Cyberrobust

Med denne rapport sammenfattes Ishøj Kommune status i forhold til Center for Cybersikkerheds anbefalede indsatsområder for cyberberedskab. Rapporten er målrettet den kommunale ledelse og indgår som del af de initiativer KL's ledelse har igangsat som handlingsanvisende rapportering.

Rapporten er baseret på dette og tidligere års baseline-undersøgelser. Dermed er der historik for organisationens egen udvikling og benchmark med øvrige kommuner.

Spørgsmålene er udvalgt og prioriteret så de i størst muligt omfang afspejler Center for Cybersikkerheds anbefalede indsatser for styrket cyberberedskab. Uddybende materiale kan findes blandt baseline-platformens øvrige rapporter og ved brug af analysemodulet. Hvis kommunen har besvaret de udvidede spørgerammer, indgår det i rapporten.

Center for Cybersikkerhed har udpeget 10 områder, der dækker grundlæggende indsatsområder for cybersikkerhed.

De 10 områder er:

1: Beredskabsplanlægning og krisestyring
2: Opdatering af operativsystemer og applikationer
3: Backup
4: Forsvarsmekanismer
5: Logning og monitorering
6: Netværk og internetvendte services og -systemer
7: Adgangskontrol og rettighedsstyring
8: Fjernadgang til systemer
9: Awareness
10: Leverandørstyring

Hvor de 10 områder primært retter sig mod faktiske beskyttelsestiltag, er der flere forudsættende indsatser, der skal/bør være fokus mod. Det indgår i organisationens system for sikkerhedsstyring – ISMS. I denne rapport er medtaget fire områder, der vurderes kritiske for at have et solidt cyberforsvar.

De fire indsatser er:

1. Ledelse af cybersikkerhed
2. Roller og ansvar
3. Årshjul med kontrol og opfølgning
4. Fortegnelser over udstyr og applikationer

Datagrundlag
Data er indsamlet i perioden 22-05-2024 til 28-05-2024

Data vedrører Ishøj Kommune

Rapporten baserer sig på organisationens resultater fra 2024

Der er status for 123 spørgsmål ud af 308. Spørgsmål besvaret med ’Ved ikke’ og ’Ikke relevant’ indgår ikke i denne rapport.

Denne rapport er genereret på enablor d. 08-07-2024 af Lars Møller Sørensen.

Forklaringer

Organisationens sikkerhed angives i rapporten ud fra organisationens modenhed og sikkerhedsindsatsernes kritikalitet. Data til denne rapport er fra besvarelsen af spørgsmål om organisationens cyberrobusthed. Spørgsmålene er besvaret af kommunen selv på modenhedsskalaen nedenfor.

Modenhed er vurderet for implementering af hver sikkerhedsforanstaltning på følgende skala:

Utilstrækkeligt implementeret
- 0: Nej (foranstaltningen er ikke implementeret)
- 1: Nej, men det planlægges (foranstaltningen er planlagt implementeret)
- 2: Under 1/3 implementeret

Delvist implementeret
- 3: Under 2/3 implementeret

Tilstrækkeligt implementeret
- 4: Over 2/3 implementeret
- 5: Ja (foranstaltningen er fuldt implementeret)

Kritikalitet af sikkerhedsindsatser er vurderet ud fra konsekvensen ved manglende implementering. Følgende skala er anvendt:

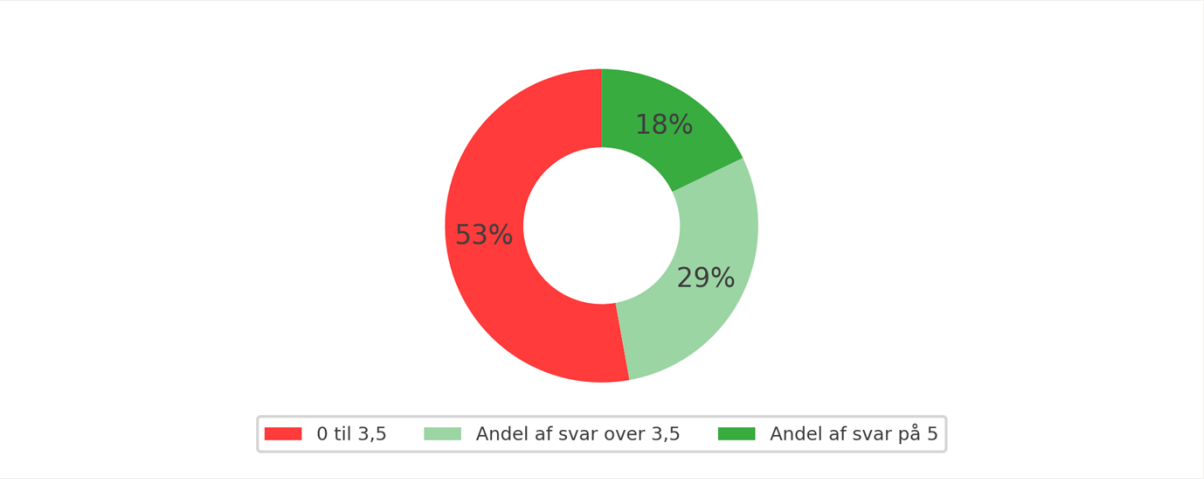
	Konsekvens	Beskrivelse
1	Lav	Få mindre ulemper, som kan overkommes uden større indsats.
2	Medium	Betydelige ulemper, som kan overkommes med få besværligheder.
3	Høj	Betydelige konsekvenser, som kun kan overkommes med alvorlige vanskeligheder.
4	Meget høj	Betydelige eller endog uoprettelige konsekvenser, som måske ikke overvindes.

Alle spørgsmål er opmærket med indsatsens sikkerhedsfunktion baseret på Rammeværk for Cybersikkerhed (læs mere under afsnit om sikkerhedsfunktioner).

Samlet niveau for cyberrobusthed

Status

Fordelingen af kommunens svar i forhold til anbefalingerne fra Center for Cybersikkerhed, samt de forudsættende områder fremgår af nedenstående graf, der viser kommunens svar fra laveste til højeste svarniveau:



For spørgsmål, hvor organisationen har svaret at sikkerhedstiltaget er fuldt implementeret, er værdien 5 (mørkegrøn). For spørgsmål, hvor det er vurderet, at sikkerhedstiltaget er næsten men ikke helt implementeret, er værdien mellem 3,5 og 5 (lysegrøn), og hvor det er vurderet at sikkerhedstiltag ikke er tilstrækkeligt implementeret, er værdien under 3,5 (rød).

Risiko

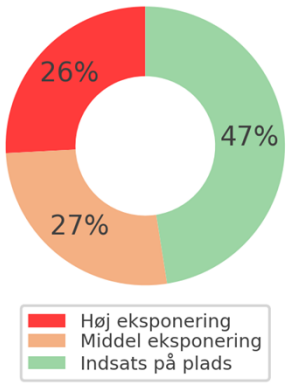
Spørgsmål fra KL Baseline er vurderet ift. konsekvens ved manglende indsats. Det gælder også for cybersikkerhed, hvor alle foranstaltninger og indsatser for cybersikkerhed er vægtet i forhold til den potentielle skade, der kan opstå ved brud.

I tabellen herunder ses organisationens eksponering for cybertrusler som implementering af sikkerhedsindsatser (modenhed) ift. konsekvensen ved manglende indsats (kritikalitet).

Antal spørgsmål

Modenhed	Lav				Høj
5	4	0	3	5	10
4-5	5	0	5	13	12
3-4	1	0	10	8	9
2-3	3	0	7	6	4
1-2	1	0	3	2	6
0-1	0	0	0	2	1

