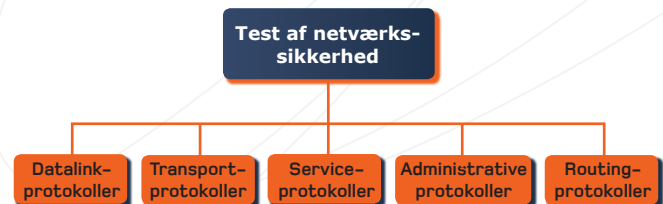


Ezena vurderer at en række eksternt tilgængelige netværk og langt størstedelen af alle interne netværk, indeholder væsentlige sårbarheder. Værktøjer til at udnytte disse sårbarheder kan downloades fra Internettet. Resultatet er som oftest at insiders, og til tider også outsiders, kan overtage kontrollen med hele netværkssegmenter. Indeværende ydelse er således en sikkerhedstest af selve netværket.



**K**orrekt implementeret netværkssikkerhed er vigtigt for at sikre at følsomme systemer og services ikke gøres tilgængelige over offentlige netværk. Ligeledes sikrer netværkssikkerhed imod aflytninger, imod ændringer af data under transporten, samt imod angreb der forsøger at gøre netværket utilgængeligt. Indeværende ydelse er en test der sikrer kunden at dette forsvar fungerer efter hensigten.

I en verden hvor mindst 70 % af alle tab som følge af sikkerhedshændelser skyldes insiders, er sikkerheden på virksomhedens intranet ligeledes essentiel. Mens virksomhedens servere og klienter ofte er godt beskyttet, vurderer Ezena at selve det interne netværk, som disse systemer anvender, næsten altid indeholder væsentlige sårbarheder. Disse sårbarheder gør det muligt for en insider at overtage kontrollen med hele netværkssegmenter via værktøjer, frit tilgængelige på Internettet. Malware eller eksterne angribere, der har hacket adgang til et givent netværkssegment, vil ligeledes kunne udnytte disse teknikker til at krænke datas fortrolighed, integritet og tilgængelighed på virksomhedens intranet eller segmenter heraf.

Når Ezena foretager en test af virksomhedens netværkssikkerhed, fokuseres der ikke på de enkelte systemer på netværket, men derimod på sikkerheden i selve de netværksprotokoller som de fleste af disse systemer er afhængige af. Testen tilbydes bl.a. på de netværkssegmenter hvorpå virksomhedens medarbejdere befinder sig, på DMZ'er og VLANs, samt fra eksterne netværk som eksempel Internettet.

Konkret forsøger Ezentas sikkerhedsspecialister at krænke

datas fortrolighed, integritet og tilgængelighed på de testede netværkssegmenter via kontrollerede angreb mod følgende protokolgrupper:

### Datalinkprotokoller

Disse protokoller anvendes således at netværksstakken ved hvilket format en datapakke skal have for at kunne transmitteres over en given type netværk (f.eks. Ethernet, Token Ring, ATM el. FDDI). Ezena undersøger sårbarhederne i disse protokoller, herunder muligheden for bl.a. ARP-, RARP- og BOOTP-spoofing. Broadcastpakker undersøges for mulige informationslækager. Anvendes VLANs bliver disse ligeledes testet med henblik på at afdække ofte forekommende konfigurationsfejl og sårbarheder heri.

### Transportprotokoller

Hermed refereres til de protokoller i netværks- og transportlaget, som er "end-to-end", forstået på den måde at de transporterer data hele vejen fra afsenderen til modtageren. Hvor det er muligt, søger Ezentas sikkerhedsspecialister at udnytte de medfødte sikkerhedsmæssige svagheder i TCP-, UDP- og IP-protokollerne. Yderligere undersøges IP-broadcastpakker for mulige informationslækager. Endelig hører sikkerhedstest af firewalls regelsæt ligeledes hovedsagligt under denne protokolgruppe.

### Serviceprotokoller

Serviceprotokoller giver den information som er nødvendig for at transporten af datapakker kan finde sted. Ezena foretager en sikkerhedstest af netværket mhp. at identificere usikre serviceprotokoller. Navneoversættelse (DNS) og dynamisk netværkskonfiguration (DHCP) søges manipuleret med henblik på udførelse af bl.a. man-in-the-middle-angreb. Potentielle informationslækager i serviceprotokollerne afdækkes. Medfødte sårbarheder i ICMP udnyttes hvor det er muligt.

### Administrative protokoller

Administrative protokoller anvendes til at administrere netværksenheder som f.eks. switches, routers og firewalls. Ezena foretager en sikkerhedstest af netværket mhp. at identificere usikre administrationsprotokoller. Eksempler herpå er telnet og TFTP, men også protokoller der anvender svag kryptering. Yderligere kontrolleres SNMP for konfigurationsfejl og sårbarheder.

### Routingprotokoller

Routingprotokoller anvendes til at fastsætte hvilken rute data pakker skal tage. Ezentas sikkerhedsspecialister søger at identificere de anvendte routingprotokoller mhp. at lokalisere konfigurationsfejl eller sårbarheder i disse. RIP og OSPF er eksempler på routingprotokoller, der ofte er sårbare.

### Option: wardialing

Modemmer anses af mange som værende fortidens levn. Netop derfor overses de ofte, og kan til tider udgøre netværkets svageste led. Ezena erfarer således at mange, specielt ældre og større organisationer, ofte har en række modemmer som de ikke har kendskab til, og som er tilgængelige over det offentlige telefonnet. Typiske eksempler inkluderer bl.a. indgange til organisationens mainframe og PBX (system til fjernstyring af organisationens telefonsystem).

Ved udførelse af en wardialing opnår organisationen et overblik over hvilke systemer der kan opnås kontakt til over det offentlige telefonnet. Konkret foregår dette ved at alle organisationens telefonnumre ringes op via specialudstyr, som samtidig registrerer på hvilke telefonnumre modemmerne svarer. Opkaldene foretages typisk uden for normal arbejdstid således at sikkerhedstesten medfører mindst mulig gene.

Efterfølgende penetration testing af de identificerede systemer kan foretages efter aftale med kunden.