

NetDesign IPT sikkerhedsworkshop *Valg af IPT sikkerhedsfeatures og udarbejdelse af implementeringsplan*

Jesper Munk
System Engineer

Virksomhedens fordele ved NetDesign IPT sikkerhedsworkshop

Med NetDesign's IPT sikkerhedsworkshop kan virksomheden til en fast, begrænset pris (normalt 12 konsulenttimer*) komme godt i gang med vurdering og forbedring af IPT sikkerheden:

- Få overblik over IPT og relevante data sikkerhedsfeatures med vægt på operationelle aspekter (systemadministrationsmæssige omkostninger).
- Et kvalificeret bud på valg af IPT og data sikkerhedsfeatures.
- Overordnet implementeringsplan.

* Med forbehold for arten og kompleksiteten af virksomhedens netværk, herunder for netværk med over 300 IPT brugere.

Indhold

IPT sikkerhed er en business enabler	2
Hvor er det NetDesign's IPT sikkerhedsworkshop kan bidrage?	4
NetDesign IPT sikkerhedsworkshop	5

IPT sikkerhed er en business enabler

Forudsætningen for, at virksomheden kan udnytte de mange nyttige features i IPT og generelt Unified Communications er, at sikkerheden er i orden.

Dermed bliver IPT sikkerhed reelt forudsætningen for, at virksomheden

- kan forbedre sin produktivitet v.hj.a. IPT.
- kan udvikle nye måder at drive forretning baseret på IPT.
- Eksempler:
 - IPT over det åbne Internet i IPSec VPN til mindre afdelingskontorer og hjemmearbejdspladser (også kaldet Small Office Home Office (SOHO)).
 - IPT over det åbne Internet til en medarbejder pc med VPN klient, der fx er opkoblet på et udenlandsk hotel.
 - Integration af data applikationer og IPT:
 - CTI løsninger: fx kalenderintegration.
 - Call Center løsninger, der gør brug af data applikationer.

På samme måde er IPT og Unified Communications sikkerhed reelt forudsætningen for, at virksomheden kan udnytte avancerede IPT og Unified Communications løsninger:

- Wireless IPT
- IPT mobility, herunder kombinerede IPT og GSM telefoner, fx Nokia GSM telefoner med Cisco Skinny klient.
- Unified messaging, d.v.s. integration af voice mail og e-mail.
- Presence tjeneste, d.v.s. automatisk lokalisering af en medarbejder og opkobling til ham med den bedste af de kommunikationsmuligheder (video, voice, Web conference, e-mail), han netop nu råder over og er villig til at bruge.
- Collaborative applikationer
 - avancerede multimedia konference tjenester
 - integration med mail og kalender systemer, fx Outlook
 - baseret på Presence tjeneste

Konklusionen er, at for virksomheden er dette *offensive* perspektiv for IPT og Unified Communications sikkerhed, at den reelt gør det muligt at udnytte IPT og Unified Communications muligheder for produktivetsforbedringer og skabelse af nye måder at drive forretning på, langt vigtigere end det *defensive* perspektiv, nemlig at sikkerheden også er det, der forhindrer indbrud i virksomhedens IPT og Unified Communications systemer.

Virksomhedens proces med forbedring af IPT sikkerhed

Virksomheden bør som minimum vurdere sin IPT sikkerhed og fastlægge behovet for forbedringer. Forbedringsbehovene skal prioriteres ud fra forretningens behov, og virksomheden bør udarbejde en trinvis implementeringsplan for forbedringerne.

I nogle tilfælde kan behovet for forbedringer være begrænset.

Processen består af følgende trin

1. Udpeg de forretningsmæssige værdier skal beskyttes, og prioriter disse.
 - Eksempler: omdømme; kommunikation med kunder v.hj.a. IPT; fortrolighed for telefonsamtaler; kunde- og produkt-informationer; hvor højt sikkerhedsniveau er nødvendigt?
 - Prioriter ud fra forretningens behov
 - Ledelsen skal tage ansvar for prioriteringen
 - Pas på ikke at "skjule" prioriteringerne i teknik.
2. Udpeg de reelle trusler mod de forretningsmæssige værdier, d.v.s. udpeg mulige angreb og sandsynligheden for, at de lykkes. Sammenhold dette med den forretningsmæssige betydning af de systemer, der angribes. Resultatet er en liste over trusler, der skal beskyttes imod, prioriteret ud fra forretningens behov. Ovenstående kaldes også en *sikkerhedsanalyse*.
3. Implementer beskyttelse på grundlag af den prioriterede liste over trusler:
 - Vælg og implementer tekniske IPT og data sikkerhedsfeatures.
 - Vælg og implementer passende organisatoriske procedurer.
4. Vurder og mål effektiviteten af beskyttelsen
5. Gå jævnlige hele processen igennem igen, fx hver 12-24 måneder.

Bemærk, at sikkerhedsanalysen, trinene 1 og 2, ofte er det mest krævende for virksomheden, fordi den her skal klargøre sin forretningsmæssige prioritering, og ledelsen og organisationen skal tage ansvar for overholdelse af prioriteringen.

