

Telependling: Regler og sikkerhet

Hjemmekontor. Telependling. Bredbånd. SOHO. Begrepene og deres praktiske betydning er blitt en del av vårt vokabular – og praktiske liv. Et voksende antall av oss utfører en stadig større del av vårt arbeid uten å befinne oss i arbeidsgiverens lokaler. Vi har fått større fleksibilitet, nye valgmuligheter og i mange tilfeller bedre produktivitet.

SOHO – Small Office, Home Office

I likhet med enhver medalje har imidlertid også denne sin bakside. Ferske undersøkelser blant norske 'hjemmekontorister' viser at å arbeide i ensomhet slett ikke representerer noen ønskesituasjon for mange – i alle fall ikke lenge, selv om omgivelsene er aldri så kjente og kjære. Etter uker eller måneder 'i ensomhet' dukker det opp 'syndromer' – ulike former for plager – som er direkte relaterbare til den nye arbeidssituasjonen.

Noen overraskelse er ikke dette. Sosial kontakt hører med til menneskets mest grunnleggende behov – et faktum som har vært kjent i årtusener. Videre er det erfaringsmessig naturlig at nye former for arbeid og arbeidsmiljø tar tid for å gå seg til: Vi trenger praktisk erfaring med hensyn til hvilke parametre som er kritiske for trivselen i en ny situasjon, og hva som skal til for å få det hele til å fungere.

Erfaring og konsolidering

Likeledes er det et velkjent faktum at mennesker er forskjellige og har ulike behov. Vi er kort og godt inne i en konsolideringsfase der de siste års erfaringer oppsummeres og systematiseres, slik at de kan benyttes som grunnlag for andre generasjons 'hjemmekontorer'. Denne konsolideringen startet allerede for et par år siden i USA, der mellom 30 og 40 millioner mennesker arbeidet borte fra kontoret ved utgangen av 2001.¹ 22% av disse arbeider fra hjemmet, mens 7,5% arbeider fra såkalte *telework*-sentre – kontorfellesskap i lokalmiljøet som er opprettet for nettopp å ta vare på de sosiale problemstillingene. At tilsvarende tilbud nå dukker opp på våre kanter, er med andre ord både naturlig og nødvendig.

Problemen som har dukket opp i forbindelse med hjemmekontor eller hjemmearbeid, er totalt sett beskjedne i forhold til fordelene. Store internasjonale undersøkelser, blant annet i regi av organisasjonen ITAC (*International Telework Association & Council* – www.telecommute.org), viser at de fleste telependlere arbeider mer og er mer tilfreds med både seg selv og jobben enn tidligere. Mens konfliktene mellom privatliv og arbeid til å begynne med oppleves som betydelig hos de

¹ En fersk studie fra amerikanske Cahners InStat/MDR anslår antallet mobile og fjern-brukere til ca. 78 millioner i USA.

flESTE, går det seg til over tid. Den enkelte lærer å utnytte fleksibiliteten konseptet gir til å 'være hjemme' og 'på jobb' på ulike tidspunkter i løpet av dagen, i stedet for å tvinge et gammelt mønster over på en ny situasjon.

Ballen ruller, og det er ingen vei tilbake til tradisjonelle kontor-forhold. Den såkalte X-generasjonen, aldersgruppen fra 28 til 36 år, vektlegger fleksibilitet og personlige mål i større grad enn karrieremessige, og søker arbeidsgivere som kan tilfredsstille disse behovene. Det betyr – blant annet – økt bruk av telependling og fleksibel arbeidstid.

Vi skal la de sosiale sidene av problemstillingene ligge i denne omgang, og konsentrere oss om de tekniske og prosedyremessige utfordringene. Til tross for tilgjengeligheten av all verdens teknologi og erfaringer, står vi også her overfor et betydelig lerret som må blekes. Årsaken er delvis å finne i dårlige eller manglende forberedelser: Hjemmekontorer og fjernarbeid har vokst frem på bakgrunn av muligheter, ikke som en planlagt progresjon eller utvidelse av tilbudet til medarbeidere. Situasjonen er analog med introduksjonen av epost på 90-tallet: Ukontrollert, ustrukturert, tilfeldig og til tider kaotisk.

Videre dukker det opp tekniske, praktiske og sikkerhetsmessige problemstillinger i tilknytning til at medarbeidere skal ha tilgang til de samme verktøy, hjelpemidler og informasjon utenfor som innenfor organisasjonen.

