Ubudne gæster slippes ind i firmaets net af medarbejderne

Af Kent Krøyer
kk@ing.dk

Selv om man bruger navnløse access points, MAC-filtrering og kryptering, er det vanskeligt at vide, om der har været ubudne gæster i firmaet gennem det trådløse netværk.

Selv et firma med en solid, gennemført sikkerhedspolitik kan ikke være helt sikker. For en dag kommer en uvidende ansat til at forbinde et billigt, ubeskyttet access point (AP) fra detailhandelen med firmaets netstik – inde bag firewall'en. Og så er firmaets sikkerhedspolitik lagt i grus. Måske endda i årevis, uden at nogen opdager det. For det nye access point tilbyder automatisk IP-numre til enhver wardriver, der kommer forbi på gaden, uden at sætte spor i det interne netværk.

Faren gik rigtigt op for firmaet Airwave i Californien i 2000, som oprindeligt byggede hotspots, og siden da har firmaet koncentreret sig om at bygge systemer, der kan styre og sikre trådløse netværk. Både helt små og de helt store med hundredvis af AP'er.

Som eksemplet viser, handler det ikke kun om at sikre mod kriminelle wardrivere, der kommer forbi, men i endnu højere grad om, at der ikke ved tilfældigheder opstår huller i sikkerheden på grund af firmaets ansatte. Konsulentfirmaet Gartner Group forventer, at inden for det kommende år vil 70 procent af alle sikkerhedsbrud stamme fra fejlindstillede AP'er.

Airwaves produkt, et stykke management software med navnet Rapid (Roque Access Point Identification), kan fungere i netværk med mange forskellige fabrikater af AP'er, blot de er i den professionelle klasse, som kan skanne efter fremmede AP'er sideløbende med den almindelig funktion. Softwaren kan endda bruges i et netværk helt uden AP'er.

Rapid giver alarm hos firmaets it-chef, hvis der pludselig dukker et ukendt AP op i netværket eller blot i firmaets nabolag. Det skal sikre, dels mod et såkaldt "evil twin attack", hvor et fremmed AP giver sig ud for at være et lokalt firma-AP. Og det skal også sikre mod ansattes fumleri, som kan medføre, at et AP vender tilbage til sin ubeskyttede fabriksindstilling. For eksempel under en fejlsøgning.

Alarmen indeholder besked om AP'ets fabrikat, indstillinger og MAC-nummer, og den fortæller, hvilken switch det er koblet til, så it-afdelingen kan finde det og neutralisere det. Hvis AP'et ikke er direkte forbundet til netværket, fortæller alarmen, hvilke lokale AP'er, der har detekteret det fremmede. På den måde kan man spore sig frem til det.

»Hvis det nu bare er en venlig nabo, der har fået sig et trådløst acces point?«

»Så kan det registreres som venligt, og it-chefen kan vælge frekvenser, der er ugeneret af naboen,« siger *Jan Buis*, der er chef for den europæiske markedsføring.

»Og hvis naboen senere skifter frekvens eller kryptering?«

»Så udløser det en alarm, så it-afdelingen er sikker på at bemærke det,« siger han.

Rapid forhandles i Danmark af firmaet Airwire i Virum. □

Se artiklen på nettet
ing.dk/0507ab
Med link til blandt andet:
- White papers fra Airwaves