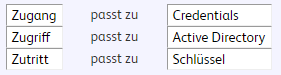
Vor – und Nachbearbeitungsübungen

# SW01

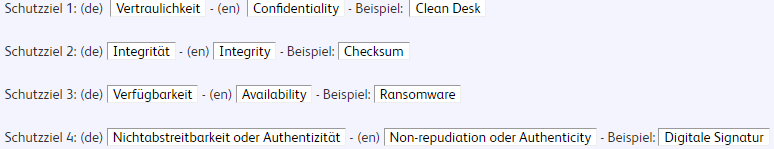
Das Ziel der Informationssicherheit ist die Sicherheit vorhanden Informationen. Diese Sicherheit wird durch Risiken bedroht. Ein Risiko wird wie folgt berechnet: Eintretenshäufigkeit x Schadenhöhe. Zur Mitigation (Behandlung von Risiken) werden Massnahmen benötigt, um das Restrisiko zu senken und möglichst klein zu halten.

Es Gibt folgende Mitigationsmöglichkeiten:

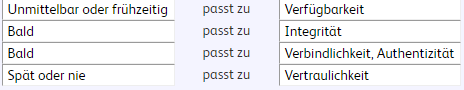
* Risiko eliminieren
* Risiko reduzieren
* Risiko transferieren
* Risiko akzeptieren



Die 4 Schutzziele mit jeweils einem Beispiel:



Die 4 Schutzziele mit den jeweiligen Entdeckungszeiträumen.



Die Massnahmen zur Erhöhung der Informationssicherheit müssen immer in drei Bereichen eingeführt werden. Nämlich in folgenden:

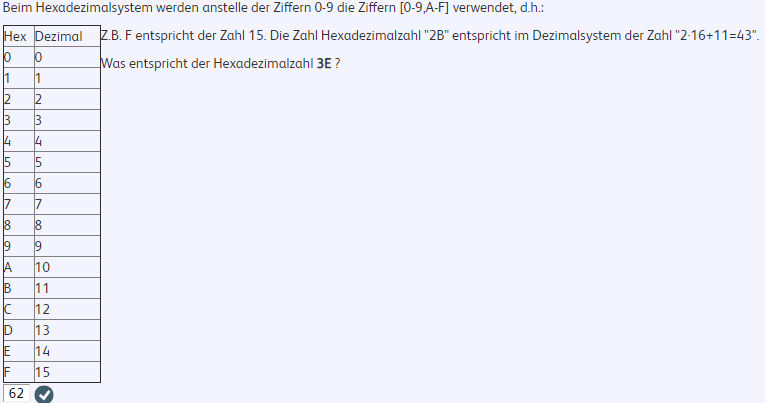
* Menschen
* Prozesse
* Technik

# SW02

Hashwerte und ihre Zeichen:

Der MD5-Hash ist 32 Zeichen lang. DER SHA1- Hash ist 40 und der SHA-512-Hash ist 128 Zeichen lang.

## Hexadezimalsystem



## Modulo

Beim Addieren modulo 26 werden jeweils Zahlen addiert, das Resultat ist aber immer der Rest, wenn die Summe durch 26 geteilt wird.

Z.B.

* 25 + 1 = 26 ≡ 0 (mod 26)
* 13 + 17 = 30 ≡ 4 (mod 26)
* 3 + 4 = 7 ≡ 7 (mod 26)
* 15 + 17 modulo 26 = 6

# SW03

Beispiel Aufgabe:

Alice und Bob machen das Diffie-Hellman-Protokoll um einen gemeinsamen Schlüssel zu vereinbaren:

Alice wählte n=2833 und g=641 und a=13 zufällig. Sie rechnet A=ga=1150 mod 2833.

Sie schickt n, g und A an Bob.

Bob wählt b=20 zufällig und schickt B=g20=23 mod 2833 an Alice.

Was ist der gemeinsame Schlüssel?

* Der Wert ist 482

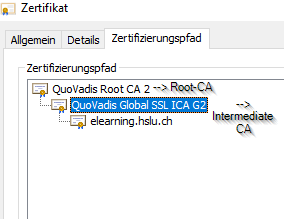
Gemäss BSI - Bundesamt für Sicherheit in der Informationstechnik soll die Schlüssellänge für RSA (Factoring Modulus) in den Jahren 20182020 mind. **2000** sein.

