



Informationssäkerhet i en ny tid

Beslutsunderlag: En gemensam och verksamhetsnära kunskapsgrund för all personal och ökad trygghet i Beredskapebergs kommun.

ARTIKELNUMMER: 19

MÅLGRUPP: ALL PERSONAL



Varför behövs en gemensam kunskapsgrund nu?

- **Det digitala hotlandskapet har förändrats:** Cyberincidenter och utpressningsvirus fortsätter att drabba svenska kommuner och störa samhällskritisk service.
- **Ny cybersäkerhetslag för kommuner:** Den nya cybersäkerhetslagen (som implementerar NIS2) träder i kraft 15 januari 2026. Den innebär tydligare krav på riskanalyser och säkerhetsåtgärder.
- **Människor, inte bara teknik:** Tekniska skydd räcker inte. Att utbilda ledning såväl som personal är ett explicit krav för ett systematiskt cybersäkerhetsarbete.

En sårbarhet räcker

Varje enskild medarbetare är en nyckelperson i vårt gemensamma försvar. Utbildning höjer lägstanivån i hela organisationen.

Mindre osäkerhet. Större handlingskraft.

Konfidentialitet (Sekretess)

Informationen är endast tillgänglig för de som har behörighet att se den.

- Skyddar personuppgifter
- Säkrar socialtjänstärenden
- Bygger medborgarförtroende

Riktighet (Integritet)

Informationen är korrekt och kan inte manipuleras av obehöriga.

- Garanterar medicindoser
- Korrekt fakturahantering
- Pålitliga beslutsunderlag

Tillgänglighet

System och information fungerar och är nåbara när de behövs.

- Tryggar hemtjänstbesök
- Säkrar löneutbetalningar
- Rättssäker administration

En kurs för hela kommunen

Målgrupp	Mål och verksamhetsnytta
Medarbetare	■ Gemensam referensram för cyberhot och informationspåverkan ■ Förståelse för varför säkerhetsrutiner finns i vardagen ■ Minskad rädsla att larma vid misstänkta händelser
Enhetschefer	■ Underlag för att leda och följa upp lokalt säkerhetsarbete ■ Etablerar förväntad standard för all personal
IT- och Säkerhetsteam	■ Fler tidiga varningar vid nätfiske och incidenter ■ Snabbare isolering av drabbade datorer förhindrar spridning

30 minuter som omsätter risk till agerande

Del 1

VARFÖR? Förstå hoten mot oss.

Cyberangrepp, utpressningsvirus och informationspåverkan — hur händelser nationellt och globalt påverkar Beredskapebergs verklighet.

Del 2

HUR? Skydda dig själv och kommunen.

Verktyg för digitalt självförsvar: de fem källkritiska frågorna, hantering av nätfiske, starka lösenordsfraser, 2FA och säkert distansarbete.

Del 3

STEG FÖR STEG. Agera rätt när något händer.

Scenarieövningar i incidenthantering: misstänkta mejl, utpressningsvirus och hantering av desinformation på sociala medier.

Omfattning: **67 interaktiva sidor**

Tidsåtgång: **~30 minuter**

Uppföljning: **Kunskapsquiz efter varje del**

Hoten får konsekvenser i vardagen

Utpressningsvirus (Ransomware)

- Angripare krypterar filer och gör journaler eller bokföringssystem otillgängliga.
- Sårbarheter lamslår snabbt service: hemtjänst utan medicinlistor, obetalda löner.
- Incidenter som den i Kalix kommun visar behovet av manuell reservrutin.

Leverantörsattacker

- Angrepp mot ett underliggande IT-system drabbar alla anslutna kommuner samtidigt.
- Känsliga personuppgifter i exempelvis personalsystem kan läckas.
- Säkerheten beror på att vi ställer krav på, och larmar om, externa system.

Informationspåverkan

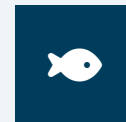
- Desinformation (falska nyheter) som sprids för att så splittring eller undergräva tillit.
- Syftet kan vara att skapa obefogad panik och överbelasta kommunens resurser.
- Ett starkt psykologiskt försvar och källkritik bygger på medveten personal.

Vardagliga vanor gör skillnad



Fem källkritiska frågor

- Vem är avsändaren?
- Varför finns informationen? Hur presenteras den?
- Stämmer det med andra källor? När publicerades den?



Hantera nätfiske

- Avslöja brådska, hot och falska erbjudanden
- Granska länken (hålla över) innan du klickar
- Upptäck vilseledande avsändaradresser



Våra digitala lås

- Skapa långa lösenordsfraser istället för svåra koder
- Använd alltid Tvåfaktorsautentisering (2FA)
- Unika lösenord för varje tjänst



Skydda informationen i vardagen

- Anslut endast via kommunens VPN vid distansarbete
- Lås alltid skärmen när du lämnar datorn
- Undvik okända USB-minnen helt och hållet

När något händer: agera lugnt och snabbt

Din absolut viktigaste insats är att **larma snabbt**. IT-supporten tar hellre emot tio ofarliga misstankar än missar en verklig attack.

Misstänkt e-post / Nätfiske

1. STOPP

Klicka inte på några länkar och öppna inte bilagor.

2. GRANSKA

Titta efter felaktiga avsändare, hot eller stressade uppmaningar.

3. RAPPORTERA

Använd phishing-knapp eller vidarebefordra mejlet till IT.

4. RADERA

Ta bort mejlet från inkorgen så ingen annan klickar.

Misstänkt dataintrång (Ransomware)

1. ISOLERA

Koppla bort nätverkskabel eller stäng av Wi-Fi omedelbart.

2. RÖR INGET

Stäng inte av datorn. Bevara den digitala brottsplatsen för IT.

