umsetzungsmassnahmen und geforderte Konfigurationen definieren, so dass die Anforderungen nach BSI erfüllt sind.
- Die Konfigurationen an einer virtuellen Maschine oder einem vorhandenen Gerät (z.B. Handy) umsetzen. Die Umsetzung in einem Protokoll zur Nachvollziehbarkeit festhalten. Benutzer gemäss den getroffenen Massnahmen schulen.
- Ein Benutzerendgerät isolieren und einen Wiederanlauf vornehmen. Mit einem Protokoll die Vorgehensweise zur Nachvollziehbarkeit festhalten.

Zu überprüfende Handlungsziele 2 ICT-Endgeräte gemäss Vorgabe auf eine entsprechende Sicherheits-Konfiguration hin überprüfen. 3 ICT-Endgeräte gemäss vorgegebenen Sicherheitsmassnahmen konfigurieren. 4 Unsichere oder befallene ICT-Endgeräte in einem Ereignisfall isolieren und die nötigen Massnahmen zur Schadensbegrenzung, Analyse und Wiederanlauf einleiten

Bewertung

HZ2 45%

HZ3 45%

HZ4 10%

Siehe beigelegtem Bewertungsraster.

Praxisbezug

ICT-Fachleute müssen in der Lage sein, entsprechende Schutzmassnahmen an einem Computer, Natel, Tablet umzusetzen, die Nachvollziehbarkeit dokumentieren, und Kunden für einen Sicheren Umgang schulen können.