# SW04

In einem X.509-Zertifikat (Standard zum Erstellen digitaler Zertifikate) sind folgende Anhaben enthalten:

* Angaben zum Zertifikatsinhaber
* Gültigkeitsdauer
* Öffentlicher Schlüssel
* Angaben zum Aussteller
* Signatur des Austellers

## Zertifikatspfad von derHSLU Webseite



## Public Key Kryptographie

Bob hat sich ein (Public Key, Private Key)-Paar erstellt. Als er letztes Mal Alice getroffen hat, hat er ihr seinen Public Key gegeben und Alice hat ihn bei sich gespeichert.

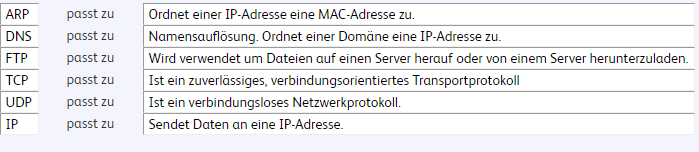
Später hat sich Alice auch ein (Public Key, Private Key)-Paar erstellt. Seitdem hat sie aber Bob nicht mehr getroffen und konnte ihm deshalb ihren Public Key noch nicht geben.

Die beiden möchten trotzdem miteinander kommunizieren.

* Alice kann Bob eine verschlüsselte Nachricht schicken, welche dieser entschlüsseln kann.
* Alice kann Bob eine signierte Nachricht senden, welche dieser lesen kann.
* Alice kann Bob eine verschlüsselte und signierte Nachricht schicken, welche dieser lesen kann.
* Bob kann Alice eine signierte Nachricht senden, welche diese lesen kann.
* Alice kann prüfen, dass die signierte Nachricht von Bob signiert wurde.

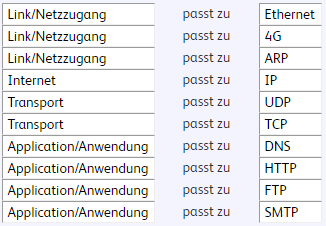
# SW05

Was passt zu welchen Protokollen:



Der TCP/IP-Protokollstapel wird normalerweise in 4 Schichten, Netzzugang, Internet, Transport und Anwendung, unterteilt.

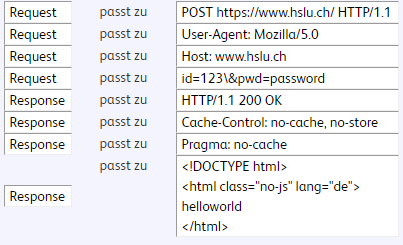
Hier die Zuordnung folgender Protokolle zu den TCP/IP-Protokollstapel:



# SW06

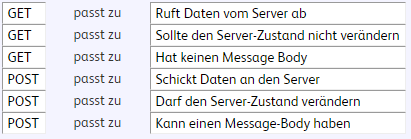
## http Request und Response

HTTP besteht aus Requests und Responses.



## http Request Methoden

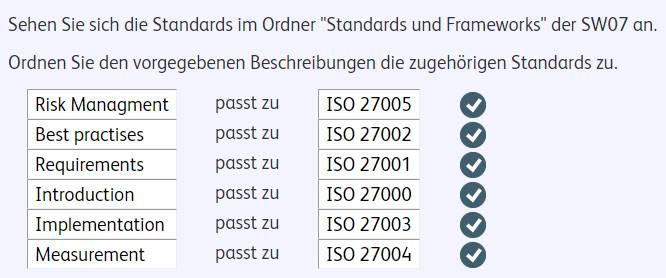
* GET
* POST
* PUT
* HEAD
* PATCH
* OPTIONS
* DELETE



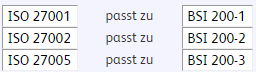
# SW07

Hier die Zuordnung des ISO Standards zu deren Inhalten:





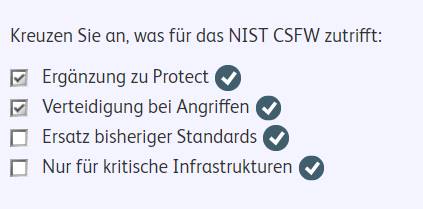
Hier die Zuordnung der ISO Standards zu den passenden BSI-Standards:





## NIST Cyber Security Framework

Die bisherigen Standards decken die NIST Functions Identify und Protect ab. NIST setzt einen grossen Fokus auf Detect , Respond und Recover.



