Det trådløse netværk: Et forretningsaktiv, der skal sikres med jernnæve og tilgås med varsomhed

by Mette Nielsen - torsdag, maj 12, 2016

http://perspektiv.tdc.dk/det-traadloese-netvaerk-et-forretningsaktiv-der-skal-sikres-med-jernnaeve-og-tilgaas-med-varsomhed/

Det trådløse netværk: Et forretningsaktiv, der skal sikres med jernnæve og tilgås med varsomhed

Den gode nyhed er, at det trådløse netværk er blevet en hjørnesten i mange virksomheders infrastruktur. Den dårlige nyhed er, at det gør det til et interessant mål for hackere.

Hvis man tager et kig ind i en tilfældig dansk virksomhed, vil mange af de ansatte arbejde på en bærbar computer. Og mange af disse bærbare computere vil – hvis ikke de er placeret i en dockingstation – koble sig på virksomhedens netværk via et trådløst netværk.

Det trådløse netværk er med andre ord blevet mange virksomheders primære, interne kommunikationslinje. Det gør det til et vigtigt forretningsaktiv. Men det gør det også til et oplagt mål for hackere.

Skævvridning mellem muligheder og sikkerhed

Dion Jensen er sikkerhedsekspert i TDC Sikkerhed. Han betragter det trådløse netværk som en del af en større mobilitetsbølge, der lige nu skyller ind over hele verden.

“Virksomheder og medarbejdere arbejder mere og mere mobilt – fra deres bærbare computere, fra deres smartphones og fra deres tablets. Den øgede mobilitet har vist sig at være en stor gevinst, fordi det har øget virksomhedens produktivitet og den enkeltes fleksibilitet,” siger han.

“Men mobiliteten kan kun øges, hvis man samtidig giver brugerne adgang til mere og mere forretningskritisk data fra deres mobile enheder. De er jo ikke effektive, hvis de ikke kan tilgå den information, de har brug for – når de har brug for den. Her er der sket en skævvridning. For mens der er kommet flere og flere forretningsapplikationer, er udbredelsen af sikkerhedsløsninger ikke fulgt med. Groft sagt har mange virksomheder haft travlt med at åbne op for den mobile adgang til kerneforretningen, men i skyndingen har de glemt at sikre adgangen.”

Sikkerhedsopgaven er den samme

Risikoen ved ikke at have styr på den mobile sikkerhed er, at hackere eksempelvis kan sidde i en bil på parkeringspladsen foran virksomheden og stille et falsk trådløst netværk til rådighed for de ansatte. Det

falske netværk ligner til forveksling det rigtige virksomhedsnetværk. Men når de intetanende medarbejdere logger på netværket, kan hackerne se alle de data, der bliver udvekslet: et såkaldt *man in the middle*-angreb.

Samme logik går igen på mobilnetværket. Hvis en medarbejder logger på et kompromitteret trådløst netværk i eksempelvis lufthavnen eller på hotelværelset, er der fri adgang til virksomhedsdata for de kriminelle.

“Som sådan er der ikke noget nyt ved at sikre et trådløst netværk i dag sammenlignet med tidligere. Forskellen på dengang og nu er, at vi bruger det trådløse netværk til at tilgå og udveksle meget mere forretningskritisk information. Jeg tror ikke, at alvoren af det faktum er gået op for folk endnu og derfor halter beredskabet,” siger Dion Jensen.

Flere brugere på trådløse netværk

Han forklarer, at worst case scenario på et trådløst netværk eksempelvis er et DDoS-angreb, der lægger det trådløse netværk ned, så medarbejderne ikke kan tilgå det eller eksempelvis benytte deres Lync-telefoni til at ringe og fejlmelde det. Det kan også være et hackerangreb, hvor de kriminelle opsnapper vigtige data i luften, uden at virksomheden opdager det.

> “Hvis udgangspunktet er, at de kriminelle befinder sig der, hvor brugerne er, så skal vi begynde at sikre os bedre mod angreb foretaget imod brugeren via trådløse netværk. For brugen af trådløse netværk er i vækst og vil fortsætte med at være det,” siger Dion Jensen.

Pas på burgerrestauranten

Han opfordrer virksomheder til at kigge nærmere på de mobile sikkerhedsløsninger, der allerede findes på markedet. Det kan eksempelvis være løsninger til mobiltelefonen, der detekterer, at et *man in the middle*-angreb er i gang, og som derfor blokerer for adgangen til det kompromitterede trådløse netværk. Flere mobile device management-løsninger (MDM) kan i dag også pakke vigtige forretnings-apps ind i en kryptering, så informationen fra enheden og virksomheden ikke så let kan opfanges.

“Udover de konkrete sikkerhedsløsninger er der også et mentalt forandringsarbejde, der skal gøres. Virksomheder og ikke mindst deres ansatte er nødt til at forstå, at man ikke kan sidde på en burgerrestaurant, hoppe på et gratis WiFi og begynde at læse virksomhedsmails eller benytte andre forretnings-apps. Det går ikke,” siger Dion Jensen.

Adgangen til data er central

Han forklarer, at det heller ikke er nok, at de data, der ligger lokalt på medarbejderens telefon, er krypteret. Såkaldt *shoulder surfing* er eksempelvis meget udbredt. Tænk bare på, hvor mange der har fået afluret deres pinkode til telefonen af deres egne nysgerrige børn. Det kan også let ske i det offentlige rum. Her er det bare ikke børn, men professionelle kriminelle, der aflurer koden og får adgang til følsomme oplysninger.

“I dag er det mindst ligeså vigtigt at fokusere på, hvad en telefon har *adgang* til. Næsten alle data tilgås i skyen, over mobilnetværket eller over det trådløse netværk. Derfor skal medarbejderne have en løsning, der etablerer en krypteret forbindelse mellem deres mobile enheder og virksomhedens netværk,” slutter Dion Jensen.