Øving 4 - Sikkerhet på net

Kontotilgang:

Alle på gruppen har fått en eller flere accounter hacket.

1. Hvordan skjedde det?

   Dette skjedde sannsynligvis med at en account blei breachet så har passordet og emailen blitt testet på flere nettsider heilt til dem kom seg inn en plass.

2. Hva var konsekvensene av det som skjedde?

   Enn av oss mistet Origin brukeren og bruker navn blei endret og personen slettet alle vennene på vennelista.
   Enn av oss fekk Steam brukeren hacket, men ingenting blei endret uten om at et par spill hadde blitt brukt.
   Enn prøvde og komme seg inn på en av sosiale median brukeren, men de kom seg ikke inn.

3. Hva er worst case scenario for det som skjedde

   worst case scenarioen for Steam brukeren er en kan få tak i bankkontoen, og en får enn email adresse så vist en bruker same passord på begge kunne hackeren fått tak i emailen og med den kan en få tak i så og sei alle brukeren personen har som er koblet opp til den emailen.
   Origin brukeren kan komme opp i det same som Steam brukeren.
   Sosial media brukeren kan miste masse personlig informasjon om seg selv og andre, som igjen kan bli misbrukt i framtid.

4. Endret personen noen rutiner etter at det ble gjort? Hvorfor/hvorfor ikke?

   Som blei nevnt i oppg. 2 så endret hackeren brukernavnet og slettet vennene til Origin brukern, brukene benyttet 2 faktor identifikatoren etterpå.
   Steam brukeren fikk ingenting endret, passord og identifikator blei slått på.
   Hackeren som prøvde og komme seg inn på sosiale medie brukeren kom seg ikke inn så ingenting ble endre, passord blei endret.

5. Identifiser hvilke forholdsregler fra forelesningen som kunne vært med på å hindre at dette skjedde.

   Enn kunne ha endret passord oftere, og brukt 2 faktor identiteter. Ikke bruk passord manager til viktige tjenester som f.eks. email, paypal og sosiale medier.

Identifisert kontoer:

1. Kartlegg hvilke 3 kontoer gruppa har til felles og bruker mest (Facebook, Gmail, Instagram, osv)

   Facebook, Gmail, Steam, discord, Origin, Uplay, Twitch, osv.

2. dokumenter den informasjonen dere selv mener er mest sensitiv på hver av disse.

   Den informasjonen som er mest sensitiv er nok Mail og Facebook. På facebook står veldig mye informasjon om deg selv og via messenger har en masse informasjon om venner og andre en kommuniserer med.

   På mail kan en få tilgang til andre nettsider som er tilkoblet til den mail adressa.

3. Diskuter hva denne informasjonen kan brukes til av uvedkommende.

   Facebook informasjonen kan bli brukt til og få videre informasjon om andre venner eller familie. Kan bli brukt som blackmail eller solgt til andre for å tjene penger.

   Mail adressa kan bli brukt som identifikator for mindre ting og en kan få tilgang til mer sensitiv informasjon. Kan låse kontoen og blackmaila personen til å betale en vis med penger for å få tilbake kontoen.

   Forbedring:

   1. Har gruppa samme passord på flere tjenester? I så fall hvilke typer og hvorfor?

      Alle på gruppa har brukt same passord på flere brukere.
      Som oftest blir det brukt på tjenester som ikke blir sett på som viktig eller innholder så «viktig» informasjon. F.eks. netflix, viaplay, osv.

   2. Velg ut de mest sensitive tjenestene og dokumenter hvorfor disse ble valgt

      Alle tjenester der en kan bruke bankkort f.eks. Steam, paypal, Battle.net, osv.

   3. Dokumenter passordkravet til hver tjeneste. Bytt passord på de viktigste tjeneste så de har ulike passord.

      Som oftest er det 7- 32 karakterer + et nummer og store og små bokstaver og en kan ikke bruke passord som ligner på bruker navnet

   4. Dokumenter fordel og ulemper med en password manager (som Lastpass o.l.)

      Fordelen er at manageren husker alle passorda og en slepper og taste da inn hver gang en skal inn på brukere. Ulempen er at manageren husker alle passorda en har tillatt den å huske, så vist manageren blir hacka så får hackeren tilgang til alle passorda som manageren har fått lov til å huske