Denne guide er oprindeligt
udgivet på Eksperten.dk

COMPUTERWORLD

Trådløse hotspots - Brug dem sikkert

Hotspots er blevet populærer i vores byer og mange mennseker benytter dem flittigt. Læs her hvordan du gør det sikkert også

Skrevet den **03. Feb 2009** af **bufferzone** I kategorien **Sikkerhed / Kryptering** | ★★★☆☆

Du bør også kigge på denne artikel
http://www.eksperten.dk/artikler/1269

HotSpots

kryptering
Langt de fleste af os ved godt at vores trådløse netværk skal sikres. Vi kender teknologier som WEP og WPA og ved at WPA er langt bedre en WEP som igen er langt bedre end ingen ting. Mange af os ved også, at SSID broadcast skal slås fra og at vi skal anvende MAC adresse filtrering. Nogle af os gør os endda den ulejlighed at se på placering af vores udstyr og bruger andre antenner, så vores net dækker inden for vores bopæl, men ikke kan rækkes udenfor, hvor dette er muligt.
Men hvad nu når du sidder på Café Central Park, Cafe Cox, Nørrebro Bibliotek, 7-Eleven (Ved Vesterport eller Amagerbrogade), McDonald's eller et af de mange hundrede andre hotspots i Danmark og er på nettet der. Her kan du jo ikke uden videre kryptere og selv om du kunne, er der jo andre der er på inden for krypteringens grænser.

Der er en masse potentielle muligheder for en person der enten er nysgerrig eller decideret er ude på ballade. Hvis du vil undgå (eller i det mindste gøre det svært) at andre kan læse dine passwords, mails eller se hvad du chatter om og med hvem, er det vigtigt at du tænker dig om og ved hvordan du skal begå dig. Selvom nettet bruges til mange ting, vil jeg her koncentrere mig om surfing, mail og instant messaging. IM.

Surf the web
Hvad enten du surfer på nettet I caféen eller hjemme, er der faktisk et universelt råd jeg kan give, der vil fjerne en masse problemer for dig og en masse muligheder for hackeren. Lad være med at anvende Internet Explore. Selv Microsofts nyeste release, version 7, der netop var annonceret at skulle kunne håndtere alle de sikkerhedsproblemer IE har haft og stadig har, så blev der fundet kritiske sårbarheder i denne allerede få dage efter den var udgivet. Selv i dag hvor IE 7 har været på gaden i nogen tid findes stadig nye huller og sårbarheder der kan anvendes.
Du bør i stedet anvende Firefox, Opera eller hvis du er MAC burger så Safari. Alle disse browsere er gratis, hurtige og med et meget bedre sikkerhedsrygte end IE. Selv har jeg anvendt Firefox i flere år, og er begejstret for dens mulighed for at anvende tredjeparts extensions, der betyder kraftigt forøget funktionalitet, også på sikkerhedsområdet og for dens sikre og hurtige måde at køre på. De enkelte steder hvor jeg en gang imellem er nødt til at anvende IE, bruger jeg version 6 med alle de patches og strammet op så meget jeg kan (forbyd alt hvad du kan og tillad så lidt som muligt).

Når du så browser rundt på nettet skal du være lidt vågen og tænke dig om. Alarmklokkerne skal især ringe når du skal indtaste fortrolige og kritiske oplysninger som brugernavne, passwords, konti numre, kreditkort numre, CPRnumre eller anden følsom data der kan bruges af andre. Disse oplysninger skal beskyttes, og dette gøres normalt med SSL kryptering. Normalt, når du bare surfer rundt på nettet, ser URL'en i browserens adresselinie således ud':

"https://www.mitkrypteredesite.dk".

Den store forskel kan være svær at se, men læg mærke til at den ene starter med http og den anden med https. Det lille s betyder at forbindelsen er krypteret med SSL og at dine data er krypteret og dermed ikke umiddelbart kan læses hvis de opfanges af andre.

Hvis du bare læser eller ser på forskellige hjemmesider, så kan du være helt rolig. Det er først når du selv skal til at indskrive oplysninger du skal passe på.
Hvis du skal tilgå dit hjemmenet eller din arbejdsplads fra en offentlig Café bør du anvende VPN. Dette er ikke så vanskeligt at sætte på og jeg regner med at skrive en artikel om dette emne snart, så hold øje.

Email
Email kan man bruge på to grundlæggende forskellige måder, enten via en browser, webmail som det kaldes f.eks. Hotmail, Gmail eller andet, eller via et klientprogram f.eks. Outlook, Thunderbird, AppelMail eller andet.

Web Mail
Web mail er meget populært og ganske praktisk. I dag er det oven i købet muligt at få en webmail konto med rigtig meget plads, f.eks. Gmail der jo har over 2 Gb. plads pr bruger, så man kan have alt sin mail og mange dokumenter, billeder og andet liggende online. Mange at de almindelige pop3 mailkonti, man får af sit firma eller hos sin internetudbyder, giver også mulighed for at tilgå sin mail via webmail før den hentes ned på computeren.

