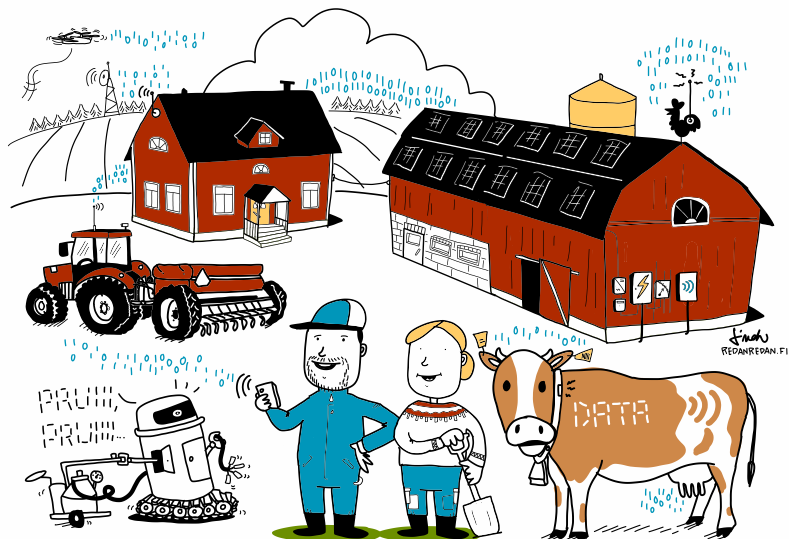


CYBERGUIDE FÖR LANTGÅRDAR



ARBETSGRUPP

Markus Lassheikki

Juha Niemi

Jussi Nikander

Mikko Laajalahti

Kalle Luukkainen

Panu Moilanen

Juha Mantila

Ossi Hietala

Jarkko Ilomäki

Juha Nuutila

Tuomo Tikkanen

Jussi-Pekka Kotilainen

ILLUSTRATIONER

Linda Saukko-Rauta

Redanredan Oy

LAYOUT

Ossi Hietala

UTGIVARE

Jyväskylä universitet och
Försvarsutbildnings-
föreningen MPK 2018

TRYCKERI

Sata-Seri, Raumo

ISBN

978-951-39-7973-7 (tryckt)

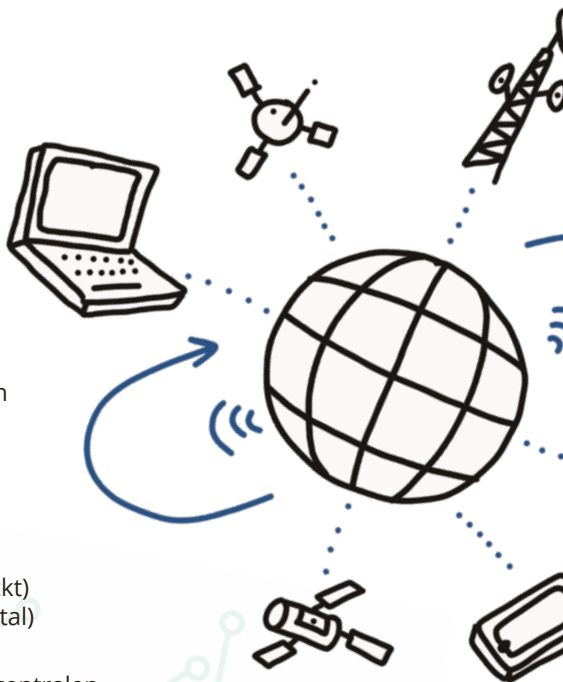
978-951-39-7974-4 (digital)

MÖJLIGGÖRARE

Försörjningsberedskapcentralen
ICT-Suomi ry

CREATIVE COMMONS -LICENS

Denna guide publiceras under
CC BY-NC-ND 4.0 -licensen.



VARFÖR BEHÖVS CYBERSÄKERHET PÅ LANTGÅRDAR?

Cybervärlden har även nått gårdarna genom datasystem och automation.

Datasystemen är idag en organisk del av lantbrukens verksamhet. Utan datasystem fungerar inte gården. Boskapsdjurens välfärd är beroende av att all utrustning fungerar, till exempel ventilation, utfodring, tillförsel av vatten och mjölkning av kor. Utrustningen innehåller datateknik och står oftast i förbindelse med olika informationssystem via internet. Detta gör att också lantbruken utsätts för hot från cybervärlden via internet.

Vid lantbruken skapas mängder av värdefull information som bör lagras på ett säkert sätt. Informationen bör bevaras och skyddas mot obehörig åtkomst eller missbruk.

Lantbrukens investeringar är ofta långfristiga. Redan i början av upphandlingen är det viktigt att försäkra sig om att utrustningen och systemen fungerar som förväntat, är kompatibla med gårdens övriga utrustning och är informationssäkra.

Lantbruksproduktionen är viktig för Finlands försörjningsberedskap.

