Datasäkerhetsmetoder, sista träffen

Social engineering

Lite återkoppling på utkasten

LINKÖPING UNIVERSITY

Social Engineering

- Socialt samspel handlar om sedvänjor, kultur och tradition
- Man kan utnyttja detta genom så kallad Social Engineering
- Vi attackerar människan bakom maskinen

`https://www.youtube.com/watch?v=1c7scxvKQOo`

Vilka sociala “svagheter” kan vi utnyttja?

Det finns flera skäl till att social engineering fungerar

1. Otydligt ansvar
2. Upplevda fördelar
3. Tillit
4. Moraliskt ansvar
5. Skuld

Vilka sociala “svagheter” kan vi utnyttja?

Det finns flera skäl till att social engineering fungerar

1. Otydligt ansvar
    - “Detta är redan godkänt av nån annan, släpp in mig.”
2. Upplevda fördelar
3. Tillit
4. Moraliskt ansvar
5. Skuld

Vilka sociala “svagheter” kan vi utnyttja?

Det finns flera skäl till att social engineering fungerar

1. Otydligt ansvar
2. Upplevda fördelar
    - Offret tror sig få en fördel av handlingen
    - “Din chef vill att du gör det här”
3. Tillit
4. Moraliskt ansvar
5. Skuld

Vilka sociala “svagheter” kan vi utnyttja?

Det finns flera skäl till att social engineering fungerar

1. Otydligt ansvar
2. Upplevda fördelar
3. Tillit
    - Offret vill vara hjälpsamt
4. Moraliskt ansvar
5. Skuld

Vilka sociala “svagheter” kan vi utnyttja?

Det finns flera skäl till att social engineering fungerar

1. Otydligt ansvar
2. Upplevda fördelar
3. Tillit
4. Moraliskt ansvar
    - Offret övertygas om att det är “rätt” åtgärd
    - Kanske handlingen fixar nåt påhittat problem
5. Skuld

Vilka sociala “svagheter” kan vi utnyttja?

Det finns flera skäl till att social engineering fungerar

1. Otydligt ansvar
2. Upplevda fördelar
3. Tillit
4. Moraliskt ansvar
5. Skuld
    - Offret övertygas om att hen gjort något fel
    - Och handlingen rättar till felet

Vilka sociala “svagheter” kan vi utnyttja?

Det finns flera skäl till att social engineering fungerar

1. Otydligt ansvar
2. Upplevda fördelar
3. Tillit
4. Moraliskt ansvar
5. Skuld

Man vill vara hjälpsam

Social Engineering: Sikta mot toppen!

- Tisdag–torsdag förra veckan: konferens i Göteborg
- Kl 11:10 kom ett epostmeddelande till vår administratör:

```
Från: Jan-Åke Larsson [mailto:jan-ake.larsson@liu.se]
Ämne: SV: omedelbar betalning(13:12:16)

Hej,

Kan du göra en banköverföring till Storbritannien idag?

Best Regards...
Jan-Åke Larsson
```

- Brevet i HTML innehåller LiUs logga och en bild av mig
- Kl 12:32 gör vår administratör en *forward* av meddelandet till vår fakturahanterare *och mig*

Whaling

- Meddelandet var så kallad whaling (eller “CEO fraud”)
- Om det är noga förberett så kallas det ibland “spear-phishing”
- Ofta riktat mot högsta ledningen (jag är Prefekt, dvs högsta chef på ISY), men målet är egentligen ekonomiavdelningen
- Enligt FBI har denna typ av attacker genererat mer än 2.3 miljarder USD i förluster sedan 2013.
- Jo, också riktat mot LiU . . .

Det slutade väl i detta fall

- Det fanns ett “Reply-to:“ fält riktat mot en falsk epostadress under attackerarens kontroll
- Men administratören gjorde en forward, inte ett svar
- Jag upptäckte detta inom ca 20 minuter och hörde *omedelbart* av mig till både administratör och ekonom, och lite senare LiUs Incident Response Team
- Ingenting hände, men våra rutiner hade antagligen stoppat utbetalningen i vilket fall

Motåtgärder

- Policy/Rutiner
  - LiU: “Fakturor ska attesteras av två olika personer”
  - Personligt exempel: “Skicka aldrig passnumret per epost”
  - Företagsexempel: “Låna aldrig ut ditt lösenord”
  - Men rutiner behöver en fungerande infrastruktur
- Medvetenhet
- Teknologi

Motåtgärder

- Policy/Rutiner
- Medvetenhet
  - Man måste veta om att social engineering förekommer
  - Man bör känna till hur vanliga attacker fungerar
  - Alla i organisationen måste känna till det
- Teknologi

Motåtgärder

- Policy/Rutiner
- Medvetenhet
- Teknologi
  - Epostsignaturer
  - Autentisering

Rapporterna, allmänna kommentarer

- Gör en tydlig struktur: sekretess för sig, dataintegritet för sig och tillgänglighet för sig, hot-brist-skada, osv
- Se till att diskussionen handlar om er specifika situation, inte bara en allmän beskrivning av begreppen som sådana
- En vanligt fel är att blanda CIA, framförallt sekretess och tillgänglighet. Tillgänglighet handlar om att man *ska* kunna komma åt det man har tillåtelse att läsa och skriva.
- Tänk noga på sannolikheten att hoten realiseras, det har betydelse för prioriteringen
- Koppla rangordningen av riskerna med prioriteringen av åtgärderna, den stora svårigheten brukar vara att få till en välmotiverad prioritering

