

BROCHURE · NOVEMBER 2026

FOR STORE OWNERS · GROCERY RETAIL

Keep the store open. Keep digital intruders out.

A handbook on basic cybersecurity for the checkout, cameras, refrigeration and other connected equipment in your store.

XERTIFIED AB · UPPSALA, SWEDEN

XERTIFIED.COM

Your store is full of small computers

The checkout, the cameras, the refrigeration and the alarm are all connected. Inside them are small computers that you rarely see. Many of them can be reached remotely, often by more people than you think.

Attacks on this kind of equipment are becoming more common. An attacker can stop the checkout, watch through the cameras or switch off the cooling. For a store, that can mean closed doors and goods you have to throw away.

This brochure helps you protect the connected equipment in your store. You do not need to be a technician. Most of it is about asking the right questions to the right person. Small steps make a big difference.

How to use this brochure

Step 1

Go through the checklist

Page 4 has eight habits. Start with them.

Step 2

Fill in the inventory

On page 5 you list your equipment and your suppliers.

Step 3

Read about your equipment

Pages 6 to 8 cover responsibility, suppliers and equipment.

Step 4

Keep the brochure

Take it out when you change supplier or equipment.

DO THIS TODAY · THREE THINGS IN 15 MINUTES

1. **Put up the emergency numbers.** Write down the numbers for the refrigeration contractor, the IT supplier and the alarm company where staff can see them.
2. **Call one supplier.** Ask how they reach your equipment remotely, and who at their company can do it.
3. **Check the router.** Ask the IT supplier whether the factory password has been changed on the router and the wireless network.

Everything connected can be attacked

A store has many systems that are connected to the network. Each one can become a way in for an attacker. If one system stops, it can affect the whole store.

Checkout system

Without the checkout, you cannot sell anything.

Cameras

An attacker can watch the store or move on into the network. Read about cameras

Refrigeration

A fault can force you to throw away goods.

Planning systems

Schedules, orders and deliveries can stop.

Access control and alarms

Doors and alarms can stop working.

Ventilation and heating

A service company often manages them remotely.

How attackers usually succeed

- **The equipment is visible on the internet.** Attackers constantly search for equipment that responds.
- **The software is old.** It has not received security updates for several years.
- **The factory password is still in place.** Such passwords can often be found on the internet.
- **Suppliers share logins.** No one knows any longer who has access.
- **Everything is on the same network.** From a camera, the attacker reaches the checkout.
- **No one notices.** No one sees who connects, or when.

THE LESSON

What is visible on the internet can be attacked. Equipment that gets no updates becomes easier to attack every year.

Read why updates cannot keep up

Eight habits for a safer store

Start here. Each habit makes it harder for an attacker to get into your store.

01

Know what is connected

Make a list of all equipment that is connected to the network or to the internet.

02

Nothing reachable from the internet

Ask your suppliers to check that no device can be reached directly from the internet.

03

Change the factory password

Every device should have its own strong password. Do not share passwords between suppliers.

04

Update or protect

Ask how long the equipment gets security updates. Protect equipment that no longer gets any.

05

Remote access only when needed

A supplier should only connect when there is a job to do, and only to its own equipment.

06

Divide the network

The checkout, the office, the refrigeration and the cameras should not share one network.

07

See who has been connected

Ask your suppliers to show who connected, when and why.

08

Have a plan

Write down who you call and what you do if a system stops working.

Tip: Bring the checklist next time the refrigeration contractor or the IT supplier is in the store. Go through it together.

Take stock of your equipment

Write down the equipment that is connected. Ask the supplier if you do not know the answer.

Equipment	Supplier and phone	Reachable from the internet?	Gets updates?
Refrigeration system			
Cold rooms and freezers			
Ventilation and heating			
Cameras			
Alarm and access control			
Checkout system			
Planning system			
Router or modem			
Other:			

How secure is your store?

Statement	Good	OK	Not yet
I know which equipment is connected.	☐	☐	☐
No equipment can be reached directly from the internet.	☐	☐	☐
The factory passwords have been changed.	☐	☐	☐
I know which suppliers have remote access.	☐	☐	☐
I have a plan if a system stops working.	☐	☐	☐

Start with what you ticked under Not yet.

Who is responsible for what?

You may own the store but not the checkout system or the network. The chain, the landlord or a supplier may manage them. Find out who is responsible for each system.

Then you know who to ask, and who to call when something happens. Tick who is responsible.

System	The store	The chain	The landlord	Supplier
Network and router	☐	☐	☐	☐
Checkout system	☐	☐	☐	☐
Refrigeration	☐	☐	☐	☐
Cameras and alarm	☐	☐	☐	☐
Access control	☐	☐	☐	☐
Ventilation and heating	☐	☐	☐	☐
Planning system	☐	☐	☐	☐

> **Put it in the contract.** Agree on who changes passwords, installs updates and closes remote access when a job is finished.

Insurance

More and more insurers ask how you protect your systems. Some policies require basic protection before they pay out.

- Read the terms, or ask your insurer what applies to you.
- Ask whether the policy covers goods you must throw away and sales you lose after a cyberattack.
- Keep the checklist, the inventory and this table. They show what you have done.

