TSIT01 Datasäkerhetsmetoder

Föreläsning 10: Social engineering
Backuper, intrusion detection
Rapporterna och presentationerna

Ingemar Ragnemalm

Social engineering

Socialt samspel handlar om känslor, sedvänjor, kultur och tradition

Man kan utnyttja detta genom så kallad *Social Engineering*

Människan bakom maskinen attackeras

https://www.youtube.com/watch?v=lc7scxvKQOo

Vilka sociala “svagheter” kan utnyttjas?

Det finns flera skäl till att social engineering fungerar

Hjälpsamhet och pliktkänsla:

1. Tillit

2. Moraliskt ansvar

3. Skuld

Vilka sociala “svagheter” kan utnyttjas?

Det finns flera skäl till att social engineering fungerar

Hjälpsamhet och pliktkänsla:

1. Tillit

Avsändaren låter pålitlig, känd

2. Moraliskt ansvar

3. Skuld

Vilka sociala “svagheter” kan utnyttjas?

Det finns flera skäl till att social engineering fungerar

Hjälpsamhet och pliktkänsla:

1. Tillit

2. Moraliskt ansvar

Offret känner att det är "rätt" åtgärd
Handlingen kanske fixar ett påhittat problem

3. Skuld

Vilka sociala “svagheter” kan utnyttjas?

Det finns flera skäl till att social engineering fungerar

Hjälpsamhet och pliktkänsla:

1. Tillit

2. Moraliskt ansvar

3. Skuld

Offret övertygas om att det gjort något fel
och handlingen rättar till felet

Vilka sociala “svagheter” kan utnyttjas?

Det finns flera skäl till att social engineering fungerar

Hjälpsamhet och pliktkänsla:

1. Tillit

2. Moraliskt ansvar

3. Skuld

Man vill vara hjälpsam

Vilka sociala “svagheter” kan utnyttjas?

Det finns flera skäl till att social engineering fungerar

Personliga mål:

1. Otydligt ansvar

2. Upplevda fördelar

3. Rädsla

4. Annan emotionell manipulation

Vilka sociala “svagheter” kan utnyttjas?

Det finns flera skäl till att social engineering fungerar

Personliga mål:

1. Otydligt ansvar

"Detta är redan godkänt av någon annan, släpp in mig"

2. Upplevda fördelar

3. Rädsla

4. Annan emotionell manipulation

Vilka sociala “svagheter” kan utnyttjas?

Det finns flera skäl till att social engineering fungerar

Fler möjligheter:

1. Otydligt ansvar

2. Upplevda fördelar

Offret tror sig få en fördel av hanteringen
"Du har vunnit 1000 kronor"

3. Rädsla

4. Annan emotionell manipulation

Vilka sociala “svagheter” kan utnyttjas?

Det finns flera skäl till att social engineering fungerar

Fler möjligheter:

1. Otydligt ansvar

2. Upplevda fördelar

3. Rädsla

"Någon drar pengar från ditt konto"

4. Annan emotionell manipulation

Vilka sociala “svagheter” kan utnyttjas?

Det finns flera skäl till att social engineering fungerar

Fler möjligheter:

1. Otydligt ansvar

2. Upplevda fördelar

3. Rädsla

4. Annan emotionell manipulation

"Jag tycker du är en jättefin person. Kom och bli medlem i klubben och chatta med mig"

Vilka sociala “svagheter” utnyttjar Filer mot Kam?

Hjälpsamhet (och viss pliktkänsla?)

Upplevda fördelar

Maskerad till äldre man = ser ofarlig ut = tillit

Social engineering: Sikta mot toppen!

Jan-Åke (ISYs prefekt) var på konferens

Då kom E-post 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 innehöll LiUs logga och bild på Jan-Åke

Adminstratören gör forward till fakturahanterare och till Jan-Åke

Whaling

Meddelandet var "whaling" eller "CEO fraud"

Kallas ibland "spear phishing"

Riktas mot högsta ledningen (i detta fallet ISYs prefekt) men målet är ekonomiavdelningen

Dessa attacker har enligt FBI orsakat mer än 2.3 miljarder dollar i förluster sedan 2013

Detta slutade väl

Det fanns en "reply-to" till en falsk adress men administratören gjorde ett "forward"

Upptäcktes därför inom 20 minuter och Jan-Åke kontaktade adminstratören och ekonomen samt även LiUs Incident Response Team.

