BROSCHYR · NOVEMBER 2026

FÖR DRIFT- OCH SUPPORTCENTRALER

Ni har nycklarna till era kunder.

En handbok i säker fjärrservice för er som sköter passersystem, kyla, kameror, fastighetssystem och annan utrustning åt andra.

XERTIFIED AB · UPPSALA

XERTIFIED.SE

Era vägar in är värdefulla

Ni når hundratals anläggningar på distans. Det gör er snabba när något går fel. Det gör er också till ett mål för angripare.

En angripare som tar sig in hos er kan nå alla era kunder på en gång. Det räcker med ett lösenord som har läckt eller ett konto som många delar. Därför ställer kunderna allt fler frågor om hur ni arbetar.

Den här broschyren hjälper er att göra fjärrservicen säker. Den ger er också svar på de frågor som kunderna ställer.

Så använder ni broschyren

Steg 1

Gå igenom checklistan

Sidan 4 har åtta vanor för en säker driftcentral.

Steg 2

Förbered svaren

Sidan 5 har kundernas vanligaste frågor och exempel på bra svar.

Steg 3

Fördela ansvaret

Sidan 6 visar vad ni och kunden bör komma överens om.

Steg 4

Planera för det värsta

Sidan 7 visar vad ni gör om en väg in har missbrukats.

GÖR DET HÄR I VECKAN · TRE SAKER

1. **Lista era vägar in.** Skriv upp alla verktyg, VPN, öppna portar och routrar som ni använder för att nå kunderna.
2. **Hitta de delade kontona.** Ta reda på vilka inloggningar som flera personer använder, också hos underleverantörer.
3. **Kontrollera dem som har slutat.** Se till att ingen som har slutat det senaste året fortfarande har åtkomst.

Ett intrång hos er blir ett intrång hos alla

Ni sköter många system åt många kunder. Varje system har ofta ett eget verktyg och en egen väg in. Ju fler vägar in, desto svårare är det att se vem som använder dem.

Passersystem

Någon kan öppna dörrar för fel personer.

Kyl och frys

Varor kan bli förstörda på en natt.

Kameror och larm

Någon kan se in eller stänga av larmet.

Fastighetssystem

Någon kan stänga av värme, ventilation och klimat.

Hissar och rulltrappor

Människor kan bli stående eller instängda.

Laddstolpar och energi

Laddning och elförsörjning kan störas.

Så brukar angripare lyckas

- **Inloggningar läcker.** Ett stulet lösenord fungerar ofta hos flera kunder.
- **Konton delas.** Ingen vet längre vem som har tillgång, eller om underleverantören har det.
- **Vägen in står alltid öppen.** Verktyg och öppna portar fungerar dygnet runt, också när ingen arbetar.
- **Utrustningen är gammal.** Den får inga säkerhetsuppdateringar och syns på internet.
- **Ingen ser vad som händer.** Det finns ingen logg över vem som anslöt, till vad och när.

LÄRDOMEN

En väg in som alltid står öppen kan användas av vem som helst som hittar den.

Läs varför uppdateringarna inte hinner med

Åtta vanor för en säker driftcentral

Varje vana gör det svårare att använda er som väg in till kunderna.

01

Vet vilka vägar in ni har

Ha en aktuell lista över alla verktyg, konton och anslutningar till varje kund.

02

Inga öppningar in hos kunden

Utrustningen ska inte gå att nå direkt från internet. Anslutningen ska gå ut från kundens nätverk, inte in.

03

En person, en inloggning

Varje tekniker har en egen inloggning. Det gäller också underleverantörer.

04

Starkt skydd vid inloggning

Använd mer än ett lösenord, till exempel en hårdvarunyckel eller ett smart kort.

05

Åtkomst per enhet och tid

Teknikern når bara den enhet som ärendet gäller, och bara så länge arbetet pågår.

06

Kunden godkänner

Låt kunden godkänna åtkomsten, i alla fall till de viktigaste systemen.

07

Logga allt

Spara vem som anslöt, till vad, när och hur länge. Kunden ska kunna få loggarna.

08

Stäng direkt

Ta bort åtkomsten samma dag som någon slutar eller ett uppdrag tar slut.

> **Tips:** Gå igenom checklistan med varje underleverantör. Deras brister blir era brister.

Frågor era kunder kommer att ställa

Kunderna har börjat fråga hur leverantörerna når deras utrustning.
Ha svaren klara. Här är exempel på svar som bygger förtroende.