Målet med denna guide är att ge dig praktisk information och råd så att du bättre kan beakta cybervärldens utmaningar och möjligheter i vardagen på lantbruket.

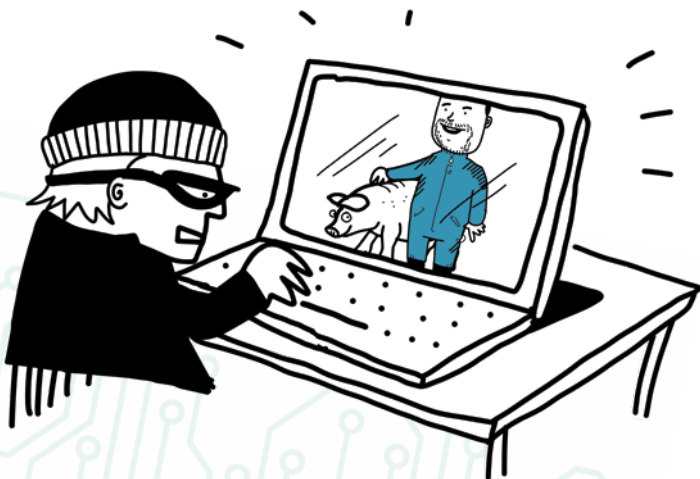
Utöver denna guide rekommenderar vi att du också läser [CYBERGUIDEN: VAD DU BEHÖVER VETA OM CYBERVÄRLDEN](#) som getts ut av Försvarsutbildningsföreningen (MPK) och Jyväskylä universitet.

CYBER- OCH INFORMATIONSRISKER PÅ LANTGÅRDAR

Cyberriskhanteringen börjar med att göra sig medveten om riskerna. De cyberhot som oftast påverkar lantgårdar är störningar orsakade av väder och misstag som gårdens egen personal gör.

Då elavbrott vid t.ex. oväder slår ut utrustning måste man kunna starta om den. Åskväder och vattenskador kan dessutom förstöra utrustning. Den kan också gå sönder av andra orsaker, till exempel kan gnagare orsaka överraskande fysiska skador.

Användarna kan av misstag göra skador vilka kan leda till större problem, särskilt i ett dåligtplanerat cybersystem. Alltid då man gör ändringar i datasystemen är det viktigt att förstå och dokumentera vad man gör, så att man inte av misstag orsakar problem för sig själv. Det är också klokt att vara aktsam när man ber om hjälp som berör datasystemen. Den hjälp man anlitar





skall kunna sin sak och känna till gårdens cybermiljö. Också en sakkunnig kan göra misstag i en obekant miljö.

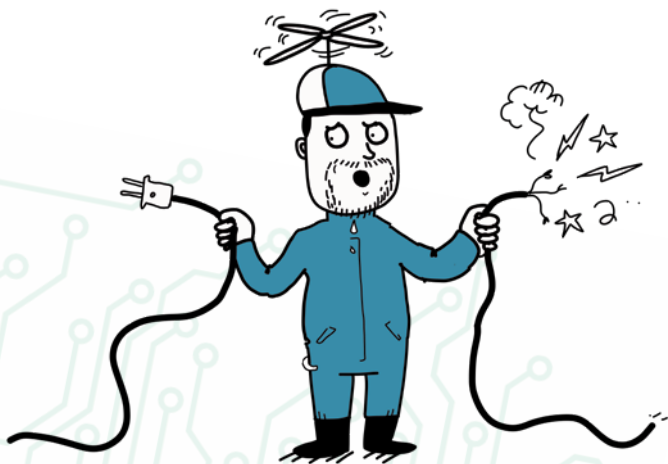
Lantbruk kan också bli utsatt för cyberattacker av flera slag. Alltid är det inte gården själv som är målet för attacken. Exempelvis kan ett skadligt program av en slump komma åt att tränga sig in i gårdens datasystem om de ej är tillräckligt skyddade. Naturligtvis kan gården också vara mål för en cyberattack. Då kan exempelvis bildmaterial från övervakningskameror i byggnader avsedda för djur vara av intresse för obehöriga.

Det är också klokt att överväga vad man själv berättar om gården i olika sociala medier. Det är lätt att saker tas ur sitt sammanhang, särskilt när det gäller frågor som delar åsikter, till exempel bildmaterial man själv lagt ut kan också försöka användas mot gården.