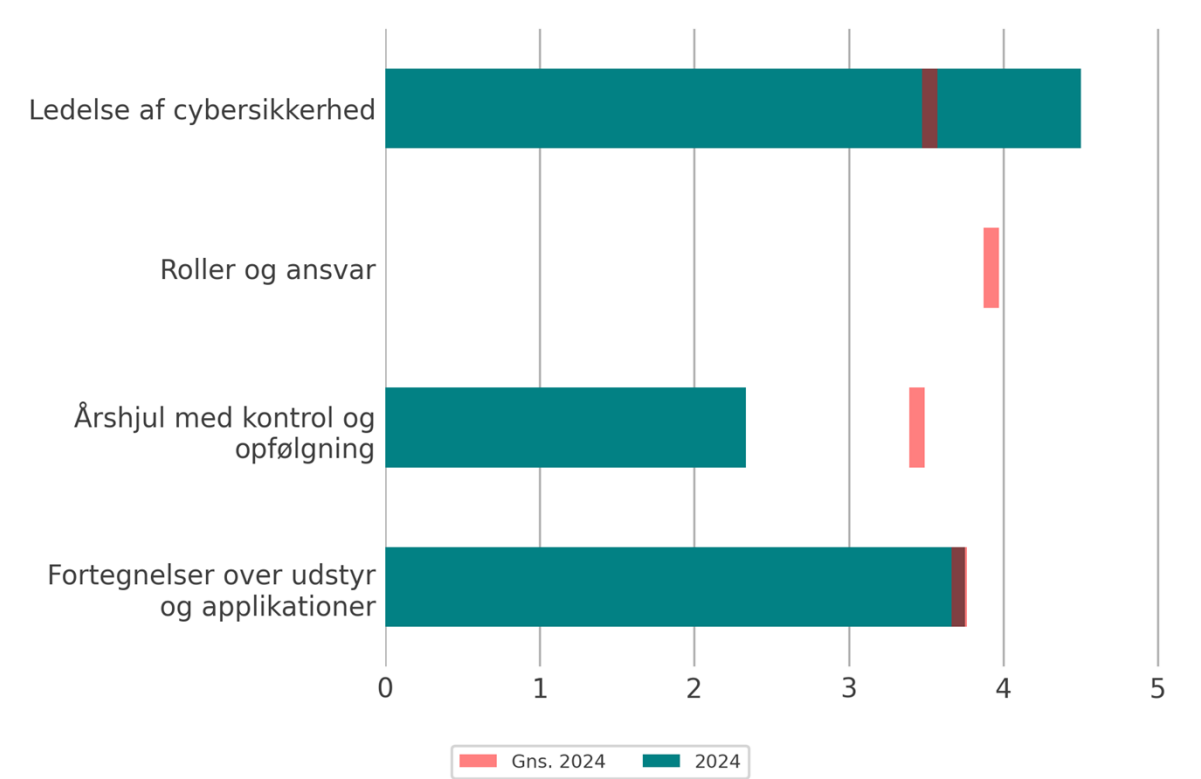
Kritikalitet



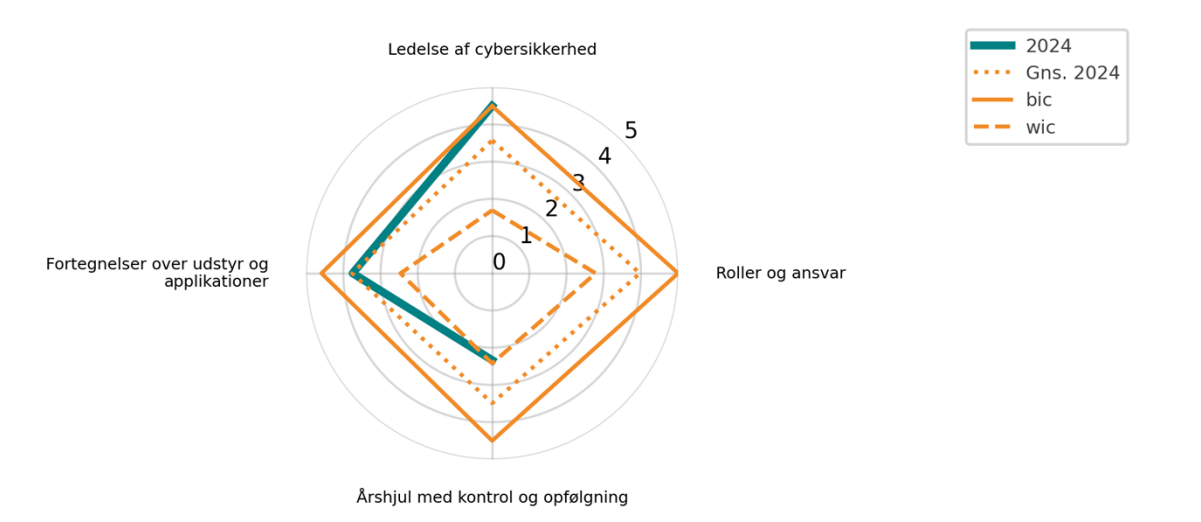
Organisatoriske forhold

Indsatser for cybersikkerhed er ikke kun begrænset til de tekniske værktøjer, der retter sig mod diverse angrebstyper, men er med forudsæt i ledelsens opmærksomhed og de roller og ansvar, der er lagt ud i organisationen.

Grafen viser kommunens forudsætninger for at arbejde med cyberrobusthed og kan anvendes som en indikator for, hvor godt organisationen er klædt på til at arbejde med cyberberedskab.



Kommunens indsats og status i forhold til øvrige danske kommuner:

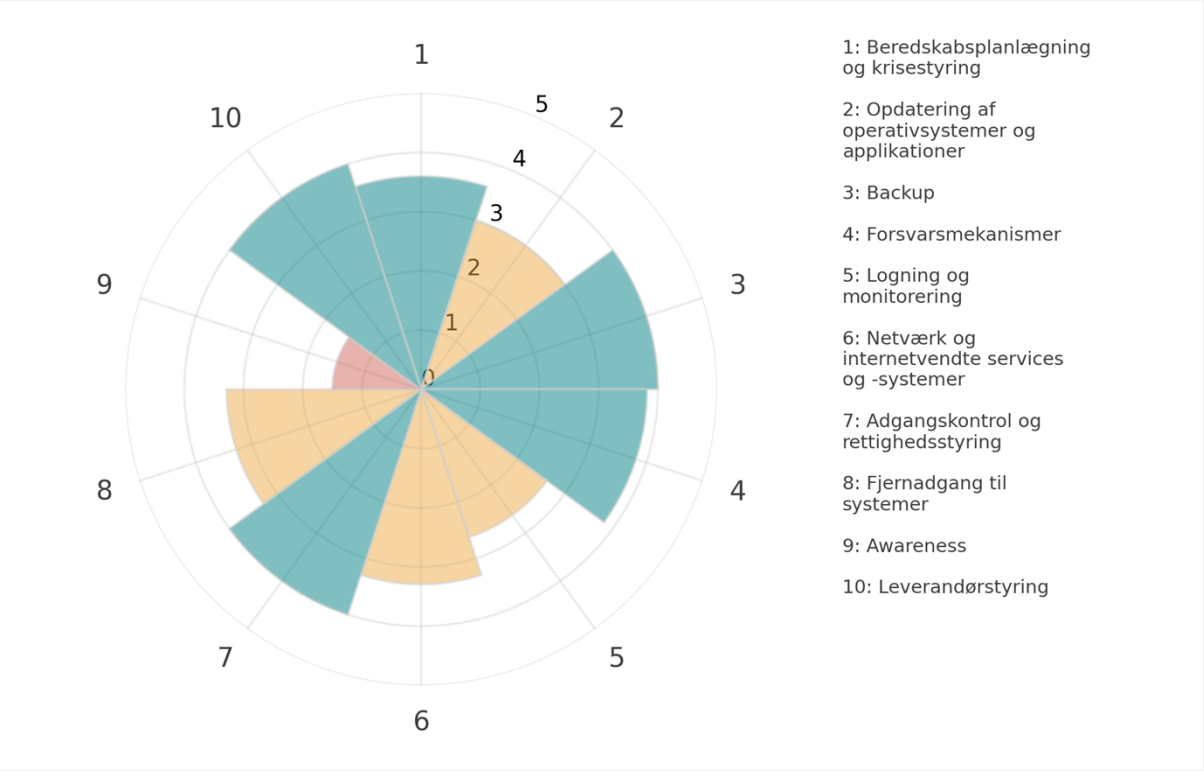


Center for Cybersikkerheds 10 indsatser

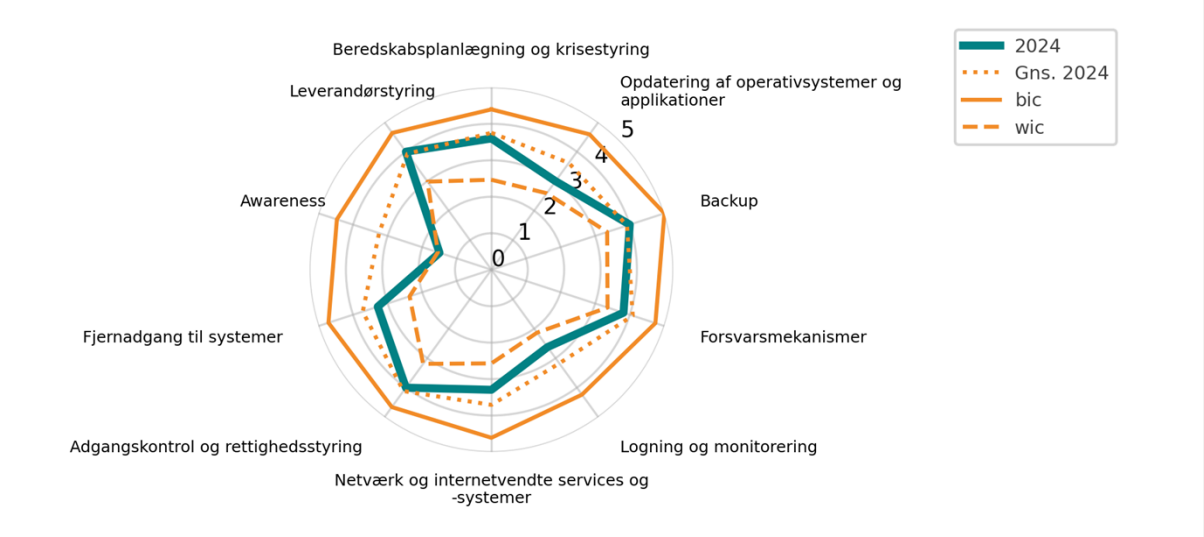
De 10 indsatsområder i Center for Cybersikkerheds anbefalinger er inddelt i 32 tiltag. I dette afsnit behandles de 10 indsatser overordnet.

