ComputerWorlds kronik den 19-08-2005:

Den gode, den onde og den skødesløse

Den danske debat om sikkerhed på nettet er præget af en simpel model af aktørerne: Der er den gode - IT- og sikkerheds-eksperten. Der er den onde - skurken, som smitter, spammer og spionerer. Og der er den skødesløse - brugeren, hvis dårlige vaner og mangel på viden om sikkerhed forårsager kostbart besvær.

Henrik Lykke Nielsen fra Captator siger: ”Mange alvorlige sikkerhedsproblemer skyldes først og fremmest dårlige brugervaner og mangel på brugeruddannelse.”

Mark Hall fra Computerworld slår i sin klumme den 1. juli til lyd for en *Endlösung* på besværet: Medarbejdere, der fjumrer med sikkerhedsprocedurer, bør straffes, først med en advarsel, så med inddragelse af ferie og til slut med fyring. Så kan de lære det!

Sikkerhedsprocedurer er for det meste sikre. Men er sikkerhed den eneste kvalitetsparameter? Er det for eksempel kværulanteri at protestere over en adgangskode på mindst 25 tegn, som en dansk bank indførte for nogle år siden? Er det urimeligt at brokke sig over en adgangskontrol, der skelner mellem store og små bogstaver i adgangskoder, som naturligvis af sikkerhedsgrunde ikke vises på skærmen mens man indtaster dem? Er det fyringsgrund at nægte at spilde sin tid på en sikkerhedsvejledning, som er skrevet på nørdsk?

Sikkerhed må aldrig blive så besværlig, at det virker som om det er *brugeren* der er fjenden.

De brugere, som jeg møder, er logiske og bevidste om hvordan de bruger deres tid fornuftigt. Men deres logik er ofte meget forskellig fra sikkerhedseksperternes. Desværre findes der mange sikkerhedsfolk, som ikke interesserer sig for brugervenlighed og social engineering. Social engineering er læren om hvordan man lokker brugere til at overtræde sikkerhedsregler, f.eks. ved at klikke på en vedhæftet fil eller udlevere en adgangskode til en uautoriseret person.

En sikkerhedsekspert, der blindt afviser uhensigtsmæssig brugeradfærd som ”dårlige brugervaner”, er i sig selv en sikkerhedsrisiko.

Brugerforståelse er nødvendig. Her er nogle eksempler:

Vi er vel alle enige om, at det er en god idé at beskytte sit trådløse netværk bl.a. med kryptering. Men hvor er de forståelige, brugertestede vejledninger som fortæller den typiske bruger præcis hvad han skal gøre? Netsikker nu!-webstedet giver råd som ”Slå broadcastmeddelelser fra i dit trådløse netværk” og ”Husk at ændre SSID” uden yderligere detaljer om fremgangsmåden. Underforstået: Hvis du ikke forstår dette, så er du dum. Windows XP Magasinet offentliggjorde for nylig en lidt mere detaljeret vejledning i hvordan man sikrer sit netværk. Vejledningen gik ud fra, at man vidste god besked om emnet i forvejen, og undlod at besvare rimelige begynderspørgsmål som f.eks. ”Hvad er hexadecimal? Hvorfor er der fire *keys* og ikke kun én?”

Vi mangler forbilledlige eksempler på hvordan man forklarer sikkerhed på en brugervenlig måde. Viden om sikkerhed er ikke nok til at skabe rigtig sikkerhed.

En klassisk formaning lyder: En god adgangskode opfylder fire krav: Den er mindst otte tegn lang, den indeholder både store og små bogstaver, den indeholder tal, og den indeholder specialtegn som #, % og {.

Udgangspunktet er forkert. Det forsøger at gøre en god adgangskode til brugerens problem. Hjælp brugere i stedet for at give dem komplicerede formaninger, hvis formål er uklart. Tilbyd at generere en adgangskode, som er et fornuftigt kompromis mellem sikkerhed og noget brugeren kan huske, f.eks. ”uldsodatank”. Kontrollér de adgangskoder som brugere selv foreslår, og advar høfligt og med forståelige argumenter, hvis en bruger foreslår en mindre sikker adgangskode - og foreslå samtidig et bedre alternativ.

Det er sådanne tankebaner vi skal ind på: Hjælp og forebyg i stedet for at formane og true.

Brugere er tillidsfulde. Mange brugere har en flowerpower model af internettet: Verden er god og smuk, og jeg bidrager til det ved selv at være venlig og hjælpsom. Uden denne tillid havde virus, phishing osv. ikke mange chancer.

Nogle synes at denne tillid er naiv og farlig, andre synes at den er positiv. Pierre Omidyar, grundlæggeren af eBay, synes f.eks. at eBays vigtigste bedrift er at det har lært 135 millioner mennesker at de kan have tillid til en helt fremmed person.

Nogle steder på nettet er tillid altså ønskværdig, andre steder er mistro på sin plads. Hvordan skal brugere kende forskel? Svaret er, at det skal de ikke. Et godt sikkerhedssystem beskytter dem både med forståelige og rettidige gode råd og ved f.eks. at amputere skadelige elementer fra e-mails.

Brugere vil have sikkerhed, som er nem at bruge. Det som nogen kalder skødesløst, kalder andre effektivt i en travl hverdag. Det kan være mere besværligt for IT-folk at lave nemme sikkerhedssystemer - men det er vel ingen undskyldning for at lægge byrder på brugerne?

