

BROSCHYR · NOVEMBER 2026

FÖR DIG SOM DRIVER EN BUTIK · DAGLIGVARUHANDEL

Håll butiken öppen. Håll digitalt obehöriga ute.

En handbok i grundläggande cybersäkerhet för kassa, kameror, kyla och annan uppkopplad utrustning i butiken.

XERTIFIED AB · UPPSALA

XERTIFIED.SE

Din butik är full av små datorer

Kassan, kamerorna, kylan och larmet är uppkopplade. I dem sitter små datorer som du sällan ser. Många av dem går att nå på distans, ofta av fler än du tror.

Angrepp mot sådan utrustning blir vanligare. En angripare kan stoppa kassan, se genom kamerorna eller stänga av kylan. För en butik kan det betyda stängda dörrar och varor som du måste slänga.

Den här broschyren hjälper dig att skydda den uppkopplade utrustningen i din butik. Du behöver inte vara tekniker. Det mesta handlar om att ställa rätt frågor till rätt person. Små steg gör stor skillnad.

Så använder du broschyren

Steg 1

Gå igenom checklistan

Sidan 4 har åtta vanor. Börja med dem.

Steg 2

Fyll i inventeringen

På sidan 5 skriver du upp din utrustning och dina leverantörer.

Steg 3

Läs om din utrustning

Sidorna 6 till 8 handlar om ansvar, leverantörer och utrustning.

Steg 4

Spara broschyren

Ta fram den när du byter leverantör eller utrustning.

GÖR DET HÄR I DAG · TRE SAKER PÅ 15 MINUTER

1. **Sätt upp journumren.** Skriv upp numren till kylentreprenören, it-leverantören och larmföretaget där personalen ser dem.
2. **Ring en leverantör.** Fråga hur de når din utrustning på distans, och vem hos dem som kan göra det.
3. **Kontrollera routern.** Fråga it-leverantören om fabrikens lösenord är bytt på routern och det trådlösa nätverket.

Allt som är uppkopplat kan angripas

En butik har många system som är anslutna till nätverket. Vart och ett kan bli en väg in för en angripare. Om ett system stannar kan det påverka hela butiken.

Kassasystem

Utan kassa kan du inte sälja något.

Kameror

En angripare kan se in i butiken eller ta sig vidare i nätverket. Läs om kameror

Kyl och frys

Ett fel kan tvinga dig att slänga varor.

Planeringssystem

Schema, beställningar och leveranser kan stanna.

Passersystem och larm

Dörrar och larm kan sluta fungera.

Ventilation och värme

Ett serviceföretag sköter dem ofta på distans.

Så brukar angripare lyckas

- **Utrustningen syns på internet.** Angripare söker hela tiden efter utrustning som svarar.
- **Programvaran är gammal.** Den har inte fått säkerhetsuppdateringar på flera år.
- **Fabrikens lösenord sitter kvar.** Sådana lösenord går ofta att hitta på internet.
- **Leverantörer delar inloggningar.** Ingen vet längre vem som har tillgång.
- **Allt sitter i samma nätverk.** Från en kamera når angriparen kassan.
- **Ingen märker något.** Ingen ser vem som ansluter eller när.

LÄRDOMEN

Det som syns på internet kan angripas. Utrustning som inte får uppdateringar blir lättare att angripa för varje år.

Läs varför uppdateringarna inte hinner med

Åtta vanor för en säkrare butik

Börja här. Varje vana gör det svårare för en angripare att ta sig in i din butik.

01

Vet vad som är uppkopplat

Gör en lista över all utrustning som är ansluten till nätverket eller till internet.

02

Inget ska nås från internet

Be dina leverantörer kontrollera att ingen enhet går att nå direkt från internet.

03

Byt fabrikens lösenord

Varje enhet ska ha ett eget, starkt lösenord. Dela inte lösenord mellan leverantörer.

04

Uppdatera eller skydda

Fråga hur länge utrustningen får säkerhetsuppdateringar. Skydda utrustning som inte får några längre.

05

Fjärråtkomst bara vid behov

Leverantören ska bara komma in när det finns ett ärende, och bara till sin egen utrustning.

