Rekommendationer till ledningen:

1. **Förbättra organisationens säkerhetskultur genom att sätta tydliga mål och förväntningar för säkerhet, regelbundet kommunicera vikten av säkerhet, uppmuntra medarbetare att rapportera säkerhetshändelser och förbättringsförslag, och föregå med gott exempel.**
2. **Arbeta systematiskt och riskbaserat och tilldela nödvändiga resurser utifrån riskanalysen.**
3. **Investera i utbildningar för en kompetenshöjning och ökad medvetenhet hos medarbetarna.**
4. **Investera och delta i cyberkrisövningar.**
5. **Inventera regelbundet vilka potentiella utmaningar som bromsar säkerhetsarbetet och använd Infosäkkollen och It-säkkollen för att identifiera brister.**

Rekommendationer till personal med ansvar för informations- och cybersäkerhet:

Incident- och kontinuitets-hantering	**Medarbetarnas kunskaper**	**Behörighets-hantering**	**Ändringshantering**	**Digitala leveranskedjor**
6. Leta aktivt efter tecken på skadlig aktivitet och använd tjänster eller tekniska verktyg för att tidigt upptäcka cyberangrepp.	10. Utbilda medarbetare regelbundet för att kunna motstå social manipulation, använda starka lösenord och säker hantering av dem.	14. Inventera och identifiera alla behörigheter från olika informations-system.	18. Säkerställ att personal med rätt kompetens utför ändringar.	22. Införa tydliga klausuler vid upphandling om informationsplikt från leverantörer om it-incidenter.
7. Inför arbetssätt för att enkelt kunna anmäla och följa upp säkerhetshändelser.	11. Använd flerfaktors-autentisering.	15. Säkerställ att endast behöriga användare och informationssystem har åtkomst.	19. Kartlägg informationssystem regelbundet och upprätta en testmiljö som så långt det är möjligt efterliknar produktions-miljön och testa ändringar innan de införs.	23. Granska och dokumentera beroenden i organisationens infor-mationssystem, särskilt gällande externa leverantörer.
8. Planera och öva för cyberangrepp.	12. Markera extern e-post och använd tekniska verktyg för att filtrera bort e-post med skadliga länkar eller bilagor.	16. Inför arbetssätt för att regelbundet granska behörigheter.	20. Uppdatera organisationens kritiska informationssystem som exponeras mot internet när nya sårbarheter upptäcks.	24. Planera och inför egna arbetssätt för hantering av it-incidenter hos en leverantör.
9. Inför och öva kontinuitetsplaner för exempelvis kommunikation under en cyberkris.	13. Använd tekniska verktyg för att regelbundet se över användning av svaga, läckta eller stulna lösenord.	17. Använd automatiserad behörighetshantering för planering och verifiering av föränderliga organisationsbehov.	21. Basera sårbarhetsanalysen på information om nya sårbarheter, säkerhetsuppdateringar, generella råd och rekommendationer för att öka motståndskraften genom omvärldsbevakning, exempelvis genom att regelbundet besöka MSB:s webbplatser.	25. Inför alternativa arbetssätt om något skulle inträffa en tjänst hos en leverantör, som organisationen är beroende av för att kunna fortsätta sin verksamhet.

Ur MSB rapport Cyberangrepp mot samhällsviktiga informationssystem : 25 rekommendationer för stärkt skydd mot cyberangrepp