FOR OPERATIONS AND SUPPORT CENTRES

You hold the keys to your customers.

A handbook on secure remote service for those who manage access control, refrigeration, cameras and building systems for others.

XERTIFIED AB · UPPSALA, SWEDEN

XERTIFIED.COM

Your ways in are valuable

You reach hundreds of sites remotely. That makes you fast when something goes wrong. It also makes you a target for attackers.

An attacker who gets into your systems can reach all your customers at once. One leaked password or one shared account is enough. That is why customers are asking more and more questions about how you work.

This brochure helps you make remote service secure. It also gives you answers to the questions customers ask.

How to use this brochure

Step 1

Go through the checklist

Page 4 has eight habits for a secure operations centre.

Step 2

Prepare your answers

Page 5 has your customers' most common questions and examples of good answers.

Step 3

Divide the responsibility

Page 6 shows what you and the customer should agree on.

Step 4

Plan for the worst

Page 7 shows what to do if a way in has been misused.

DO THIS WEEK · THREE THINGS

1. **List your ways in.** Write down every tool, VPN, open port and router you use to reach customers.
2. **Find the shared accounts.** Find out which logins several people use, including at subcontractors.
3. **Check the leavers.** Make sure no one who left in the past year still has access.

A breach at your end is a breach at every customer

You manage many systems for many customers. Each system often has its own tool and its own way in. The more ways in, the harder it is to see who uses them.

Access control

Doors can be opened or locked for the wrong people.

Refrigeration

Goods can be ruined in one night.

Cameras and alarms

Someone can watch or switch off the alarm.

Building systems

Heating, ventilation and air conditioning can be switched off.

Lifts and escalators

People can be stranded or trapped.

Chargers and energy

Charging and power supply can be disrupted.

How attackers usually succeed

- **Logins leak.** A stolen password often works at several customers.
- **Accounts are shared.** No one knows any longer who has access, or whether the subcontractor does.
- **The way in is always open.** Tools and open ports work around the clock, even when no one is working.
- **The equipment is old.** It gets no security updates and is visible on the internet.
- **No one sees what happens.** There is no log of who connected, to what and when.

THE LESSON

A way in that is always open can be used by anyone who finds it.

Read why updates cannot keep up

Eight habits for a secure operations centre

Each habit makes it harder to use you as a way in to your customers.

01

Know your ways in

Keep an up-to-date list of every tool, account and connection to each customer.

02

No openings at the customer

Equipment should not be reachable directly from the internet. Connections should go out of the customer's network, not in.

03

One person, one login

Every technician has their own login. That includes subcontractors.

04

Strong sign-in

Use more than a password, for example a hardware key or a smart card.

05

Access per device and time

The technician reaches only the device the job concerns, and only while the work is going on.

06

The customer approves

Let the customer approve access, at least to the most important systems.

07

Log everything

Record who connected, to what, when and for how long. The customer should be able to get the logs.

08

Close at once

Remove access on the same day someone leaves or a contract ends.

Tip: Go through the checklist with each subcontractor. Their weaknesses become your weaknesses.

Questions your customers will ask

Customers have started asking how suppliers reach their equipment. Have your answers ready. Here are examples of answers that build trust.

The customer's question	A good answer
How do you reach our equipment?	Through an encrypted connection that goes out of your network. No inbound ports are open.
Can you reach anything else on our network?	No. We only reach the equipment we manage.
Does every technician have their own login? Subcontractors too?	Yes. Everyone has their own login, and no one shares an account.
Can we approve each connection?	Yes. You can approve each request before the connection opens.
Can you show who was connected?	Yes. We log who connected, to what, when and for how long.
What happens when a technician leaves?	Their access is closed the same day.
How will we know if something happens?	We tell you at once and give you what you need for any incident report.

> **Tip:** Put the answers in your quotes and contracts. Then the customer does not need to ask.

Read about access the customer approves

Who is responsible for what?

You and the customer share responsibility for security. Put the division in the contract, so nothing is forgotten.

Task	You	Customer	Manufacturer
Decide who gets access	☐	☐	☐
Approve a connection	☐	☐	☐
Run the remote access system	☐	☐	☐
Keep and hand over logs	☐	☐	☐
Update the equipment	☐	☐	☐
Report incidents	☐	☐	☐

The requirements coming your way

- **NIS2.** Customers in scope must set requirements for their suppliers. Those requirements end up with you. Read about NIS2
- **CER.** The EU directive on critical entities sets resilience requirements for essential services. Most EU countries already apply it. Read about CER
- **Insurance.** More and more insurers ask how you protect access to your customers. Ask what your policy requires.

If a way in has been misused

1. **Close the way in.** Disconnect the tool or connection that was used.
2. **Block logins.** Block accounts and certificates that may be affected.
3. **Find out which customers are affected.** Other customers may be reachable the same way.
4. **Contact the customers directly.** Tell them what you know and what you are doing.
5. **Secure the logs.** Save them before they are overwritten. Customers and the police may need them.
6. **Help customers report.** Some customers must report the incident to an authority within 24 hours.
7. **Report to the police and your national CSIRT.** In Sweden, use polisen.se and CERT-SE at cert.se.
8. **Learn from what happened.** Change your routines so the same thing cannot happen again.

Prepare now

Role	Name	Phone
Incident lead		
Person who closes access		
Customer contact		
Insurer		

Words to know

Remote access	When someone reaches the equipment from a distance, over the network.
Open port	An opening in the router that lets traffic in from the internet.
Shared account	A login that several people use. You then cannot see who did what.
Hardware key	A small device for signing in. You plug it into the computer or hold it against it.
Log	A record of who did what, and when.
CSIRT	A team that helps organisations handle cyber incidents. Every EU country has a national one.

More information

CSIRTs Network	The national CSIRTs in the EU, from ENISA.
cert.se	CERT-SE, Sweden's national CSIRT.
ncsc.se	The Swedish National Cyber Security Centre.

How Xertified can help

With XoT, your technicians reach the right device for a set time, with no open ports at the customer. Every technician has their own login, and the customer can approve each connection. One XMS can manage many customers and keep them fully separate.

Become a partner and offer secure remote service to your customers.

xertified.com/industries/operations-and-support-centres · info@xertified.com · +46 18 265 06 06

Read about becoming a partner