18.

Biometrie a bezpečnostní politika – pojmy, druhy, hlediska hodnocení, možnosti využití. Bezpečnostní politika a analýza rizik.

Autentizace a její faktory

- něco co znáte: PIN, heslo
- něco co máte: klíč, karta, token
- něco co jste: Biometrie, otisky prstů, rozpoznávání tváře, rozpoznávání oka (duhovka, sítnice), analýza DNA

Základní biometrická operace

- registrace
- validace/identifikace

Hodnocení výkonosti biometrie

- FMR (False Match Rate) – Relativní množství chybných pozitivních verifikací
- FMNR (False Non-Match Rate) – Relativní množství chybných negativních verifikací
- FTE (Failure To Enroll) – Relativní množství neúspěšných registrací (tj. jaké množství lidí nelze vůbec zaregistrovat)

Přehled biometrických metod

1. **Otisk prstu**

- Dnes nejrozšířenější
- Vysoká spolehlivost
- Snadné použití
- Bezpečnost i pohodlí (sejmout prst je snazší než zadat heslo)
- Dnes celkem odolné proti falšování

2. **Rozpoznávání obličeje**

- Dostupné snímače
- Očekává se značný rozvoj
- Snadné falšování

3. **Rozpoznávání podle duhovky**

- Vysoká spolehlivost
- Vyžaduje speciální kamery
- Odolné proti falšování

4. **Rozpoznávání podle sítnice**

- Mapa cév na očním pozadí
- Velmi speciální snímače.
- Velmi odolné proti falšování

5. **Rozpoznávání podle hlasu**

- Dostupné snímače
- Mikrofon v PC
- Telefon
- Snadné použití

6. **Další způsoby**

- DNA
- Geometrie dlaně
- Podpis
- Dynamika úhozů na klávesnici
- Spektrum kůže
- Rty
- Nehty

Bezpečnostní politika – soubor zásad a pravidel, organizace jimi chrání svá aktiva

Typy bezpečnostní politiky:

- promiskuitní – vše povoleno
- liberální – co není povoleno, je napsáno
- konzervativní – co je povoleno, je napsáno
- paranoidní – vše zakázáno kromě konkrétních podmínek

Certifikace – proces ohodnocení, atestace a testování kvality.

Organizační struktura:

- Rada – ruší bezpečnostní problematiku firmy
- Manažer – řídí implementace, zajišťuje vzdělání zaměstnanců
- Správce IS – výkonný orgán,
- Auditor –hlavní kontrolní orgán, vyhodnocuje činnosti BP.

Akreditace – formální uznání, že systém splňuje požadavky certifikace.

Evaluace – zhodnocení bezpečnosti IS/ICT.

Riziko – možnost, že se stane událost s dopadem na výsledek projektu, lze se před ní bránit.

Hrozba – neodvratitelný proces s dopady, lze pouze zmírnit následky.

Audit – kontrola, např. finanční, bezpečnostní, měla by splňovat detekci, rozlišení, analýzu, agregaci, archivaci, zpracování bezpečnostního poplachu a generování zprávy.

Risk management – zabývá se identifikací, eliminací, minimalizací a řízením rizik.

Risk management analýza – hl. součástí je identifikace rizik, kterou by měl každý projekt začít.

Rizika – ohrožení života, zdraví a živ. pros., komerční a smluvní vztahy, ekonomické okolnosti, politické, přírodní, environmentální, fyzické, technické, technologické a lidské hrozby.

FTA – strom poruch.
ETA – strom událostí.
HAZOP – Hazard And Operability Study, analýza nebezpečí, ohrožení a provozuschopnosti.
HACCP – Hazard Analysis And Critical Control Points.
ZHA – Zurich Hazard Analysis.