3. LARMA

Ring IT-supporten direkt via telefon (använd inte en infekterad dator).

Desinformation / Falsa rykten

1. ENGAGERA DIG INTE

Att svara ger ryktet mer spridning i sociala medier.

2. SPRID INTE

Dela inte inlägget för att klaga – alla delningar hjälper attacken.

3. RAPPORTERA INTERNT

Ta en skärmdump och skicka till chef och kommunikation.

Deltagaren tränar på verkliga situationer



Berättarröst och interaktivitet

Kursen drivs av en tydlig svensk berättarröst. Deltagaren styr tempot, kan pausa och repetera valda moment.



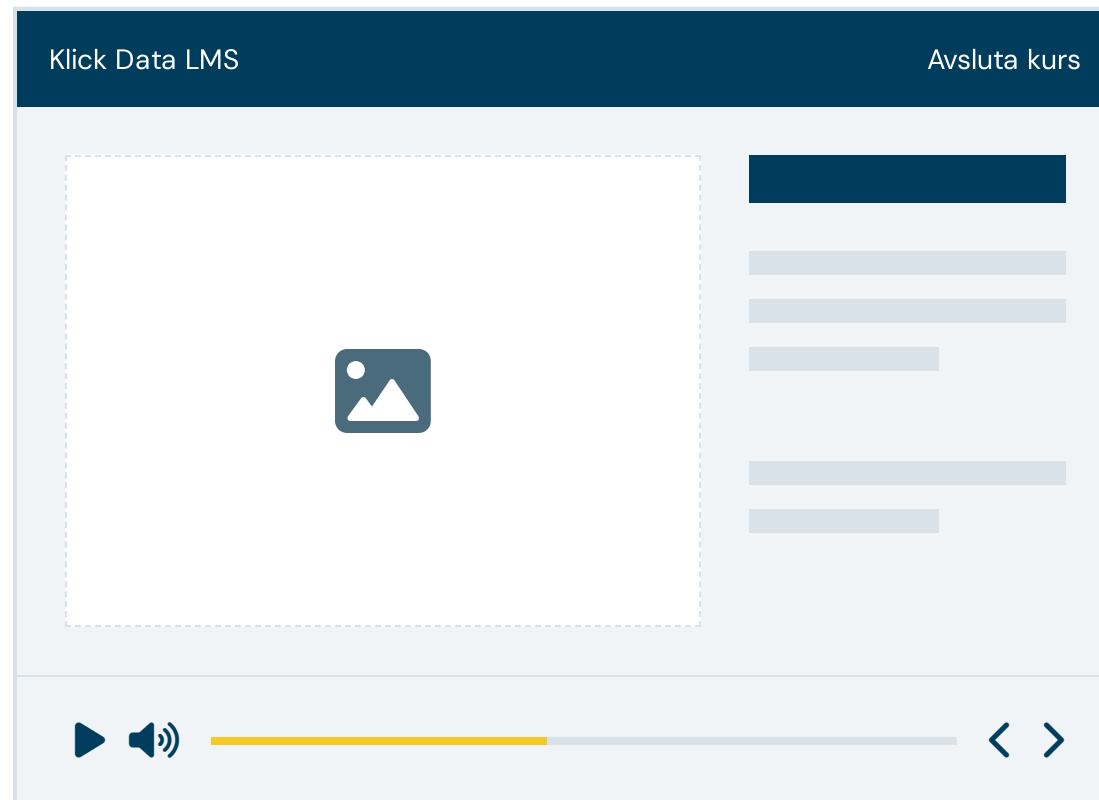
Visuellt stöd och transkribering

Berättelsen stöds av punktlistor, relevanta illustrationer och ett öppet textmanus för ökad tillgänglighet.



Scenariobaserade övningar

Kunskapen förankras direkt genom övningar kring misstänkta mejl, låsta filer och desinformation.



Uppföljning som går att verifiera

Unik certifikatkod säkerställer att genomförandet är äkta.

Ett K3-certifikat utfärdas endast efter en verifierad signering i LMS-systemet. Certifikatet ger kommunen ett konkret underlag för sin uppföljning och kompetenskartläggning.

- ✓ Resultat i realtid via kunskapstester
- ✓ Varje diplom har en unik identifieringskod
- ✓ Publik kontroll kan göras direkt på nätet
- ✓ Verifieringen kräver inget K3-konto eller inloggning

Certifikatet utgör ett verifierbart underlag för en avslutad utbildning. Det utgör inte yrkeslegitimation eller garanti för praktisk handhavandekompetens.



K3-CERT-2026-948123

verify.k3.io



Ett införande som passar kommunens vardag

1

Förankra lokala rutiner

Koppla kursens budskap till kommunens egna riktlinjer, utpekade kontaktvägar och IT-supportens telefonnummer innan utrullning.

2

Genomför pilot

Testa utbildningen med en avgränsad arbetsgrupp. Säkerställ att inloggning och SCORM-moduler (eller K3) fungerar i er miljö.

3

Bred distribution

Lansera modulen (via Klick Data LMS eller ert eget SCORM 1.2-kompatibla LMS) för hela målgruppen. Ställ in en måldeadline.

4

Följ upp & repetera

Analysera certifikats-rapportering för att se genomförandegrad. Etablera en rutin för att inkludera utbildningen i framtida nyanställningar.

Gör informationssäkerhet till en gemensam vana

1. Boka genomgång

Se utbildningsmaterialet och SCORM-funktionerna i detalj under en gemensam visning.

2. Fastställ ramar

Välj målgrupp, integrationsmodell (LMS) och godkänn kommunens lokala kontaktinformation.

3. Starta pilot

Lansera testgruppen och mät resultat före bred utrullning till hela personalstyrkan.

