



Folketingets Indenrigs- og Boligudvalg  
Christiansborg

14. december 2021

## Svar på Indenrigs- og Boligudvalgets spørgsmål nr. 67 (Alm. del) af 3. november 2021 stillet efter ønske fra Preben Bang Henriksen (V)

### Spørgsmål

Vil ministeren 1) redegøre for det samlede billede af it-sikkerheden i landets 98 kommuner og 5 regioner, herunder hvilke elementer de enkelte kommuner og regioner har etableret for at sikre et tilfredsstillende niveau af sikkerhed blandt deres ansatte og folkevalgte og 2) redegøre for kendte sager, hvor it-kriminelle/hackere har tilegnet sig adgang til en kommune eller regions personfølsomme oplysninger eller anden data?

### Svar

Jeg har til brug for besvarelsen af spørgsmålet indhentet bidrag fra Digitaliseringsstyrelsen, som oplyser følgende:

Ansvar for at sikre et passende cyber- og informationssikkerhedsniveau i kommuner og regioner ligger hos den enkelte kommune eller region. Digitaliseringsstyrelsen er ikke bekendt med det samlede billede af cyber- og informationssikkerheden i kommuner og regioner. I forhold til spørgsmålet om, hvilke elementer de enkelte kommuner og regioner har etableret, tolkes spørgsmålet således, at det vedrører konkrete tekniske og organisatoriske tiltag. Den internationale standard for informationssikkerhed, ISO 27001, sætter de organisatoriske rammer for arbejdet med informationssikkerhed i både kommuner og regioner. Det er på den baggrund vurderingen, at kommuner og regioner har etableret et stort antal elementer, men at det vil være vanskeligt at udarbejde et samlet overblik.

For så vidt angår kendte sager, hvor it-kriminelle/hackere har tilegnet sig adgang til en kommune eller regions personfølsomme oplysninger eller anden data, er der indhentet oplysninger fra Datatilsynet for, hvor mange anmeldelser de har modtaget fra kommuner og regioner opdelt på hændelsestyper. Datatilsynets oplysninger fremgår af tabel 1.

**Tabel 1****Kommuner og regioners anmeldelser til Datatilsynet i perioden uge 17 2020 til oktober 2021**

	Kommuner	Regioner
<b>Hændelsestype</b>	<b>3915</b>	<b>400</b>
Brevpost bortkommet	10	1
Brute force/credential stuffing	1	1
Forkerte oplysninger / rigtig modtager	425	38
Hacking	22	2
Offentliggørelse	812	66
Ransomware	1	-
Rigtige oplysninger / forkert modtager	1798	159
Social engineering	7	-
Tab/tyveri af (mobile) enheder	41	7
Usikker transmission	347	15
Andet	451	111

Kilde: Datatilsynet.

Digitaliseringsstyrelsen vurderer, at hændelsestyperne ”brute force/credential stuffing”, ”hacking”, ”ransomware” og ”social engineering” kan betegnes som it-kriminalitet/hacking. I kommunerne var der i alt 31 hændelser og i regionerne 3 hændelser af disse typer i perioden uge 17 2020 til og med oktober 2021. For både kommuner og regioner svarer det til knap 1 pct. af anmeldelserne.

Der er desuden indhentet oplysninger fra Forsvarets Efterretningstjenestes Center for Cybersikkerhed vedrørende de indberetninger, som de har modtaget om it-kriminalitet/hacking mod kommuner eller regioner. Center for Cybersikkerhed oplyser følgende:

”FE’s Center for Cybersikkerhed (CFCS) har ikke et samlet billede af it-sikkerheden i landets 98 kommuner og fem regioner. I overensstemmelse med Den fælles-offentlige digitaliseringsstrategi 2016-2020 underretter kommuner og regioner om større sikkerhedshændelser, jf. aftale om ”Styr på informationssikkerhed i alle myndigheder” af 4. maj 2016.

CFCS har gennem underretningsordningen for kommuner og regioner i 2021 indtil videre modtaget fire indberetninger fra kommuner om større sikkerhedshændelser, hvoraf tre også er angivet at være indberettet til Datatilsynet. I 2020 modtog CFCS syv indberetninger om større sikkerhedshændelser fra kommuner, hvoraf én også er indberettet til Datatilsynet, samt én indberetning fra en region.”

Med venlig hilsen

Nicolai Wammen  
Finansminister