Faktablad

Avdelningen för cybersäkerhet och säkra kommunikationer
Publ.nr MSB1520 – mars 2020

Fjärranslutningstekniker för industriella informations- och styrsystem

Tillgång till interna resurser via fjärranslutning är en viktig del i många verksamheters arbetsprocesser. Det är kritiskt för informations- och driftsäkerheten att fjärranslutningens säkerhet upprätthålls Att upprätta och hantera säkerheten i fjärranslutning kan vara en komplex process. Detta faktablad syftar till att förse intressenter med säkerhetsrelaterade rekommendationer vilka kan användas som stöd under arbetsprocessen vid beslut kring fjärranslutningar. Faktabladet är baserat på en studie vilken finns att tillgå via MSB:s hemsida.

Grundläggande säkerhetsfilosofi och policyer

En användare av ett system bör inte ges mer tillgång till systemets funktionalitet och dess innehåll än nödvändigt. Principen om minsta möjliga rättigheter bör appliceras, baserad på användarens arbetsuppgifter. Denna princip begränsar sannolikheten för stora konsekvenser, orsakade av både antagonist och handhavandefel.

Utöver denna grundläggande princip bör en plan för hur en organisation eller individ ska agera i en särskild situation utarbetas. Organisationen bör formulera och besvara en rad frågor innan anskaffning av funktionalitet för fjärranslutning. Detta för att skapa och tillämpa fjärranslutningsspecifika policyer.

- Vilka organisatoriska mål är fjärranslutningsfunktionalitet tänkt att uppfylla?
- Finns det grupper av anställda som behöver fjärranslutningsmöjligheter för att utföra sina uppgifter?
- Kan effektiviteten hos de anställda och organisationen som helhet förbättras genom fjärranslutningsmöjligheter?

Generella säkerhetspolicyer

Autentisering bör appliceras för att kontrollera en användares identitet och behörighet vid ex. inloggning. För att starkare verifikation av uppgiven identitet finns även bland annat flerfaktorsautentisering att tillgå.

Kryptering bör appliceras på all kommunikation som färdas utanför organisationens interna nätverk. Val av kryptering bör baseras på vedertagna och rekommenderade standardalgoritmer.

Åtkomstkontroll bör utformas utefter principen om minsta möjliga rättigheter. En användare bör inte ges rättigheter som om den befann sig i organisationens interna nätverk.

Användarkategorier Utifrån ett systems perspektiv kan alla användare delas in i kategorier där varje kategori innehåller en uppsättning behörigheter utifrån de behov som en användare i gruppen har gentemot systemet. Det finns sannolikt även individuella skillnader i behörighet för användare inom en användargrupp

Tekniklösningar för fjärranslutning

Tunnlar

Vanligtvis i form av VPN. Den krypterade anslutningen mellan klientenhet och VPN-gateway utgör tunneln. Krypteringen av tunneln skyddar kommunikationen mot både avlyssning och manipulering av innehåll.

Kontakta oss:
Tel: 0771-240 240
registrator@msb.se
www.msb.se

Myndigheten för samhällsskydd och beredskap

Vidare bör organisationen definiera vilka fjärranslutningstekniker som ska tillåtas för tillgång till de interna resurserna. Det är viktigt att definiera vilka användare som ska ges tillgång till vilken typ av information, som ovan nämnt bör principen om minsta möjliga åtkomst appliceras.

Fjärranslutningstekniker

Bland kommersiella aktörer finns det idag fyra vanligt förekommande kategorier av fjärranslutning: tunnlar, applikationsportaler, fjärråtkomst till skrivbord samt direkt applikationstillgång. Kategorierna har gemensamma nämnare.

- De har alla möjlighet att kryptera kommunikationskanalen för att skydda dataflödet.
- De är beroende av den fysiska säkerheten hos klienterna.
- Olika typer av autentiseringsmekanismer kan användas för alla kategorier.
- De flesta implementationer möjliggör, avsiktlig och oavsiktlig, lagring av data på klientenheter.

Fjärranslutningar används vanligtvis utanför organisationens interna nätverk, även fysiskt, vilket kan leda till ökad exponering.

Sammanfattning

De flesta hot och risker relaterade till fjärranslutningar kan motverkas med hjälp av de nämnda tekniska lösningarna. Det är dock viktigt att komplettera med ytterligare säkerhetsfunktionalitet, som generell säkerhetsfilosofi och organisationspolicyer. Vissa risker kan dock ej genom tekniska lösningar motverkas eller mildras. Det är därför viktigt att vara medveten om eventuella risker och minimera effekterna av relaterade konsekvenser.

Rekommendationer

Innan beslut om implementation av fjärranslutningsteknik tas bör organisationen:

- Identifiera sitt behov av fjärranslutning.
- Identifiera vilken typ av information och vilka funktioner som behöver tillgängliggöras via fjärranslutning.
- Utföra en säkerhetsanalys av identifierat behov av fjärranslutning, typ av information samt funktioner.
- Justera eller införa tillägg av säkerhetspolicyer.

När dessa åtgärder är genomförda kan kravställning och upphandling av tekniklösning för fjärranslutning påbörjas.

Applikationsportaler

Server som via ett centraliserat gränssnitt ger tillgång till en eller flera applikationer via de interna applikationsservrarna. Skyddar kommunikation till och från användarenheten samt kan autentisera och hantera åtkomstkontroll.

För tunnlar finns applikationsklientmjukvaran och data lokalt i användarenheten medan det för portaler generellt finns i portalservern.

Det finns primärt tre vanligen använda typer av portaler:

- Webbportaler
- Virtual Desktop Infrastructure (VDI)
- Terminal server

Fjärråtkomst

Det finns två primära metoder för fjärråtkomst till skrivbord, direkt och indirekt. Direkt anslutning uppnås genom att en fjärrenhet direkt ansluter till en PC i en organisations interna nätverk. Indirekt anslutning innebär att kommunikationen går genom en mellanliggande server.

Direkt applikationstillgång

Vissa applikationer kan nås direkt via en webbläsare där applikationen själv står för säkerheten i kommunikationen. Det vanligast exemplet på en sådan applikation är webbmail, där användaren via en webbläsare ansluter till en server som kör en webbmailapplikation.

Servern kommunicerar med HTTP över TLS (HTTPS) för att skydda kommunikationen och autentiserar användaren innan tillgång till användarens epost medges.

Hela studien
Fjärranslutning – Fjärranslutningstekniker för informations- och styrsystem:

Rapportnr: MSB 2018-03308, finns att tillgå via www.msb.se

Kontakta oss:
Tel: 0771-240 240
registrator@msb.se
www.msb.se

Myndigheten för samhällsskydd och beredskap