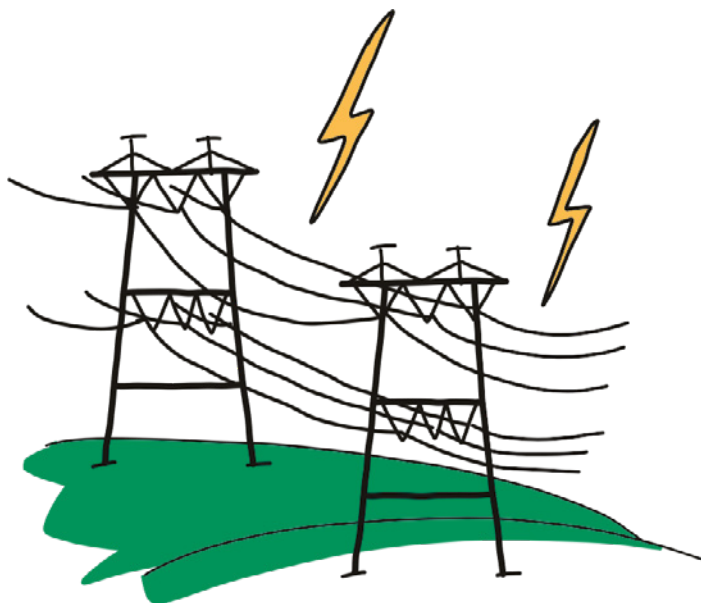
ELTILLFÖRSEL OCH ELSÄKERHET: ALLT ÄR BEROENDE AV EL!

Cyberutrustning behöver el för att fungera, och för att fungera pålitligt krävs el av god kvalitet. På landsbygden är elavbrott och spänningsvariationer att räkna med. Med hjälp av utrustning för avbrottsfri kraft (UPS) kan datautrustningen skyddas mot elavbrott och spänningsvariationer. Elnätet skall förses med överspänningsskydd i flera steg för att uppnå en hög skyddsnivå. Elsäkerhetsföreskrifterna ger goda grunder också för en cybersäker verksamhet. Med tanke på datanätets funktion är det viktigt att kablarna installeras korrekt och att teknikrum jordas rätt, så att de har samma potentialnivå som den övriga utrustningen. Vid en elsäkerhetsbesiktning är det bra att också granska datanätverkets funktionsnivå.

Dimensionera reservelverk (aggregat) för att hålla igång produktionen i olika driftförhållanden. Ett aggregat med bräns-



lemotor ger betryggande effekt. Vid lång kontinuerlig drift av aggregatet är bränsleförbrukningen emellertid betydande. Vid dimensionering av ett reservverk är det klokt att eftersträva en betryggande effektmarginal samt begränsa drifttiden för att minimera bränsleförbrukningen. Detta innebär att all inkopplad viktig utrustning skall kunna drivas av reservverket samtidigt. Exempelvis vid mjölkningsdags skall man kunna kyla mjölken, få varmt tvättvatten och ladda utrustningens batterier. Reservkraften skall nå ut till all kritisk utrustning på gården.



