Infopaket om jordbrukets cybersäkerhet

jamk | Jyväskylän ammattikorkeakoulu

Jord- och skogsbruks-ministeriet

Digitaliseringen för med sig nya hotbilder för gårdarna

I takt med att digitaliseringen av jordbruket tilltar blir gårdarna allt mer beroende av digitala tjänster och system. Samtidigt som många arbetsskeden förenklas när man inför nya system kan det också öka hoten som internet för med sig.

I infopaketet hittar du svar på följande frågor:

- Vad ska du tänka på när du utvecklar säkerheten i din digitala miljö?
- Hur ser ett mönsterjordbruk ut med tanke på cybersäkerheten?

Ett mönsterjordbruk ur cybersäkerhetens vinkel

Huvudbyggnad

- Man kan identifiera bedrägerier.
- Aktuella cyberhot följs upp på Cybersäkerhetscentrets webbplats.
- Företagets datorer är separata från de för hemmabruk.
- Antivirusprogram och bekämpning av sabotageprogram är i bruk.
- Spel och andra extra program har tagits bort från företagets enheter.
- Starka lösenord är i bruk för e-post och andra datasystem.
- Alla användare har egna användaruppgifter för de tjänster som behövs.
- Uppdateringar som installeras automatiskt är i bruk.
- VPN-förbindelse är i bruk.
- Reservåtgärder har planerats för undantagssituationer.
- Regelbunden säkerhetskopiering är i bruk och kopior förvaras på annan plats än originalet.
- UPS-reservströmkälla finns för datorer som styr/övervakar produktionen.
- Mobil reservförbindelse utöver fast internetanslutning finns.
- Man har flera sätt att identifiera sig i banken.
- Informationen behandlas på behörigt sätt (med beaktande av EU:s allmänna dataskyddsförordning GDPR).

Produktionslokaler

- Maskinparken har kartlagts och kritiska system identifierats.
- Kritiska system är säkrade med reservström.
- Man har övat på att starta om apparaterna.
- Man har funderat på hur man ska gå till väga om systemen är ur bruk.
- Utrustningen är fysiskt skyddad mot både olovlig användning och utmanande förhållanden.
- En plan har gjorts upp för underhåll och uppdatering av maskinerna, kontroll av fysisk kondition, förnyelse av föråldrade apparater/system.
- I upphandlingarna har man beaktat datasäkerheten och anordningarnas hållbarhet i utmanande förhållanden.

Gårdens datanät

- Det trådlösa nätverket använder en skyddad anslutning och ett starkt lösenord.
- Från internet syns endast nödvändig utrustning i lokalnätet.
- Nätet är uppdelat enligt apparatgrupp.
- Endast datasäkra nätverksenheter införskaffas.

Molntjänster

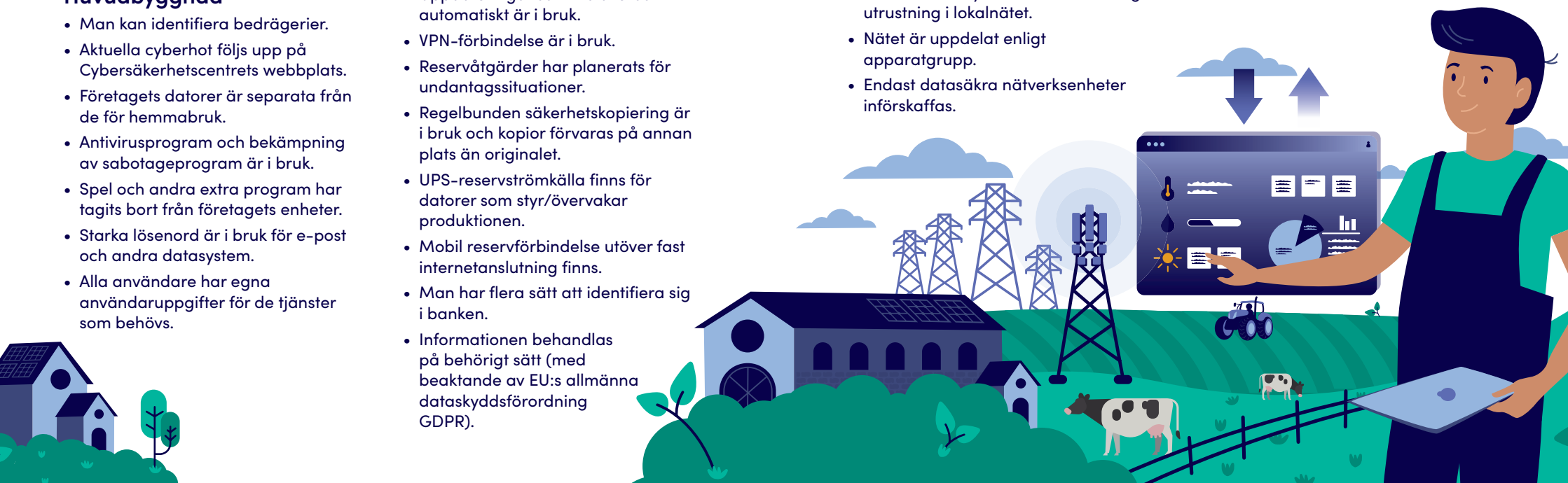
Vipu, Wisu, Wakka, Google Drive m.m.

