Trådløs sikkerhed - Hvad bør jeg tænke på

Trådløs sikkerhed er et problem for mange. Rigtig mange trådløse netværk er piv åbne, og det kan faktisk relativt enkelt sikres meget bedre. Læs her hvordan du gør.

Skrevet den **04. Feb 2009** af **bufferzone** I kategorien **Sikkerhed / Generelt** | ★★★☆☆

Trådløs sikkerhed - Dette bør du tænke på.

Trådløse netværk er nærmest pr. definition usikre, hvis du bare smider dit netværk i drift, uden at tænke dig om, er dit netværk, dine ressourcer og dine data sat til fri afbenyttelse af alle der er tæt nok på og skulle have lyst til dette. Nogle gange sker det oven i købet at beboere i bebyggelser, hvor der er flere trådløse netværk i de forskellige lejligheder, anvender hinandens net, uden at vide, eller bemærke det.

1. Fysiske forhold.
Det første du bør overveje er den fysiske placering af dit Accesspoint. Hvis du placere dette forkert, vil signalet kunne nås langt uden for din bolig, ud i det offentlige rum (det hedder det faktisk), ind til dine naboer og ud i andre områder hvor du ikke kan kontrollere hvem der sidder med et trådløst netkort og en PC. Ved at placere dit Accesspoint/router klogt, kan du måske opnå at signalet kun kan nås inden for dit eget område, og dermed har du fjernet en meget står den af problemet.
Retningsbestemte antenner, kan både bruges til at forøge rækkevidden og til at styre hvor signalet kan nås. Standard antennen på et Accesspoint er en såkaldt rundstråleantenne, der stråler cirkulært. Da de færreste huse er cirkulærer betyder dette at du ofte er nødt til at bruge et kraftigt signal får at række hele din bolig, og dermed også stråler ud over et stort område uden for. Hvis du bruger retningsbestemte antenner, kan du styre retningen hvor signalet stråler og dermed kun stråle inden for dit eget område.
Når du har opsat dit Accesspoint, bør du kontrollere hvorfra du kan nå dit netværk. Gå en tur med din bærbare og se hvor langt ude du stadig er på. Den viden du her opnår, kan du måske udnytte til at skærme. Aludampspær anvendes som isolering, og det har den egenskab at det kan skærme trådløse signaler på godt og ondt. Hvis du alligevel skal sætte din bolig i stand, kunne du overveje at skærme ind til naboer ig ud mod vejen, og på den måde begrænse det område hvor du stråler.

2. Generelt sikring.
Næste skridt er at sikre de maskiner der skal på dit net. Her taler jeg om helt almindelige råd du kan læse i min artikel "Sikkerhed på din private Computer" (http://www.eksperten.dk/artikler/32). Sørg for at bruge gode lange password alle de steder du har mulighed for det, læs min artikel "Gode passwords, hvad er det" (http://www.eksperten.dk/artikler/71), og krypter dine data, hvis du har XP eller Windows 2000.

3. Adskil via DMZ
Hvis du har et kabel netværk, hvor du f.eks. har nogle ressourcer du ønsker at beskytte. Det kunne være filservere og maskiner med fortrolig data på, bør du separere dit trådløse net fra dette net, helst fysisk og hvis du ønsker forbindelse, så kobler du det trådløse net på kabelnettet som DMZ. Dit kabel netværk forbindes til en firewall, der har tre netkort. Kort 1 til dit kabel netværk, kort 2 til Internettet og kort 3 som DMZ med det trådløse netværk tilkoblet. Opsæt regler mellem disse netkort, så du kan styre hvad der kan passere firewallen.

4. Brug VPN
Hvis du vil have ordentlig sikkerhed på dit trådløse netværk, med stærk kryptering af alle forbindelser, kan du anven VPN oven på dit trådløse netværk. Denne løsning giver høj sikkerhed, men kræver at du installere en VPN klient oven på alle de maskiner der skal tilgå det trådløse netværk.