Når først den forretningsmæssige prioritering er på plads, er det relativt ligetil, om end forbundet med omkostninger, at udvælge og implementere de relevante tekniske features. Den forretningsmæssige prioritering i sikkerhedsanalysen afgør alle de tekniske og budgetmæssige valg, der altid skal træffes.

Det optimale er en systematisk og veldokumenteret sikkerhedsanalyse.

Offentlige virksomheder skal have en IPT sikkerhedspolitik (krav om overholdelse af DS484), hvilket forudsætter en sikkerhedsanalyse.

Gode råd:

- Der er mange, komplekse IPT og data sikkerhedsfeatures
- "Letvægtsudgaven" af features giver oftest 75% af sikkerhedsgevinsten for 25% af indsatsen
- Mange features findes allerede i udstyret. De skal blot enables
- *Derfor*
 - Skab overblik over behovet for data og IPT sikkerhedsfeatures
 - Lad forretningen prioritere
 - Vælg letvægtsudgaven af features
 - Brug de features, der allerede er der
 - Udarbejd en trinvis implementeringsplan over 2-3 år

Hvor er det NetDesign's IPT sikkerhedsworkshop kan bidrage?

NetDesign's IPT sikkerhedsworkshop kan bidrage *efter, at virksomheden har udført sin sikkerhedsanalyse, til valg og implementering af IPT sikkerhedsfeatures* gennem følgende:

- Give et overblik over eksisterende IPT sikkerhedsfeatures med fokus på operationelle forhold, herunder især systemadministrationsmæssige omkostninger ved at implementere og vedligeholde de enkelte features.
- Give støtte til fastlæggelse af et første bud på valg af IPT sikkerhedsfeatures i overensstemmelse med virksomhedens IPT sikkerhedspolitik, overordnet design for disse og første bud på overordnet implementeringsplan for disse.

På grundlag af IPT sikkerhedsworkshopens resultater kan virksomheden foranledige udarbejdelse af endeligt valg af IPT sikkerhedsfeatures, detaljeret design og implementeringsplan for disse, samt den egentlige implementering af disse.

NetDesign IPT sikkerhedsworkshop

NetDesign kan tilbyde følgende *IPT sikkerhedsworkshop* til støtte for virksomhedens valg og implementering af IPT sikkerhedsfeatures:

IPT sikkerhedsfeature gennemgang (ca. 4 timers varighed):

- gennemgang af eksisterende IPT sikkerhedsfeatures med fokus på operationelle aspekter. For hver feature gennemgås funktion, fordele, ulemper og systemadministrationsmæssige omkostninger ved implementering og vedligeholdelse. For at skabe overblik og for at anbefale en generel rækkefølge for implementering, inddeles features i 3 niveauer efter grad af integration i eksisterende komponenter, kompleksitet, opnået sikkerhedsniveau m.v.
Gennemgangen af IPT sikkerhedsfeatures vil normalt blive fokuseret på de features, der umiddelbart fremtræder som mest relevante for virksomheden ud fra virksomhedens IPT sikkerhedspolitik, og arten af dens data og IPT løsninger. NetDesign vil forudgående tage en dialog (kan være per telefon) med virksomheden om dette, og studere tilgængelig dokumentation for virksomhedens løsninger.
- første drøftelse af, hvilke IPT sikkerhedsfeatures, der er relevante for virksomheden, og udpegning af tekniske og budgetmæssige udfordringer og valg.

NetDesign dokumenterer resultatet af drøftelserne.

Mellemliggende periode:

- Virksomheden gør sig overvejelser om de tekniske og budgetmæssige valg.
- NetDesign undersøger evt. visse tekniske spørgsmål, identificeret på ovenstående møde.

Design møde (ca. 4 timers varighed):

- Drøftelserne om valg af IPT sikkerhedsfeatures videreføres på grundlag af virksomhedens overvejelser og beslutninger, og en dyberegående dialog om disse ting.
- Første bud på valg af IPT sikkerhedsfeatures udarbejdes.
- Første bud på overordnet teknisk design og implementeringsplan for de valgte IPT sikkerhedsfeatures udarbejdes.

NetDesign dokumenterer resultatet af mødets drøftelser.

Konsulenttimeforbruget til workshoppen vil *normalt være ca. 12 timer* med forbehold for kompleksiteten og arten af virksomhedens netværk, herunder for netværk med over 300 IPT brugere.

På grundlag af IPT sikkerhedsworkshoppens resultater kan virksomheden efterfølgende foranledige, at der tages et endeligt valg af IPT sikkerhedsfeatures og udarbejdes detaljeret design og implementeringsplan for disse, og, at den endelige implementering foretages.

Bemærk:

Da IPT er en applikation, der kører ovenpå IP netværket, vil mange IPT sikkerhedsfeatures være data netværk features. Fx beror høj tilgængelighed for IPT tjenesten på et data netværk, der er gjort robust gennem redundans.