CHILL

TILL DÖ

Psykologien bag hacking

Fejl 40 – Psykologien bag hacking
1. udgave 2008

Forfatter: Chill
Redaktion: Britt Malka
Omslag: Chill
DTP: Chill
Cor Ectur: Britt Malka
Tryk: www.lulu.com

Hjemmeside: www.fejl40.com

Hackademiet: www.hackademi.com og www.hackademi.net

Indholdsfortegnelse

1. Sikkerhedens svageste led

Kun 2 ting er uendelige, universet og den menneskelige dumhed, og jeg er ikke sikker på førstnævnte (Einstein).

Et firma kan købe den bedste sikkerhedsteknologi, der findes, og uddanne sine ansatte i at håndtere det. Firmaet kan have trænet folk til at låse alt, før de går hjem, og de kan have vagter, der bevogter bygningen om natten.

Dog er dette firma fuldstændig sårbart, og det skyldes den menneskelige faktor.

I årevis har jeg nemt, meget nemt, skaffet mig en masse vigtige og fortrolige oplysninger.

Det eneste, jeg har behøvet at gøre var: at spørge om dem.

Det giver nemlig en falsk sikkerhed at mene, at når man har spækket systemet med sikkerhedsprocedurer, firewalls, biometriske oplysninger, tjek af fingeraftryk m.m., så er den hellige grav velforvaret.

Følelsen af sikkerhed er som oftest kun indbildning; indbildning, som bliver forstærket, når naivitet eller uvidenhed kommer ind i spillet.

Social Engineering-angreb lykkes, enten når folk er dumme eller uvidende om visse ting.

En klassiker

Siden jeg var barn, har jeg altid været interesseret i at lave tryllekunster — for mine venner, for mine børn og familien.

Når man lærer enkelte teknikker, kan man nemt manipulere andre (hvilket faktisk er det, der sker ved tryllekunster).

Jeg har fx i årevis rystet folk ved at kunne gøre samme nummer som den berømte Uri Geller. Nemlig at bøje skeer og gafler.

Foran folks beundrende øjne kunne jeg vise dem, hvordan jeg, blot med psykisk energi, kunne bøje skeer og gafler.

Først da min kone troede på mine evner, afslørede jeg tricket for hende.

Og tricket er nemt — uhyre nemt. Hvordan gjorde jeg det?

Nemt: Jeg bøjede dem med fingrene, ganske enkelt.

Og det er lige før, at det tog mig længere tid at overbevise folk om det, end at overbevise dem om mine "psykiske kræfter".

Hvorfor det?

Svaret kom prompte fra min kone : — Jamen, jeg har ikke set noget!

... Altså kan det ikke være sket. Fordi vi tror, hvad vi ser.

Her er det dette princip, jeg benyttede mig af, og de fleste vil være mere tilbøjelige til at tro på psykisk kraft end på, at de ikke havde set noget, som ellers er så indlysende. Bøje skeer, det kan jo ikke gøres ubemærket, vel? Ikke medmindre jeg er fuldstændig dum eller naiv ... Det er jeg nemlig ikke ...

Virkelig?

Tryllekunstnerens bedste tricks er at tiltrække offerets opmærksomhed på noget andet end det, der sker. Groft sagt kunne man sige, at imens du kigger på hans venstre hånd, sker der noget i højre.

Det er lige præcis på den måde, Social Engineering foregår: Den udøvende vil være uhyre venlig, spændende og hjælpsom, du vil være taknemmelig for at have mødt ham, altimens han "tømmer dine lommer" med den anden hånd, så at sige.

En af de mest kendte historier er Stanley Mark Rifkin-sagen.

Du vil kunne finde mange detaljer på nettet om den sag, men jeg giver dig en forklaring her, som vil illustrere det (og prøv bagefter at sværge, at hverken du eller nogen i dit firma ville kunne falde for det). Historien illustrerer det godt, fordi den bruger mange af de principper, som vi kommer til at pille lidt fra hinanden senere i bogen.

Ingen kender alle detaljer i sagen, da Rifkin aldrig afslørede det hele (du tror da vel heller ikke, at jeg fortæller ALLE mine tryllekunster, vel?), så derfor er det følgende en rekonstitution bygget på de forskellige rapporter og fortællinger, der er rundt omkring.

Det hele skete i 1978. Rifkin arbejdede for et firma, som skulle udvikle et backup-system for en stor bank, Security Pacific, i tilfælde af, at deres hovedcomputer gik ned.

Derfor havde han adgang til det lokale, hvor pengeoverførslerne foregik (flere milliarder dollars hver dag), og hvortil kun meget lidt personale ellers havde adgang.

I en B-film ville han have forsøgt at hacke sig ind i den store maskine, men vi andre ved, at dette ville være meget dumt ... Der er nemlig en nemmere – meget nemmere – måde at gøre det på.

Rifkin fik, i den tid han var på stedet, lært lidt af den jargon, der benyttedes på stedet, og de forskellige principper bag pengeoverførsler.

Han havde fået at vide, som alle på stedet, at de få, der havde tilladelse til at udføre bankoverførsler, fik en hemmelig kode, der blev skiftet hver morgen, og som blev givet dem af centralen.