Kundens fråga	Ett bra svar
Hur når ni vår utrustning?	Via en krypterad anslutning som går ut från ert nätverk. Inga portar är öppna in.
Kan ni nå något annat i vårt nätverk?	Nej. Vi når bara den utrustning som vi sköter.
Har varje tekniker en egen inloggning? Även underleverantörerna?	Ja. Alla har en egen inloggning, och ingen delar konto.
Kan vi godkänna varje anslutning?	Ja. Ni kan godkänna varje begäran innan anslutningen öppnas.
Kan ni visa vem som var inne?	Ja. Vi loggar vem som anslöt, till vad, när och hur länge.
Vad händer när en tekniker slutar?	Åtkomsten stängs samma dag.
Hur får vi veta om något händer?	Vi berättar direkt och ger er underlag för en eventuell incidentrapport.

> **Tips:** Skriv in svaren i era offerter och avtal. Då behöver kunden inte fråga.

Läs om åtkomst som kunden godkänner

Vem ansvarar för vad?

Ni och kunden delar ansvaret för säkerheten. Skriv in fördelningen i avtalet, så att inget glöms bort.

Uppgift	Ni	Kunden	Tillverkaren
Bestämma vem som får åtkomst	☐	☐	☐
Godkänna en anslutning	☐	☐	☐
Driva systemet för fjärråtkomst	☐	☐	☐
Spara och lämna ut loggar	☐	☐	☐
Uppdatera utrustningen	☐	☐	☐
Rapportera incidenter	☐	☐	☐

Kraven som kommer till er

- **NIS2.** Kunder som omfattas av cybersäkerhetslagen måste ställa krav på sina leverantörer. Kraven hamnar hos er. Läs om NIS2
- **CER.** En ny lag om motståndskraft föreslås gälla från 1 januari 2027. Den ställer krav på samhällsviktiga verksamheter. Läs om CER
- **Försäkringen.** Allt fler försäkringsbolag frågar hur ni skyddar åtkomsten till kunderna. Fråga vad er försäkring kräver.

Om en väg in har missbrukats

1. **Stäng vägen in.** Koppla bort verktyget eller anslutningen som har använts.
2. **Spärra inloggningar.** Spärra konton och certifikat som kan vara påverkade.
3. **Ta reda på vilka kunder som påverkas.** Andra kunder kan nås på samma sätt.
4. **Kontakta kunderna direkt.** Berätta vad ni vet och vad ni gör.
5. **Säkra loggarna.** Spara dem innan de skrivs över. Kunderna och polisen kan behöva dem.
6. **Hjälp kunderna att rapportera.** Vissa kunder måste rapportera incidenten till en myndighet inom 24 timmar.
7. **Polisanmäl och rapportera.** Gör en polisanmälan på polisen.se. Rapportera incidenten till CERT-SE på cert.se.
8. **Lär av det som hände.** Ändra rutinerna så att samma sak inte kan hända igen.

Förbered er redan nu

Roll	Namn	Telefon
Ansvarig för incidenter		
Den som stänger åtkomst		
Kontakt mot kunderna		
Försäkringsbolag		

Ord att kunna

Fjärråtkomst	När någon når utrustningen på distans, via nätverket.
Öppen port	En öppning i routern som släpper in trafik från internet.
Delat konto	En inloggning som flera personer använder. Då går det inte att se vem som gjorde vad.
Hårdvarunyckel	En liten dosa för inloggning. Den sätts i datorn eller hålls mot den.
Logg	En lista över vem som gjorde vad och när.
Incident	En händelse som stör eller skadar system, till exempel ett angrepp.

Mer information

cert.se	Sveriges nationella funktion för it-incidenter. Här rapporterar ni en incident.
ncsc.se	Nationellt cybersäkerhetscenter. Råd och stöd om cybersäkerhet.
polisen.se	Polisanmälan. Telefon 114 14, vid akut fara 112.

Så kan Xertified hjälpa

Med XoT når era tekniker rätt enhet under en bestämd tid, utan öppna portar hos kunden. Varje tekniker har en egen inloggning, och kunden kan godkänna varje anslutning. En XMS kan hantera många kunder och hålla dem helt isär.

Låset gör också kundernas utrustning osynlig för obehöriga, även när den inte får uppdateringar.

Bli partner, säkra era kunders enheter och erbjud säker fjärrservice.

xertified.se/branscher/drift-och-supportcentral · info@xertified.com · 018-265 06 06

Läs om att bli partner