5. WEP, WPA og WPA2
WEP er ikke længere godt nok til netværk der skal beskyttes. Et WEP krypteret netværk kan i dag brydes ganske hurtigt, hvis der er meget trafik på det og er det et privat netværk er det kun et spørgsmål om tid for der er fanget pakker nok. WPA giver bedre sikkerhed og bør bruges i stedet for WEP. Husk at ligegyldigt hvilken form for kryptering, skal du vælge så mange bits kryptering som muligt og vælge en værdi man ikke umiddelbart kan gætte, ellers er den værdiløs.
Efterfølgeren til WPA er kommet, det kaldes WPA2 og giver naturligvis bedre sikkerhed en WPA. Kontroller fabrikantens hjemmeside for at se om der skulle være kommet en firmware upgrade til dit accesspoint så den understøtter WPA2. Gør den ikke det, er det ingen katastrofe, indtil videre kan du vente til du alligevel skal skifte. Hold øje med denne artikel, skulle forholdele ændres, vil jegrette artiklen så det fremgår.

6. MAC adresse filtrering.
Du bør altid anvende filtrering på MAC adresser, også selvom det er lidt besværligt at slå til og konfigurere. Denne foranstaltning gør det en del svære for en hacker at operere på dit net, idet han nu ikke blot skal cracke krypteringen, men også skaffe overblik over hvilke MAC adresser der anvendes samt vælge en der ikke er i brug når han går på. MAC adresse filtrering er en meget simpel autentificering af dine klienter, men sammen med alle de andre ting du tager i anvendelse giver den bedre sikkerhed

7. SSID navngivning og broardcast.
Når du første gang konfigurere dit trådløse netværk, skal du vælge en WLAN-identifikation (SSID). Mange anvender deres familienavn eller firmanavn, og det er en rigtig dårlig ide, da dette let kan gættes. Du bør anvende de samme råd for navngivning af SSID som du anvender ved valg af password.
De fleste Accesspoint's er som standard sat til at acceptere SSID association requests via broadcast. Dette betyder at der hurtigt kan etableres trådløse forbindelser, men samtidig at dit trådløse net annoncere sig selv ud til hele verden, du kan lige så godt udsende skriftlige invitationer til alle hanckere i miles omkreds. SSID Broadcast Associations skal slås fra.

8. Tænk som en hacker.
Du kan selvfølgelig opsætte dit netværk, og vente på at der sker noget, for så at forsøge at finde ud af hvad derer sket og hvordan, men du kunne også være proaktiv og selv undersøge mulighederne, og anvende nogle af de værktøjer hackerne selv bruger til at opdage hvad der sker.
Først bør du skabe overblik over hvor stort et område du dækker med dine antenner. Husk i den forbindelse at arbejde i tre dimensioner og også kontrollere om du kan nå dit net på etagerne over og under dig, også i nabo ejendommen.
Anvend Intrution Detection værktøjet Kismet. Kismet er et 802.11 layer 2 wireless network detector, sniffer, og intrusion detection system. Kismet virker sammen med et hvert trådløst netkort, der supportere raw monitoring (rfmon) mode, og kan sniffe 802.11b, 802.11a, og 802.11g trafik.
Kismet er fuldstændigt passivt og kan ikke detectes når det kører. Kismet automatisk trackser alle netwærk inden for rækkevide, den kan også detecte (eller finde) hidden networks, angrebsforsøg, finde uautoriserede (rogue) Accesspoints, and uautoriserede brugere (f.eks. hackere).
Kismet understøtter Multiple packet sources, Channel hopping, IP block detection, Cisco product detection via CDP, Ethereal/tcpdump compatable file logging, Airsnort-compatable "interesting" (cryptographically weak) logging og Hidden SSID decloaking.
Læs mere om dette uunværlige trådløs hacker værktøj på http://www.kismetwireless.net og brug det til at beskytte dig selv.

9. Tilpas effekten.
Når dit net er opsat og kører, bør du skrue effekten net, så du begrændser rækkeviden at dit Accesspoint mest muligt. Prøv dig frem til du finder den mindst acceptable effekt

10. Logging.
Husk logging, og husk at kikke i din log jævnligt. Alle de steder du kan logge, bør du gøre dette og gøre gennemsyn af dine logs til en fast rutine. Dine logs er det værktøj du skal bruge til at opdage at der er noget i gang. Hvis du ikke opdager det her, vil du først blive opmærksom på et angreb når skaden er sket, og der er det ofte forsendt.