- Starka lösenord är i bruk (skilda lösenord för varje tjänst).
- De viktigaste uppgifterna säkerhetskopieras till molnet.
- Man använder tjänster som identifieras som tillförlitliga.
- Multifaktorsautentisering används alltid när det är möjligt.

Givare och arbetsmaskiner

Näringshalts-, fukt- temperaturgivare, övervakningskameror, traktorer m.m.

- Via nätet når man apparaterna endast via datorer/smarta enheter som är avsedda för ändamålet.
- De ursprungliga lösenorden har bytts ut.
- Man har spärrat servicenummer i telefonabonnemangen.



Checklista för gårdarnas cybersäkerhet

I skick

- [ ] Satsa på cybersäkerhet, utbilda dig själv och andra anställda kring aktuella hot. Lär dig identifiera nätbedrägerier och kom ihåg att vara uppmärksam när du hanterar e-post, länkar och egna användaruppgifter.
- [ ] Använd starka lösenord, undvik att använda samma lösenord på olika konton och byt lösenord regelbundet.
- [ ] Ge inte dina egna användarnamn och lösenord till någon annan. Varje anställd får egna användaruppgifter enligt behov.
- [ ] Byt ut de lösenord som kommit som fabriksinställning mot starkare lösenord.
- [ ] Använd i mån av möjlighet multifaktorsautentisering.
- [ ] Uppdatera regelbundet användarrättigheterna och ta bort användaruppgifterna när arbetstagarens anställningsförhållande upphör.
- [ ] Använd skilda datorer och smarta enheter för att sköta företaget och för hemmabruk.
- [ ] Kontrollera att de trådlösa nätverk som används är skyddade med ett starkt lösenord.
- [ ] Kartlägg nätverksanslutna enheter och gör upp en plan för att uppdatera operativsystem, programvara och enheter så fort som möjligt när uppdateringarna blir tillgängliga. Följ tillverkarnas besked.
- [ ] Sträva till att förnya föråldrade system.
- [ ] Ta bort program och tjänster som inte är nödvändiga från apparaterna.
- [ ] Överväg att ta i bruk en VPN-förbindelse.
- [ ] Se till att datasäkerheten har beaktats när du skaffar ny utrustning. Välj med fördel enheter som har ett datasäkerhetsmärke.
- [ ] Skydda apparaterna fysiskt mot olovlig användning, men även i mån av möjlighet mot utmanande förhållanden.

- [ ] Identifiera kritiska funktioner och planera hur man ska gå tillväga om systemen inte fungerar, till exempel vilka arbeten som kan utföras manuellt.
- [ ] Säkerställ produktionsanläggningarnas reservkraft och vid behov tryckvattnet i händelse av elavbrott.
- [ ] Se också till att datorer som styr produktionen är kopplade till en reservströmkälla.
- [ ] Ha förutom en fast nätanslutning även en mobilanslutning som reserv.
- [ ] Organisera regelbunden säkerhetskopiering av data och förvara flera fysiska kopior på olika platser, såsom extern hårddisk, DVD, molntjänst. Säkerställ också att du kan återställa informationen från säkerhetskopior om situationen så kräver.
- [ ] Säkerställ att personuppgifter och andra känsliga uppgifter behandlas korrekt under hela deras livscykel.
- [ ] Installera och uppdatera regelbundet antivirusprogram och bekämpning av sabotageprogram, helst automatiskt.
- [ ] Om möjligt, ställ in e-postprogrammet så att bilder och länkar som meddelanden innehåller inte visas. *
- [ ] Fundera på förhand på kommunikationen i en undantagssituation.