Status

Hvis ikke alle spørgsmål er medtaget / besvaret kan grafen (hjulet) nedenfor have tomme områder.



Kommunens indsats og status i forhold til øvrige danske kommuner:



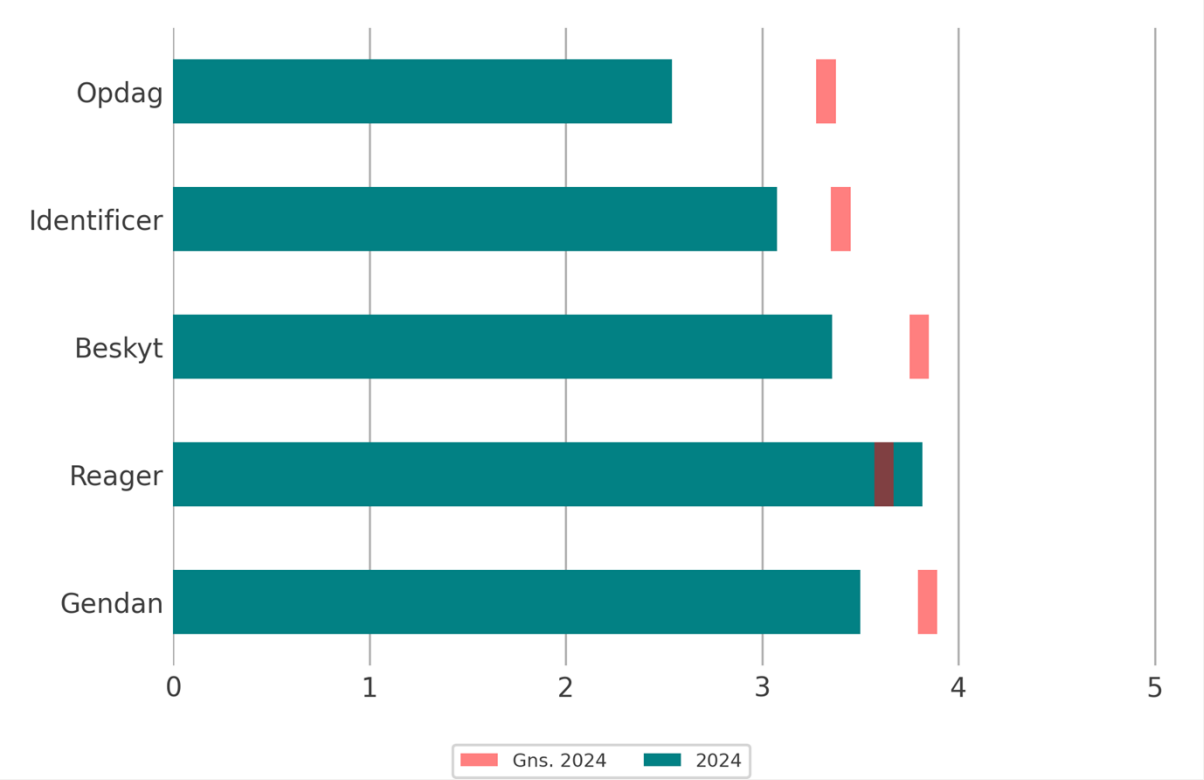
- Beredskabsplanlægning og krisestyring
  Gennemgang og afprøvning af beredskabs- og nødplaner. Opdatering af kontaktlister og roller/ansvar.
- Opdatering af operativsystemer og applikationer
  Sikring af regelmæssig sikkerhedsopdatering af operativsystemer, fagsystemer, internetklienter, onlinesystemer o.l.
- Backup
  Backup af forretningskritiske data inklusive test af backups og afprøvning af reetablering.
- Forsvarsmekanismer
  Sikring af effektiviteten af firewalls og antivirusprogrammer på netværk, servere og enheder.
- Logning og monitorering
  Logning af adgang til forretningskritiske systemer og systemer der indeholder fortrolige eller følsomme data samt sikring af logdata og regelmæssige stikprøver.
- Netværk og internetvendte services og -systemer
  Segmentering og overvågning af netværk samt scanning for sårbarheder på netværksgrænser.
- Adgangskontrol og rettighedsstyring
  Administration og gennemgang af almindelige og privilegerede adgange. Sikring af brugerkonti med multifaktorlogin og stærke passwords.
- Fjernadgang til systemer
  Sikring af kommunikation med systemer, når brugeren befinder sige uden for kommunens matrikel, fx ved hjemmearbejde eller arbejde på rejsen.
- Awareness
  Uddannelse og træning af ansatte i sikker og korrekt dataanvendelse.
- Leverandørstyring
  Kontrol med leverandører og sikring af rapportering ved evt. hændelser.

Sikkerhedsfunktioner

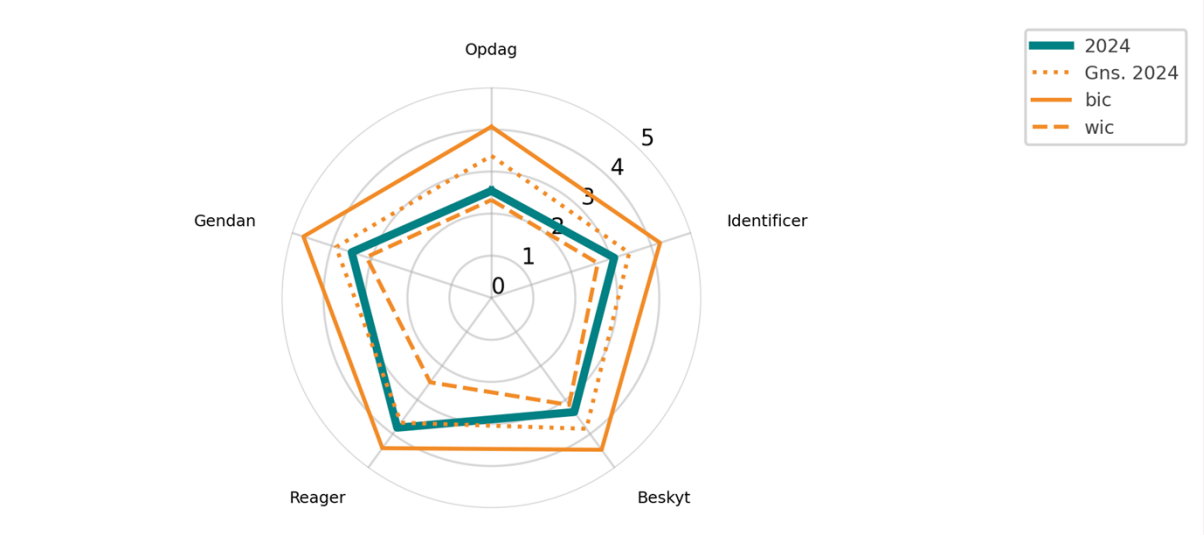
En organisations indsats for cybersikkerhed kan opdeles i fem overordnede sikkerhedsfunktioner. Hver for sig udgør funktionerne et centralt element i forsvaret og samtidig en sammenhængende kæde, hvor det ene område, danner forudsætning for det næste.

Grafen viser niveauet for implementering af sikkerhedsindsatser ift. sikkerhedsfunktioner.