Bra rutiner hade antagligen stoppat betalningen i alla fall.

Phishing

En form av social engineering där personliga meddelanden används för att få fram personlig information som kan användas för intrång.

Kan vara E-post, genom meddelandesystem men även på socala media.

Phishing-attacken via LiU IT

Meddelande som sade sig ha svar på supportfråga, med länk. Målet var våra lösenord. Angreppstyp: Tillit.

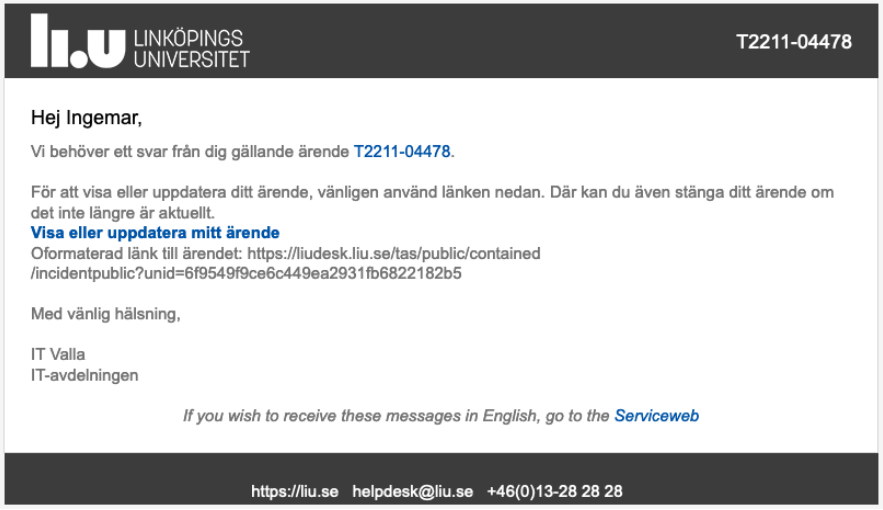
Meddelandet var exakt LiU ITs normala meddelanden! Ingen information om vad saken gäller, bara en länk, logga in här!

Den falska länken var lätt att se genom att hovra över den, MEN de som läser på mobilen ser inte detta. Många blev lurade och fick sina lösenord läckta!

Även idag har LiU IT samma system. Samma information men med en ärenderad. Bra nog?

Phishing-attacken via LiU IT

Så här ser ett vanligt meddelande ut:



LINKÖPINGS UNIVERSITET

T2211-04478

Hej Ingemar,

Vi behöver ett svar från dig gällande ärende T2211-04478.

För att visa eller uppdatera ditt ärende, vänligen använd länken nedan. Där kan du även stänga ditt ärende om det inte längre är aktuellt.
Visa eller uppdatera mitt ärende
Oformaterad länk till ärendet: https://liudesk.liu.se/tas/public/contained
/incidentpublic?unid=6f9549f9ce6c449ea2931fb6822182b5

Med vänlig hälsning,

IT Valla
IT-avdelningen

If you wish to receive these messages in English, go to the Serviceweb

https://liu.se helpdesk@liu.se +46(0)13-28 28 28

Ospecifikt! Klicka på länken... Bluffvänligt system!

Rektors julgåva

Detta kom lagom före jul härom året:

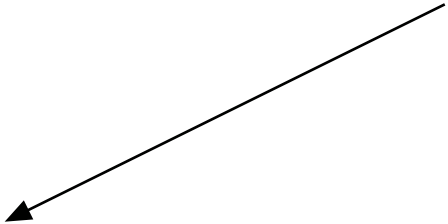
Phishing-larmet slog till direkt hos oss!

