UVOD

SolarWinds

Ubačen maliciozni kod u programsku podršku Orion IT za nadzor i upravljanje mreža

napad slučajno otkrila tvrtka FireEye

Primjer **napada na dobavni lanac (engl. supply chain attack)**

Colonial Pipeline

ucjenjivački napad

Tvrtka koja obavlja transport nafte i derivata uz jugoistočnu obalu SAD-a •

Ulaz u mrežu tvrtke napravljen pomoću **kompromitiranih vjerodajnica** •

Faktori koji utječu na sigurnost IS-a

- Ljudski faktori
  - Nedostatak edukacije u području sigurnosti
  - Nedostatak komunikacije po pitanju sigurnosti
  - Nedostatak svijesti
  - Nedostatak kulture
  - Neodgovarajuće ponašanje
- Organizacijski faktori
  - Nedostatak budžeta
  - Kratki rokovi
  - Nedostatak podrške menadžmenta
  - Nedostatak odgovarajuće procjene rizika
  - Nepostojanje sigurnosnih procedura
- Tehnološki faktor
  - Ranjivosti u IT imovini
  - Nedovoljni ili neodgovarajući sigurnosni mehanizmi

Sigurnost (engl. security) - Kontinuirani proces čijim provođenjem se osigurava određeno stanje (sustava i/ili podataka/informacija). Željeno stanje je definirano određenim zahtjevima.

Kada su zahtjevi ispunjeni, kažemo da je sustav i/ili informacija sigurna. Ako neki od zahtjeva nije ispunjen, kažemo da se desio incident, odnosno, da je narušena sigurnost.

Tri temeljna zahtjeva

- **Tajnost/Povjerljivost**
- **Cjelovitost/Integritet**
- **Raspoloživost**

Dodatni zahtjevi

- **Autentičnost**
- **Neporecivost**

Da bi se desio incident moraju postojati dva preduvjeta: **ranjivost i prijetnja**

Prijetnja (engl. threat) je bilo kakav događaj koji može iskoristiti ranjivost te na taj način prouzročiti štetu.

• Izvori prijetnji su ljudski (**namjerni ili slučajni**) ili prirodni

Načini postizanja sigurnosti

-Tako da uklonimo prijetnje i/ili ranjivosti

Kako djelovati na prijetnje?

- Djelovanje na motiv
- Podizanje cijene

Ranjivosti se mogu **ukloniti ili ublažiti kontrolama**

Kontrole su zaštite koje primjenjujemo u sustavu

Sve kontrole svrstavamo u tri velike grupe

- **Fizičke kontrol**e – kamere, zaštitari, ograde, … •
- **Tehničke kontrole** – vatrozidi, antivirus, … •
- **Administrativne kontrole** – politike, procedure, pravilnici

Informacijski sustav je bilo koji organizirani sustav za prikupljanje, organizaciju, pohranu i razmjenu informacija

- Informacijski sustav ne uključuje nužno računala i/ili računalnu mrežu
- Iako su današnji informacijski sustavi nezamislivi bez njih
- Informacijski sustav uključuje i ljude i procese
- Informacijski sustav uključuje sve na čemu se nalaze informacije značajne za tvrtku
- Uz napomenu: koje nisu javno objavljene!

Informacijska tehnologija (IT) je primjena računala i telekomunikacijske opreme za pohranu, dohvat, prijenos i obradu podataka, često u poslovnom kontekstu.

U IT-ju temeljni zahtjev je tajnost •

Informacija ne smije biti poznata neovlaštenim osobama •

U Operational Technology OT-u temeljni zahtjev je raspoloživost

prvenstvena zadaća je upravljanje fizičkim procesima