Sikkerhedstiltag

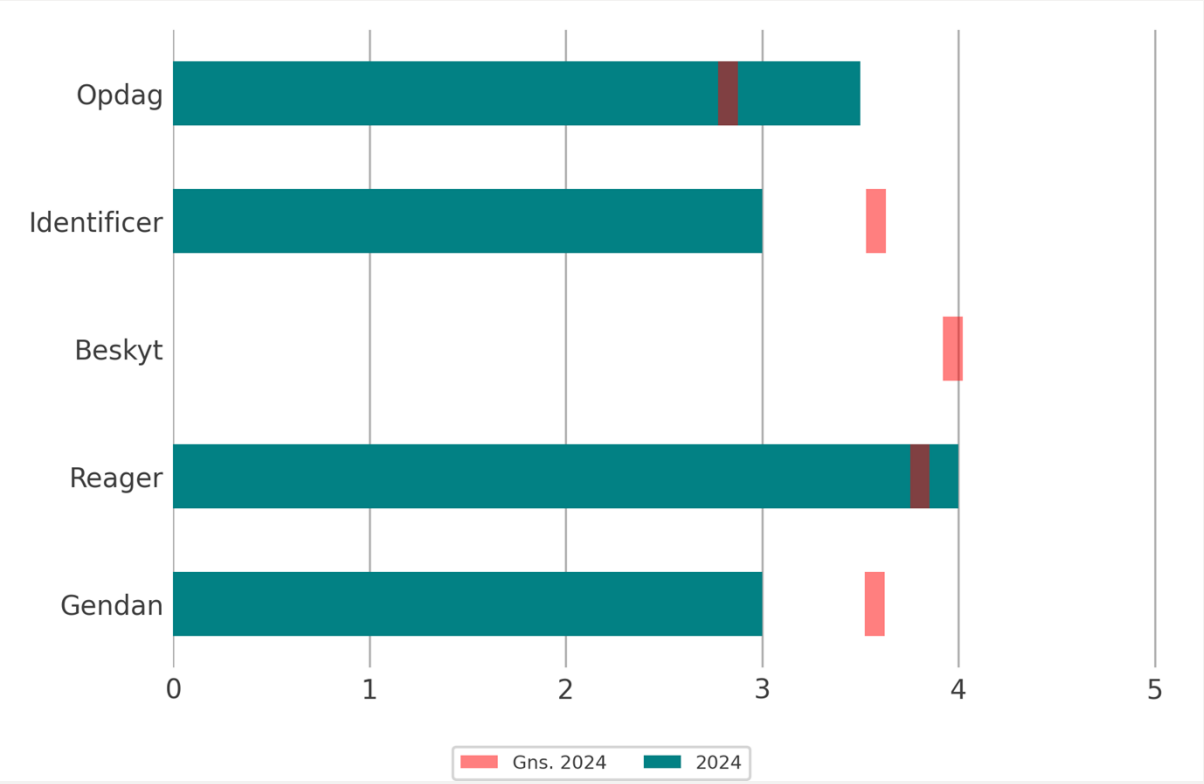


Kommunens indsats og status i forhold til øvrige danske kommuner:



1: Beredskabsplanlægning og krisestyring

Status

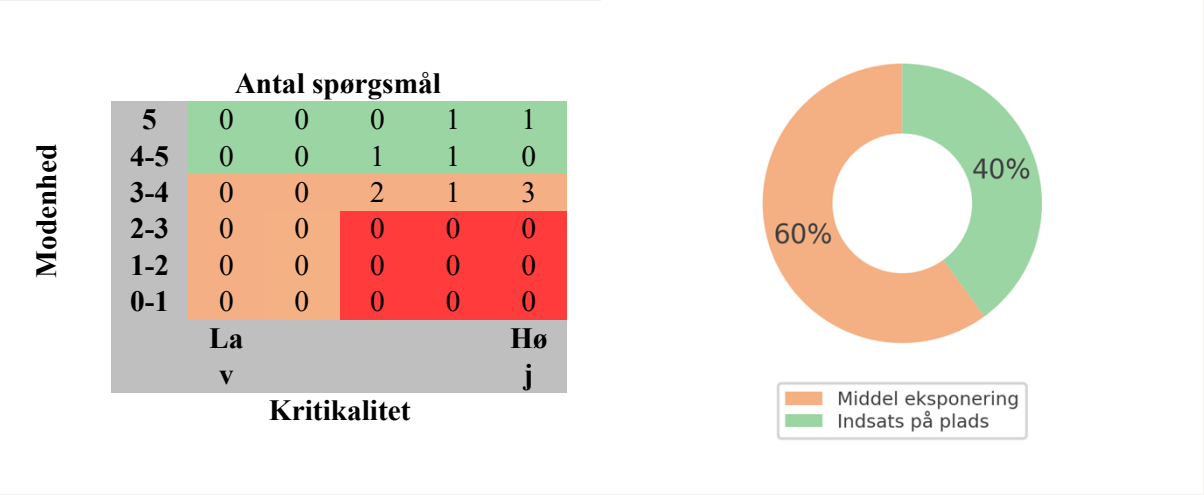


Grafen viser implementeringen af sikkerhedstiltag på sikkerhedsfunktioner. I tabellen herunder vises antallet af spørgsmål som organisationen har besvaret og hvor mange spørgsmål, der i alt afdækker organisationens indsatser fordelt på sikkerhedsfunktioner.

Sikkerhedsfunktion / Type	Spørgsmål besvaret	Spørgsmål i alt
Opdag	2	2
Identificer	2	4
Beskyt	0	7
Reager	5	8
Gendan	1	1

Risiko

I tabellen herunder ses organisationens eksponering for cybertrusler som implementering af sikkerhedsindsatser (modenhed) ift. konsekvensen ved manglende indsats (kritikalitet).



Indsatsområder

Kritiske tiltag med utilstrækkelig implementering

0 kritiske tiltag med lavt svar, hvor konsekvenser kan have stor betydning for sikkerheden.

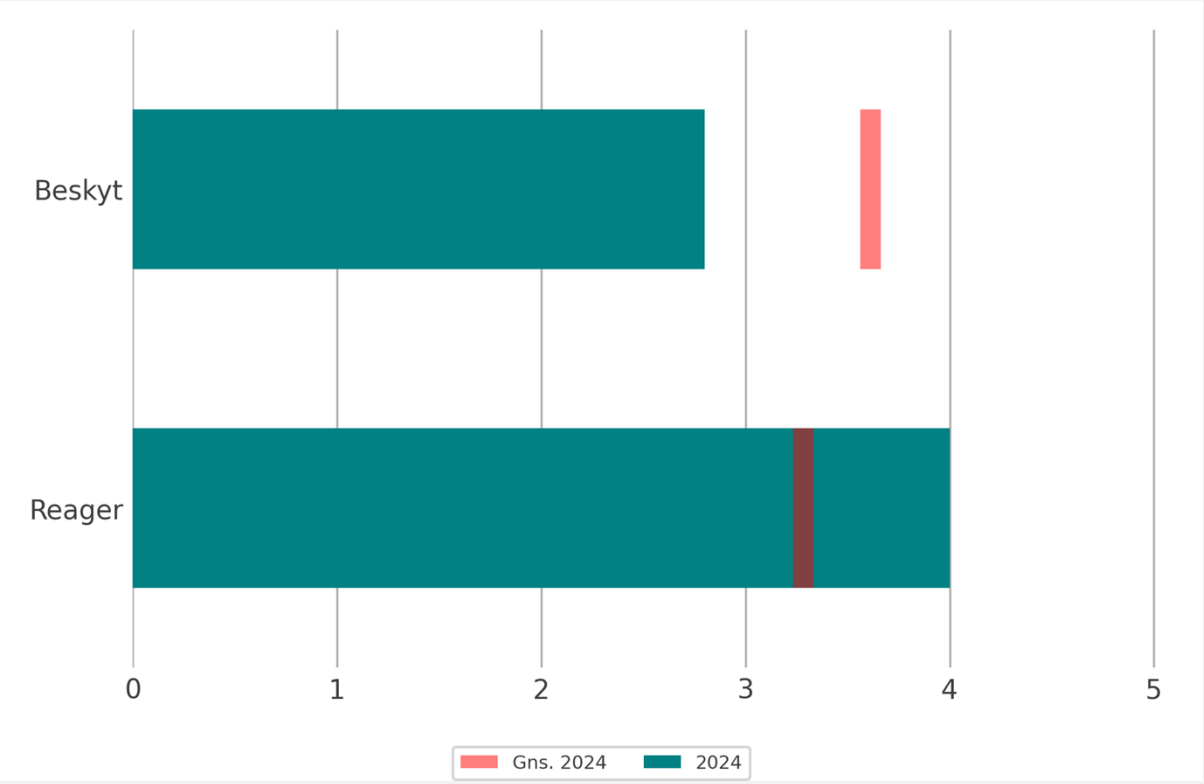
Ikke-kritiske tiltag med utilstrækkelig implementering

6 ikke-kritiske tiltag med lav implementering, hvor konsekvenser kan have stor betydning for sikkerheden.