Nu er et menneske ikke en computer, og når man skifter kode hver dag, siger det sig selv, at de ansatte kan have svært ved at huske den. Derfor skrev vagten koden på et stykke papir, som var lagt et sted, hvor han nemt kunne komme til at se det.

Rifkin bestemte sig for at få fingrene i den kode.

Det var nemt: Han gik ned til centralen, tog notater om forskellige daglige procedurer, så at “backup-systemet” ville kunne fungere med hovedcomputeren, og imens han snakkede med vagten og tog notater, skrev han koden ned.

Lige så nemt som at få en hund til at gø.

Ved 15-tiden gik han ned i bankens indgang og ind i en telefonboks dér. Han smed en mønt i apparatet og ringede til bankens overførselslokale.

Ifølge beretningerne var samtalen noget lignende denne:

– Hej, det er Mike Hansen fra den Internationale Valuta afdeling, sagde han til den kvinde, der tog røret. Jeg vil gerne foretage en overførsel.

Hun spurgte efter lokalnummeret, hvilket var standard-procedure, og Rifkin kendte, naturligvis som langt de fleste i banken, afdelingens numre.

– Ja, det er 286.

– Fint, og hvad er koden?

– 4789, svarede han, imens hans hjerte bankede som sindssygt, fortalte han bagefter.

Koden blev accepteret, og han gik videre med instrukserne:

– Jeg vil gerne have ti millioner og to hundretusinde dollars overført fra Irving Trust Company i New York over til Woxhod Handels Bank of Zurich, Schweiz. Her havde han allerede fået lavet bankkonto.

– Okay, det er forstået, svarede kvinden. Nu mangler jeg bare inter-office koden.

Det havde Rifkin ikke tænkt på. Åbenbart var denne detalje smuttet, og han anede intet om det. Han fik sved på panden, men han holdt hovedet koldt. Han lod som om, at alt var i den skønneste orden, og svarede med det samme uden at spilde tid på en sigende tavshed:

– Jeg skal lige tjekke det ud, jeg ringer dig op igen om lidt.

Han ringede til en anden ansat i banken, og lod som om han ringede fra overførselafdelingen og fik vedkommende til at opgive koden, hvorefter han ringede tilbage til overførselafdelingen og gav koden videre.

Pengene blev overført til Schweiz i et snuptag.

Han smuttede selv dertil og vekslede 8 millioner dollars til diamanter, som han gemte i sit bælte, som han tog med tilbage til USA.

Rifkin fik dermed lavet historiens største bankkup uden så meget som at løsne et skud og uden at hacke sig ind på nogen computer overhovedet. Han fik bare folk til at give ham pengene.

Pudsigt nok er dette kup registreret i Guiness Rekordbogen som "største computer kup", når computeren egentligt aldrig blev brugt.

Det er lige præcis disse teknikker, denne bog handler om: De teknikker, der blev brugt her (og i andre tilfælde), og hvordan du kan forhindre, at disse bliver brugt mod dig eller mod dit firma.

Denne historie burde kunne klargøre for dig, hvor vildledt vores idé om sikkerhed er i det hele taget.

Sådanne sager forekommer mange gange hver dag. Måske ikke en 10 mio. sag hver gang, naturligvis, men hver dag foregår den slags. Du er måske det næste offer, eller faktisk kan det meget vel være, at det foregår lige nu.

Tillidsbrud

I de fleste tilfælde er gode Social Engineers folk med et godt menneskekendskab. De er charmerende, høflige, og man kommer hurtigt til at kunne lide dem. Det er de karaktertræk, som behøves for at kunne lave en hurtig overføring, eller "rapport" som man kalder det i NLP, og dermed vækker de hurtigt tillid.

En veløvet Social Engineer er i stand til at få fat i stort set en hvilken som helst oplysning ved at bruge forskellige strategier og taktikker.

Selv om seje programmører har bygget seje (og dyre!) programmer, har meget få, hvis ikke ingen, taget sig af at patche fejl 40, som forbliver det største sikkerhedshul nogensinde.

I den vestlige verden er vi ikke altid klar over forskellige risici. Vi er heller ikke trænet i at mistænke hinanden. Vi har lært, at vi skal "elske vores næste" og stole og tro på hinanden.

Disse er værdier, vi gerne vil fortsætte med at bygge vores civilisation på, og det er egentlig en slags drømmeverden, i hvilken vi gerne vil leve. Vi vil gerne leve i en verden, hvor alle kan stole på hinanden, og alle kan lide hinanden og alt det her.

Ret irrationelt, egentligt!

Og en svaghed af rang!

Ja, naturligvis ved vi, at alle ikke er flinke og ærlige, men vi lever, som om de var det. Det er en slags uskyld, vi har, godt bekræftet af idealiserede amerikanske films og serier, og vi vil nødigt slippe det.

Vi har bygget en idé om frihed og har svært ved at forbinde et sted med lås, slå og spærringer som et rart sted at være.