Följande rekommenderade åtgärder kan kräva hjälp av en sakkunnig:

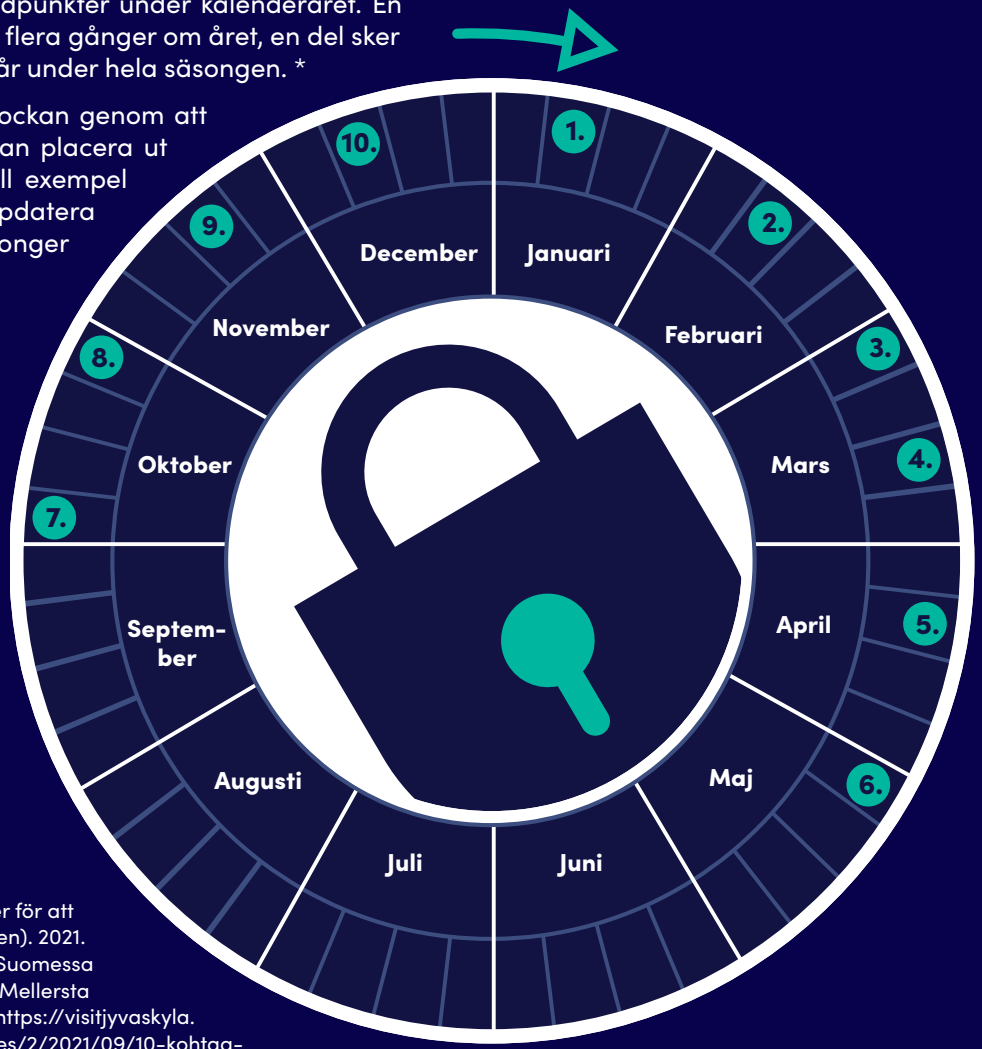
- [ ] Använd brandväggar, förhindra allt utom nödvändig trafik mellan det egna nätet och internet.
- [ ] Tillåt trafik till övervakningskamerasystem endast från nödvändiga IP-adresser.
- [ ] Genomför segmentering av nätet, förutsätt segmentering till exempel av leverantören då nya system installeras.
- [ ] Skapa endast en uppsättning användaruppgifter med administratörsrättigheter som används för att installera programvara. Skapa egna användaruppgifter som inte har administratörsrättigheter för alla användare, som är till för grundanvändning.
- [ ] Ta bort onödiga fjärrförbindelseprogram och RDP-portar som används för fjärranslutning.*
- [ ] Ta i bruk logginsamling och uppföljning av loggar. Tips: www.kyberturvallisuuskeskus.fi/sv/aktuellt/anvisningar-och-guider/sa-har-samlar-du-och-anvander-loggdata