Vackra ord

Lovar ekonomisk fördel

Extern, okänd länk

Vi klickade INTE på den!



Falskt alarm!

...förrän vi fick veta att det var äkta...

Falskt alarm... vilket tyvärr också gör skada genom förlorad tid och blir man inte avtrubbad av att det "ropas varg" för ofta?

Minskar tyvärr inte

Phishing attacks up 40 percent in 2023

By Ian Barker | Published 3 days ago | Follow

No Comments

Har du hört den förut?

Fiske efter säkerhetsfrågor

En form av phishing på sociala media.

INGEN bryr sig om vad din hund hette - utom informationsfiskaren!

Ändå får varje sådan postning *tusentals* svar - på grund av kärleken till hunden och att man spontant vill svara på en personlig fråga.

01001001 01000011 01000111

Telefonbedrägerier

Rädsla kombinerat med tillit.

Telefonsamtal, det är från banken. "Det pågår en attack mot ditt konto!" Men det är bedragaren som ringer!

Spelar på din panikkänsla.

En annan form:

"Vi are kallink from Vindoze! Dere is a problem vid your komputter."

Typiskt kommer de att vilja att du installerar skadlig programvara eller liknande. Även detta bygger på att skrämma dig.

Gamla vanligt mål

Rädsla används ofta mot gamla

En ny variant nyligen: Någon ringde min svärmor från "banken" och sade att bankkortet skulle bytas *och de skulle skicka någon att göra det*.

Lyckligtvis var hennes reaktion helt korrekt - hon låste dörren.

Falska fakturor

Mest en fråga om tillit samt dåliga rutiner.

Antingen är fakturan påhittad, men ser äkta ut, eller så är det ett erbjudande som maskeras som faktura.

Går igenom om fakturor hanteras utan verifiering.

Nigeriabrev

En klassiker. Baseras på personliga fördelar eventuellt kombinerat med moralskt ansvar. Effektivt när det når chefsnivå.

Motåtgärder: Policy/Rutiner

LiU: Fakturor skall attesteras av två olika personer

Företagsexempel: Låna aldrig ut ditt lösenord

Fungerande infrastuktur behövs

Motåtgärder: Medvetenhet

Man måste veta om att social engineering förekommer

Man bör känna till hur vanliga attacker fungerar

Alla i organisationen måste känna till det

Lär dig och andra känna igen social engineering.

Motåtgärder: Teknologi

E-post-signaturer

Autentisering

Social engineering

Går alltid ut på att få ett offer (inte alltid den som skadas) att göra något olämpligt.

Detta kan öppna för intrång eller direkt skapa en betalning.

Kräver, tyvärr, att vi är misstänksamma, känner igen bluffar och har rutiner för att täppa till våra egna svagheter.

Tyvärr behövs alla de där dubbelkollarna och verifieringarna.

TSIT01 Datasäkerhetsmetoder

Föreläsning 10: Del 2: Backuper, intrusion detection

Ingemar Ragnemalm

Lösenord

Tidigare föreläsningar:

- Starka lösenord
- Biometri, fingeravtrycksläsare mm
- Elektroniska nycklar, RFID, QR-koder...

Fråga för rapporterna: Effektivitet, kostnad?

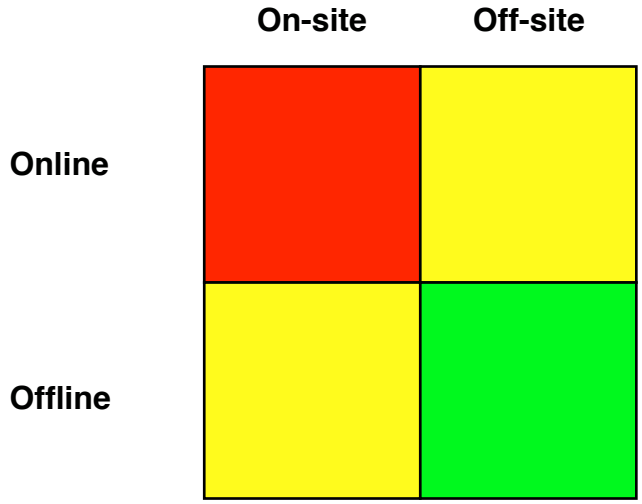
Åter till dessa backuper

3-2-1-metoden, vad betyder den?

