Klasse: ITB U
Fach: LF2
Lehrer: Hr. Epping
Datum:

Berufskolleg Hilden
des Kreises Mettmann • Europaschule

IT-Sicherheit, Informationssicherheit und Datenschutz

1. Schutzziele im Vergleich: Welche Beschreibung passt zu welchem Schutzziel?

Schutzziele	Beschreibungen
1) Datenschutz 2) Datensicherheit 3) IT-Sicherheit 4) Informationssicherheit	a) Dieser Begriff zielt auf den Schutz aller Informationen (digital/analog). b) Unter diesem Begriff wird der Schutz der privaten, personenbezogenen Daten eines jeden Menschen verstanden. c) Sie bezieht sich allgemein auf den Einsatz von Informationstechnik und gewährleistet, dass die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen geschützt sind. d) Es geht um den Schutz aller Daten in Unternehmen, unabhängig davon, ob diese einen Sachbezug oder einen Personenbezug haben, ob digital oder analog. e) Bürgern wird das Recht auf informationelle Selbstbestimmung gewährt.

Lösung: 1b, 1e, 2d, 3c, 4a

2. Wofür steht die Abkürzung „DSGVO“? **Datenschutzgrundverordnung**

3. Wofür steht die Abkürzung „BSI“, wenn es um Datenschutz in der IT geht?

   Das Bundesamt für Sicherheit in der Informationstechnik (BSI) befasst sich mit allen Fragen rund um die IT-Sicherheit in der Informationsgesellschaft. Ziel des BSI ist es, den sicheren Einsatz von Informations- und Kommunikationstechnik in unserer Gesellschaft zu ermöglichen und voranzutreiben.

4. Ab welcher Firmengröße (Anzahl der Mitarbeiter) muss die Firma einen Datenschutzbeauftragten benennen? Und wer darf diesen Posten ausüben?

   Das Unternehmen beschäftigt mindestens 10 Mitarbeiter

   Datenschutzbeauftragter kann ein interner (geschulter) Mitarbeiter oder ein externer Beauftragter sein. Verallgemeinert gilt, dass bei folgenden Mitarbeitern aufgrund einer Interessenkollision keine Benennung zum DSB erfolgen kann: **Geschäftsleitung, z.B. Vorstand oder Geschäftsführer. Betriebsleiter. Leiter der EDV.**

5. Nennen Sie mind. 5 Beispiele für personenbezogene Daten.
   - **Name, Alter, Familienstand, Geburtsdatum**
   - **Personalausweisnummer, Sozialversicherungsnummer**
   - **Adressdaten sowie Telefonnummer, E-Mail-Adresse**
   - **Konto- und Kreditkartennummer**
   - **Bonitätsdaten**
   - **Kraftfahrzeugnummer, Kfz-Kennzeichen**
   - **Gesundheitsdaten und genetische Daten**
   - **rassische und ethnische Herkunft**
   - **politische Meinungen**
   - **religiöse oder weltanschauliche Überzeugungen**
   - **Gewerkschaftszugehörigkeit**
   - **Werturteile wie zum Beispiel Zeugnisse**
   - **Vorstrafen**
   - **IP-Adresse und Cookies**
   - **Meinungen, Beurteilungen oder Einschätzungen**

6. Für wen gilt die DSGVO?

   Die Datenschutzverordnung gilt für:

   - **alle Unternehmen, die in der EU ansässig sind.**
   - **Allerdings müssen sich auch außereuropäische Unternehmen an die neuen Regelungen halten. Das gilt aber nur wenn sie:**
     - **eine Niederlassung in der EU haben oder**
     - **personenbezogene Daten von EU-Bürgern verarbeiten**

7. Was ist richtig?
   a) Beim Datenschutz wird im Unternehmen ausschließlich an den Schutz der Unternehmensdaten gedacht.
   b) Offiziell informiert das BSI zur IT-Sicherheit.
   c) Informationssicherheit ist im IT-Grundschutzkompendium des BSI oder in der ISO 9000 beschrieben.
   d) Integrität der Daten bedeutet Korrektheit der Daten.
   e) Beim Phishing werden durch Tricks Logindaten unrechtmäßig erlangt.
   f) Echotet ist ein Botnetzvirus.