* Källa: Ransomware Attacks on Agricultural Cooperatives Potentially Timed to Critical Seasons. 2022. Ett pressmeddelande från USA:s federala polis. Hänvisad till 6/2022. https://www.ic3.gov/Media/News/2022/220420-2.pdf

Årsklocka för cybersäkerhet

Gårdens årsrytm omfattar flera hektiska perioder. Åtgärderna för att säkerställa cybersäkerheten kan till stor del förläggas utanför dessa perioder. För detta ändamål kan en årsklocka göras upp, där åtgärderna indelas i lämpliga tidpunkter under kalenderåret. En del av åtgärderna kan upprepas flera gånger om året, en del sker en gång om året och en del pågår under hela säsongen. *

Det lönar sig att göra upp årsklockan genom att först lista alla åtgärder och sedan placera ut dem vid lämpliga tidpunkter. Till exempel lönar det sig att se över och uppdatera apparater som används vissa säsonger innan de tas i bruk. **



Listan över åtgärder kan till exempel se ut så här:

1. Uppdatering av beredskapsplanen.
2. Byte av lösenord.
3. Kartläggning av den digitala verksamhetsmiljön/uppdatering av helhetsbilden.
4. Kontroll av hur säkerhetskopieringen fungerar.
5. Uppdateringar + fysisk kontroll av givare/arbetsmaskiner.
6. Byte av lösenord.
7. Byte av lösenord & användarrättigheter uppdateras.
8. Uppdateringar + fysisk kontroll av övervakningskamerasystem.
9. Kartläggning av aktuella hot & repetition/uppdatering av de anställdas cybersäkerhetskunnande.
10. Uppdateringar + fysisk kontroll av enheter som är anslutna till produktionslokalens nät.

* Källa: 10 kohtaa kyberturvallisuuden parantamiseksi matkailualalla (10 punkter för att förbättra cybersäkerheten i resebranschen). 2021. Matkailun vastuullisuus näkyväksi Keski-Suomessa (Gör hållbarheten inom turismen synlig i Mellersta Finland)-projektet. Hänvisad till 6/2022. https://visitjyvaskyla.fi/professionals/wp-content/uploads/sites/2/2021/09/10-kohtaa-kyberturvallisuuden-parantamiseksi-matkailualalla.pdf

** Källa: Laajalahti, M. & Nikander, J. 2017. Luonnonvara- ja biotalouden tutkimus 32/2017 - Alkutuotannon kyberuhat (Undersökning inom naturresurser och bioekenomi 32/2017 - Primärproduktionens cyberhot). Hänvisad till 5/2022. https://jukuri.luke.fi/bitstream/handle/10024/539088/luke-luobio_32_2017.pdfluke-luobio_32_2017.pdf

Vill du veta mer om cybersäkerhet inom primärproduktionen?

Handboken Cybersäkerhet inom primärproduktionen är till för hantering av cyberavvikelser (på finska)

Ladda ner den kostnadsfria handboken!

Med hjälp av handboken kan primärproducenten:

- ✓ Utvidga sin förståelse av cybersäkerhetens betydelse i den digitala verksamhetsmiljön.
- ✓ Förstå aktuella cyberhot som riktas mot branschen.
- ✓ Få konkreta anvisningar för hantering av cyberavvikelser.

IInfopaketet och handboken är produkter av projektet Kyberpoikkeamanhallinnan prosessit ja toimintaohjeet elintarviketuotannossa ja –jakelussa (Processer och anvisningar för hantering av cyberavvikelser i livsmedelsproduktionen och -distributionen). Projektet har finansierats av jord- och skogsbruksministeriet och genomförts av IT-institutet vid Jyväskylä yrkeshögskola.

Mer om detta på finska
www.jyvsectec.fi/elintarvikeketju

jamk | Jyväskylän ammattikorkeakoulu

Jord- och skogsbruks-ministeriet