Sikkerhet på hjemmebane

Mens utbredelsen av telependling – sporadisk, regelmessig eller permanent – tiltar med akselererende hastighet, forblir forholdene knyttet til sikkerhet uoversiktlige. En lang rekke produkter rettet mot dette segmentet har kommet på markedet de siste tre årene, og har forenklet situasjonen vesentlig, men mange grunnleggende spørsmål er stadig ubesvart: Hvor god sikkerhet må vi ha, hva skal til for å etablere den, hva er de største truslene, hvor skal grensene mellom privat bruk og jobb gå, og så videre.

Telependling – et spørsmål om båndbredde

Ansikt-til-ansikt-faktoren er den største innvendingen vi møter i tilknytning til telependling: Telefon, chat, epost og on-line diskusjoner er vel og bra, men kan aldri erstatte øye-til-øye kontakten. Heller ikke dette er imidlertid noe teknisk problem: Med tilstrekkelig båndbredde er ikke dette bare mulig, men relativt enkelt – med billig kamerateknologi og lett tilgjengelig programvare.

Den nylig etablerte grupperingen Telework Consortium [www.teleworkconsortium.org] tar mål av seg til å akselerere utbredelsen av telependling ytterligere, gjennom å legge forholdene til rette for virkelige bredbånds-forbindelser. At leverandører av nettopp båndbredde, som AT&T og SPC, står sentralt i initiativet, er naturlig. Første trinn på programmet er å lage demonstrasjoner som viser hvordan dette kan og bør fungere i praksis. Ethernet-forbindelser på 20-30 Mbps vil snu opp-ned på situasjonen, og vil gjøre videokonferanser og -telefoni av høy kvalitet til en selvfølge på linje med telefoni.

"Vi vil i første omgang demonstrere hvilket glimrende kost/nytte-forhold slike løsninger gir" sier en talsmann for organisasjonen, som holder til i Virginia, USA.

Risiko og trusler

En oversikt over tekniske og infrastruktur-relaterte fakta er nødvendig når trusselbildene skal etableres og evalueres:

- ✓ På våre kanter er ISDN-forbindelser fortsatt dominerende, men på vikende front til fordel for (TV-)kabel og xDSL. Når sikkerhetsmessige forhold skal evalueres, er det rimelig å legge permanente forbindelser til grunn, og glemme ISDN.
- ✓ Klientene er overveiende Windows-baserte systemer, i de fleste tilfeller eldre enn Windows 2000.

- ✓ Systemene brukes av flere familiemedlemmer, og gjerne flere generasjoner.
- ✓ Utstyret eies som regel av arbeidsgiveren, og de fleste brukere har flere maskiner i familien, mens et fåtall så langt har laget lokalnett hjemme.
- ✓ Direkte (oppringte) forbindelser til arbeidsstedet er fortsatt vanlige, men på vikende front.
- ✓ Få arbeidsgivere har utviklet en policy som regulerer ansvar, rettigheter, krav, ressurser og andre forhold knyttet til telependling. Likeledes hører det til unntakene at brukere får opplæring før de tar i bruk en hjemmekontor-løsning.
- ✓ En forutsetning for effektiv telependling er at brukeren har tilgang til (omtrent) de samme verktøy og data som om vedkommende hadde vært 'på kontoret'.

Disse forholdene munner ut i følgende åpenbare trusler og risikomomenter:

- ✓ Brukerne oppfatter 'hjemmekontoret' som ekvivalent med det tradisjonelle kontoret, men enda mer privat/beskyttet. De ter seg deretter – i sin omgang med dokumenter, IT-systemer, pålogging og bruk/oppbevaring av passord. I realiteten er hjemmekontoret langt mindre sikkert enn det tradisjonelle kontoret, både teknisk og praktisk.
- ✓ De sikkerhetsmekanismene – inklusive viruskontroll – som måtte finnes på systemene, kommer i veien for 'annen bruk' – spill, nedlastinger etc. og blir ofte satt ut av funksjon.
- ✓ Selv der kommunikasjon mellom hjemmestyret og kontoret er sikret – med for eksempel VPN, er risikoen for infeksjon av virus, trojanske hester og lignende, overhengende fordi hjemmesystemene lett kan brukes som springbrett. Likeledes er det ikke bare mulig, men relativt trivielt å få en slik hjemmemaskin til å fungere som ruter mellom det åpne Internettet og det antatt sikre interne nettverket.
- ✓ Den tilgjengelige båndbredden (farvel til analoge modem og ISDN) åpner for og stimulerer til et annet bruksmønster enn tidligere. Det betyr flere nedlastinger over et større spekter som i sin tur øker risikoen for ubudne gjester i form av virus og lignende.