Derfor antager de fleste af os, at vi ikke vil blive fuppet af andre. Det bygger vi på det princip, at sandsynligheden for dette er meget lav.

Angriberen, som kender dette princip, får sin efterspørgsel til at lyde så fornuftig, at han ikke vækker mistanke, altimens at han udnytter offerets tillid.

Se blot på vores lufthavne i dag.

Ja, sikkerhed er vigtig, fordi vi frygter terroristangreb.

Derfor er der skærpet sikkerhed og i mange lande, fx Frankrig, har vi bevæbnede militærfolk og betjente i lufthavnen, og de er parate til at sprænge din kuffert i luften, hvis den ikke har navneskilt, og hvis du ikke er i nærheden.

Dog blev det afsløret i 2006, at i Frankrigs største lufthavn (og verdens 6. største), gik og kom over 70 islamister, hvoraf flere var kendt i forbindelse med terrorisme, som de ville. Hvordan? Ganske enkelt: I Roissy er der rengøringsfolk. Disse rengøringsfolk er ansat af forskellige rengøringsfirmaer, og på den måde skaffede kendte terrorister sig adgang til alle dele af lufthavnen.

Før attentaterne i 2001 var der sandeligt også kontrol i lufthavnen. Der har altid været våbenkontrol.

Virkede de ikke den 11. september?

Selvfølgeligt virkede de udmærket. Problemet var ikke maskineriet, men de ansatte i lufthavnen.

Og det, at bruge bedre udviklede maskiner og flere våben, vil ikke hjælpe ret meget.

I dag, mere end nogensinde, skal vi droppe ønsketænkning og idéer om jorden, der bliver til et paradis, hvor alle elsker hinanden og stoler på hinanden.

Det er på tide at stoppe med at slukke hjernen, når vi tænder for skærmen – man skulle af og til tro, at det var samme knap.

Vi skal til at vågne op til virkelighedens verden. Vi skal lære at blive opmærksomme og holde op med først at forstå det, der er sket, efter det er sket. Vi skal uddanne os i den slags og, især, uddanne personalet i firmaet.

Et spørgsmål om balance

Alt her i verden er et spørgsmål om balance.

Vi kan ikke have sådanne sikkerhedshuller (fejl 40) i vores systemer og vores firmaer. Det er en åben dør til at blive udnyttet og berøvet.

På den anden side, hvis et firma har for mange sikkerhedsprocedurer, vil det være en hindring for business og aktivitet.

Det vil blive svært, hvis ikke umuligt, at vokse for sådan et firma, der så risikerer mest at ligne en institution.

Fiffet er at finde en balance mellem sikkerhed og produktivitet.

Andre bøger, som fx nogle af de andre jeg har skrevet[1], har været koncentreret om det tekniske bag hacking. Om software og hardware, deres huller, deres (hvis mulige) modtræk.

[1] Hackerguiden - Hacking træk og modtræk (www.hackerguiden.com) og Hacking uden snor - Hemmelighedernde bag Wi-Fi-Hacking (www.wifibogen.com).

Jeg omtaler emnet fejl 40 jævnligt, dels i disse bøger, dels i de kurser, jeg har givet, og denne bog fokuserer på det.

Bogen vil fortælle dig, hvordan du bliver manipuleret, hvordan du, eller dine medarbejdere, kan blive manipuleret, og naturligvis også, om hvordan du kan gardere dig imod det.

Det bliver svært, fordi vi har en meget lang historisk baggrund for at blive manipuleret. Vi er eksperter – så at sige – i at blive manipuleret.

Vi har allesammen været i kontakt med verdens bedste og mest effektive Social Engineers, nemlig vores forældre!

De gjorde det naturligvis for "vores bedste", når de rent faktisk gjorde det for det "de mente var det bedste" (der er en vigtig forskel mellem de to begreber).

Forældre havde deres grunde, på samme måde som enhver Social Engineer har sine grunde til at gøre det, han gør.

Vi er måske ikke enige i det, men han har helt afgjort sine grunde, mål og ideologi for at forsvare sine handlinger.

Om ikke andet ville mange af os synes, at 1 million dollars vil gøre den enkelte bedre gavn end en eller anden stor verdensbank, der udnytter folk rundt omkring, og som er forsikret alligevel ... Hov ... Der var jo det, vi ville: Mål, ideologi, grunde.

Hvor mange gange har jeg ikke hørt folk fortælle mig, at hvis kassedamen laver en fejl til deres fordel, hvis det er et lille sted, en lille købmand, så vil de sige det, men hvis det er i en stor concern, så vil de ikke, fordi "de har jo alligevel penge nok".

Som om det kun er tyveri at stjæle fra de små.

Er det ikke nemt at berettige disse handlinger?

Jo, nemlig.

Vi er konditioneret af god træning: forældre, ideologi, sans for retfærdighed og uretfærdighed, og derfor kan vi forholdsvis nemt selv blive ofre.

I en fuldkommen verden ville vi kunne stole blindt på hinanden, leve i fryd og gammen, og vi ville vide, at alle er ærlige og til at stole på.

Men vi lever ikke i en fuldkommen verden.

Så lad os gå på opdagelse sammen.