- Allt i tre kopior
- Minst 2 media
- En på annan plats

3 och 1 viktiga, 2 tveksam

Backupmatrisen



Fyra fall

Online, on-site: Enkelt, billigt, osäkert

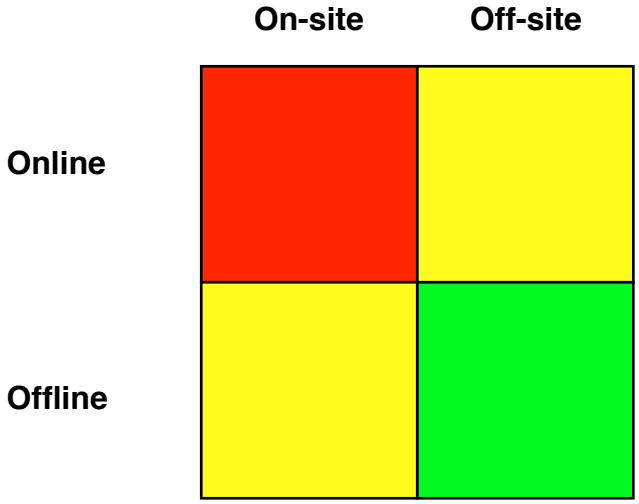
Offline, on-site: Känsligt mot onsite, inbrott, bränder mm

Online, off-site: Känsligt mot onlineattacker

Offline, off-site: Mycket säkert men dyrt

Dessutom: Skrivbarhet, förstörbarhet on-line.

Backupmatrisen vs 3-2-1



Val av backuper

Grafen tidgare? Om en av de tre kopiorna är på grönt eller två på var sin gul är säkerheten hög! Alla behöver (bör) inte vara på grönt!

WORM: Säkert mot onlineattacker men dyrt!

Räcker "röd" backup med tanke på den låga skadan?

Automatisk eller manuell? Automatisk är billigare i tid och säkrare i hur ofta det görs! Manuell är säkrare i kontroll, insyn.

Kostnad, behov, lämplighet?

Intrusion detection

Intrusion detection

Hur ser vi att en attack pågår?

Kan vi identifiera angriparen?

Kan vi stoppa angreppet?

Kan vi vilseleda angriparen?

Intrusion Detection Systems (IDS) finns för att hantera detta.

Misstänkt beteende

Angripare beter sig annorlunda.

Problem: Gråzoner. False positives och false negatives måste undvikas.

Hur kan beteenden analyseras?

- Obseverbara mätvärden
- Statistiska metoder
- Deep learning/AI

Typer av IDS

Host-baserade (HIDS)

Analyserar händelse inom systemet

Nätverksbaserade (NIDS)

Analyserar händelser på nätverket

Honeypots

"Honungsfällor", falska system för att lura angripare

- Skyddar de äkta systemen
- Samlar information om angriparen
- Får angriparen att hänga kvar så admin kan införa åtgärder

Vanliga användare har ingen anledning att besöka. Fullt synliga för angripare.

Typer av honeypots

"Low interaction", honungsfällan är en ren emulator. Enkel, saknar många funktioner.

"High interaction", ett faktiskt system, en separat dator med avsiktligt lägre säkerhet. Måste installeras med försiktighet.

Placering av honeypots

Utanför brandväggen: Lättåtkomlig för angripare, låg risk för övriga systemet. Kan inte upptäcka interna attacker.

Innanför brandväggen: Svårare att komma åt, detetekterar attacker inom systemet, men kan utnyttjas för att angripa det!

Script-honeypots

En slags honungsfälla är det dåliga attackscriptet!

Script kiddies vill ha färdiga scripts. Så ge dem dessa scripts... som går fel.

Kan både bromsa attacker och leverera information.

