advenica

LÖSNINGSBESKRIVNING

# Säker fjärråtkomst

Många organisationer är beroende av fjärråtkomst via RDP, till exempel för att leverantörer skall kunna utföra underhåll, eller att driftpersonal skall kunna övervaka en anläggning. Säker fjärråtkomst löser många av de säkerhetsrisker som annars är förknippade med sådana lösningar.

Utmaning

## Fjärråtkomst på ett säkert sätt

Behovet att kunna styra och övervaka system på distans är stort. Ibland används generella anslutningar som IPSec eller TLS för att koppla samman datornät på distans. IT-säkerhetsmässigt innebär sådana anslutningar att båda systemen exponeras för summan av de hot som gäller för något av de bägge systemen. Gemensamt för många system för fjärranslutning är att de är universella och har anpassningar och funktioner för allt från kontorsarbete till systemadministration. Det innebär även att det finns risker för såväl felkonfiguration som implementationsbuggar.

Utöver att överbrygga geografiska avstånd används protokollen också i ökande grad som en säkerhetshöjande åtgärd. Ofta används då en jumpserver som mellanhand. Tanken är att avgränsa möjligheten för oönskad trafik från användarens PC till målsystemet. Den programvara som användaren önskar använda körs då på jump-servern, och kommunicerar via standardprotokoll med målsystemet. Några risker med sådana lösningar är:

### 1. Risk att obehöriga använder anslutningen

De flesta system har funktioner för att autentisera användaren så att obehöriga inte kan utnyttja anslutningen. Det förekommer dock att fokus ligger mer på enkelt handhavande eller prestanda än säkerhet.

### 2. Risk att anslutningen utnyttjas vid fel tidpunkt

När leverantörer ska göra åtgärder i systemet riskerar man att de missbrukar sin behörighet vid andra tillfällen än den avtalade tidpunkten. Det behöver inte handla om ett avsiktligt missbruk, det kan lika gärna handla om att leverantörens ITsystem kan vara utsatt för en attack, och att det leder till en följdattack.

### 3. Risk att anslutningen används för fel syfte

Det är mycket vanligt att anslutningen har större behörighet än vad som behövs för att lösa den egentliga uppgiften. Det medför då risk dels att användaren kan göra avsiktliga, eller oavsiktliga, misstag. Det innebär också att man exponeras för risken för följdattack ifall användarens system är attackerat.

### 4. Risk att anslutningen ansluter periferienheter

Flera av protokollen har funktioner för att ansluta periferienheter. Det kan handla om högtalare och mikrofoner, skrivare eller flyttbara media som USB-stickor eller hårddiskar. Ibland finns möjligheten att konfigurationsmässigt stänga av dessa funktioner, men innebär i så fall att man måste kunna lita på att det är implementerat på ett säkert sätt – vilket inte alltid är fallet.

**Lösning**

## Säkert och enkelt att använda

Fjärråtkomst kan göras säker genom att använda RDP och skydda jumpservern med en explicit säkerhetslösning. En sådan lösning är SecuriCDS ZoneGuard för RDP. Anslutningen från användarens PC görs som vanligt med RDP mot ZoneGuard. Användaren autentiseras, och det säkerställs att anslutningen sker till ett godkänt målsystem och vid en tidpunkt som är tillåten. Därefter säkerställer ZoneGuard att endast skärmbildsinformation tillåts passera från målsystemet till användaren. Åt andra hållet överförs endast tangentbordskommandon och musrörelser. Det är till och med möjligt att begränsa så att till exempel endast vissa tangentbordskombinationer är tillåtna. Ingen annan information tillåts passera, vilket eliminerar riskerna med till exempel generell kommunikation, felkonfigurationer i jumpservern eller dess mjukvara. Likaledes hindras åtkomst till periferienheter som annars hade inneburit ökad risk.

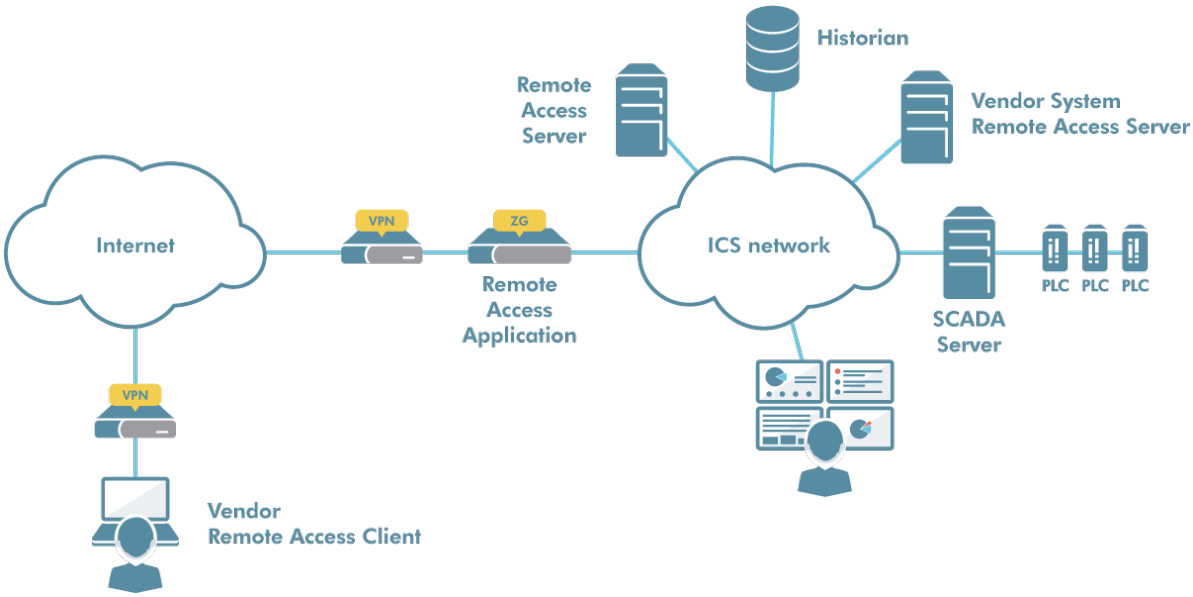
**Fördelar**

## Säkerhet och funktion

Genom att utnyttja RDP och skydda kommunikationen med ZoneGuard uppnår man både säkerhet och funktion:

- Endast behöriga användare kan utnyttja anslutningen vid tillåtna tidpunkter.
- Anslutningen kan endast ske mot avsedda system.
- Ingen risk för överföring av skadlig kod på nätverksnivå.
- Ingen exponering mot periferienheter.
- Spårbarhet: vem gjorde vad och när?

Läs mer om ZoneGuard på advenica.com.




advenica

Advenica tillhandahåller expertis, hög assurans och cybersäkerhetslösningar i världsklass för kritisk data-inmotion upp till Top Secret-klassning. Med oss stärker länder, myndigheter och företag informationssäkerheten och digitaliserar ansvarsfullt. Bolaget grundades 1993 och har EU-godkännande på högsta säkerhetsnivå. Våra unika produkter designas, utvecklas och tillverkas i Sverige.

**Läs mer på advenica.com**



ISO 9001 CERTIFIED
ISO 14001 CERTIFIED