   Das IT-Grundschutz-Kompendium ist die grundlegende Veröffentlichung des IT-Grundschutzes. Zusammen mit den BSI-Standards bildet es die Basis für alle, die sich umfassend mit dem Thema Informationssicherheit befassen möchten.

8. Sicherheitsvorfälle: Welche Cyberkriminelle Methode passt zu welcher Beschreibung?

Methode	Beschreibung
1) Phishing 2) Keylogger 3) Nicknapping 4) Scareware 5) Malware (Malicious Software) 6) Ramsomware 7) Botnetz 8) DoS (Denial of Service) 9) CEO-Fraud oder „Cheftrick“	a) Ein Verbund von Rechnern (Systemen), die unbemerkt von einem fernsteuerbaren Schadprogramm (Bot) befallen sind b) Schadprogramme, die wie Viren, Würmer oder Trojanische Pferde c) Methode der Angreifer, „Chefmails“ an Mitarbeiter, insbesondere des Rechnungswesens, zu senden, um damit Betrügereien zu unternehmen. d) Da drunter versteht man den Missbrauch des Klarnamens oder Alias-Namens einer Person, oft in Zusammenhang mit gestohlenen Passwörtern oder anderen persönlichen Daten. e) Schadprogramme, die den Zugriff auf Daten und Systeme einschränken oder verhindern und diese Ressourcen nur gegen Zahlung eines Lösegeldes (engl. ransom) wieder freigeben f) Hard- oder Software zum Mitschneiden von Tastatureingaben g) Manipulierte Webseiten und Websites/E-Mails mit Links zu Anmelde- oder Prüfseiten, mit denen Passwörter und Login-Daten abgegriffen werden. h) Verweigerung des Dienstes, z. B. durch gekaperte Computer, die Server durch Massenanfragen zusammenbrechen lassen. i) Angstsoftware, die der Nutzer selbst auf seinem System installiert, weil ihm ein Schaden vorausgesagt wird. j) Wortspiel aus „Password“ und „Fishing“ oder „nach Passwörtern angeln“.

Lösung: 1g, j; 2f; 3d; 4i; 5b; 6e; 7a; 8h; 9c

9. Geben Sie für jedes der drei Schutzziele von Datensicherheit ein konkretes Beispiel an.

Sicherheitsmaßnahme	Vertraulichkeit	Integrität	Verfügbarkeit	Begründung
Sichere Passwörter wählen	x			Der Zugriff Fremder auf die Benutzerdaten wird besser geschützt.
Regelmäßige Datensicherung der Patientendaten				
Verschlüsselung der Festplatten				
Zentrale Bearbeitung wichtiger Dokumente auf Server				
Hashwertüberprüfung bei Softwareinstallation				

Schutzmaßnahme	Vertraulichkeit	Integrität	Verfügbarkeit	Begründung
Sichere Passwörter wählen	x			Der Zugriff Fremder auf die Benutzerdaten wird besser geschützt.
Regelmäßige Datensicherung der Patientendaten			x	Daten können bei Verlust der Originaldaten wiederhergestellt werden.
Verschlüsselung der Festplatten	x			Inhaltliche Nutzung der Daten ist für unberechtigte Benutzer nicht möglich.
Zentrale Bearbeitung wichtiger Dokumente auf Server		x		Kein unterschiedlicher Bearbeitungsstand der Dokumente (z. B. auf Clients).
Hashwertüberprüfung bei Softwareinstallation		x		Wenn der zusammen mit der Software übermittelte Hashwert identisch ist mit dem berechneten Hashwert, kann man davon ausgehen, dass die Software keinen eingeschleusten Trojaner beinhaltet.

Andere Lösungen mit sinnvollen Begründungen sind möglich.