Rolf Molich
DialogDesign

Reaktion på kronikken i læserbrev trykt i ComputerWorld 26-08-2005:

En replik om sikkerhed

Læserbrev fra Peter Munck, IT-chef Kuben A/S:

I Computerworld fredag den 19. august skriver Rolf Molich (RM) i kronikken "Den gode, den onde og den skødesløse" om sikkerhedseksperters tendens til at opfatte brugerne som fjender.

Som udgangspunkt mener RM, at brugerne er tillidsfulde og gerne vil bidrage med venlighed og hjælpsomhed til det, de ifølge RM opfatter som en god og smuk verden: Internettet. På den anden side har vi så sikkerhedseksperterne, der i yderste konsekvens sammenlignes med koncentrationslejrkommandanter, som skal gennemføre en "Endlösung" over for alle de formastelige brugere.

Det kan da aldrig være brugerens ansvar at sikre et trådløst netværk

RM bringer nogle eksempler på sikkerhedsprocedurer og -vejledninger, som ikke virker. Hovedsynspunktet er, at sikkerhed aldrig må blive så besværlig, at det virker, som om brugeren er fjenden. Det er jeg helt enig i, men bortset fra tilfældet med passwords på 25 karakterer synes jeg, at det andet eksempel er misforstået: Det kan da aldrig være brugerens ansvar at sikre et trådløst netværk – det er jo netop sikkerhedsekspertens arbejde, og det skal brugeren overhovedet ikke blandes ind i.

Jeg er også enig med RM i, at sikkerhedseksperters og brugeres logik er helt forskellige, og det er der vel ikke noget specielt overraskende i. Min egen erfaring er, at et stort flertal af brugerne accepterer et vist niveau af sikkerhed, og så er der et mindretal, der er helt ligeglade. Enten fordi de ikke forstår det, eller også fordi de mener, at det på ingen måde angår dem. Netop derfor bliver balancen mellem sikkerheds- og brugerhensyn hårfin: Jo mere restriktive sikkerhedsprocedurerne er, des større er sandsynligheden for, at brugerne opfører sig uhensigtsmæssigt eller helt negligerer gældende regler. Eksempelvis vil lange og komplicerede passwords med stor sandsynlighed medføre, at password'et står på en post-it, der er klistret fast til skærmen (den lidt snedigere bruger sætter det på undersiden af tastaturet).

Ud over at jeg er uenig med RM i eksemplerne mener jeg også, at han glemmer eller forbigår to helt essentielle forhold, der til enhver tid må være udgangspunktet for diskussioner om sikkerhed:

For det første hvorfor vi skal have sikkerhed og sikkerhedsprocedurer, og for det andet hvem, der er ansvarlig for disse ting. Det første kan besvares med, at man har sikkerhed og sikkerhedsprocedurer dels for virksomhedens skyld, men så sandelig også for den enkelte brugers egen skyld. Fornuftigt implementeret og anvendt skal sikkerhedsprocedurerne kunne af- eller bekræfte en mistanke om urent trav hos en bruger, og det er ikke sikkerhedsekspertens ansvar at få brugeren til at forstå det.

For det andet er det altså ikke sikkerhedseksperternes ansvar at få brugerne til at forstå og rette sig efter sikkerhedsprocedurerne. Det er og bliver virksomhedsledelsens opgave at fastlægge det ønskede sikkerhedsniveau, og ud fra det man beslutter at fastlægge politikker, procedurer og regler, som brugerne skal efterleve i det daglige. Niveauet skal selvfølgelig tilpasses virkeligheden og den type forretning, man driver, men i den sammenhæng er sikkerhedseksperten "bare" en rådgiver.

Rolf Molichs svar trykt i ComputerWorld 02-09-2005:

Tak til Peter Munck, IT-chef Kuben A/S, for hans replik til min kronik om brugervenlig sikkerhed den 19. august.

Jeg er enig i at det ikke bør være brugerens arbejde at sikre et trådløst netværk. Det er sikkerhedsekspertens arbejde. Desværre er der jo en del firmaer og private hjem, hvor der ikke lige er råd til at hyre en sikkerhedsekspert til at få det trådløse netværk som er købt på tilbud i Netto, til at fungere forsvarligt rent sikkerhedsmæssigt. Og vi er forhåbentlige enige om, at privat sikkerhed også er firmasikkerhed, specielt i lyset af den enorme datatransmission som dagligt sker mellem arbejde og privat i form af bærbare computere på bagsædet i en bil. Derfor er forståelige og gennemprøvede vejledninger vigtige.

Peter Munck påpeger korrekt, at det er virksomhedsledelsens opgave at fastlægge det ønskede sikkerhedsniveau. Et af mine ærinder med kronikken var at påpege, at ledelsen i sin beslutningsproces ikke kun skal støtte sig til IT-chefer og sikkerhedseksperter, men også til brugere eller til folk med reel forstand på brugeres adfærd hvad sikkerhed angår. Sikker sikkerhed opnår man ikke kun med undervisning og formaninger. Det kræver også fornuftige, brugervenlige sikkerhedsprocedurer, som er beskrevet så det er til at forstå. Holdninger som "Jeg er jo selv bruger og kan derfor selv vurdere hvad der er behov for" og "Brugerne er det svageste led i sikkerhedskæden" er ikke befordrende for sikker sikkerhed.