Suppliers who reach the store remotely

The refrigeration contractor, the ventilation company and the alarm company often need to reach their equipment. That makes it faster to find and fix faults. But an attacker can also use every way in.

Questions to ask your suppliers

1. How do you reach our equipment? Through an open port, a shared account or a secure connection?
2. Can you reach anything else on our network than your own equipment?
3. Does every technician have their own login?
   - Do you give logins to your subcontractors? If so, does every person there have their own login?
4. Can we approve each connection before it is opened?
5. Can you show who connected, when and for how long?
6. What happens to the access when a technician leaves your company?
7. How long does the equipment get security updates?

Good answers

- We only connect when you have a job for us.
- Every technician has their own login, including at our subcontractors.
- We only reach our own equipment.

Warning signs

- We have an open port. It has always worked.
- All technicians use the same password.
- The subcontractor uses our account.
- We do not know.

Read about secure remote access without open ports

Protect the equipment in the store

Refrigeration

The controller shows temperatures, sends alarms and runs the defrost cycle.

Cameras

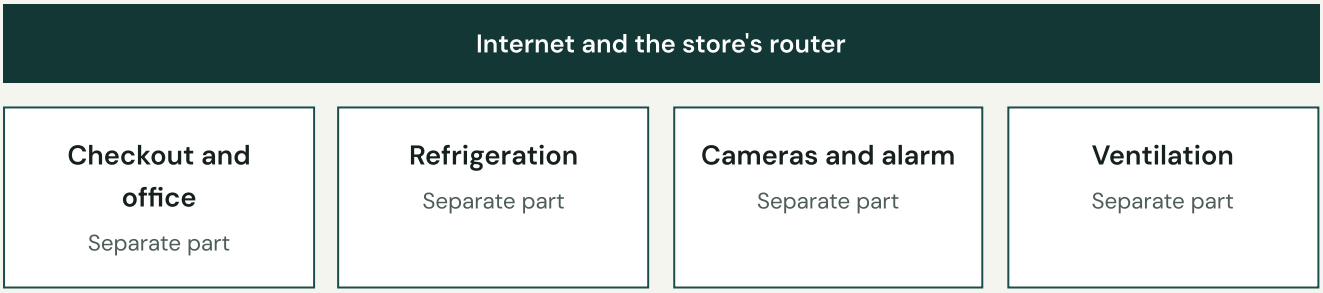
Cameras often have factory passwords and old software. An attacker can use them to spy.

Alarms, access and ventilation

The alarm company or a service company often manages them remotely. Ask how, and who has access.

Divide the network

If everything is on the same network, an attacker who gets into a camera can reach the checkout. So divide the equipment into separate parts. Each part reaches only what it needs. Read about dividing the network



What to do

- Ask your suppliers if any equipment can be reached from the internet. The answer should be no.
- Ask how long the equipment gets security updates.
- Change the factory password on all equipment.
- Ask the IT supplier to divide the network. Give customers a separate wireless network.
- Make sure alarms reach someone around the clock, also at weekends.

OLD EQUIPMENT?

Some equipment has had no security updates for years. Protect it until you can replace it.

THINK ABOUT IT

If someone takes over a camera, what else on your network can they reach?

If a system stops working or something seems wrong

1. **Find out what is affected.** The checkout, the cameras, the alarm, the refrigeration or something else?
2. **Call the supplier's emergency line.** Tell them what you see and when it started.
3. **Close remote access** together with the supplier, until you know what has happened.
4. **Document.** Write down what happened, when it happened and which goods you threw away. Take photos. Your insurer will need the evidence.
5. **Protect the goods.** Check the temperatures with a thermometer. Throw away goods that have been too warm. Follow your food safety routines.
6. **Report the attack to the police.** In Sweden, use polisen.se or call 114 14.
7. **Report the incident** to your national CSIRT. In Sweden, that is CERT-SE at cert.se.
8. **Tell the chain and your insurer.** Other stores may also be affected.

Prepare now

Fill in the list and put it up where staff can see it.

Contact	Name	Phone
Refrigeration contractor, emergency line		
IT supplier		
Checkout supplier		
Alarm company		
Contact at the chain		
Insurer		

Words to know

Controller	A small computer that runs, for example, the refrigeration system.
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.
Factory password	The password the equipment has when it is delivered. It can often be found on the internet.
Router	The device that connects the store's network to the internet.
Security update	New software that fixes flaws an attacker could exploit.
Dividing the network	Splitting the network into separate parts so that an attack does not spread.
Incident	An event that disrupts or damages your systems, for example an attack.
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.
polisen.se	The Swedish Police. Phone 114 14, or 112 in an emergency.
livsmedelsverket.se	The Swedish Food Agency, on the cold chain and food safety.

How Xertified can help

We put a lock in front of each connected device. The device is invisible to anyone without permission. A supplier gets access to the right device for a set time, and you see who was connected. You do not need to replace the equipment.

xertified.com/industries/grocery-retail · info@xertified.com · +46 18 265 06 06

Book a meeting or a demo