|  |  |  |
| --- | --- | --- |
| **2. Ausbildungsjahr** | **Fachinformatiker/in Fachrichtung Systemintegration – Fachinformatiker/in Fachrichtung Anwendungsentwicklung** | |
| **Fach** | ITK (Informations- und Telekommunikationssysteme) – mit dem berufsübergreifenden Fach Deutsch/Kommunikation | |
| **Lernfeld 7** | LF 7 Vernetzte IT Systeme (100 UStd.) | |
| **Lernsituation 7,2** | Sichere Mailkommunikation durch End-to-End Verschlüsselung (16 UStd.): | |
| Einstiegsszenario  Sie arbeiten als Auszubildender in der IT Abteilung des mittelständischen Werkzeugherstellers Burn IT. Auf Grund einer fehlgeleiteten Mail mit sensiblen firmeninternen Daten (Konstruktionszeichnungen für einen Patenantrag und interne Kostenkalkulation) fordert Ihre Geschäftsleitung von Ihrem Abteilungsleiter, dass unverzüglich Maßnahmen eingeleitet werden, die eine sichere Kommunikation aller Beteiligten (Ingenieure, technische Mitarbeiter und Sekretariat) gewährleistet. Da alle internen Ressourcen der IT Abteilung an dem diesbezüglichen Projekt „VPN“ gebunden sind, das aber erst in einigen Monaten fertig gestellt und implementiert werden kann, fordert Ihr Abteilungsleiter Sie und Ihre Mitauszubildenden auf, eine schnelle und einfach zu bedienende Lösung für den Übergangsphase zu planen, entwickeln, bereitzustellen und die Mitarbeiter, insbesondere das nicht-technische Personal, in die Bedienung einzuweisen.  Ihr Vorgesetzter leitet Ihnen den Vorfall der fehlgeleiteten Mail weiter [siehe Mailverlauf im Anhang] und bittet Sie, sich auf ein erster Gespräch vorzubereiten, bei dem Sie mit ihm die wesentlichen Anforderungen besprechen. | | Handlungsprodukt   * (Führen eines) Kundengesprächs zur Erfassung des internen Kundenauftrags auf Basis eines vorbereiteten Gesprächsleitfadens. (2 Ustd.) * Erarbeitung eines Lösungskonzepts auf Grundlage der aus dem Kundengespräch gewonnenen priorisierten Kriterien. (2 Ustd.) * Umsetzung des Lösungskonzeptes als portable Mailanwendung mit PGP auf USB-Sticks (Thunderbird portable plus EnigMail). (2 Ustd.) und grün * Planung und Durchführung einer Kryptoparty zur Nutzereinweisung und Generierung der notwendigen Keys für technisch unterschiedlich versierte Nutzergruppen (Binnendifferenzierung im Unterricht). (8 Ustd.) * Erstellung einer Verfahrensanweisung und Firmenrichtlinie zur zukünftigen sicheren Nutzung von Emails (Differenzierungsangebot Zusatzleistung). * Abschließende Evaluation der Lösung hinsichtlich der Ausgangslage und der internen Kundenanforderungen (2 Ustd.)   Hinweise zur Lernerfolgsüberprüfung und Leistungsbewertung   * Testen der Installation im Demomodus |
| Wesentliche Kompetenzen\*   * Begründete Auswahl und Installation einer Kundenlösung * Berücksichtigung sicherheitsrelevanter Verfahren bei vertraulicher Emailkommunikation und möglicher negativer Auswirkungen bei Nicht-Berücksichtigung für das Unternehmen. * Adressatengerechte Kommunikation bei der Problemerfassung; Dokumentation und Kundeneinweisung. * Sensibilisierung Nicht-technischer Kunden für sicherheitsrelevante Vorgänge und Verfahren.   Selbsteinschätzung und Reflexion bereitgestellter Anwendungen im Hinblick auf die Akzeptanz des Users. | | **Konkretisierung der Inhalte**  Bestandsaufnahme nach Anforderungsanalyse  - Verschlüsselungsarten (symmetrisch, asymmetrisch, hybrid, Einwegverschlüsselung/Hash), Verschlüsselungsverfahren (PGP), Schlüsseltauschverfahren und Public Key Infrastructure (PKI)  - Wechselwirkung von vernetzten lT-Produkten und betrieblicher Organisation am Beispiel Email  - End-to-End Verschlüsselung im Abgrenzung zur Leitungsverschlüsselung  - Planung, Aufbau und Konfiguration von Anwendungssoftware  - Datensicherheit und Auswirkungen auf betriebliche Abläufe  - Qualitätsprüfung  - Inbetriebnahme und Übergabe  - Dokumentation und Kundeneinweisung |
| Lern- und Arbeitstechniken  Diskussion und Reflexion der Wirksamkeit der implementierten Verfahren im Hinblick auf die tatsächliche Anwendung durch den Laien. | | |
| Unterrichtsmaterialien/Fundstellen | | |
| Organisatorische Hinweise  *Unterrichtliche Voraussetzung:*  *(ITK) Eigenschaften „sicherer“ Kommunikation (Vertraulichkeit, Verbindlichkeit, Integrität, Authentizität) sowie Theoretische Grundlagen der kryptografischen Verfahren (siehe oben) sind Gegenstand vorausgegangener LS „Leitungsverschlüsselung per TLS“.*  *(DEU) Grundlagen eines Kundengespräches und Erstellung eines Fragenkatalogs als Gesprächsleitfadens. (POL)*  *Bereitstellung von Sticks, Fachräumen und Internetzugang*  *Abgrenzung: Unterrichtliche Nachbereitung, für welche Anwendungszwecke der Einsatz geeignet ist und gegen welche weiteren Sicherheitsrisiken die Lösung keinen Schutz bietet.* | | |

Farbkodex: Medienkompetenz, Anwendungs-Know-How, Informatische Grundkenntnisse

\* Fettgedruckte Kompetenzen sind dem Bildungs-/Lehrplan entnommen

**Autorenteam:** Volker Stern, Georg-Simon-Ohm- Berufskolleg der Stadt Köln

Jan Dohms, Georg-Simon-Ohm- Berufskolleg der Stadt Köln