

Trådløse computere, netværk og mobiltelefoner er blot få eksempler på kommunikation der foregår trådløs. Denne kommunikation udgør ofte en væsentlig sikkerhedsrisiko. De trådløse enheder anvender normalt traditionel radioteknologi – dvs. de udsender og modtager radiosignaler, også uden for virksomhedens fysiske perimenter. Samtidig er der tale om relative nye netværksteknologier, hvorfor sikkerhedsbrister oftest ses både i selve protokollerne samt i den enkelte virksomheds konkrete implementering af dem.



Test af trådløs sikkerhed tilbydes overordnet inden for to områder: Systemer der kommunikerer over kort distance (WPAN – Wireless Personal Area Network) og over længere distance (WLAN – Wireless Local Area Network).

Inden for **WLAN** er 802.11 den mest udbredte standard. Med det rigtige udstyr vil disse netværk typisk kunne tilgås langt uden for virksomhedens perimenter. Nye undersøgelser fra Danmark indikerer at næsten halvdelen af alle 802.11 netværk fortsat er helt åbne. Dertil kommer at en væsentlig del af de "beskyttede" netværk fortsat anvender WEP – en krypteringsprotokol der oftest relativt let kan brydes. Er 802.11 netværket sårbart kan det betyde at virksomhedens data kan aflyttes af alle der kan opnå kontakt med det. Afhængig af de aflyttede data og virksomhedens netværksarkitektur vil denne sårbarhed evt. yderligere kunne udnyttes til at trænge dybere ind i virksomhedens interne systemer – eller angreb vil kunne rettes mod andre i virksomhedens navn.

Inden for **WPANs** er Bluetooth og IrDA (infrarød) de mest udbredte. IrDA er interessant ud fra et sikkerhedsmæssigt synspunkt, fordi protokollen ingen beskyttelse indeholder – det overlades således til den enkelte applikationsudvikler at implementere den nødvendige sikkerhed. Til gengæld kræver IrDA oftest at de kommunikerende enheder befinder sig maks. en meter fra hinanden så de kan se hinan-

den ("line of sight"). Dette ligger en naturlig begrænsning på hvem der kan angribe den pågældende enhed. Derfor fokuserer Ezentas sikkerhedsspecialister især på Bluetooth. Modsat IrDA anvender Bluetooth traditionel radioteknologi med en officiel maks. afstand på 10 el. 100 meter (afhængig af udstyrets klassificering). Undersøgelser har dog vist at disse enheder kan nås fra væsentlig længere afstande, blot antaget at angriberen har tilsluttet en ekstern antenne til eget udstyr. Bluetooth ses i dag implementeret i bl.a. mobiltelefoner, PDA'er, bærbare, access points, m.m. – alt sammen udstyr som en ondsindet person ofte vil kunne overtage kontrollen med hvis Bluetooth-implementeringen viser sig at være sårbar.

Sikkerhedstests af WLANs og WPANs kan hver tilbydes som separate produkter - eller de kan kombineres i overensstemmelse med kundens behov. Sikkerhedstest af analoge og WMAN-systemer tilbydes ligeledes ved forespørgsel.

Sikkerhedstest af Wireless LANs

Ezentas sikkerhedsspecialister gennemgår sikkerheden i virksomhedens 802.11b/a/g netværk. Konkret forsøger Ezentas sikkerhedsspecialister at krænke datas fortrolighed, integritet og tilgængelighed via bl.a.:

- Forsøg på dekryptering af WEP/WPA/WPA2/ 802.1x/VPN
- Forsøg på omgåelse af øvrige beskyttelsesmekanismer i access points/ad hoc-netværk
- Replay-angreb
- Specielle konsulentdesignede frames
- Man-in-the-middle-angreb
- Grafisk mapning af både åbne og lukkede access points baseret på GPS-koordinater
- Vurdering af signaludbredelse ved anvendelse af special udstyr
- DoS-test

Sikkerhedstest af Wireless PANs

Ezentas sikkerhedsspecialister gennemgår sikkerheden i virksomhedens Bluetooth-enheder. Konkret foretages følgende:

- Enumeration af fabrikant-, model- og firmware-information
- Enumeration af tilgængelige servicer via Bluetooth-enhederne
- Forsøg på at krænke datas fortrolighed og integritet i de fundne enheder
- Evt. forsøg på misbrug af tidligere oprettede pairs
- DoS Test

IrDA-sikkerhedstest kan tilbydes som option.