



Vi är säkra på en sak – virus utvecklas ständigt och attackerna ökar, såväl allmänna som riktade.

Vi är lika säkra på en annan sak – TeleComputings tjänst AntiVirus följer utvecklingen och erbjuder er ett uppdaterat och effektivt viruskydd som undviker onödiga och kostsamma stopp och dataförluster.

Vi blir mer och mer beroende av vår IT-miljö. Det sprids i dag över 50 000 virus och riktade angrepp som båda innebär säkerhetsrisker och påverkar verksamhetens IT-system. Vi riskerar driftstopp, instabilitet och förlust av data.

I allt större utsträckning är datorer ständigt anslutna till Internet, i såväl offentlig som arbets- och hemmiljö, och riskerar därmed att bli angripna. Många datorer har ett antiviruskydd men det förekommer att skyddet inte aktivt uppdateras.

TeleComputing har ett tydligt mål: att hålla våra kunders datorer och system uppdaterade och skyddade mot virus för att undvika stopp och dataförluster, som skulle orsaka våra kunder stora kostnader och irritation. Vi har en mycket genomtänkt och väl genomarbetad strategi med rutiner och system för att säkra och undvika stopp och dataförluster i vårt datacenter.

Stationära, bärbara och hemmadatorer skyddas effektivt mot virus. Uppdatering sker regelbundet och datorer anslutna till tjänsten kontrolleras så att de har det senaste skyddet installerat. Vid brådskande virusshot trycks uppdateringar ut till anslutna datorer.

Vår säkerhetsavdelning bevakar och går igenom loggar för att kontrollera att anslutna datorer inte är smittade. De som utvecklar virus försöker alltid hitta vägar in bakom systemen och ibland händer det att virus tar sig in på datorer trots att viruskyddet är uppdaterat. Normalt ska viruskyddet ta hand om det. Om viruset är av en typ som skyddet inte klarar



av att ta bort så agerar vår säkerhetsavdelning och ger dig hjälp och råd om hur det skall tas bort.

Med TeleComputing AntiVirus har era datorer och system ett mycket bra skydd och ni undviker stopp och dataförluster.

AntiVirus ger er:

Antiviruskydd på klient samt information till användaren eller organisationens IT-kontakt vid eventuella angrepp tillsammans med vägledning och råd om hur man ska agera.

Daglig kontroll och uppdatering till senaste version av programvara och definitionsfiler.

Daglig kontroll att senaste version av programvara är installerad.