Listen fortsetter: Litteratur og media er fulle av eksempler på hvor liten avstanden er fra trygghet til regulære katastrofer.² Samtidig ser vi av artikkelen på side 20, at tilsvarende gjelder også den andre veien – fra mangelfull til grunnleggende sikkerhet.

Tilbake til god sikkerhet

God sikkerhet forutsetter fokus på helheten. Å sikre et system eller en avdeling er meningsløst, det er hele virksomheten som alltid må være

² Boken "Hacking Exposed" av Scambray, McClure og Kurtz (McGraw-Hill) er et glimrende eksempel. Den foreligger nå i tredje utgave i tillegg til at det er laget en egen utgave for Windows 2000.

målet i en sikringsprosess. Når brukerne flytter ut – eller hjem, utvides grensene for hva vi regner som virksomhetens interne nettverk, og utfordringene må håndteres deretter. Forutsetning nummer én er med andre ord at tilfredsstillende sikkerhet allerede er på plass internt i virksomheten.

Policy for eksterne brukere

Neste trinn er å få på plass en policy – et sett grunnregler som regulerer bruken av eksterne forbindelser og hjemmekontorer. Eksistensen av en slik policy er nødvendig for å skape ryddige forhold, og ikke minst for å etablere og opprettholde bevissthet rundt problemstillingene.

Den tilpasses til lokale forhold, oppdateres regelmessig – og kan for eksempel inneholde følgende elementer:

- ✓ Hvem kan telependle: Definerer roller og stillinger som kvalifiserer til å jobbe hjemmefra. I noen tilfeller kan det også være naturlig å angi hvor mye (100%, 50%, 10% etc.).
- ✓ Tjenester for telependlere: Nettverkstjenester, applikasjoner og verktøy som er tilgjengelige for eksterne brukere. Her kan det om nødvendig differensieres mellom ulike brukergrupper.
- ✓ Informasjonsrestriksjoner – dersom det finnes klassifiserte informasjonstyper som ikke tillates aksessert utenfra.
- ✓ Autentisering: Hvilke krav som stilles til identifikasjon av eksterne brukere før de får tilgang til nettverk og andre ressurser.
- ✓ Overordnet spesifisering av programvare og utstyr som er godkjent for telependling – for eksempel personlig brannmur, viruskontroll og operativsystem. Detallspefisikasjoner (leverandører, produktnavn og så videre) legges i et tilstøtende dokument.
- ✓ Integritet, transportsikring: Krav til sikring av forbindelsen mellom brukerens utstyr og det interne nettverket (for eksempel VPN og kryptering). Igjen legges tekniske og produktrelaterte detaljer i et tilstøtende dokument.
- ✓ Kontroll og vedlikehold: Hvem har ansvaret for at utstyret opprettholder sitt opprinnelige nivå med hensyn til sikkerhet (herunder installasjon, vedlikehold, oppdateringer/oppgraderinger, ny programvare, og overvåking). Hvordan skal problemer håndteres, hvem kan ta fysisk hånd om utstyret?
- ✓ Brukerens ansvar: En klargjøring av rolle og ansvar i forbindelse med sikkerhet i eksterne omgivelser, herunder hva som kan og ikke kan gjøres av konfigurasjonsendringer, installasjon/fjerning av programvare, eksterne tilkoblinger, og ikke minst hvem som kan bruke utstyret.

En policy skal beskjefte seg med overordnede forhold, ikke med teknologi eller mekanismer. For eksempel kan den angi at alle eksterne forbindelser skal skje via kryptert VPN, men ingen ting om løsning,

produkt, leverandør, hastighet og lignende parametre. På den måten blir policy-dokumentet relativt stabilt, mens tilstøtende dokumenter opptar dynamikken i hverdagen, knyttet til produkter, versjoner, systemer og infrastruktur.

Fallende priser på utstyr og båndbredde har gjort en rekke av problemstillingene vi tar opp ovenfor langt enklere. For eksempel vil det i de fleste tilfeller finnes flere PCer i hjemmet, hvilket reduserer behovet for å la andre enn medarbeideren selv ha tilgang til bedriftens utstyr. Derfor ser vi stadig oftere klare og konsise restriksjoner med hensyn til bruk – for eksempel:

- ✓ Utstyret kan kun benyttes av [brukeren].
- ✓ Programvare skal ikke installeres eller fjernes, tjenester skal ikke aktiveres eller stoppes, og konfigurasjoner skal ikke endres.
- ✓ Virksomhetens data skal aldri lagres lokalt, all databehandling skal skje uten at filer flyttes til eksterne systemer.
- ✓ Etc.