De fleste web mailudbydere anvender SSL (https) til at beskytte din logon, men logon er også alt der beskyttes. Kun dit password og brugernavn er beskyttet med kryptering, men dine mails, både dem du skriver og dem du læser, kører via ganske almindeligt http og er derfor frit tilgængelige på det trådløse net for alle der lytter med.

Hvis du har lyttet til mit råd ovenfor og anvender FireFox som browser, og bruger Gmail, er der en løsning på dette problem. Download og installer extensionen "CustomizeGoogle" som du kan hente her https://addons.mozilla.org/extensions/moreinfo.php?id=743&application=firefox (du kan oven i købet gøre det fra din favorit café via trådløst netværk da den køre via https). Når du har installeret denne extention, åbner du Tools, vælger CustomizeGoogle Options og klikker Gmail fanebladet. På dette faneblad afkrydser du "Secure (switch to https)" og trykker OK for at lukke vinduet.

Næste gang du logger på Gmail vil du se at både logon og den videre behandling af mails sker via https. Denne løsning er god, da du ikke behøver at tænke yderligere efter du har installeret og konfigureret CustomizeGoogle. Det skal også nævnes her, at du faktisk manuelt kan skifte til https ved at skrive https i stedet for http i browserens adresselinie, men dette skal gøres manuelt, hver gang du åbner din browser.

Både Hotmail og Yahoo mail har mulighed for at anvende SSL til Logon, men gør det ikke som standard. For at gøre dette skal du klikke på linket "Sign in using enhanced security" eller "Submit over SSL" som du sikkert aldrig har lagt mærke til da de er ret små og diskrete. Det er dog kun logon der beskyttet og du kan ikke beskytte din læsning og skrivning af mails i disse tjenester.

Hvad angår brug af den webmail der følger med din internetkonto eller den du har fra dit arbejde, så er du nødt til at spørge direkte der hvor du har fået den.

Mail via klientprogram
Når du arbejder med mails med en almindelig mailklient som f.eks. Outlook, bruger du to protokoller, nemlig POP3 til at hente mail og SMTP for at sende mails. Begge protokoller er driftsikre og gode, men helt uden sikkerhed. Dette betyder at både mails, brugernavne og passwords sendes i helt klar tekst, lige til at læse for enhver. Dette er selvfølgelig et problem i dagligdagen når du sidder hjemme, men problemet er meget større når du er på et offentligt trådløst net, for her sidder der mennesker du ikke kender på samme lokale netværk som dig, og her er det en smal sag at sniffe tingene op.

Ligesom med webmail gælder det at både logon, læsning (mails hentes ned på din pc via POP3) og skrivning (mails sendes via SMTP) af mails skal beskyttes med SSL (eller anden krypterings teknologi f.eks. VPN). Hvordan dette gøres afhænger af hvilken udbyder du har og hvilken mailklient du bruger. Du bør kontakte din ISP eller kikke på deres hjemmeside for instruktioner. De fleste har secure POP3 og en del har også secure SMTP, men langt fra alle. Hvis din udbyder ikke tilbyder dette, så skift til en anden udbyder, brug sikker webmail hvis det udbydes eller undlad at bruge denne konto fra Caféen.

Igen kunne løsningen være at anvende Gmail, der også kan køre fra din mailklient. Gmail løsningen håndterer yderligere et problem vi har når vi ønsker at sende mail sikkert. Selv om din mailudbyder tilbyder secure SMTP, vil du oftest ikke kunne anvende din egen udbyders SMTP server når du sender fra en Café. For ikke at blive spam relay center begrænser mange netværksejere deres net således at du tvinges til at anvende deres SMTP server. Selvom denne kan anvende secure SMPT, kan du være rimelig sikker på, at den der står bag disken ikke har den fjerneste anelse om hvordan det sættes op. Gmail har adskillelige sider der beskriver hvordan du skal sætte din mail klient op til at sende om modtage sikkert. Se her:

https://mail.google.com/support/bin/search.py?query=smtp&Action.Search=Search&type=f&lr=lang_en&ctx=en%3Asearchbox

Igen læg mærke til https, læs trygt denne side fra din favorit café. Med Gmail bør du kunne både logge på, læse og skrive mails i fred for forstyrrende nysgerrige øjne.

Instant Messenging
Instant Messenging er en ret populær kommunikations form især blandt unge mennesker og den har da også ganske mange fordele. En af ulemperne er at kommunikationen i reglen er ganske ukrypteret og dermed ikke egnet til private, fortrolige diskussioner. Det første du bør undersøge er om den IM klient du anvender, kan krypterer, og husk også at dem der sidder i den anden ende også helst skal kunne krypterer hvis du vil være helt sikker.

