

Hvordan få et sikkert trådløst nettverk - åtte enkle grep.

Alle snakker om det, men få vet hva som trengs. Åtte enkle forhåndsregler er alt som skal til. For de aller fleste potensielle kunder, finnes alle nødvendige elementer tilgjengelig i produktet som selges, mens for de kunder med spesielle behov, kan sikkerheten ivaretaes via tredjeparts sikkerhetssystemer. Sagt på en annen måte, er det nå ikke lenger noen grunn til å la sikkerheten være årsaken til å IKKE velge et trådløst nettverk i dag.

Flere kunder har holdt tilbake investeringer i trådløse nettverk nettopp pga sikkerhets hensyn. De er meget klar over at et dårlig konfigurert WLAN kan åpne deres nettverk for angrep. Og for å understreke akkurat dette punktet har tidligere undersøkelser vist at så mye som 80 % av alle sikkerhetsangrep kommet som følge av dårlig konfigurerte nettverk, og ikke dårlig sikkerhetsutstyr. Hvis vi sammen kan demonstrere at trådløse nettverk kan være sikre, er det langt enklere å videre demonstrere de klare fordeler som et trådløst nettverk kan tilby.

Gjennom åtte enkle grep kan du enkelt sikre dine kunders trådløse nettverk:

1. Gjør en "site survey" av bedriften - hvordan bør det trådløse nettverket designes
2. Foreta en vurdering av tilgjengelighet og sikkerhet i forhold til din kundes trådløse nettverk.
3. Skru av SSID Broadcast
4. Påse at Standard Passord endres
5. Skru på WEP kryptering
6. Skru på WPA kryptering
7. Bruk filtrering av tilgang på MAC adresse nivå
8. Vurder å benytte trådløs VPN

La meg kort ta for meg hvert enkelt punkt.

Gjør en "site survey" av bedriften - hvordan bør det trådløse nettverket designes

Det enkleste form for site survey som verktøy er ofte å finne i den trådløse klienten som installeres på PC-en. I tillegg finnes det diverse verktøyer på markedet som kan hjelpe til å foreta en site survey for enkelt å plassere de trådløse aksess punktene slik at man får optimal dekning og sikkerhet av kontoret eller bedriften. Network Stumbler og Wildpackets er to selskaper som leverer verktøy for denne jobben. En site survey vil kunne lokalisere eventuelle sikkerhetshull; usikrede aksess punkter. I tillegg vil en site survey være et verdifullt verktøy for å evaluere løpende det trådløse nettverket. Dette kan gjøres basert på MAC adresser, krypteringsnivå, SSID navn, hvilke kanaler som brukes, og styrken på signalet.

Foreta en vurdering av tilgjengelighet og sikkerhet i forhold til din kundes trådløse nettverk

Det er viktig å vurdere hvor mye av bedriften som skal ha tilgang til det trådløse nettverket opp mot sikkerhetsnivået. Derfor må man først bestemme seg for hva det trådløse nettverket skal brukes til. Hvor skal det trådløse nettverket være, og hvilken signalstyrke skal man ha. Som et eksempel vil man redusere signalstyrken på det trådløse signalet om det kun er meningen at man skal kunne tilkobles det trådløse nettverket i et møterom. For bedrifter som har kontor i samme bygning som flere andre bedrifter er dette en effektiv måte å hindre at uvedkommende kobler seg inn på nettverket, ikke nødvendigvis for å gjøre noe galt, men kanskje for å "låne" litt gratis båndbredde. Gratis applikasjonen Boingo har blitt veldig utbredt i den senere tid som en enkel applikasjon for å finne andre trådløse nettverk innenfor rekkevidde. Kombinert med signalstyrke kan man også begrense utenforstående å komme seg inn ved å definere båndbredde på et minimumsnivå. Kun når man er innenfor rekkevidde på for eksempel 11 Mbps vil man være tilkoblet.

Skrum av SSID Broadcast

Det første en potensiell hacker ser etter er SSID-en (Service Set Identifier). Selve navnet på det trådløse nettverket. Hvert aksess punkt sender ut sin SSID slik at klienter kan lokalisere det trådløse nettverket og assosieres med det nærmeste aksess punktet. Et av de enkleste metoder for å sikre det trådløse nettverket er å slå av denne funksjonen. Så lenge de klienter som skal bruke seg av det trådløse nettet vet SSID-en, og bedriften ikke skal tilby aksess til andre, er det ingenting i veien for å slå av dette.