Du kan selvfølgelig altid stille spørgsmål her på eksperten, og du er velkommen til at kontakte mig på kim@bufferzone.dk med spørgsmål, kommentarer, rettelser (stavefejl og andet). Jeg beder om at du ikke stiller spørgsmål i artiklens kommentare, derkan jeg jo ikke besvare dem

Kommentar af perj d. 03. Feb 2004 | 1

God konstruktiv beskrivelse.

Kommentar af tbendiksen d. 30. Mar 2005 | 2

Kommentar af portnoy d. 28. Jun 2004 | 3

God og let at forstå.

Kommentar af mulvad d. 09. Apr 2004 | 4

Udemærket rådgivning .. men som andre siger gerne lidt flere detaljer.

Kommentar af korup d. 28. Jun 2004 | 5

Kommentar af x-masman d. 03. Feb 2004 | 6

God generel beskrivelse af hvordan man opretter et sikkert WLAN. For at komme med en lille smule kritik, kunne jeg godt tænke mig lidt mere dybdegående information - specielt for nybegyndere. F.eks. mere information om SSID, forskellen på WEP og WPA, måske mere information om DMZ, hvad man skal kigge efter i loggen. Ellers godt

Kommentar af cone63 d. 15. Mar 2004 | 7

enig med x-masman, savner mere uddybning til os begyndere ;)

Kommentar af lomse d. 27. Jan 2004 | 8

Kommentar af gano707 d. 27. May 2004 | 9

Kommentar af trumf d. 20. Sep 2005 | 10

Hvad med RADIUS.
Jeg savner lidt info om de forskellige krypteringsmetoder, samt forskellen mellem personal og enterprice... ellers fin grundlæggende artikel.

Kommentar af knudvaldemar d. 30. Mar 2004 | 11

Kommentar af ravsted_dk d. 26. Jan 2004 | 12

Kommentar af kenp d. 27. Jan 2004 | 13

rigtig god vejledning i hvad man har af muligheder for at sikre sit trådløse net, så man kan se hvilke

muligheder man har udover det som normalt er indbygget også.

Kommentar af covst d. 01. Nov 2004 | 14

Kommentar af kalsmose d. 10. Aug 2004 | 15

Kommentar af aniels21 d. 15. Feb 2004 | 16

Kommentar af michaelc d. 13. Apr 2004 | 17

God intro

Kommentar af baxos d. 02. Feb 2004 | 18

Kommentar af xited d. 08. Nov 2004 | 19

Perfekt gennemgang af de forskellige huller i sikkerheden, takker for hjælpen...

Kommentar af redhat9user d. 05. Nov 2004 | 20

Takker. For en ellers erfaren netværksbruger er det en fremragende primer til trådløse netværk.

Kommentar af ttj d. 26. Aug 2004 | 21

Kommentar af pocket d. 10. Jun 2004 | 22

Kommentar af suxor d. 04. Apr 2004 | 23

Rimelig artikel, men går ikke nok i dybden om HVORDAN man så slår de forskellige ting til, og hvad de i grunder gør ved ens netværk...

Kommentar af b_ball d. 14. Feb 2005 | 24

Kommentar af minus d. 17. Nov 2004 | 25

lækkert artikel :)

Kommentar af hifi-flemming d. 18. Feb 2004 | 26

Kommentar af jetdirect (nedlagt brugerprofil) d. 27. Jun 2004 | 27

Kommentar af mightynqb d. 18. Jul 2004 | 28

Kommentar af jenni d. 10. Nov 2004 | 29

Kommentar af 123freddy d. 29. Jan 2005 | 30

OK.

Kommentar af carstennielsen d. 01. Mar 2005 | 31

Kommentar af hrlaust d. 17. Jun 2005 | 32

Kommentar af planbanan d. 20. Mar 2006 | 33

Kommentar af dkmgg d. 11. Mar 2006 | 34

Kommentar af mejeristen d. 09. Nov 2006 | 35