Počítačová bezpečnosť

1. Riadenie prístupu v OS a aplikáciách
   - motivácia, ciele, hrozby, príklady zraniteľností
   - používatelia a skupiny používateľov
   - riadenie prístupu v OS: modely, MAC, DAC, RBAC, ACL, prístupové práva, SELinux a pod.
   - riadenie prístupu vo webových aplikáciách, správa spojení (útoky a ochrana)

2. Autentizácia
   - motivácia, ciele, hrozby, príklady zraniteľností
   - identifikácia, autentizácia a autorizácia
   - metódy autentizácie používateľov a systémov, viacfaktorová autentizácia
   - autentizačné protokoly
   - ukladanie hesiel v OS a aplikáciách

3. Bezpečnosť v sieťach
   - motivácia, ciele, hrozby, príklady zraniteľností
   - riadenie prístupu v sieťach – Radius, WiFi
   - bezpečný komunikačný kanál – VPN, IPSec, TLS
   - kryptografické metódy využívané v bezpečnostných protokoloch

4. Základné sieťové služby a ich bezpečnosť
   - motivácia, ciele, hrozby, útoky, príklady zraniteľností jednotlivých služieb/protokolov
   - TCP/IP, smerovacie protokoly, DNS a DNSSEC, SNMP a iné
   - ochrana perimetra/zón – firewall (princípy činnosti, funkčnosť)
   - konfigurácia bezpečnostných vlastností sieťových služieb v OS

5. Redundancia a efektívnosť reprezentácie dát
   - motivácia, ciele a relevantné hrozby
   - konštrukcie samoopravných kódov a ich využitie v praxi
   - RAID (typy, vlastnosti, použitie v súborových systémoch a inde)
   - kompresia údajov (stratová, bezstratová) – metódy, konštrukcie a použitie v praxi

6. Dôvernosť údajov
   - motivácia, ciele, hrozby, príklady zraniteľností; dôvernosť pri prenose a uložení údajov
   - klasifikácia údajov
   - legislatívne prostredie a požiadavky
   - kryptografické metódy zabezpečenia dôvernosti údajov (šifrovanie)
   - správa kryptografických kľúčov

7. Integrita a autentickosť údajov
   - motivácia, ciele, hrozby, príklady zraniteľností
   - integrita a autentickosť pri prenose a uložení údajov
   - integrita v počítačových sieťach (CRC, v bezpečnostných protokoloch a pod.)
   - kryptografické metódy zabezpečenia autentickosti údajov (podpisové schémy, MAC a pod.)

8. Elektronický podpis, PKI a ich aplikácie
   - Vlastnoručný podpis ako bezpečnostná funkcia.
   - Elektronický podpis. Implementácia elektronického podpisu pomocou digitálneho. Vytváranie a overovanie elektronických podpisov.
   - Certifikát verejného kľúča (význam, hlavné položky a ich význam). Rušenie certifikátov, zoznam zrušených certifikátov. Časové pečiatky. Elektronická pečať.
   - Certifikačná autorita. Koreňová certifikačná autorita, krížová certifikácia. Certifikačná cesta, certifikát verejného kľúča R-CA. Iné typy certifikátov (atribútové, mandátové a ich použitie).

9. Dostupnosť
   - motivácia, ciele, hrozby, príklady zraniteľností; dostupnosť služieb a dostupnosť dát
   - dostupnosť pri výpadku IT komponentov (failover) a dostupnosť pri záťaži (rozkladanie záťaže)
   - podpora pre zvýšenie dostupnosti v sieťových protokoloch: smerovanie, DNS, Anycast a pod.
   - zálohovanie, RAID, klastre a pod.
   - havarijné plány a plány obnovy činnosti

10. Klasifikácia informácie a systémov
   - Zmysel a podstata klasifikácie. Kritériá klasifikácie informácie (CIAA).
   - Klasifikácia informácie. Klasifikácia systémov.
   - Kategórie opatrení. Súbory opatrení pre jednotlivé triedy systémov. Metodika BSI Grundschutz.

11. Systém riadenia informačnej bezpečnosti (ISMS)
   - Motivácia, legislatívne požiadavky, medzinárodné a domáce štandardy
   - Postup pri zavádzaní ISMS. Bezpečnostná politika (obsah, vypracovanie, správa). Bezpečnostné štandardy a praktiky.
   - Analýza rizík, návrh opatrení, správa rizík. Bezpečnostné roly. Bezpečnostný manažment.
   - Vzdelávanie, tréning a zvyšovanie povedomia v informačnej bezpečnosti.
   - Riešenie bezpečnostných incidentov. Kontinuita činnosti. Certifikácia ISMS.

12. Bezpečný vývoj aplikácií
   - zraniteľnosti lokálnych a webových aplikácií, opatrenia
   - bezpečné programovanie – princípy, príklady vo vybraných programovacích jazykoch
   - revízia kódu, statická analýza kódu