Exempel: Team Fortress 2

Svårt säkerhetsproblem: Attacker i angriparens egen dator!

Red hat. Anfall på deras egen planhalva.

Antag att de flesta är script kiddies. Publicera "fusk" som fungerar dåligt. Lura script kiddies att använda dem.

Plötsligt flyttas problemet till dem, de måste lura ut vad som är fusk!

Är det en honeypot?

Rapporterna

Lite kommentarer.

Era egna rapporter tittar vi på vid redovisningarna.

Rapporterna, allmänt

• tydlig struktur, sekretess för sig, dataintegritet för sig, tillgänglighet för sig, hot-brist-skada…

• diskutera den specifika situationen, inte allmän beskrivning av begreppen

• blanda inte ihop delarna, t.ex. sekretess och tillgänglighet

• tänk noga på sannolikhet för att hot realiseras, viktigt för prioriteringen

• koppla rangordningen av risker med prioritering av åtgärder, välmotiverad prioritering brukar vara svårt

Vanliga styrkor

Över lag brukar kursdeltagarna vara bra på att

- använda CIA samt riskanalys, hot-risk-skada
- ta en sak i taget, analys först, åtgärder sedan
- strukturera upp i relevanta delar

Prioriteringarna tenderar att vara bättre än tidigare! :)

Vanliga svagheter

Inte hålla isär saker, blanda åtgärder för tidigt.

Att gå direkt från CIA till åtgärder utan riskanalys.

Otydliga prioriteter. Saknad kvantifiering, dålig sammanställning.

Blanda C, I och A.

Otydlig risk-åtgärdskoppling.

Lite få åtgärder ibland. En risk - en åtgärd är ofta inte nog.

Tänkte du på att...

Det finns ibland flera sätt att implementera en åtgärd. Dessa har olika kostnad och effektivitet och är därmed olika åtgärder.

Om din definition av hotagent (angriparen) skiljer sig från boken så behöver du ge din definition. Fast följ hellre boken/kursen.

Datasäkerhet så väl som fysisk säkerhet är inte bara en fråga om att komma in. Ibland bär angriparen iväg utrustningen.

Jo, ett kassaskåp går att stjäla... om det inte sitter fast.

Formfrågor

Mindre viktigt men bra med...

- Numrering gör det ofta lättare att läsa
- Proffsigt utseende ger en bra intryck hos kunden

men mindre bra med

- Stycke utan innehåll / staplade rubriker
- Sunkiga MS-mallar
- Språkfel (lyckligtvis inte i titeln förra året!)

Generellt

Det finns alltid flera svagheter och många åtgärder.

Det kan vara så mycket som ett dussin av varje.

Tid är också en kostnad. Räkna in det. Det är inte gratis bara för att det inte har en prislapp.

Presentationer i december, och inlämning i januari

Alla skall ha fått tider. (Ett svarsutskick kom bort, skall vara åtgärdat.)

Inlämning i vårt inlämngsysterm, göra senast innan VT1 börjar. Vid problem, E-post.

Presentationer en månad innan?

Presentationerna görs på era preliminära resultat.

Viss återkoppling är möjlig.

Ni har möjligheten att modifiera innan inlämning.

Ni behöver inte vänta till januari.

Presentationerna är om förståelse

Er förståelse för problemet är i fokus!

ChatGTP-åtgärd.

Presentera med minimalt med anteckningar, gärna på tavlan!

Snyggt presentationsmaterial är ofta värdefullt i andra kurser - men inte här.

Ni kan ta fram rapporten men gör det sist!

Att presentera på tavlan

Prata inte framför en tom tavla

Skriv rubriker!

Använd tavlan för att förtydliga sammanhang, och för att sammanfatta resultat

Tydlighet: Skriv inte för fort så det går att läsa, använd svart eller blå penna.

Vi ses nästa vecka!

Alla skall har fått bra tider - och meddelats dem!

Alla är i Kärnan:

Ingång 25 (motten av B-huset) 1 tr, korrdidor A ett steg söderut