Slike 'stramme tøyler' kan umiddelbart virke overdrevent restriktive, men dagens situasjon med hensyn til trusler og generell kvalitet på programvare, gjør det nødvendig å gå så kraftig til verks for å opprettholde god sikkerhet. Store internasjonale konserner, ikke minst i data-bransjen, har derfor lagt seg på en slik linje – med gode resultater.

Opplæring av brukere

Brukere som forstår sin egen rolle og sitt ansvar er en forutsetning for å etablere sikkerhet som fungerer. Via opplæring får den enkelte innsikt i risikoene, forskjellene mellom 'kontoret' og 'hjemmekontoret', og hvorfor å låne bort utstyret ikke bare er en dårlig ide, men direkte farlig. Videre skal opplæringen inneholde en innføring i hvordan risikoene kan minimaliseres gjennom enkle forholdsregler – for eksempel passord av god kvalitet, skjermbeskyttere, makulering av dokumenter – for ikke å snakke om praktisering av god hygiene i forbindelse med epost.

Beskyttelse av utstyr og kommunikasjon

Selv om vi forlanger at virksomhetens data aldri skal være lokalt lagret, er behovet for å beskytte brukerens utstyr stort. Innbrudd eller innsyn er i mange tilfeller alt som skal til for at en inntrenger kommer seg videre – eller blir i stand til å lamme virksomhetens nettverk. Overgangen fra oppringte samband til permanente forbindelser aksentuerer problemstillingen ytterligere.

En brannmurløsning på hver enkelt maskin er derfor påkrevet³ – fortrinnsvis en som løpende kan kontrolleres og styres sentralt. Produkter som er utelukkende lokale, kan forandres eller stoppes av brukeren uten at forholdet oppdages. Slike forandringer kan like godt

³ Se artikkelen "Skal det være en personlig brannmur?" i Mellvik-Rapporten nr. 75.

være tilfeldige som overlagte – dagens systemer er altfor kompliserte til at alminnelige brukere kan ha oversikt over følgeskadene knyttet til selv enkle endringer. Derfor er bannmurprodukter med sentralisert styring og konfigurasjon en forutsetning for pålitelig sikkerhet.

Tilsvarende betraktninger kan gjøres for virusbeskyttelse: Den må ikke bare finnes, men være under sentral kontroll, slik at vi for det første kan kontrollere at den er i funksjon, og for det andre kan sørge for automatiske rutiner som oppdaterer signaturfiler. Jo færre oppgaver brukeren selv har ansvaret for, desto bedre blir sikkerheten.

Eksistensen av god viruskontroll hos den enkelte bruker er imidlertid ikke tilstrekkelig i seg selv. Som vi har diskutert i tidligere artikler, er viruskontroll kurering av symptomer – som per definisjon alltid henger etter virusutviklerne. Det betyr at sjansen for infeksjon er betydelig større enn null uansett hvilken løsning vi installerer. Å sørge for viruskontroll ved inn- og ut-passering av virksomhetens nettverk, også for VPN-baserte fjernbrukere, er derfor en god regel.

Sikring av utstyret handler ikke bare om teknisk sikkerhet, men også om fysisk sikring og sikkerhetskopiering. Denne siden får sjelden oppmerksomhet – og forenkles vesentlig dersom vår policy ikke tillater lokalt lagrede data. Finnes kritiske data lokalt, er det nødvendig å vurdere verktøy for kryptering av disk-filer, og å ha mer eller mindre automatiske rutiner for sikkerhetskopiering. Med bredbåndsforbindelse til virksomhetens nettverk, kan sistnevnte forhold løses både enkelt og transparent, mens lokal datakryptering fordrer forberedelser og omtanke: Kryptering har i seg selv liten verdi dersom nøkler og passord er lett tilgjengelige. En integrasjon med autentiserings-mekanisme mot det interne nettverket er derfor sterkt å foretrekke.

Kommunikasjonssikring

Siste ledd i kjeden er pålitelig autentisering og sikring av kommunikasjonskanalen mellom brukerens system og det interne nettverket. I praksis er dette den minst krevende delen, fordi den har fått så stor oppmerksomhet de siste årene, og derfor er velutviklet med hensyn til teknologi og tilgjengelige produkter.

