



Vedran Hafner, sistem inženjer,  
Cisco Hrvatska

Tihomir Godec, dipl. ing.,  
RECRO-NET

**Sustav videokonferencija moderan je alat kolaboracije između pojedinaca ili tvrtki, koji na brz, jednostavan i pouzdan način premošćuje fizičku udaljenost između sugovornika.** Uvođenje videokonferencijskih sustava rezultira uštedom vremena potrebnog za organiziranje poslovnih sastanaka, smanjivanjem potrebe za čestim putovanjima, uz istodobno postavljanje i podizanje ekoloških standarda unutar tvrtke u emisiji štetnih plinova. Više je istraživanja potvrdilo da sustav videokonferencija pozitivno utječe na međuljudske odnose unutar organizacija, intenzivira komunikaciju između zaposlenika i nadređenih te smanjuje broj sati provedenih u uredu.

O rastućoj popularnosti videokonferencijskih sustava svjedoče i ovogodišnji rezultati Ciscovog vizualnog indeksa (Cisco Visual Networking Index - VNI) za razdoblje od 2009. do 2014. godine. Prema rezultatima istraživanja globalni će se IP promet do 2014. učeterostručiti, a 91 posto činit će videopromet. Za isto se razdoblje predviđa da će videokonferencije, kao temelj novog modela poslovne kolaboracije, porasti više od 10 puta, a napredni videopromet, uključujući 3-D i HDTV, nevjerojatnih 13 puta!

Videokonferenciju je u nekoliko crta najlakše opisati kao održavanje virtualnog sastanka u realnom vremenu, izme-

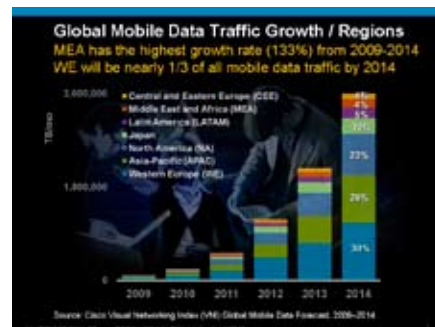
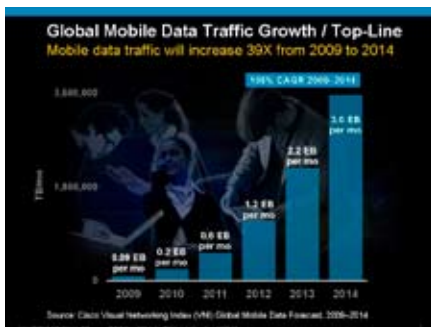
**Prednost u odnosu na klasične sastanke jest potpuna dokumentiranost videokonferencija koje se pohranjuju na hard-disk, a snimljeni se sadržaj naknadno može jednostavno pregledavati**

# Visoka sigurnost

Usluga TelePresence primjenjuje se i u Ciscovom uredu u Hrvatskoj



**Istraživanja potvrđuju da sustav videokonferencija pozitivno utječe na međuljudske odnose unutar organizacija, intenzivira komunikaciju između zaposlenika i nadređenih te smanjuje broj sati provedenih u uredu**



Procjenjuje se da će globalni promet podacima od 2009. do 2014. godine porasti čak 39 puta, najveći rast bilježit će Afrika i Bliski istok, a najveći dio otpast će na zapadnu Europu

đu sudionika na različitim lokacijama, a sve putem naprednih vizualnih, audio i interaktivnih komunikacijskih tehnologija. Jednostavna upotreba, visoka kvaliteta slike i zvuka te sigurnost prijenosa podataka svojstva su zbog kojih upotreba videokonferencije u svakodnevnom poslovanju raste iz godine u godinu. Profesionalni videokonferencijski sustavi u potpunosti su prilagođeni korisniku te su vrlo jednostavni za upotrebu. Prednost u odnosu na

klasične oblike održavanja sastanaka jest i njihova potpuna dokumentiranost – videokonferencije se pohranjuju na hard-disk, a snimljeni se sadržaj naknadno može jednostavno pregledavati.

Ipak, postoje i znatne razlike u odnosu pojedinih videokonferencijskih sustava. Usluga Skype chata primarno je namijenjena privatnim korisnicima, tj. zasni-va se na prometu koji se generira putem javne mreže, kolokvijalno rečeno "jav-



# videokonferencijskih sustava



## RECRO-NET i Cisco Telepresence u Abu Dhabiju

Jedna od zanimljivih implementacija tvrtke RECRO-NET svakako je implementacija sustava za videokonferencije i sigurnost za Abu Dhabi Education Council (ADEC), odnosno za New England Center for Children (NECC). NECC je američka neprofitna organizacija sa sjedištem u Bostonu koja je u Abu Dhabiju otvorila školu za djecu s blažim oblicima autizma. NECC je tehnološki napredna organizacija s mnoštvom osjetljivih osobnih podataka te je stoga trebalo osigurati iznadprosječnu zaštitu podataka i videokonferencije.