Spørgsmål	Svar	Gns.	Type
Er kritiske forretningsprocesser identificeret og dokumenteret?	3.0	3.56	Identificer
Er informationsaktiver (IT-systemer og data), der understøtter kritiske forretningsprocesser, identificeret og dokumenteret?	3.0	3.43	Identificer
Foretages der risikovurdering af forretningsprocesser ift. kritikalitet af services og persondata?	3.0	3.12	Opdag
Er der udarbejdet en handlingsplan for informationssikkerhed i organisationen?	3.0	3.4	Reager
Testes it-beredskabsplanen med faste intervaller, så der sikres regelmæssig træning i, afprøvning og evaluering af it-beredskabsplaner?	3.0	3.44	Reager
Har organisationen nødplaner for, hvordan kritiske processer kan videreføres, hvis en hændelse forhindrer normal drift?	3.0	3.62	Gendan

2: Opdatering af operativsystemer og applikationer

Status

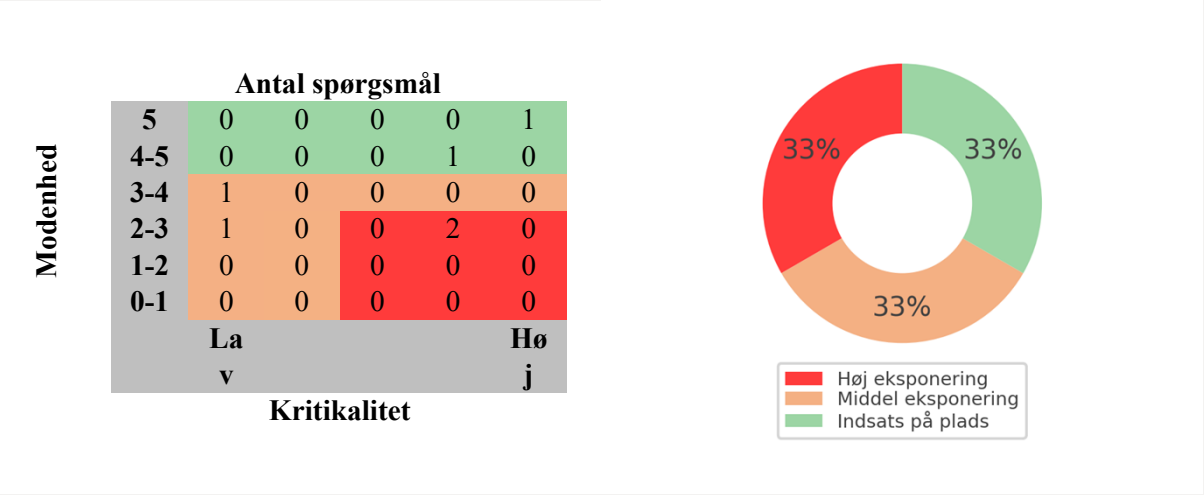


Grafen viser implementeringen af sikkerhedstiltag på sikkerhedsfunktioner. I tabellen herunder vises antallet af spørgsmål som organisationen har besvaret og hvor mange spørgsmål, der i alt afdækker organisationens indsatser fordelt på sikkerhedsfunktioner.

Sikkerhedsfunktion / Type	Spørgsmål besvaret	Spørgsmål i alt
Beskyt	5	7
Reager	1	1

Risiko

I tabellen herunder ses organisationens eksponering for cybertrusler som implementering af sikkerhedsindsatser (modenhed) ift. konsekvensen ved manglende indsats (kritikalitet).



Indsatsområder

Kritiske tiltag med utilstrækkelig implementering

2 kritiske tiltag med lavt svar, hvor konsekvenser kan have stor betydning for sikkerheden.

Spørgsmål	Svar	Gns.	Type
Anvender organisationen værktøjer, der sikrer regelmæssig og automatiseret vedligeholdelse af konfigurationer?	2.0	3.99	Beskyt
Anvender og vedligeholder organisationen standardiserede og dokumenterede sikkerhedskonfigurationer for alt autoriseret netværksudstyr?	2.0	3.86	Beskyt

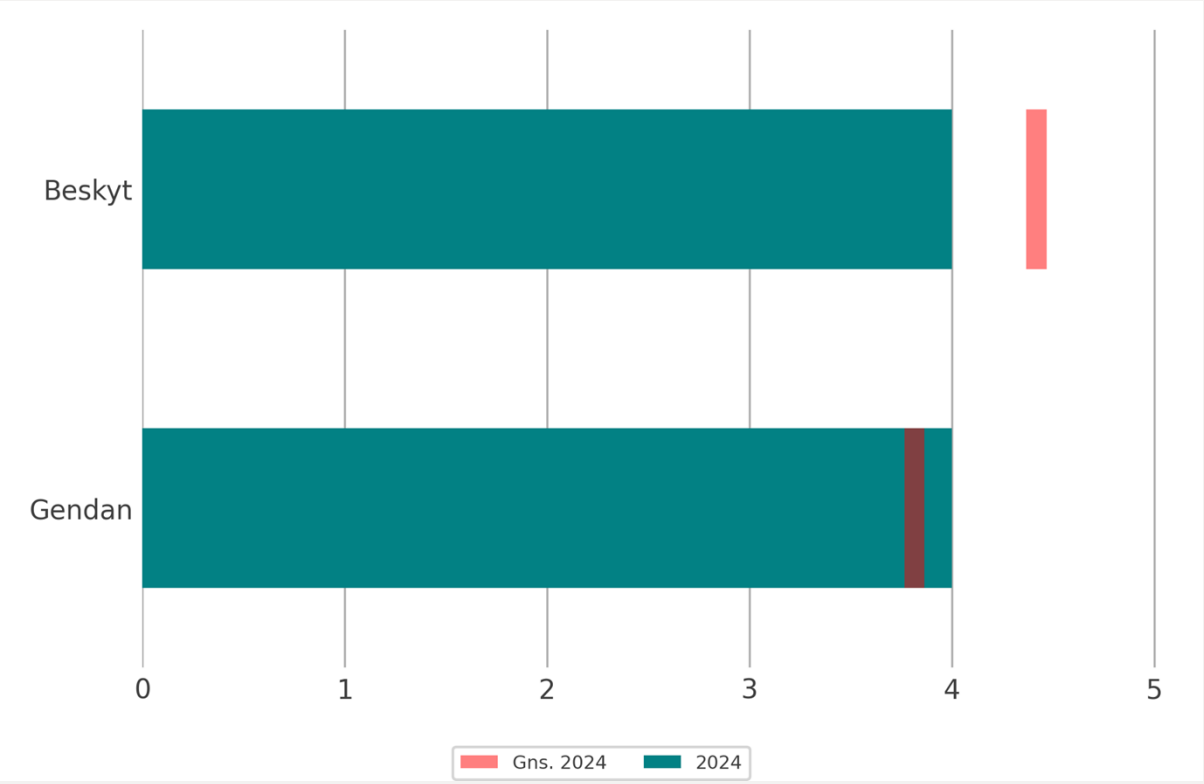
Ikke-kritiske tiltag med utilstrækkelig implementering

2 ikke-kritiske tiltag med lav implementering, hvor konsekvenser kan have stor betydning for sikkerheden.

Spørgsmål	Svar	Gns.	Type
Anvender organisationen automatiserede værktøjer for at sikre, at operativsystemer anvender seneste opdatering?	3.0	4.38	Beskyt
Sikres det, at alle netværkskomponenter er opdateret med de seneste sikkerhedsopdateringer?	2.0	3.74	Beskyt

3: Backup

Status

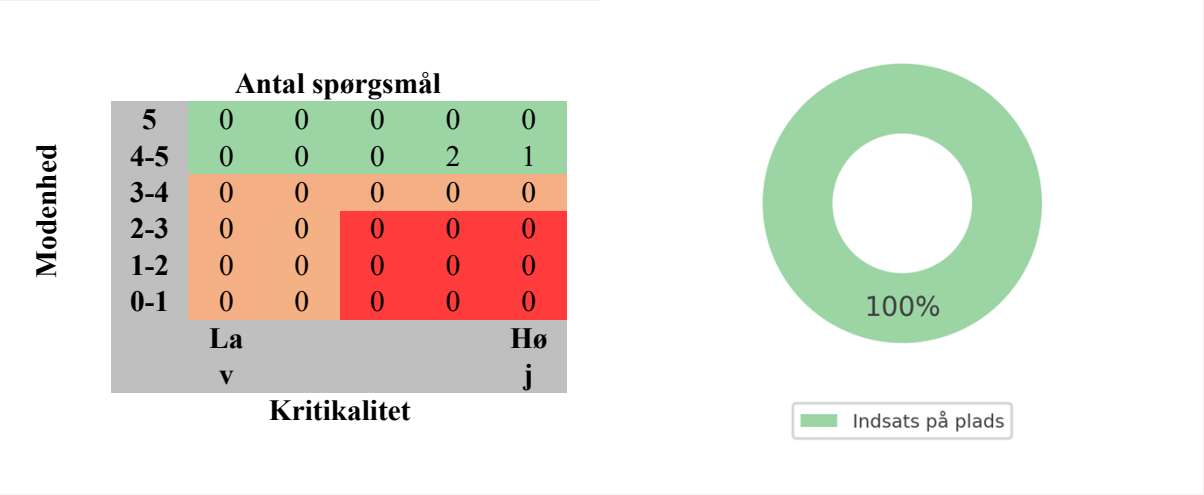


Grafen viser implementeringen af sikkerhedstiltag på sikkerhedsfunktioner. I tabellen herunder vises antallet af spørgsmål som organisationen har besvaret og hvor mange spørgsmål, der i alt afdækker organisationens indsatser fordelt på sikkerhedsfunktioner.