Hasardspel

- Tänk på sekretess också för underlaget till oddsen, kanske attackeraren vill komma åt vad som ligger bakom dem för att kunna spela bättre, alternativt ändra oddsen till sin fördel (Integritet).
- För tillgänglighet kan man fundera på om det kan finnas attacker där primärskadan är tillgänglighet och sekundärskadan är integritet (och tredjenivåskadan ekonomisk), säg att lägga ett vad och sedan DDOSa servern. I vilken situation kan detta vara fördelaktigt för en attackerare? Är detta troligt som attack?
- Man bör ha med insiderhot

Hemstyrsystem

- Hur sker kommunikationen mellan klient/lägenhet och server?
- Ska man använda dedikerad hårdvara, en webbapplikation, eller en mobilapp? Diskutera för och nackdelar
- Om det är dedikerad hårdvara kanske en enkel pinkod är bättre än ett lösenord, man måste ju vara på plats också?
- Tänk på sekretess också för förbrukningsdata. Dessa kan annars användas för att se om någon är hemma. Är ingen det, kan man ju bryta sig in ostört

Lillköpings sparbank

- En bank har höga krav på sekretess och integritet. Det svåra är att få till balans mellan dessa och tillgänglighet
- Här är insiderhoten mycket viktiga

- Ni behöver inte ha med en katastrofövning

Forskargrupp

- Forskargruppen hanterar persondata, så PUL är viktigt
- Gruppen är spridd över landet, så här bör man nämna VPN (krypterade tunnlar) så att trafiken är skyddad när den passerar över internet
- Kan utbildning vara en bra åtgärd?

Enmansfirmor (Lantbruk, mm)

- Fundera på vilka yttre hot som finns
- Anpassa CIA-analysen, och lista inte bara en typ av hot, i ett lantbruk t ex är fysiska hot viktiga men utesluter inte andra
- Kan utbildning vara en bra åtgärd?

Familjeveterinärerna/Dagligvarubutik

- Här måste man diskutera hur man skiljer man användare från varandra, hur hanteras lösenord?
- Har man skilda system för de olika uppgifterna, är det olika autentisering i de olika systemen? Har man grupper av anställda med olika behörighet eller är det personkopplat?
- Finns det riktade yttre hot (djurens rätt, t ex?)

Hemdatoranvändare

- Backup är viktigt även för en hemdatoranvändare
- En ensam användare har delvis andra krav än om det handlar om en hel familj
- Behövs det utbildning, och är det säkert att den skulle hjälpa? Kanske man ska ha ett system som är enkelt och begränsat?
- Virusskydd stoppar inte allt, och det kan vara svårt att få användaren att förstå hur farliga länkar i epost kan vara
- Hur hanterar man lösenord, backup, sociala medier, kanske ett fillager, fleranvändarsäkerhet?

En familj där föräldrarna arbetar hemma

- Som en ensam hemanvändare men med andra bekymmer
- Är hoten större pga hemarbete? Hur måste ni ta hänsyn till detta?
- En given åtgärd är en VPN-tunnel till arbetet
- Tillgänglighet är viktigare här
- Lägg arbete på struktur av rapporten, och att få den lättläst, man ska inte underskatta vikten av detta, särskilt för privatpersoner (för en säkerhetsmänniska i ett företag är det annorlunda).

Biljettförsäljning

- Insiders? Svarta marknaden för biljetter är stor
- Fundera på om det kan bli sekundärskador av en DDOS, säg att platser säljs flera gånger, eller att betalning förhindras men biljetten blir tillgänglig.
- Hur gör man biljetterna svåra att kopiera? Tänk på att en streckkod också kan förfalskas. Hur skulle man göra för att få en streckkod svårförfalskad? (Ledtråd: tänk på kryptoföreläsningen.)

Ekonomikonsulter/bokföringsfirma

- Bokföringslagen kräver en auditlog, vem som gjort vad, så detta är en krävd åtgärd. Rangordningen måste ta hänsyn till lagen.
- Samtidigt är inte sekretess för bokföring ett lagkrav (banksekretess är något annat). Däremot finns säkert ett avtal med kunden om sekretess, och man kommer säkert till domstol om man inte kan förlikas vid brott mot detta.
- Tillgänglighet är å andra sidan ett krav för bokföring

Rapporterna, allmänna kommentarer

- Gör en tydlig struktur: sekretess för sig, dataintegritet för sig och tillgänglighet för sig, hot-brist-skada, osv
- Se till att diskussionen handlar om er specifika situation, inte bara en allmän beskrivning av begreppen som sådana
- En vanligt fel är att blanda CIA, framförallt sekretess och tillgänglighet. Tillgänglighet handlar om att man *ska* kunna komma åt det man har tillåtelse att läsa och skriva.
- Tänk noga på sannolikheten att hoten realiseras, det har betydelse för prioriteringen
- Koppla rangordningen av riskerna med prioriteringen av åtgärderna, den stora svårigheten brukar vara att få till en välmotiverad prioritering