Prvi je dio projekta uključivao Ciscov uređaj za videokonferencije između Bostona u SAD-u i Abu Dhabija u UAE-u. Instaliran je i Ciscov uređaj kojim se snimaju videokonferencije ili kreiraju filmovi za potrebe edukacije. VPN tunel između Bostona i Abu Dhabija kreiran je za potrebe videokonferencijskog IP prometa te se njime, uz korištenje enkripcije AES, izravno na videokonferencijskom uređaju postiže i više nego dovoljna zaštita podataka. Investicija u tehnologiju rezultirala je višom razinom produktivnosti zaposlenika, boljom komunikacijom između poslovnica te smanjenjem interkontinentalnih putnih troškova.

nom Internetu". Usprkos pomacima u pojedinim segmentima usluge, Skype i dalje teško zadovoljava visoke potrebe i zahtjeve poslovne komunikacije. S druge strane, upravo su konzistentnost i dostupnost usluge Cisco TelePresence te potrebe za visokom kvalitetom komunikacije u svakodnevnom poslovanju glavne odlike sustava. Zbog mogućnosti prilagodbe različitim uvjetima komunikacije, bez obzira o kojoj je vertikalnoj razini komunikacije unutar i izvan tvrtki riječ, Cisco TelePresence predstavlja sustav poslovne kolaboracije koji je već u upotrebi na više 1000 lokacija diljem svijeta.

## Sigurnost videokonferencijskih sustava

U umreženom svijetu današnjice nekontrolirano širenje sve veće količine povjerljivih podataka, od izlaganja marketinških, financijskih i operativnih poslovnih funkcija, za svaku organizaciju može biti pogubno – od financijskih gubitaka do teškog udarca reputaciji organizacije, što u daljnjim koracima predstavlja potencijalnu prijetnju općenitom poslovanju. Uz to, nekontroliran pristup predstavlja znatne rizike za poslovanje bez obzira na industriju.

Sigurnosni rizici koji proizlaze iz videokonferencije odnose se ponajprije na iskorištavanje ranjivosti sustava zbog porasta broja korisnika te sve većeg protoka podataka. Istodobno rastu zahtjevi zaposlenika za pristupom modernim tehnologijama na radnome mjestu, zbog čega sve više radnika u svijetu preispituje smisao trenutnih korporativnih IT pravila. Nedavno provedeno Ciscovo istraživanje govori da, iako 82 posto globalnih kompanija ima uspostavljenu internu IT regulativu, oko 24 posto zaposlenika ne zna da takve politike uopće postoje.

Dodatnih 23 posto ispitanika tvrdi da njihove kompanije nemaju pravila o prihvatljivoj uporabi uređaja. Od ispitanika upoznatih s internim pravilima, čak 64 posto smatra da tvrtke moraju unaprijediti interne regulative u skladu s potrebama modernog načina života i rada. Navedeni brojevi ukazuju na problematiku koja se javlja u nizu tvrtki diljem svijeta - potre-

ba za ponovnim promišljanjem i nadogradnjom pravila koja bi trebala omogućiti povezanost zaposlenika s radnim mjestom i dostupnim informacijama bilo kad i bilo gdje.

Većina sustava za videokonferencije posjeduje određene ranjivosti kao što su otežan pristup nekih korisnika prema ponuđenoj usluzi te opasnost od izloženosti veće količine povjerljivih podataka. Jedan od načina prenošenja doživljava "osobnog" iskustva preko mreže, koji se odvija u stvarnom vremenu uz pomoć naprednih kolaboracijskih tehnologija, jest preko konvergirane IP mreže. No ona ponekad može biti meta napada računalnih "hake- ra". Potencijalni napadač na sustav može uhvatiti signal poruke te procijeniti birane brojeve, lokaciju sudionika razgovora i lozinke koje se koriste za pristup sustavu. Na sustav audio i videosignala najčešće se primjenjuje metoda enkripcije podataka, kojom se izmjena podataka vrši tako da se poruka, tj. informacije, učine nečitljivima za osobe koje ne posjeduju "ključ". No to

**Prema istraživanju čak 56 posto poslovnih ljudi procjenjuje da dnevno na neefikasne metode komuniciranja potroše više od 30 minuta**

samo po sebi nije dostatno, jer se ključne odrednice za dešifriranje medija moraju definirati na početku transmisije.

Najvažniju ulogu u zaštiti podataka igra autentifikacija, proces kojim se provjerava identitet korisnika određene aplikacije. Nakon uspješne provjere, aplikacija korisniku dodjeljuje točno određene ovlasti na temelju utvrđenog identiteta. To je jedna od najčešćih metoda napada – ako netko uspije prevariti sustav i prijaviti se kao valjani korisnik, na taj će način dobiti sve ovlasti koje je administrator odobrio tom korisniku. Tako se može doprijeti do povjerljivih podataka. Uspjeh takvog napada ne ovisi o tehnološkim slabostima sustava, već o zaštićenosti pristupa, sigurnosnih lozinke i sigurnosti mreže.

