

# Säkerhetsanalys



Produkter > Säkerhet > Tjänster

Många gånger är det stora skillnader mellan önskad säkerhetsnivå och vad som de-fakto är implementerat. En säkerhetsanalys lyfter fram sådana avvikelser och ger konkreta åtgärdsförslag.

IPnett erbjuder en produktberoende genomgång av de befintliga säkerhetsfunktionerna i nätverket. Baserat på en nulägesanalys, befintliga policydokument samt IPnetts egna erfarenheter inom informationssäkerhet presenteras en överblick av de säkerhetsaspekter och beslut som kunden står inför. Följande är exempel på frågor som tas upp i säkerhetsanalysen:

#### Brandväggspolicy

Hur är regelverket i din brandvägg implementerat? Behövs externa konsulter för att administrera och upprätthålla brandväggens regelverk? Har de ingående kunskap om din säkerhetspolicy, önskemål och behov? Bör brandväggsjobben kvalitetssäkras?

#### VPN och säker fjärranslutning

Användare jobbar i högre utsträckning hemifrån, företags mobiltelefoner används för såväl mail som fjärruppkoppling till kontoret, lokalkontor och partners ansluts med VPN. Hur bör dessa anslutningar säkras upp?

#### Spårbarhet

Hur autentiseras administratörer av säkerhetsfunktionerna i nätverket? Används säker inloggning? Vilka användare loggar in var, när och hur? Hur hanteras loggar från säkerhetsfunktioner?

#### Driftdokumentation

Finns rutiner för administration, dokumentation och backup av säkerhetsfunktionerna i nätverket?

#### IPv6

Är säkerhetsfunktionerna i nätverket klara för IPv6? Hur kan en övergång till IPv6 göras på t.ex. brandväggen? IPnett hjälper dig att planera för övergången till IPv6.

#### Fakta om tjänsten

- Nulägesanalys av implementerade säkerhetsfunktioner
- Genomgång av gällande säkerhetspolicy
- Genomgång av slutsatser och resultat, cirka en halv dag
- Rekommenderade förbättringsförslag baserade på IPnetts "best practices"
- Underlag för vidareutveckling av säkerhetspolicy
- Dokumentation i rapportformat