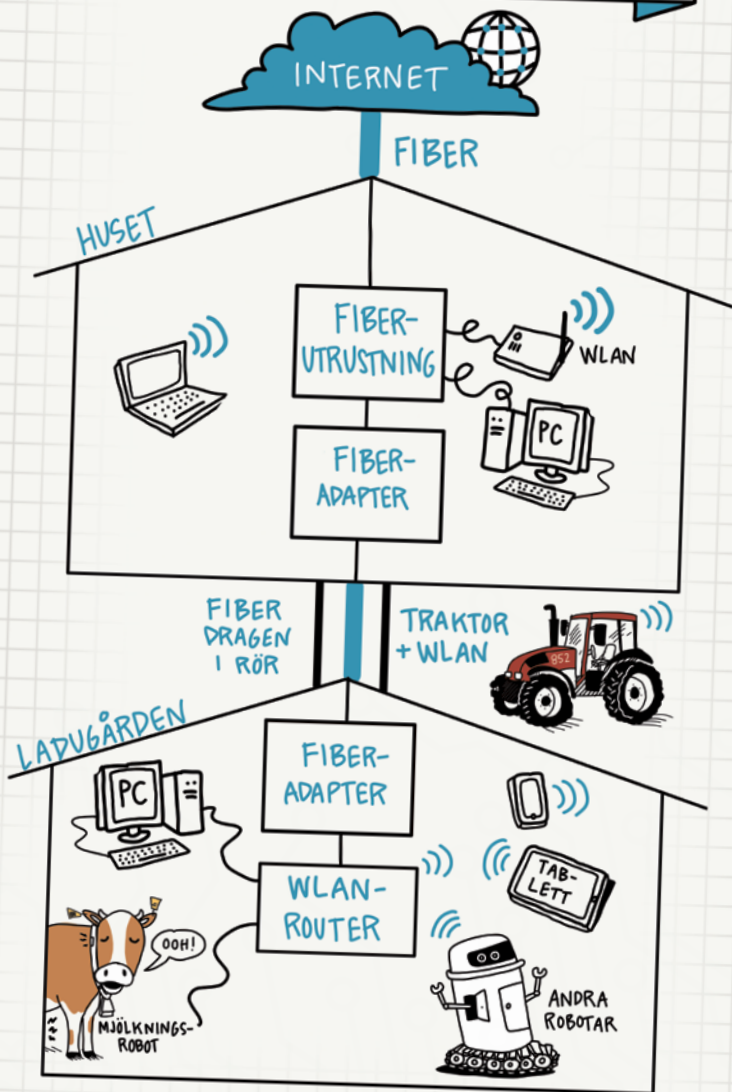
DATAFÖRBINDELSER OCH DATANÄT

Vid planeringen av datanät för ett lantbruk är det viktigt att säkerställa att nätet kan nås från alla tänkta platser. I byggbestämmelserna finns detaljerade anvisningar om planering av datanätverk för bostadsbyggnader. En viktig sak är att alla bostadsrum förses med generellt datakabelnät. Samma anvisning kan tillämpas i produktionsbyggnader; det ska finnas tillräckligt många nätslutningspunkter i de utrymmen där utrustning kommer att placeras. Mellan byggnader är det bra att installera skäligt stora kabelkanaler (110 mm), också för kommande behov, en separat kanal för datakablage och en för elkablar. Datakabel av koppar med längder över 100m kräver förstärkare. Mellan byggnader rekommenderas fiberoptisk kabel för en störningsfri funktion.

Det lönar sig att dokumentera nätverkens uppbyggnad. Vid nybygge ingår dokumentationen som en del av elplanen. Lantgårdens datanät kan dokumenteras enkelt i en skiss där apparater ritas som en rektangel och kabelanslutningar som linjer mellan dessa. En dylik enkel skiss är alltid till stor hjälp då man utreder problem i datanätet då utrustning och kablage kan lokaliseras och identifieras.

Datanätet på en lantgård består av ett lokalt nätverk, som kan vara kablat med koppar eller fiber (LAN) eller vara trådlöst (WLAN). Nätet kan stå i förbindelse med internet över mobil förbindelse (2G, 3G, 4G, 5G) eller över fast förbindelse på ett flertal olika sätt. Utrustning, maskiner och fordon har också interna nätverk, t.ex. CAN- och ISOBUS-system, som ofta också kommunicerar över externa nätverk med olika tjänster. Datanäten på ett lantbruk bör innehålla brandväggar. En brandvägg är en separat apparat eller ett program i datorn för att inspektera och kontrollera kommunikation med datorer kopplade till datanätet. Brandväggarna skall konfigureras så att de tillåter endast önskad trafik mellan datorer och blockera övrig trafik. Alla sådana förbindelser skall också i sig skyddas bra.

SKISS ÖVER GÄRDENS DATANÄT 11/2018

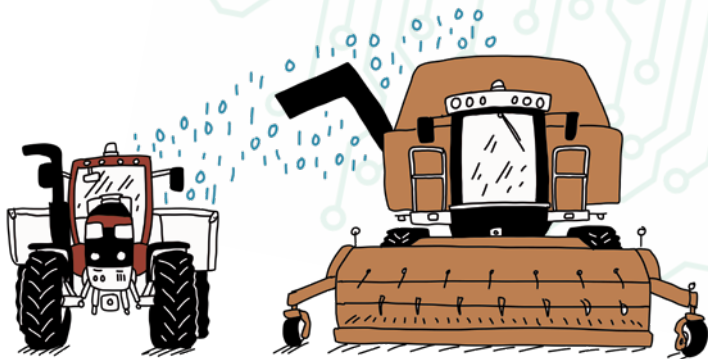


GÅRDENS INTERNA OCH EXTERNA SYSTEM

Vid gården skapas mängder av värdefull information som också kan intressera obehöriga. Denna information används för styrning av produktionen och för kommersiell certifiering av produkter. Vid upphandling av ett system eller tjänst är det viktigt att försäkra sig om vem som äger och vem har rätt att nyttja all information och att alla parterers rättigheter respekteras. Den information lantgården äger skall med hjälp av ändamålsenliga redskap också kunna utnyttjas. Företagarens skall också vara medveten om för vilka ändamål informationen vidareanvänds till. Information som skapats på lantgården kan vara konfidentiell och desutom innehålla information enligt EU:s dataskyddsförordning GDPR, och skall då hanteras rätt.

Datorer och datanät har redan länge ingått i infrastrukturen på lantgårdar. Många dagligen använda program/applikationer börjar finnas för smarttelefoner och annan mobil utrustning. Vid uppkoppling från smarttelefon bör man försäkra sig att uppkoppling mot gårdens interna datanät och datorer, antingen via gårdens nätverksanslutning eller via det lokala trådlösa nätverket sker på ett säkert sätt.





Lantbrukens internetabonnemang har ofta liknande egenskaper som ett vanligt konsumentabonnemang där internetoperatören erbjuder vissa grundläggande informationssäkerhetslösningar för abonnemanget. Vid behov att externt via internet nå lantbrukets utrustning, exempelvis övervakningskameror eller övervakning och styrning från smarttelefon, bör internetanslutningen öppnas på ett säkert sätt. Internetoperatören överför vanligen då ansvaret till abonnenten. Anslutningen bör senast då förses med en ändamålsenlig brandvägg för att skydda förbindelsen.

