GDPR

General Data Protection Regulation

a technická bezpečnosť

Apríl 2018

Compeko

Program

- **Prečo technická ochrana**
- **Ochrana súborov dát pred odcudzením**
- **Ochrana súborov dát pri odcudzení**
- **Ochrana dát pred odcudzením cez procesy**
- **Ochrana dát pri prenosoch**
- **Práca s dátami voľne „rozhádzanými“ po disku PC**
- **Ochrana prístupu do privátnych procesov**
  - **pracovnej plochy (PC, tablet, mobil...)**
  - **aplikácií**

Compeko

Prečo technická ochrana

- Nové nariadenie o ochrane osobných údajov (GDPR) ukladá okrem iných aj povinnosť chrániť osobné údaje pred zneužitím.
- Jednou zo súčastí komplexnej ochrany je aj mechanická ochrana (bezpečnostné dvere, reťaz, ...) ale aj technologická ochrana.
- Ochrana má zabrániť:
  - Odcudzeniu PC alebo servera s osobnými údajmi
  - Odcudzeniu dátových súborov s osobnými dátami
  - Využitiu / zneužitiu dát z odcudzených súborov
  - Získaniu konkrétnych dát z procesov, ktoré s nimi pracujú
  - Získaniu dát napojením sa na pracovnú plochu pracovníka oprávneného s dátami pracovať

Compeko

Ochrana súborov dát pred odcudzením

- Ide hlavne o mechanické prostriedky a rozhodnutie, kde sa dáta ukladajú
  - Jediný PC trvalo v kancelárii
  - Notebook, ktorý nosím so sebou
  - Malá lokálna sieť – server je za WC
  - Komplexná a odborne prevádzkovaná lokálna sieť
  - Overený cloudový priestor
  - Overená Cloudová platforma

- Odcudzenie „elektronické“
  - Bezpečné pripojenie na internet (ak je to možné, aktivovať iba vtedy, keď to treba)
  - Používanie firwall prípadne proxy
  - Povolenie vzdialeného prístupu do PC, siete, servera – na vyžiadanie, v bezpečnom režime

Compeko

Ochrana súborov dát pri odcudzení

- Ak neviem súbory dát dostatočne ochrániť pred krádežou, tak aspoň skomplikujem zlodejovi možnosť ich využitia
  - Kryptovaním diskov
  - Kryptovaním súborov
- Nevýhody:
  - Spracovanie vyžaduje netriviálnu dodatočnú kapacitu výkonu procesora prípadne pamäti
  - Silnejšie kryptovacie nástroje vyžadujú priamu HW podporu
  - Ak sa naruší dekódovací mechanizmus pri kryptovaní diskov, takmer isto prídeme o všetky dáta
  - Vytvorenie nekryptovanej zálohy dát prakticky anuluje všetku snahu vynaloženú pri kryptovaní.

Compeko

Ochrana dát pri prenosoch

- Ak prenášame osobné údaje cez internet, je potrebné používať „bezpečný“ prenos, inak dáta môžu byť „odchytené“ a ľahko dekódovateľné a použiteľné

- Pri prenosoch dát, ktoré nám ukladajú zákony (napr. odosielanie daňových hlásení, prehľadov, výkazov poistného, ...) je za zabezpečenie prenosových ciest zodpovedné priamo MFSR a MVSR.
- Ak odosielame dáta prostredníctvom mailov, tak radšej dáta komprimujme a ochráňme heslom (a to heslo NIKDY neuvádzajme do toho mailu)
- Pre komunikáciu mailového klienta s mail serverom používajte (ak je to možné) bezpečný port a šifrovanie TLS protokolom
- Ak sa na hromadné rozosielanie mailov používa automatický klient (napr. sendmail.exe), treba zabezpečiť, aby používal špeciálne konto určené IBA na odosielanie mailov (príjem má zakázaný)
- Ak odosielame dáta priamo funkciami internetového portálu, overme si, že prenosová cesta je bezpečná (napríklad tak, že URL musí byť https:// a nie http://)
- Nikdy nedovoľme, aby si cudzie procesy automaticky preberali dáta z nášho PC alebo servera

Compeko

Ochrana „divokých“ dát

- Ide hlavne o stanovenie pravidiel narábania s citlivými údajmi, ktoré sú v rôznych nesystematicky vytváraných súboroch typus Word, EXCEL, PPT, ... kdekoľvek na lokálnom disku
  - Takéto súbory buď nevytvárať, alebo ich pravidelne (a dosť rýchlo) mazať
  - Ak je potreba vytvárať lokálne súbory , treba ich mať systematicky uložené a príslušné adresáre monitorovať a chrániť prípadne ich pri ukladaní chrániť heslom

Ochrana prístupu do privátnych procesov

- Ide o opatrenia proti odcudzeniu dát technikou napojenia sa na rôzne procesy pracovníka, ktorý má široké oprávnenia prístupu k dátam, napr.:
  - Pripojenie sa na pracovnú plochu
  - Využitie „živej“ pracovnej plochy
  - Napojenie sa do užívateľského programu
  - Napojenie sa do služieb poskytujúcich dáta (napr. v client-server architektúre aplikácií)

- Ochrana spočíva v:
  - Zabezpečení PC, NB, TBL, MB heslom
    - pri štarte
    - pri odomknutí zamknutej obrazovky,
    - Pri vstupe do aplikačných programov
  - Automatickom ale aj manuálnom zamknutí obrazovky pri odchode od PC, NB, ...
  - Opustenie aplikácie, keď v nej práve nepracujem a najbližších 15 minút nebudem
  - Používaní systému hesiel, ktorý je komplikovaný pre strojové odhalenie ale pomerne jednoduchý pre človeka. Príklad:
    - Heslá majú byť dosť dlhé
    - Nemajú byť nikde zapísané
    - Majú sa dať ľahko a jednoznačne vytvoriť (ich používateľovi) na základe uloženej informácie typu: Farba-tvor_VORJAN#Strach PW: Cierna-pavuk_110,805#Svokra Informácia môže byť napríklad v mobile.

Compeko

Záver

Compeko