Begge elementene er åpenbart like viktige: En sikret kommunikasjonskanal har liten verdi dersom vi ikke vet hvem brukeren er – og motsatt. Vi kan oppsummere de viktigste bestanddelene i denne ligningen slik:

- ✓ Det er ønskelig med bedre autentisering enn hva rene passord kan gi. Smartkort er best, men kostbart og relativt komplisert. Passkoder av den typen vi bruker på Internett-banker, er enklere og etterhvert svært så alminnelige. De gir god sikkerhet, men er noe tungvinte. Dersom passord er eneste mulighet, er det viktig å gjennomføre stringente krav til deres lengde og sammensetning.
- ✓ VPN-teknologi finnes i utallige varianter med ulike karakteristika. Det er viktig å bruke tid på å kartlegge fordeler og ulemper – praktiske, tekniske og sikkerhetsmessige – før val-

gene gjøres [se vår artikkelserie om VPN i utgavene 58-62 og gjennomgangen av Windows 2000s VPN-muligheter i nr. 87-89]. Krypteringsalgoritmer, effektiv kapasitet, standarder og integrasjon med autentiseringsløsningen er viktige parametre i den forbindelse.

- ✓ Innkommende forbindelser til virksomhetens nettverk skal alltid termineres i en halvoffentlig sone (DMZ) inntil brukeren er autentisert og den krypterte VPN-forbindelsen satt opp.
- ✓ Løsningen skal gjøre det mulig å koble ned og sperre separate forbindelser fra brukermaskinen til Internettet mens VPN-kanalen er oppkoblet. Dermed fjernes muligheten for at brukers maskin blir stående som en åpen ruter mellom Internettet og det interne nettverket.

Siste punkt på listen er overvåking: Ingen løsning gir pålitelig sikkerhet over lang tid med mindre den løpende følges opp. Videre blir sikkerheten aldri 100%, og behovet for 'snubletråder' forsvinner ikke. IDS, *Intrusion Detection Systems*, hører hjemme i enhver sikkerhetsarkitektur, og skal blant annet flagge uvanlig aktivitet fra brukernes side. Her er plasseringen av overvåkingspunktene kritisk: Kryptert trafikk skjuler ikke bare legitim bruk, men også inntrengere som har fått kontroll over en brukers maskin. Derfor er ende-til-ende kryptering sjelden ønskelig. Selv SSL-sikret Web-trafikk bør ledes via en proxy, slik at siste trinn frem til den endelige tjeneren kan overvåkes ved behov.

'Bedre føre var enn etter snar' gjelder som aldri før: For spesielt følsomme tjenester kan den beste – kanskje eneste – løsningen være å blokkere ekstern tilgang fullstendig. Risikoen kan koste mer enn den smaker. Samtidig er det viktig å være oppmerksom på alternativene: En optimalt konfigurert Windows Terminal Server/Citrix MetaFrame løsning bringer både data, filer og behandling under god kontroll, og eliminerer behovet for lokalt lagrede data, som vi også var inne på ovenfor. Brukerens muligheter for å kopiere og lagre data som befinner seg på skjermen, får vi imidlertid ikke gjort noe med.

Oppsummering

Hjemmekontorer og fjernbrukere representerer tallrike utfordringer, sosialt, strukturelt og teknisk. En av dem er sikkerhet, en fundamental forutsetning for å tillate ekstern bruk overhodet, og samtidig en side som sjelden blir tatt godt nok vare på.

Vi kan oppsummere stoppestedene på veien til god sikkerhet for hjemmekontorer, utekontorer og andre eksterne brukere slik:

- ✓ Grunnlaget er en funksjonell og oppdatert intern sikkerhetsarkitektur.
- ✓ Neste trinn er en gjennomtenkt policy for eksterne brukere.
- ✓ Med utgangspunkt i policy og tilhørende tekniske spesifikasjoner, får brukerne opplæring som etablerer innsikt i og forståelse for egen rolle i den store sammenhengen.

- ✓ Sikring av utstyr og forbindelser – med verktøy og mekanismer under sentral kontroll, som ikke kan overstyres av brukeren uten at det umiddelbart detekteres.
- ✓ Løpende kontroll med at elementene er på plass og fungerer, også hos brukeren.
- ✓ Interne systemer som overvåker aktiviteten og flagger uvanlig/ureglementert aksess og bruk av ressurser.
- ✓ Oppfølging – overvåking og trafikk kontroll.