## ISMIS

Ein ISMS nach ISO 27001 ist ein Plan Do Check Act (PDCA) Prozess, der die professionelle Einführung und Betrieb der Informationssicherheit einer Unternehmung unterstützen soll. Dieser Prozess wird regelmässig, in der Regel jährlich oder bei signifikanten Veränderungen / neuen Risiken / Übernahmen durchgeführt. Das wichtigste Element der Sicherstellung der Qualität ist die Überwachung / Messung, auch im Rahmen von Audits und entsprechende Korrekturen.

# SW08

Eine Risiko-Analyse ist ein wichtiges Element des Risiko-Managements. Es gibt quantitative und qualitative Analysen. Bei letzterer wird das Risiko als Multiplikation der Eintretenshäufigkeit und der Schadens-Höhe eingeschätzt. Zur Vereinfachung werden keine absoluten Werte verwendet, sondern Häufigkeits- und Schadens- Kategorien gebildet.

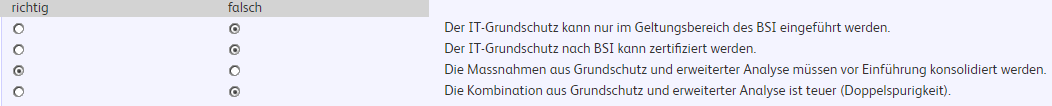
Das Risiko-Management wird mittels ISO 27005 und / oder BSI 200-3 durchgeführt. Das Ziel ist, das Risiko durch geeignete Massnahmen zu mitigieren und das Gesamt-Risiko zu minimieren oder verkleinern oder reduzieren. Das Risiko wird aus der Eintretenshäufigkeit oder Häufigkeit multipliziert mit der Schadenshöhe berechnet.

Der Risiko Management Prozess wird gemäss Standard wie folgt durchgeführt:

* Context Establishment
* Risk Identification
* Risk Estimation
* Risk Evaluation
* Risk Treatment
* Risk Acceptance

Der IT-Grundschutz hilft, die wichtigsten Massnahmen zu ergreifen. Er garantiert aber keine ausreichende Sicherheit. Dieser sollte (muss aber nicht) immer eingeführt werden, da man damit einen gute Basis für Sicherheit erhält.

IT-Grundschutz nach BSI-2



# SW09

Zu den Vorteilen der kombinierten Risiko-Analyse gehören:

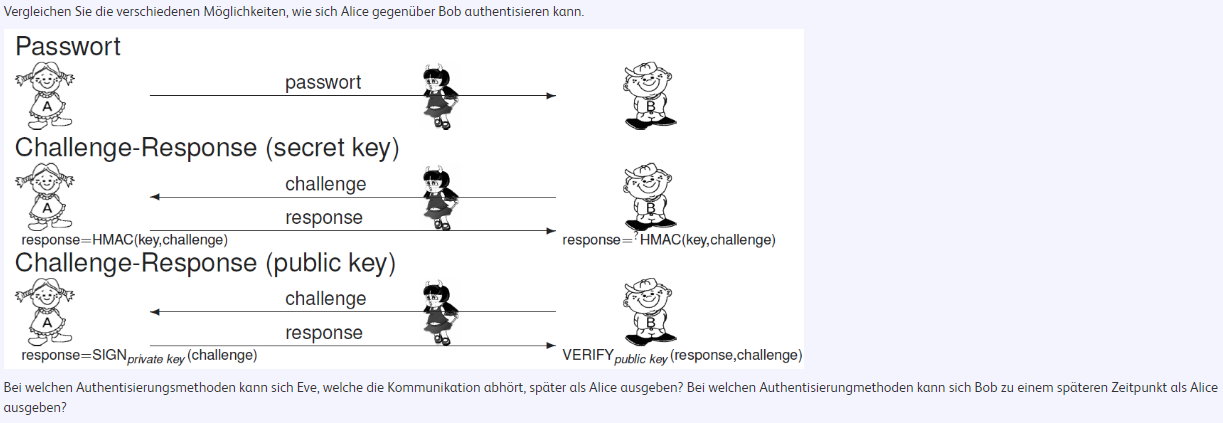
* geringere Gesamt- Kosten
* grossteils durch den Grundschutz gewährleistete Sicherheit / Abdeckung
* weitgehende Vollständigkeit durch die ergänzende Risiko-Analyse
* ca. 80 % Erfüllung bereits durch den Grundschutz (Pareto-Regel)
* bewährte Kombination der Standards ISO 27005 und BSI 200-2 und 200-3