06

Dela upp nätverket

Kassan, kontoret, kylan och kamerorna ska inte sitta i samma nätverk.

07

Se vem som har varit inne

Be leverantörerna visa vem som anslöt, när och varför.

08

Ha en plan

Skriv ned vem du ringer och vad du gör om ett system slutar fungera.

Tips: Ta med checklistan nästa gång kylentreprenören eller it-leverantören är i butiken. Gå igenom den tillsammans.

Inventera utrustningen i din butik

Skriv upp den utrustning som är uppkopplad. Fråga leverantören om du inte vet svaret.

Utrustning	Leverantör och telefon	Går att nå från internet?	Får uppdateringar?
Kylanläggning			
Kyl- och frysrum			
Ventilation och värme			
Kameror			
Larm och passersystem			
Kassasystem			
Planeringssystem			
Router eller modem			
Annat:			

Hur säker är din butik?

Påstående	Bra	Okej	Inte än
Jag vet vilken utrustning som är uppkopplad.	☐	☐	☐
Ingen utrustning går att nå direkt från internet.	☐	☐	☐
Fabrikens lösenord är bytta.	☐	☐	☐
Jag vet vilka leverantörer som har fjärråtkomst.	☐	☐	☐
Jag har en plan om ett system slutar fungera.	☐	☐	☐

Börja med det du har kryssat i under Inte än.

Vem ansvarar för vad?

Du äger kanske butiken men inte kassasystemet eller nätverket. Det kan kedjan, fastighetsägaren eller en leverantör sköta. Ta reda på vem som ansvarar för varje system.

Då vet du vem du ska fråga, och vem du ska ringa när något händer. Kryssa i vem som ansvarar.

System	Butiken	Kedjan	Fastighetsägaren	Leverantör
Nätverk och router	☐	☐	☐	☐
Kassasystem	☐	☐	☐	☐
Kyl och frys	☐	☐	☐	☐
Kameror och larm	☐	☐	☐	☐
Passersystem	☐	☐	☐	☐
Ventilation och värme	☐	☐	☐	☐
Planeringssystem	☐	☐	☐	☐

> **Skriv in det i avtalet.** Kom överens om vem som byter lösenord, installerar uppdateringar och stänger fjärråtkomsten när ett uppdrag är slut.

Försäkringen

Allt fler försäkringsbolag frågar hur du skyddar dina system. Vissa försäkringar kräver ett grundläggande skydd för att betala ut ersättning.

- Läs villkoren, eller fråga ditt försäkringsbolag vad som gäller för dig.
- Fråga om försäkringen täcker varor som du måste slänga och försäljning som du förlorar efter ett it-angrepp.
- Spara checklistan, inventeringen och den här tabellen. De visar vad du har gjort.

Leverantörer som når butiken på distans

Kylentreprenören, ventilationsfirman och larmföretaget behöver ofta nå sin utrustning. Då går det snabbare att hitta och laga fel. Men en angripare kan också använda varje väg in.

Frågor att ställa till dina leverantörer

1. Hur når ni vår utrustning? Via en öppen port, ett delat konto eller en säker anslutning?
2. Kan ni nå något annat i vårt nätverk än er egen utrustning?
3. Har varje tekniker en egen inloggning?
    - Delar ni ut inloggningar till era underleverantörer? Har i så fall varje person hos dem en egen inloggning?
4. Kan vi godkänna varje anslutning innan den öppnas?
5. Kan ni visa vem som anslöt, när och hur länge?
6. Vad händer med åtkomsten när en tekniker slutar hos er?
7. Hur länge får utrustningen säkerhetsuppdateringar?

Bra svar

- Vi ansluter bara när ni har ett ärende.
- Varje tekniker har en egen inloggning, även hos våra underleverantörer.
- Vi når bara vår egen utrustning.

Varningstecken

- Vi har en öppen port. Det har alltid fungerat.
- Alla tekniker använder samma lösenord.
- Underleverantören använder vårt konto.
- Vi vet inte.

Läs om säker fjärråtkomst utan öppna portar

Skydda utrustningen i butiken

Kyl och frys

Styrenheten visar temperaturer, skickar larm och styr avfrostningen.