Kako bi se takav scenarij spriječio, svaka organizacija treba biti "korak ispred" novih tehnologija, razvijati sigurnosne



## Interoperabilnost, kvaliteta i jednostavnost

Ključni razlozi zbog kojih tvrtke sve češće uvode vizualnu komunikaciju u dnevno poslovanje:

- Današnji sustavi, poglavito Cisco (uključujući i proizvode iz akvizicije TANDBERG), komuniciraju koristeći postojeće standarde i time osiguravaju interoperabilnost
- Ubrzan razvoj i povećana dostupnost IP mreža i infrastrukture dodatno ohrabruju korištenje vizualne komunikacije
- Znatno povećanje pouzdanosti sustava i mreža
- Vizualna i zvučna kvaliteta osiguravaju realističnost komunikacije
- Pozivi se uspostavljaju biranjem broja kao na telefonu ili korištenjem URI-ja koji je u obliku e-mail adrese i stoga lako pamtljiv
- Lakoća integracije s postojećim telefonskim rješenjima

politike unutar organizacije te provoditi redovitu edukaciju zaposlenika. Stoga bi tvrtke trebale imati fleksibilnije interne, korporacijske IT politike i pravila, u skladu s trendovima u industriji i razvoju novih komunikacijskih kanala. Suradnja između IT odjela unutar organizacije te ostalih zaposlenika od velike je važnosti, a sigurnosne politike videokonferencija trebaju biti razvijene i na vrijeme uobličene.

### Prednosti komunikacije "licem u lice"

Vizualna je komunikacija "živa" veza između ljudi na udaljenim lokacijama koja uključuje visokokvalitetnu audio i videokomunikaciju, a ponekad i razmjenu prezentacija. Cilj je vizualne komunikacije tj. videokonferencije simulacija sastanka u kojoj se sve strane vide, čuju i mogu vršiti prezentacije kao da su u istoj sobi.

Iz istraživanja koje su proveli RoperASW i TANDBERG vidljivo je da metode koje se danas koriste za komunikaciju izvan ureda – e-mail i telefon – nisu dovoljne da bi

se ostvario temelj za pametne i odgovorne poslovne odluke. Istraživanje je pokazalo da 56 posto poslovnih ljudi procjenjuje da dnevno više od 30 minuta potroše na neefikasne metode komuniciranja. Ti ljudi oduševljeno kažu da je komuni-

### Usporedo s češćim korištenjem videokonferencija javila se i potreba za zaštitom podataka te dokumenata koji se dijele putem videokonferencije, a sve češće spajanje udaljenih lokacija preko Interneta kao javne mreže, još više doprinosi razvoju svijesti o zaštiti podataka

kacija "licem u lice" u usporedbi s audio ili online/web baziranom komunikacijom razumljivija, osobnija, omogućuje brze odluke, gradi povjerenje, olakšava pregovaranje, smanjuje mogućnost krivog razumijevanja ili zabune te je bolja za detaljnija objašnjenja. Istraživanje poka-

zuje da je u današnjem umreženom svijetu, potreba za vizualnom komunikacijom veća no ikad.

Vizualna komunikacija donosi trenutne prednosti. Omogućava pojedincima i tvrtkama postizanje sljedećih ciljeva:

- Povećanje produktivnosti i efikasnosti
- Skraćivanje vremena pristupa na tržište, kao i vremena adaptacije na tržišne promjene
- Optimiziranje korištenja resursa
- Ubrzavanje donošenje odluka
- Povećanje dostupnosti informacijama
- Smanjenje troškova i vremena putovanja
- Prednost nad konkurencijom
- Redoviti i osobni kontakti s kolegama, partnerima, dobavljačima i klijentima bez napuštanja ureda
- Sudjelovanje u iznenadnim bitnim sastancima te trenutačno donošenje odluka
- Ušteda vremena, resursa i novca uz povećanu radnu učinkovitost i kvalitetu života

Videokonferencijski poziv povećava prisutnost na ključnim sastancima svih razina, kao i ujedinjenje udaljenih lokacija. Pristup dokumentima i aplikacijama u realnom vremenu znatno ubrzava proces donošenja odluka. Primjena raznih vanjskih uređaja kao što su dokument kamera ili osobno računalo drastično obogaćuje vizualnu komunikaciju.

S povećanim korištenjem videokonferencija javila se i potreba za zaštitom podataka, tj. video i audiosignala, te dokumenata koji se dijele putem videokonferencije. Sve češće spajanje udaljenih lokacija preko javne mreže – Interneta, još je više doprinijela razvoju svijesti o zaštiti podataka. Stoga Ciscovi videokonferencijski uređaji imaju ugrađenu mogućnost enkripcije video i audiopodataka. Enkripcija se odvija putem standarda AES i potpuno zadovoljava standarde javnog i privatnog sektora.

Želi li se dodatno zaštititi od neželjenog prisluškivanja, videokonferencija se neće odvijati preko javne mreže, nego preko vlastite komunikacijske mreže koja se dodatno još može zaštititi VPN tunelima. U slučaju prenošenja specifičnih i vrlo važnih, tajnih podataka dodatno se osiguranje postiže posebnim uređajima za enkripciju s vlastitim enkripcijskim algoritmima. U tom slučaju moguće je postići potpunu zaštitu prenesenih informacija. ■