En modern lantbrukstraktor med CAN-buss och ISOBUS-utrustning utgör ett självständigt datasystem med mätutrustningen som samlar traktorns driftinformation. Traktortillverkarna samlar också in information för produktutvecklingen och underhåll av traktorn. Utrustningen är konstruerad för att vara säker. Styrningen kan emellertid påverkas av annan utrustning som ansluts till traktorns databuss. Sådan utrustning skall alltid ses som eventuell säkerhetsrisk. ISOBUS är avsedd erbjuda en trygg anslutning av extern utrustning till traktorn.

Med fastighetsautomation menas styrning av bland annat ventilation och belysning.. Behovet att ansluta fastighetsautomationen till internet uppstår då man väljer fjärrövervakning och -styrning av fastigheten. Det är viktigt att försäkra sig om att internetanslutningen är skyddad mot obehörig användning från Internet.

Cyber- och informations-
risker på lantbruken

4

Elförsörjning och
elsäkerhet

6



Trygg identifiering och
goda lösenord

16

Säkerhetskopiering av infor-
mationen ger trygghet

1

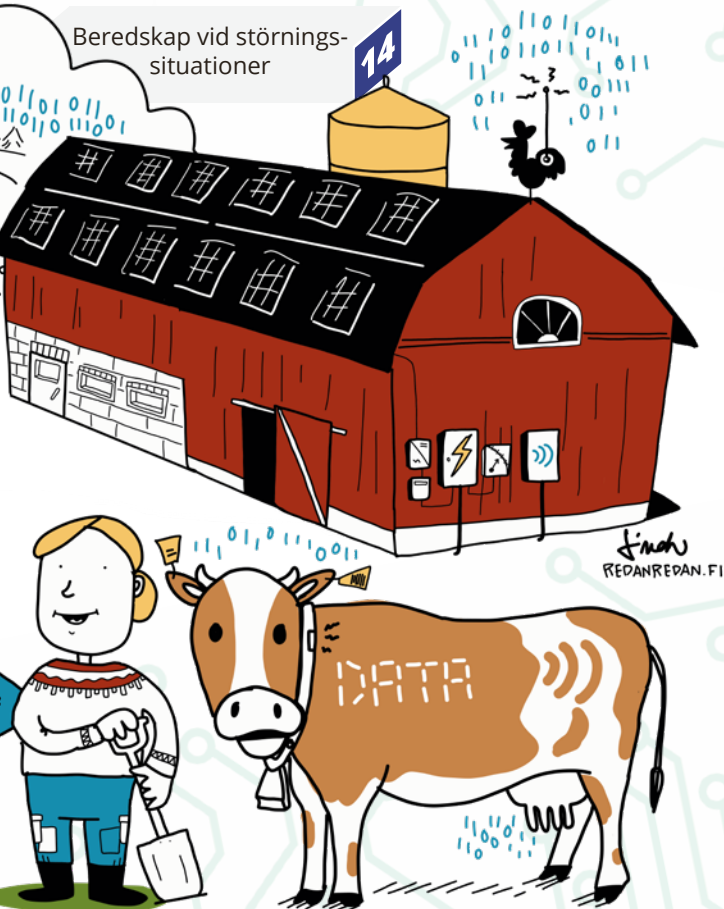
Dataförbindelser och
datanätverk

8

Lantbrukets interna
och externa system

10

Beredskap vid störnings-
situationer



Är dina anskaffningar
cybersäkra?

20

Uppdateringar
bästa skyddet

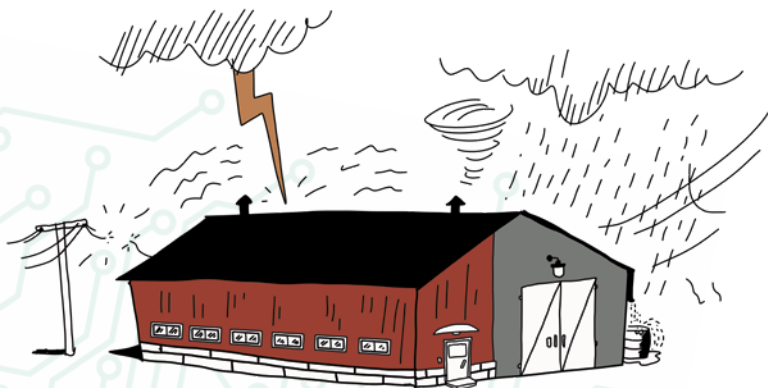
22

HUR FÖRBEREDA SIG FÖR OLIKA STÖRNINGAR

Störningar i datasystemen är alltid föargliga. Störningar kan också orsaka betydande ekonomiska förluster eller direkt fara. Följderna av störningar varierar, lantbruket kan påverkas antingen genast eller först efter en tid. Genom att göra beredskapsförberedelser höjer man lantbrukets kristolerans och gör att det går lättare att snabbare att återhämta sig efter en störning.