Påse at Standard Passord endres

De fleste leverandører leverer sine trådløse aksess enheter med prekonfigurert passord. For potensielle hackere er disse passord og standard påloggingsrutiner kjent. Så uansett hva det trådløse nettet skal brukes til bør man umiddelbart endre passordet. I tillegg kommer mange trådløse routere med DHCP (Dynamic Host Configuration Protocol) server funksjonalitet, som automatisk tildeler IP adresser og annen informasjon ut til klienter. Ved å slå av denne funksjonaliteten kan man også redusere antall uønskede klienter som forsøker å koble seg opp på det trådløse nettet. Men, det er viktig å huske på at når DHCP først er slått av, må alle klienter tildeles denne informasjonen manuelt, på lik linje som ved å slå av broadcasting av SSID-en.

Skrum på WEP kryptering

Når det kommer til kryptering, er mer kryptering alltid bedre, og noe kryptering bedre enn ingen. De fleste aksess punkter støtter i dag WEP (Dynamic Host Configuration Protocol) kryptering. Selv om WEP krypteringen er forholdsvis enkel og begrenset kan det fortsatt være en god metode for å sikre det trådløse nettet på. Ved bruk av WEP oppnår man to klare fordeler. Først og fremst "ødelegger" det for de fleste "vanlige" hackere, og for det andre annonserer det ut at det trådløse nettverket er et privat, lukket nettverk, og ikke en åpen trådløs sone. WEP bruker en delt nøkkel på enten 64- eller 128-bit kryptering. Den delte nøkkelen er en statisk enhet som sådan og vil være lik for alle klienter på det trådløse nettet. Det er nettopp dette som er svakheten i denne form for sikkerhet. De "flinke" hackerne kan på denne måten samle opp tilstrekkelig med pakke trafikk for å dekode nøkkelen og dermed få tilgang. Dette inntreffer, men sjeldent heldigvis fordi det krever mye jobb og innsats fra en hacker for å få dekodert nøkkelen. Men om man frykter dette kan en løsning være å endre nøkkelen manuelt av og til, alternativt kjøre en dynamisk endring av WEP nøkkelen - WPA som er forklart under.

Skrum på WPA kryptering

Etter at man ble kjent med svakhetene bak WEP, ble det tidlig i 2003 godkjent en ny standard av IEEE, kalt WPA (WiFi Protected Access) for dynamisk endring av WEP nøkler i et trådløst nettverk. Et WPA trådløst nettverk bruker seg av temporære nøkler, som sikrer at de delte nøklene automatisk endres. Hvor ofte kan brukerne selv endre. Dette gjør det mye vanskeligere for hackere å bryte seg inn på det trådløse nettet da en nøkkel de har klart å dekode ikke nødvendigvis er den nøkkelen som brukes lenger.

I tillegg til WPA kan man også øke sikkerheten ytterligere ved å kombinere WPA med autentisering. Et WPA basert nett kan ta bruk av en RADIUS (Remote Authentication Dial-In User Service) server slik at hver bruker først må autentiseres før han/hun får tilgang til nettverket. Dette gjøres via pålogging ved brukernavn og passord, som sjekkes opp mot RADIUS serveren.

Bruk filtrering av tilgang på MAC adresse nivå

MAC adresse filtrering (det trådløse klientkortets hardware identifikator) kan brukes for økt sikkerhet. Ved bruk av MAC adresse filtrering vil kun autoriserte MAC adresser få tilgang til aksess punktet. De godkjente MAC adressene lagres i en egen tabell i aksess punktet. Svakheterne er derimot flere. For det første kan dette være en tung prosess for større bedrifter da samtlige MAC adresser manuelt må legges inn. For det andre må noen manuelt vedlikeholde disse MAC adresse listene. Og for det tredje vil MAC adresse filtrering alene være en risiko da man kan risikere at uvedkommende kan få tilgang til klient kortet for dermed å ha full tilgang til det trådløse nettet. MAC adresse filtrering passer først og fremst for mindre bedrifter, og bør uansett benyttes i kombinasjon med andre sikkerhets metoder.

Vurder å benytte trådløs VPN

Enkelte kunder vil kreve at nettet skal sikres maksimalt, uansett. Og selv om dette vil koste, er det ikke sikkert at regningen nødvendigvis må skremme for mye. Flere selskaper, inkludert D-Link har utviklet sikkerhets produkter som benytter avanserte kryptering og autentiserings teknikker for å optimalisere sikkerheten i trådløse nettverk. Disse enhetene fungerer som Virtuelle Private Nettverks servere som innstilt for trådløs kommunikasjon.