FÖLJEBREV

2025-06-02

Sveriges Kommuner och Regioner
Kenneth Zetterberg

...

Identitets- och behörighetshantering

Följebrev till beslutsfattare i kommun

Den här följebrevet vänder sig till dig som sitter i ledningen i en kommun, som tjänsteperson eller som förtroendevald.

Kommunens ledning har det yttersta ansvaret

En god digital säkerhet är ett av våra viktigaste skydd för kritiska samhällsfunktioner och för kommunens invånare. Som politisk ledning och kommunledning är det därför mycket viktigt att prioritera den frågan. Arbetet med kommunens digitala säkerhet behöver vara både på strategisk och praktisk nivå. Det yttersta ansvaret ligger alltid hos ledningen och kan inte delegeras till it-chef eller liknande funktion.

Säkerhet kräver resurser och kostar pengar. Brister i säkerheten är dock betydligt dyrare, och konsekvenserna kan bli stora.

I det här dokumentet ger vi konkreta rekommendationer om hur kommunerna kan styra och arbeta med identitets- och behörighetshantering för att nå en god digital säkerhet.

Stora risker om den digitala säkerheten brister

Digital säkerhet brukar delas upp i tre delar: fysisk säkerhet, cybersäkerhet och informationssäkerhet. Om någon av delarna inte fungerar så riskeras helheten.

1. Brister i fysisk säkerhet öppnar för intrång.
2. Brister i cybersäkerhet gör det möjligt för hackare att låsa och förstöra samhällsviktiga verksamheter och utsätta kommunen för utpressning.
3. Brister i informationssäkerhet gör att känslig eller sekretessbelagd information kan röjas eller förstöras.

Det här bör kommunens ledning göra

Aktivt arbete med informationssäkerhet är en förutsättning för att minimera risken för att känslig eller sekretessbelagd information röjs eller förstörs. I det arbetet är det centralt att hantera digitala identiteter och behörigheter för anställda, elever och invånare på ett säkert och effektivt sätt.

- Besluta om en policy eller strategi för arbetet med identiteter och behörigheter. Policyn behöver definiera standardiserade befattningar och peka ut vem som ska ha åtkomst till vilken information. Policyn behöver vara integrerad med styrande dokument för HR.
- Använd ett ledningssystem för informationssäkerhet (LIS) som ett strategiskt verktyg. Prioritera utvecklingen och efterlevnaden av LIS.
- Säkerhetsklassa all information som ska hanteras.
- Besluta om att alla anställda ska tilldelas en e-tjänstelegitimation.
- Se till att kommunen uppfyller de tillitskrav[1] som ställs för att kommunen ska kunna vara del av det nationella digitala ekosystemet . Det skapar förutsättningar för samarbete och informationsutbyte med andra offentliga aktörer och det privata näringslivet.
- Var uthållig och följ upp arbetet med informationssäkerheten. Tänk på att förändringar i arbetssätt och anställdas synsätt på säkerhet inte bara är en fråga för it-chefen, utan för chefer på alla nivåer.

Så kan rekommendationerna användas

Den förändring eller utveckling som respektive kommun behöver genomföra är unik. För en del kan det handla om olika tekniska förändringar, men många behöver framför allt förändra rutiner och arbetsmetoder. Det går inte att jämföra kommuner med varandra, men det går att lära av varandra.

Det här dokumentet innehåller rekommendationer om konkreta arbetssätt och teknisk infrastruktur som hjälper kommunerna att på ett effektivt sätt arbeta med den förändring eller den utveckling som man behöver. Rekommendationerna visar också hur man på ett säkert sätt kan hantera utmaningar och utvecklingsbehov. Stora delar handlar om standardisering eftersom standardisering både höjer säkerheten och ökar effektiviteten.

I dokumentet finns också en presentation av Mognadstrappan. Det är ett självskattningsverktyg som hjälper kommunerna att se var man befinner sig i sin utveckling, vad man har kvar att göra och vilken del av arbetet som man bör prioritera.

[1] Digg:s arbete med tillitskraven pågår.