När en störning inträffar vet man sällan hur länge den kommer att vara, hur omfattande den är och orsaken till den. Ovissheten tär på trygghetskänslan. För att minska stress vid störningar bör man göra upp planer på hur man kan förbereda sig och hur man kan klara av olika störningar. Man kan till exempel göra upp detaljerade checklistor för olika typer av störningar och hur man då bör agera.

Störningar i eldistributionen märks omedelbart då utrustningen slocknar. Elavbrott kan vara mycket korta, men de kan också pågå i flera timmar, dagar och i värsta fall veckor. Snabba spän-





ningsspikar kan slå ut och skada utrustning. Elavbrott har också indirekta följder, till exempel att djur kan bli utan vatten om störningen drar ut på tiden.

Genom skötsel av skog intill kraftledningar och att utrusta sig med reservkraft och avbrottsfri kraft kan man gardera sig mot elavbrott. Med tanke på långvariga strömbavbrott är det bra att i förväg med bränsleleverantören avtala leverans av bränsle till gårdstanken och när den levereras. Genom att investera i avbrottsfri kraft (UPS) skyddar man känslig datautrustning mot störningar eller korta avbrott i den yttre eldistributionen.

Redan ett 3–5 timmar långt elavbrott stoppar data- och telefontrafiken i mobilnäten. Då fungerar inte längre övervakning och styrning på distans av utrustningen och ej heller orderhantering eller elektroniska myndighetsanmälningar. Fasta anslutningar är funktionssäkrare än mobilnäten vid strömbavbrott. Ett lokalt datasystem kan användas också när molnbaserade system och databaser inte är tillgängliga.

När man ingår avtal är det viktigt att tänka på att strömbavbrott och avbrott i datakommunikationen också kan påverka verksamheten hos samarbetspartners och tjänsteleverantörer utanför gården.

SÄKER IDENTIFIERING OCH BRA LÖSENORD

Gemensamma datorer på gården skall för varje användare ha personliga användarnamn och lösenord samt begränsad behörighet till program och tjänster. För installation och underhåll av program och för skapande av användarkonton sak det finnas ett särskilt administratörs- eller huvudanvändarkonto, som inte används för något annat ändamål. Det är viktigt att välja extra starka lösenord för administratörs och huvudanvändarkonton.

Tjänster där det krävs höga skyddsbehov, t.ex. e-post, molntjänster och djurregister, skall förses med starka lösenord. Fras-, bokstavs- och sifferkombinationer med över 15 tecken är starka lösenord. Bra lösenord kan man hitta på nära håll: till exempel är [RodValtraFramforHuset_852](#) ett starkt lösenord. Lösenordets längd är den huvudsakliga faktorn som ökar säkerheten. Vid behov kan man skapa ett kortare lösenord genom att kapa orden: [RoVaFrHu_852](#).

De viktigaste av rutinerna som ökar säkerheten i samband med lösenord och inloggningar är att alla har sina egna lösenord, att lösenorden är olika för olika tjänster, att de är tillräckligt långa och, om möjligt, att man använder tvåfaktorsautentisering





via sms, bankkod eller mobil-ID.

Den viktigaste datasäkerhetsrutinen är ändå användaren själv. Installera endast kända applikationer. Spara aldrig lösenord i datorns minne. Ge inte ditt personliga lösenord till någon.

E-postadressen är nyckeln till många tjänster, och med dess hjälp kan man byta lösenord och verifiera ett nytt lösenord. E-posten ska ha ett starkt lösenord som ska bytas regelbundet, till exempel varje halvår. För e-posten rekommenderas tvåfaktorsautentisering, så som verifiering via mobil-ID.

Använd aldrig ett och samma lösenord i flera olika system. Skapa olika varianter av lösenordet: [RodValtraFramforHuset_852](#), [RodValtraFramforLadan_852](#), [RodValtraNatbutiken_852](#) och så vidare. Användningen av lösenord kan underlättas med hjälp av särskilda lösenordshanterare.

SÄKERHETSKOPIERING TRYGGAR INFORMATIONEN

Säkerhetskopiering av lantbrukets information kräver planering och kan kartläggas med hjälp av tre grundfrågor: Vilken typ av information finns på gården och i vilket format? Vad är värdet av respektive information? Vilken är hotbilden om informationen går förlorad?

Bilder kan ha ett stort känslovärde, men har ett annat penningmässigt värde jämförelse med lantbruksföretagets bokföringsmaterial. Krav på säkerhetskopiering och återställning beror på hur kritisk informationen är, hur mycket lagringsutrymme behövs och hur ofta kopiering skall ske. Hotbilder är t.ex. att utrustningen går sönder eller byts ut, brand, blixtnedslag, stöld, dataintrång och nätverksproblem.

Det enklaste sättet att säkerhetskopiera mobiltelefoner och surfplattor är att använda deras egna molntjänster. Det oftast avgiftsfria lagringsutrymmet i molntjänsten räcker till för säkerhetskopiering av inställningar och kontaktinformation, extra utrymme kan köpas för t.ex. bilder.