Kameror

Kameror har ofta fabrikens lösenord och gammal programvara. En angripare kan använda dem för att spionera.

Larm, passersystem och ventilation

Larmföretaget eller ett serviceföretag sköter dem ofta på distans. Fråga hur, och vem som har åtkomst.

Dela upp nätverket

Om allt sitter i samma nätverk kan en angripare som tar sig in i en kamera nå kassan. Dela därför upp utrustningen i skilda delar. Varje del når bara det den behöver. Läs om att dela upp nätverket

Internet och butikens router

Kassa och kontor	Kyl och frys	Kameror och larm	Ventilation
Egen del	Egen del	Egen del	Egen del

Så här gör du

- Fråga leverantörerna om någon utrustning går att nå direkt från internet. Svaret ska vara nej.
- Fråga hur länge utrustningen får säkerhetsuppdateringar.
- Byt fabrikens lösenord på all utrustning.
- Be it-leverantören dela upp nätverket. Ge kunderna ett eget trådlöst nätverk.
- Se till att larmen når någon dygnet runt, också på helger.

GAMMAL UTRUSTNING?

En del utrustning har inte fått säkerhetsuppdateringar på många år. Den behöver ett skydd framför sig tills du kan byta ut den.

TÄNK EFTER

Om någon tar över en kamera, vad mer kan den nå i ditt nätverk?

Om ett system slutar fungera eller något verkar fel

1. **Ta reda på vad som påverkas.** Kassan, kamerorna, larmet, kylan eller något annat?
2. **Ring leverantörens jour.** Berätta vad du ser och när det började.
3. **Stäng fjärråtkomsten** tillsammans med leverantören, tills ni vet vad som har hänt.
4. **Dokumentera.** Skriv ned vad som hände, när det hände och vilka varor du slängde. Ta bilder. Försäkringsbolaget behöver underlaget.
5. **Skydda varorna.** Kontrollera temperaturerna med en termometer. Släng varor som har varit för varma. Följ butikens egenkontroll.
6. **Polisanmäl** angreppet på polisen.se eller på telefon 114 14.
7. **Rapportera incidenten** till CERT-SE på cert.se.
8. **Berätta för kedjan och försäkringsbolaget.** Andra butiker kan också vara drabbade.

Förbered dig redan nu

Fyll i listan och sätt upp den där personalen ser den.

Kontakt	Namn	Telefon
Kylentreprenörens jour		
It-leverantör		
Kassaleverantör		
Larmföretag		
Kedjans kontakt		
Försäkringsbolag		

Ord att kunna

Styrenhet	En liten dator som styr till exempel kylanläggningen.
Fjärråtkomst	När någon når utrustningen på distans, via nätverket.
Öppen port	En öppning i routern som släpper in trafik från internet.
Fabrikens lösenord	Lösenordet som utrustningen har när den levereras. Det går ofta att hitta på internet.
Router	Den apparat som kopplar butikens nätverk till internet.
Säkerhetsuppdatering	Ny programvara som rättar fel som en angripare kan utnyttja.
Dela upp nätverket	Att dela nätverket i skilda delar så att ett angrepp inte sprids.
Incident	En händelse som stör eller skadar dina system, till exempel ett angrepp.
Egenkontroll	Butikens egna rutiner för att maten ska vara säker.

Mer information

cert.se	Sveriges nationella funktion för it-incidenter. Här rapporterar du en incident.
ncsc.se	Nationellt cybersäkerhetscenter. Råd och stöd om cybersäkerhet.
polisen.se	Polisanmälan. Telefon 114 14, vid akut fara 112.
livsmedelsverket.se	Regler om kylkedjan och egenkontroll.
krisinformation.se	Information vid större störningar i samhället.

Så kan Xertified hjälpa

Vi sätter ett lås framför varje uppkopplad enhet. Enheten syns inte för den som saknar behörighet. Leverantören får åtkomst till rätt enhet under en bestämd tid, och du ser vem som var inne. Du behöver inte byta ut utrustningen.

xertified.se/branscher/dagligvaruhandel · info@xertified.com · 018-265 06 06

Boka ett möte eller en demo