Sikkerhedsfunktion / Type	Spørgsmål besvaret	Spørgsmål i alt
Beskyt	1	1
Gendan	2	10

Risiko

I tabellen herunder ses organisationens eksponering for cybertrusler som implementering af sikkerhedsindsatser (modenhed) ift. konsekvensen ved manglende indsats (kritikalitet).



Indsatsområder

Kritiske tiltag med utilstrækkelig implementering

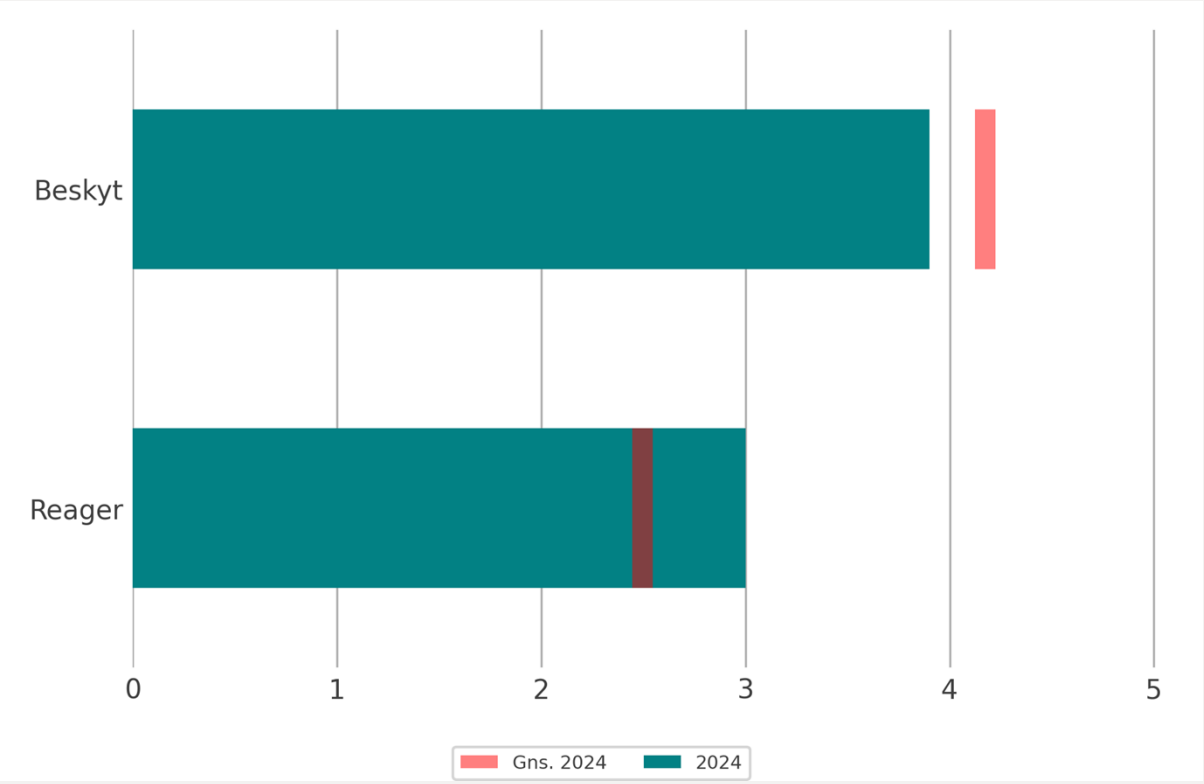
0 kritiske tiltag med lavt svar, hvor konsekvenser kan have stor betydning for sikkerheden.

Ikke-kritiske tiltag med utilstrækkelig implementering

0 ikke-kritiske tiltag med lav implementering, hvor konsekvenser kan have stor betydning for sikkerheden.

4: Forsvarsmekanismer

Status

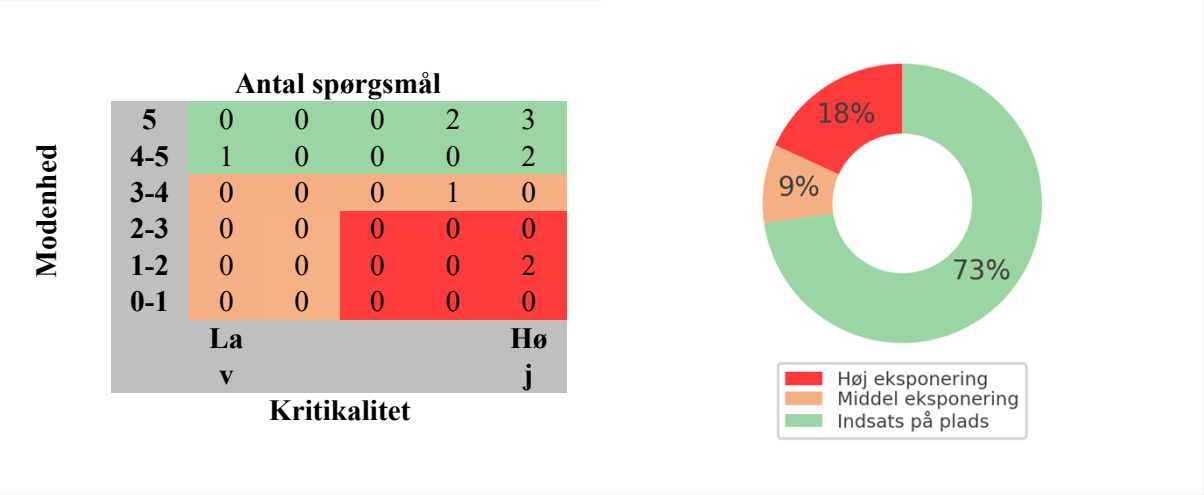


Grafen viser implementeringen af sikkerhedstiltag på sikkerhedsfunktioner. I tabellen herunder vises antallet af spørgsmål som organisationen har besvaret og hvor mange spørgsmål, der i alt afdækker organisationens indsatser fordelt på sikkerhedsfunktioner.

Sikkerhedsfunktion / Type	Spørgsmål besvaret	Spørgsmål i alt
Beskyt	10	11
Reager	1	1

Risiko

I tabellen herunder ses organisationens eksponering for cybertrusler som implementering af sikkerhedsindsatser (modenhed) ift. konsekvensen ved manglende indsats (kritikalitet).



Indsatsområder

Kritiske tiltag med utilstrækkelig implementering

2 kritiske tiltag med lavt svar, hvor konsekvenser kan have stor betydning for sikkerheden.

Spørgsmål	Svar	Gns.	Type
Anvender organisationen firewalls med change management kontrol?	1.0	3.66	Beskyt
Anvender organisationen Network Access Control?	1.0	3.16	Beskyt