Informationen i datorerna på ett lantbruk består vanligen av material från verksamheten på gården. Informationen i e-posten kan lagras lokalt, om man inte har tillgång till webmail. Säkerhetskopieringen och återställning av nätverksapplikationer och nätverkstjänster sköts vanligen av tjänsteleverantören. Detta bör finnas beskrivet och finnas med i avtalet



med tjänsteleverantören.

Särskild uppmärksamhet bör ges säkerhetskopiering av information från och inställningar på automationssystem för produktion, t.ex. mjölkningsrobotar, för att det ska gå så lätt som möjligt att återställa dem efter en felsituation. En regelbunden säkerhetskopiering till USB-minnen eller kopia till plats på datanätet är god praxis.

Med tanke på total förstörelse, till exempel brand, är det bra att ha minst en kopia av viktig information lagrad utanför gården, t.ex. i en molntjänst. Dataöverföringen bör automatiseras, men också övervakas att den fungerar rätt.

En god princip är att kopiera den senaste uppdaterade informationen till flera enheter och i olika byggnader. Återställning av informationen skall i förväg planeras och också testas att det lyckas.

Det är viktigt att känna till var informationen från respektive applikation eller tjänst finns och om den kan nå ifall nätverksförbindelsen bryts.

Har du säkerhetskopierat din viktiga information?

Kan du återställa informationen från en säkerhetskopia?

Var förvarar du din viktiga information?

Vilken information finns **i molnet** och vilken finns **lokalt**?



ÄR DINA ANSKAFFNINGAR CYBERSÄKRA?

Anskaffning av utrustning börjar med planering enligt användningsändamålet. Valet av system har stor betydelse för verksamheten på gården, vare sig det rör sig om jordbruksmaskiner eller datateknisk utrustning. Det gäller också att beakta om utrustningen skall användas enbart lokalt eller för personligt bruk, eller skall den anslutas till gårdens ICT-helhet?

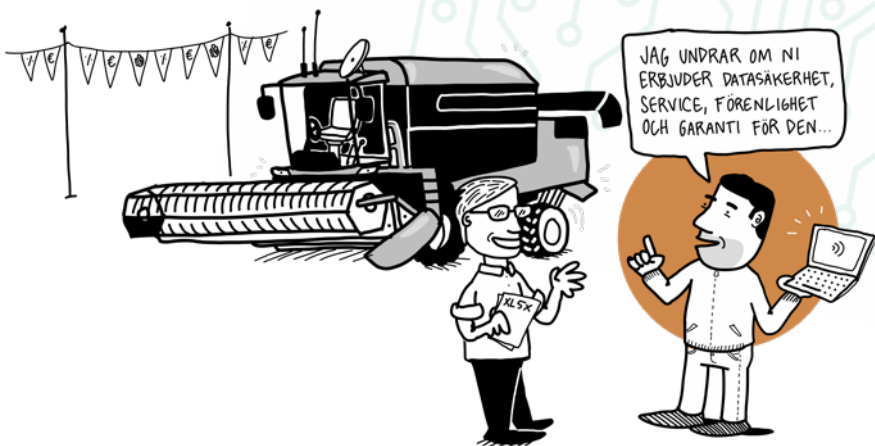
Vid större anskaffningar av maskiner eller utrustningar bör man klargöra vilket automationssystem produkten innehåller. Är systemet slutet eller är det kompatibelt med de befintliga systemen på gården? Det är bra att kartlägga villkor hur underhåll, service och reparationerna fungerar efter anskaffningen och till och med under en internationell krissituation.

Utrustningens användbarhet är av stor betydelse. Det är väsentligt hur utrustningen passar ihop med de övriga befintliga systemen. Hur lätt är det att använda information som finns i annan utrustning eller andra system, eller att dela ut information till

annan utrustning. Vid utdelning av information skall också informationssäkerheten tryggas, det vill säga vem som har behörighet till informationen i fråga.

När ett lantbruk växer från att vara ensamföretagare och blir större, skall man även överväga att övergå till datautrustning, applica-





tioner och tjänster som är avsedda för företag. Utrustning för konsumenternas hemmabruk och är endast avsedd för personligt bruk och har ej den service och tjänster som företagsverksamheten på lantbruket behöver. Utrustning tillverkad för företagsverksamhet kan ha bättre garantier och tjänster till exempel för att få service på utrustningen inom 1-2 dagar så att verksamheten kan fortsätta och informationen bevaras.

Vid anskaffningen och idriftsättning av utrustning lönar det sig att anlita sakkunniga som också förstår sig på lantbruksverksamheten. Det är ett omfattande projekt att överföra information från tidigare system, installera programvara och kringutrustning, specificera användarrättigheter, ansluta utrustningen till gårdens datanätverk, säkerställa informationssäkerheten och lägga upp säkerhetskopiering. En sakkunnig kan också ge handledning i hur utrustningens och programmets nya egenskaper används, vilket underlättar den dagliga verksamheten.