Hvis du ikke kan krypterer med din klient, kan du overveje at skifte til GAIM (kan downloades gratis her) der er en open source klient til IM. Den kan køre på de fleste operativ systemer og har support for alle de store IM netværk hvorfor du kan tale med AIM, MSN Messenger, Yahoo! Messenger, Google Talk og flere andre. Fordelen ved GAIM, udover den bredde support, er at den kan krypterer kommunikationen. Download Gaim-Encryption plugin her http://gaim-encryption.sourceforge.net/ og installer eller download Off-the-Record Messaging her http://www.cypherpunks.ca/otr/ der også virker fint med GAIM:

Hvad er problemer egentlig
Tjaaa, du tror det måske ikke, men hackere går faktisk også på Café og andre steder med Hotspots. Faktisk bruges hotspots ofte til den slags aktiviteter, da de giver hackeren mulighed for at sløre hvor han befinder sig, og hvad havde du tænkt dig de skulle bruge deres tid til mens de sidder der og kikker på verden, gæt selv.

Det behøver heller ikke være hackeren der er problemet. Jeg kender en ung pige, der ofte kom på ynglings Caféen med veninderne, hvor de flittigt brugte deres bærbare computere. Og som det så ofte sker, fik en ung mand øje på denne pige og besluttede sig for at lære hende nærmere at kende. Dette kunne gøres uden at hun i første omgang opdagede noget, men det har siden haft relativ stor betydning for hendes liv i almindelighed og hendes videre færden på de trådløse net i særdeleshed, da hun endelig slap af med ham. Efterfølgende har hun været nødt til at skifte stort set alle konti oplysninger, passwords, telefonnumre og andet og flere af veninderne ligeså, da han også begyndte at generer dem.

Hotspots og friheden til at kunne kommunikere på farten er en god ting, og de fleste kommer ikke ud for ubehagligheder. Hvis du tænker dig lidt om og anvender de muligheder der ligger i systemerne bliver det heller ikke dig.

Skulle du have kommentarer eller spørgsmål er du meget velkommen til at kontakte mig på

kim@bufferzone.dk ligesom jeg ofte er at finde her på eksperten. Stavefejl, forslag og andet modtages med kyshånd (ja ikke fejlene selvfølgelig, men den rette stavning forstås). Jeg vil bede dig om ikke at spørge i artiklens kommentarer, der kan jeg jo ikke svare.

Kommentar af frankeman d. 21. Feb 2006 | 1

Fino, en del vidste man, men dejlig konkret..

Kommentar af k. d. 27. Feb 2006 | 2

Kommentar af beta d. 08. Jul 2006 | 3

Rigtig fin artikel. Jeg er netop "gået trådløs", så her var der en lidt info at hente. Desværre er der mange "almindelige" PC brugere som ikke ved nok om sikkerheds-truslen ved at gå på nettet/trådløst. En aktikel som denne kunne med fordel postes de steder hvor "menig mand (M/K)" læser sine nyheder (tidsskrifter / avisen, mm.). Jeg tror ikke at "Menig mand (M/K)" logger ind på E, og læser denne artikel, de kender nok dårligt til sidens eksistens ;-)

Jeg ser frem til kommende artikler.

Kommentar af mrmox2 d. 19. Feb 2006 | 4

ok artikel - men den primære målgruppe er nok ikke her på e. bortset fra gmail-tricket er det for mig at se mest sund fornuft. det kunne være fint at få den i metro eller sådan noget

Kommentar af znapper d. 23. Feb 2006 | 5

Kommentar af barbarbo d. 20. Feb 2006 | 6

Rigtig god artikel og jeg tror faktisk en stor del af målgruppen kommer forbi eksperten. Jeg kunne sagtens forestille mig at bruge disse offentlige net og nu ved jeg hvordan jeg gør det sikkert

Kommentar af dach d. 21. Feb 2006 | 7

Kommentar af rasmusbl d. 21. Feb 2006 | 8

Kommentar af zypher212 d. 17. Feb 2006 | 9

Alt for lidt information som denne er desværre ofte tilfældet.
Hvis du bruger hotspots rundt omkring, så læs denne artikel, mange gode råd, og meget nyttig information. Desværre er der lidt typos som trækker lidt ned... :)

En af da bedste og mest let læste artikler til dato synes jeg (Fra bufferzone)!
Glæder mig til artiklen om VPN. :)

Kommentar af area48 d. 03. Mar 2006 | 10

God og konkret information skrevet i et let forståeligt sprog som de fleste almindelige brugere bør kunne forstå/benytte

Kommentar af blc79 d. 06. Jun 2006 | 11

Kommentar af califfo d. 17. Feb 2006 | 12

God artikel. Godt at tage emnet op, selvom jeg tvivler på at særlig mange af de unge piger der går på café også lægger vejen forbi denne artikel.

Kommentar af shako d. 25. Oct 2008 | 13

Jeg kan forestille mig du måske skulle skrive en artikel om hvordan det forgåt.. Selvfølgelig ikke en manual til hvordan man hacker (eller cracker som det rigtig heder) et netværk, og du skal ikke gøre det for min skyld, men jeg tror der er andre der kunne være intereserret i Packet sniffing og ihvertfald teorien bag.