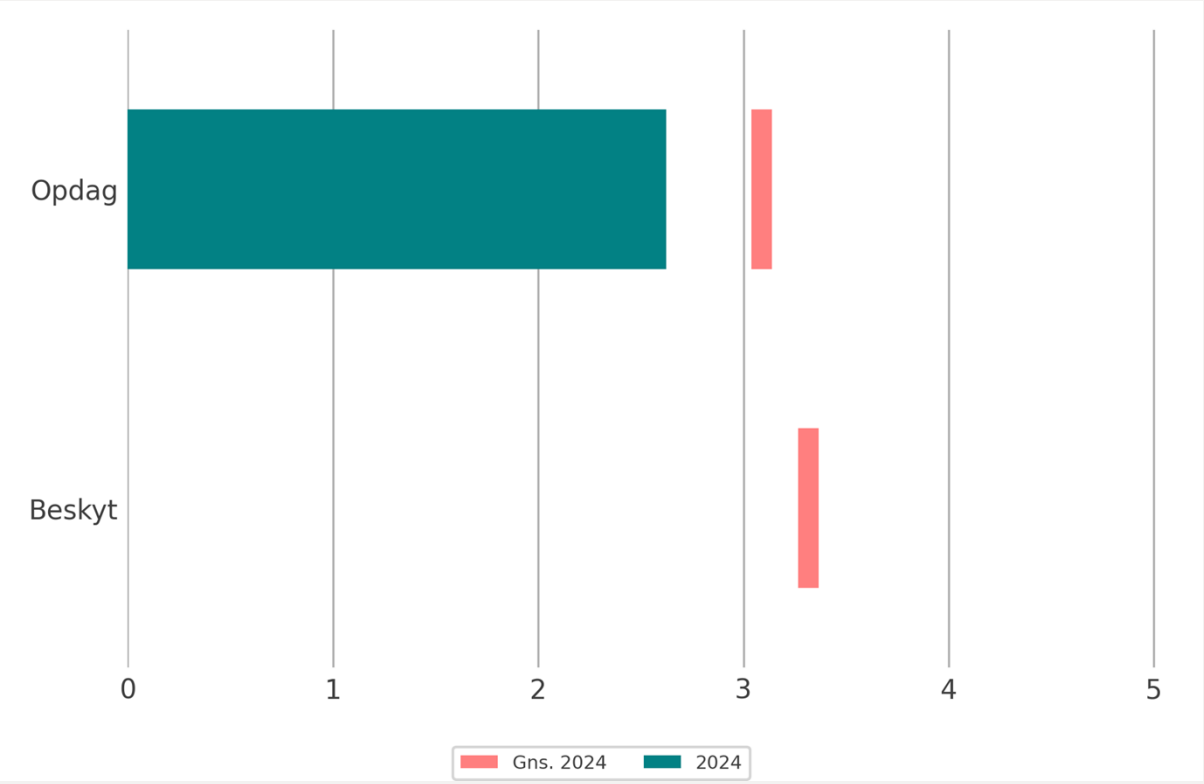
Ikke-kritiske tiltag med utilstrækkelig implementering

1 ikke-kritiske tiltag med lav implementering, hvor konsekvenser kan have stor betydning for sikkerheden.

Spørgsmål	Svar	Gns.	Type
Har organisationen en proces for fjernelse eller godkendelse af applikationer, der ikke er autoriserede?	3.0	2.54	Reager

5: Logning og monitorering

Status



Grafen viser implementeringen af sikkerhedstiltag på sikkerhedsfunktioner. I tabellen herunder vises antallet af spørgsmål som organisationen har besvaret og hvor mange spørgsmål, der i alt afdækker organisationens indsatser fordelt på sikkerhedsfunktioner.

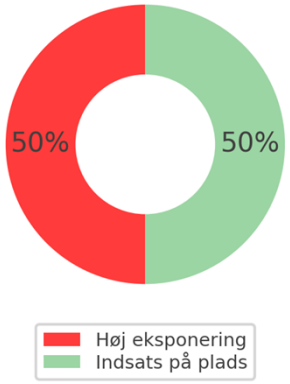
Sikkerhedsfunktion / Type	Spørgsmål besvaret	Spørgsmål i alt
Opdag	8	11
Beskyt	0	2

Risiko

I tabellen herunder ses organisationens eksponering for cybertrusler som implementering af sikkerhedsindsatser (modenhed) ift. konsekvensen ved manglende indsats (kritikalitet).

Modenhed	Antal spørgsmål				
5	0	0	0	0	0
4-5	0	0	0	1	3
3-4	0	0	0	0	0
2-3	0	0	1	0	0
1-2	0	0	1	1	1
0-1	0	0	0	0	0
	Lav				Høj

Kritikalitet



Indsatsområder

Kritiske tiltag med utilstrækkelig implementering

4 kritiske tiltag med lavt svar, hvor konsekvenser kan have stor betydning for sikkerheden.

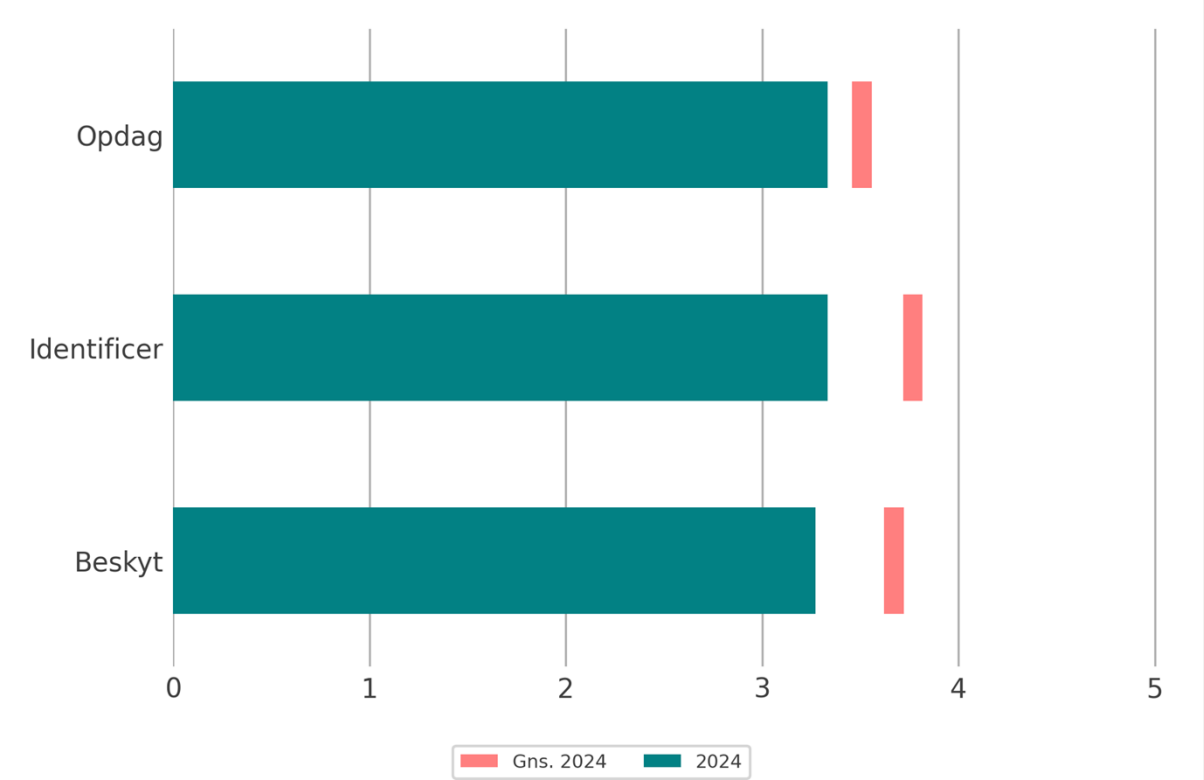
Spørgsmål	Svar	Gns.	Type
Er der etableret centraliseret Log Management?	1.0	2.75	Opdag
Sikres det, at lokal logning er aktiveret på alle systemer og netværksenheder?	1.0	3.26	Opdag
Er der installeret et SIEM-system eller tilsvarende værktøj til sammenligning og analyse af logs?	1.0	2.26	Opdag
Kontrolleres forretningskritiske systemers logs som en del af årshjulsaktiviteterne?	2.0	2.31	Opdag

Ikke-kritiske tiltag med utilstrækkelig implementering

0 ikke-kritiske tiltag med lav implementering, hvor konsekvenser kan have stor betydning for sikkerheden.

6: Netværk og internetvendte services og -systemer

Status

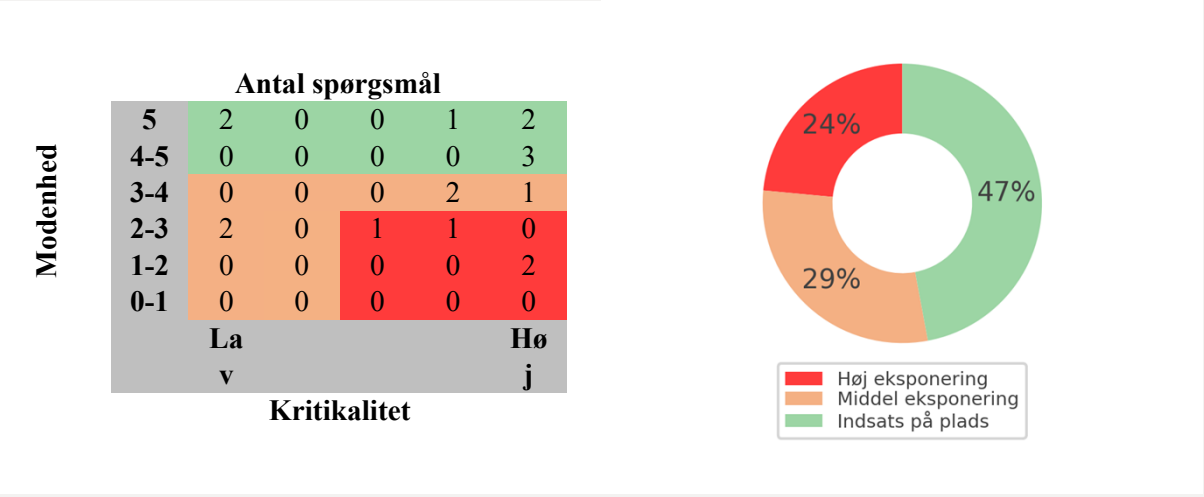


Grafen viser implementeringen af sikkerhedstiltag på sikkerhedsfunktioner. I tabellen herunder vises antallet af spørgsmål som organisationen har besvaret og hvor mange spørgsmål, der i alt afdækker organisationens indsatser fordelt på sikkerhedsfunktioner.