Cybersäkerhet och informationssäkerhet är viktiga saker för verksamheten på ett lantbruk. Det lönar sig att planera de här sakerna redan då man bygger upp ett system för behandling av lantbrukets information och tar i bruk ny utrustning, samt se över säkerheten årligen eller oftare.

UPPDATERING ÄR VIKTIGASTE SKYDDET

Det naturligaste sättet att slå vakt om lantbrukets informations-säkerhet och cybersäkerhet är att hålla gårdens alla system uppdaterade och därmed uppnå hög driftsäkerhet. Nyare datasystem och utrustning kontrollerar regelbundet om uppdateringar finns tillgängliga.

Många gårdar använder även äldre system, där användaren själv måste söka och göra uppdateringarna. Användaren måste känna till vilka åtgärder olika slags utrustning kräver för att hållas uppdaterad. Det gäller att se till, att även programvaran är uppdaterad som en del av underhållet av gårdens maskiner och utrustning.

Det är viktigt är att lägga upp planer på när utrustningen eller programvaran skall uppdateras eller förnyas. Datorutrustning har en typisk livslängd på 3–5 år under vilken tid reservdelar finns att få. Verksamheten på gården utsätts för betydligt mindre och kortvarigare störningar om man förnyar utrustningen innan den går sönder, eller om man har en klar handlingsplan hur utrustning som gått sönder ska ersättas. Att förbereda sig mot problem betalar sig igen den dag något går sönder!

En viktig del i gårdens cybersäkerhet är att använda brandväggar. En brandvägg inom datatekniken är ett program eller datautrustning som övervakar datatrafik och förbindelser som flyter genom den och tillåter endast behörig trafik att passera. Med hjälp av brandväggar kan man bygga skydd mot att bilder från övervakningskameror eller annan känslig information ej läcker ut utanför gårdens datanätverk. Dessutom kan brandväggar användas för att förhindra spridningen av skadliga program.

IT-kunskaper krävs för att installera och underhålla brandväggar, och därför är det bra att anlita en sakkunnig. Man kan också installera flera brandväggar och så dela gårdens datanät i mindre segment; till exempel en brandvägg som övervakar all nätverkskommunikation på gården och därtill separata brandväggar för alla viktiga datorer på gården för att skydda dessa.



VILL DU VETA MER?

Olika myndigheter och organisationer har ett stort utbud av webbsidor och webbmateriäl om cybersäkerhet. Där finns information och nyheter om läget i cybervärlden, också för lantbruk.

Kommunikationsverkets cybersäkerhetscenter
WWW.VIESTINTAVIRASTO.FI/KYBERTURVALLISUUS

Cyberguiden
URN.FI/URN:ISBN:978-951-39-7976-8

Kodin turvaopas: Kyberturvallisuus (på finska)
KODINTURVAOPAS.FI/KYBERTURVALLISUUS

Alkutuotannon kyberuhat (på finska)
JUKURI.LUKE.FI/HANDLE/10024/539088

Den här guiden kan laddas ned på adresserna:

- URN.FI/URN:ISBN:978-951-39-7974-4
- MPK.FI/KOULUTUKSET/KYBERTURVALLISUUS/

Bekanta dig också med Naturresursinstitutets, Försörjningsberedskapsorganisationens samt Centralförbundet för lant- och skogsbruksproducenters webbsidor:

LUKE.FI • HUOLTOVARMUUS.FI • MTK.FI

A!
Aalto-yliopisto



HUOLTOVARMUUSORGANISAATIO



JYU. Since 1863.



Mtech
DIGITAL SOLUTIONS



10 CYBERFRÅGOR FÖR LANTBRUK

JA

NEJ

1

Säkerhetskopierar du din information, även användarnamn och lösenord? Klarar du av att återställa informationen från säkerhetskopiering?

☐☐

2

Uppdaterar du systematiskt programvaran i all utrustning?

☐☐

3

Fungerar automationen på gården (ventilation, vatten, temperatur och utfodring) också vid strömavbrott eller när någon utrustning går sönder?

☐☐

4

Får du trycksatt vatten till mjölkningsroboten vid ett strömavbrott?

☐☐

5

Har du ordnat med reservkraft (aggregat) och bränsle till den?

☐☐

6

Har alla användare personliga och tillräckligt långa lösenord?

☐☐

7

Är hantering av personuppgifter säker? (se EU:s allmänna dataskyddsförordning, GDPR)

☐☐

8

Vet du vilka uppgifter tjänsteleverantörerna och systemen samlar in från gården? Kan du få dina uppgifter från tjänsteleverantören i användbar form?

☐☐

9

Utvärderar du cybersäkerheten och kompatibiliteten varje gång du skaffar ny utrustning?

☐☐

10

Har det gjorts upp en karta över gårdens datanätverk?

☐☐