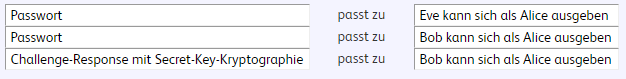
Awareness hat zum Ziel, den Faktor Mensch gebührend in einer holistischen Sicht der Informations-Sicherheit zu würdigen, weil die anderen beiden Säulen Technik und Prozess Aspekte keine ausreichende Sicherheit bieten. Wichtig für grosse Nachhaltigkeit ist, eine grundsätzliche Schulung der Mitarbeitenden mit regelmässigen Kampagnen, begleitet von flankierenden Massnahmen , zu kombinieren.

Ein sicheres Passwort sollte möglichst kompliziert sein, aber am wichtigsten ist, dass die Länge genügend lang ist.

# SW10

## Vergleich Authentisierungsmethoden





### Challenge-Response-Verfahren mit Secret Key Kryptographie

1. Bob schickt an Alice eine Challenge.
2. Alice berechnet die Response.
3. Die Response wird als Hash (segret II challenge) berechnet.
4. Bob prüft die Response

### Authentisierung mit Public-Key-Kryptographie

Alice (Client) möchte sich gegenüber Bob (Server) in einem Challenge-Response-Verfahren mit Public-Key-Kryptographie authentisieren.

* Bob benötigt Alice’s Public Key
* Um die Response zu generieren wird Alice’s Private Key verwendet

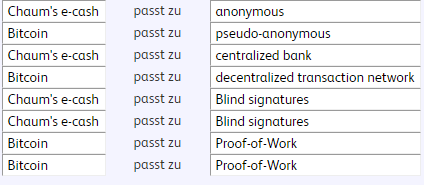
# SW11

Bei einem Zero-Knowledge Proof of Knowledge geht es darum, dass ein Prover einen Verifier überzeugen möchte, dass sie einen bestimmten Wert x kennen, ohne irgendwelche Information über den Wert x preiszugeben.

Das Dating Problem entspricht der sicheren verteilten Berechnung der AND Funktion.

Digital Cash birg neben der Fälschungssicherheit, das Problem der Anonymität und Double spending.

Zuordnung der digitalen Cashs zu deren passenden Eigenschaften:



# SW12

## Angriffe

Sie sind Betreiber einer Webanwendung und schauen sich die Requests an, welche auf Ihrem Server eingehen. Dabei sehen Sie, dass ein Benutzer beim Login anstelle eines gültigen Benutzernamens folgenden String eingegeben hat:

* x'; DROP TABLE members; --

Vermutlich versucht dieser Benutzer gerade einen SQL-Injection-Angriff

Sie sind Betreiber einer Webanwendung und schauen sich die Requests an, welche auf Ihrem Server eingehen. Dabei sehen Sie, dass ein Benutzer in einem Kommentarfeld folgenden String eingegeben hat:

<SCRIPT type="text/javascript">

var adr = '../evil.php?cakemonster=' + escape(document.cookie);

</SCRIPT>

Vermutlich versucht dieser Benutzer gerade einen Cross-Site-Scripting-Angriff

# SW13

Gegen welche Angriffe schützt URL-encryption und welche Einstellungen sind nötig, damit URL-encryption gegen diese Angriffe schützt:

* Forceful browser (Benutzer versucht durch direktes Aufrufen einer URL auf Seiten oder zu gelangen, welche eigentlich nicht (öffentlich) zugänglich sein sollten).
* Information Hiding (Benutzer sieht nicht, welche Directories und Resourcen auf dem Webserver existieren)
* Injection im URL-Parameter (z.B. SQL-injection)
* Cross-Site Request Forgery

## Gatter