Sikkerhedsfunktion / Type	Spørgsmål besvaret	Spørgsmål i alt
Opdag	3	4
Identificer	3	3
Beskyt	11	19

Risiko

I tabellen herunder ses organisationens eksponering for cybertrusler som implementering af sikkerhedsindsatser (modenhed) ift. konsekvensen ved manglende indsats (kritikalitet).



Indsatsområder

Kritiske tiltag med utilstrækkelig implementering

4 kritiske tiltag med lavt svar, hvor konsekvenser kan have stor betydning for sikkerheden.

Spørgsmål	Svar	Gns.	Type
Sikres det, at kun godkendte scripting-sprog anvendes fra webbrowsere og e-mailklienter?	2.0	3.05	Beskyt
Er det sikret, at der er tildelt aktive porte, protokoller og tjenester til udstyr, der indgår i fortegnelse over hardware?	1.0	3.03	Beskyt
Udføres der regelmæssigt portscanninger for identifikation af uautoriserede porte?	1.0	3.47	Opdag
Er organisationens netværk segmenterede ift. datas følsomhed?	2.0	3.16	Beskyt

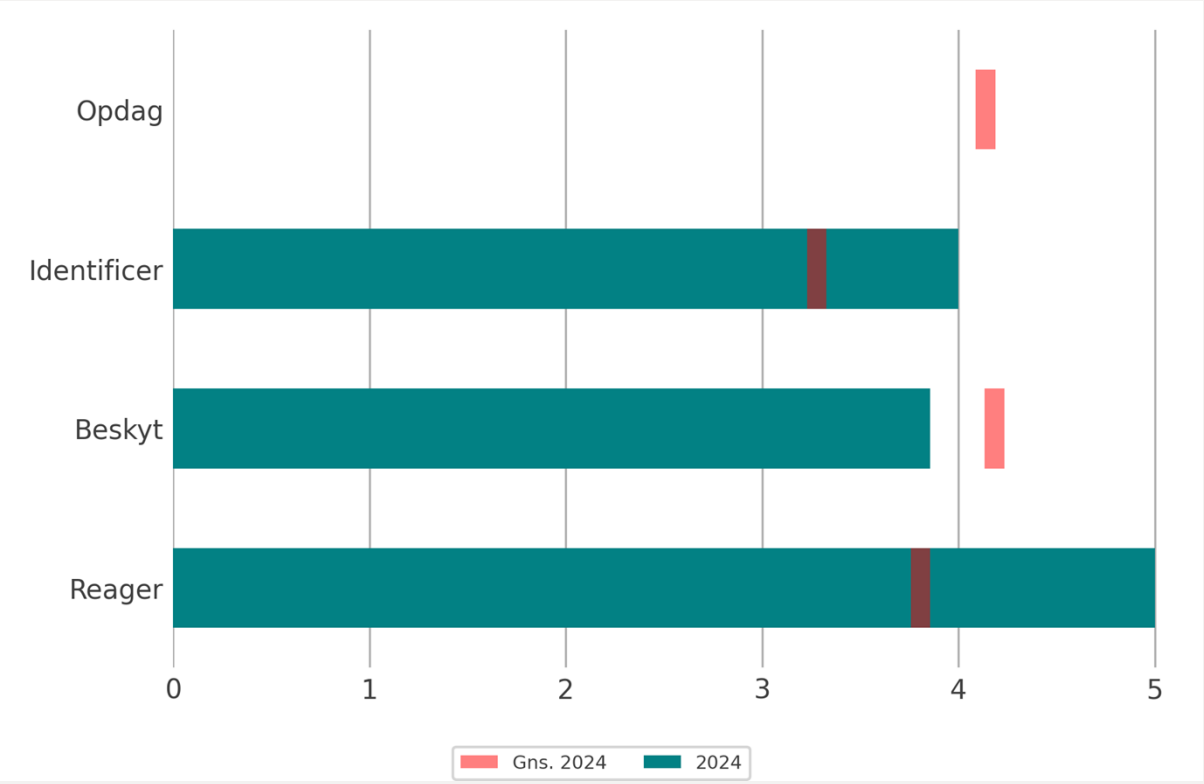
Ikke-kritiske tiltag med utilstrækkelig implementering

5 ikke-kritiske tiltag med lav implementering, hvor konsekvenser kan have stor betydning for sikkerheden.

Spørgsmål	Svar	Gns.	Type
Sikres det, at kun tilladte applikationer kan anvendes fra organisationens udstyr?	3.0	2.72	Beskyt
Sikres det, at der kun anvendes autoriserede og supporterede webbrowsere og mail-klienter?	2.0	3.8	Beskyt
Anvender og vedligeholder organisationen en fortegnelse over godkendte trådløse access points tilsluttet organisationens kablede netværk?	3.0	4.51	Identificer
Sikres det, at alle netværkskomponenter er opdateret med de seneste sikkerhedsopdateringer?	2.0	3.74	Beskyt
Anvender og vedligeholder organisationen en fortegnelse over alle netværksgrænser?	3.0	4.24	Identificer

7: Adgangskontrol og rettighedsstyring

Status

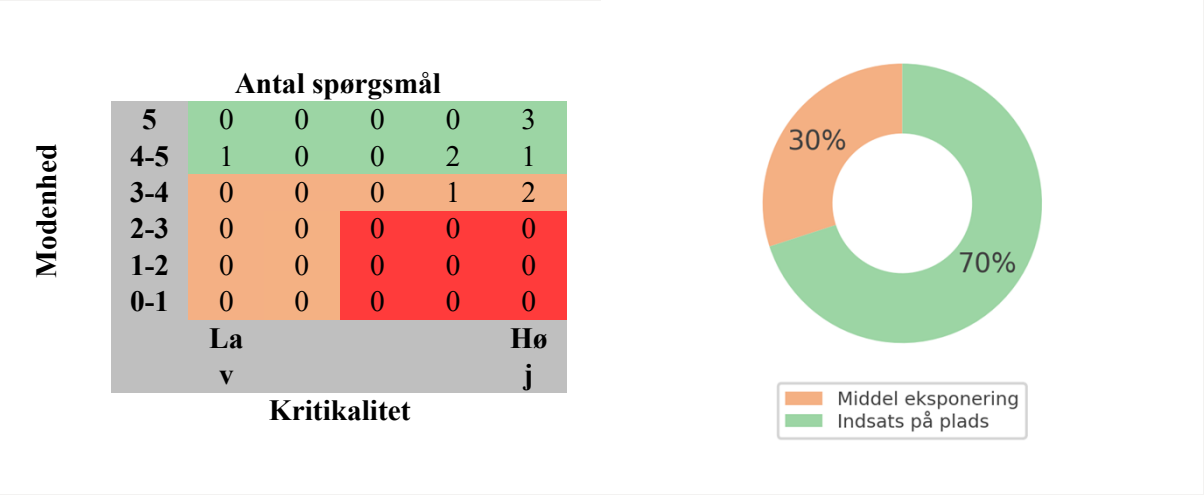


Grafen viser implementeringen af sikkerhedstiltag på sikkerhedsfunktioner. I tabellen herunder vises antallet af spørgsmål som organisationen har besvaret og hvor mange spørgsmål, der i alt afdækker organisationens indsatser fordelt på sikkerhedsfunktioner.

Sikkerhedsfunktion / Type	Spørgsmål besvaret	Spørgsmål i alt
Opdag	0	4
Identificer	2	2
Beskyt	7	13
Reager	1	1

Risiko

I tabellen herunder ses organisationens eksponering for cybertrusler som implementering af sikkerhedsindsatser (modenhed) ift. konsekvensen ved manglende indsats (kritikalitet).



Indsatsområder

Kritiske tiltag med utilstrækkelig implementering

0 kritiske tiltag med lavt svar, hvor konsekvenser kan have stor betydning for sikkerheden.

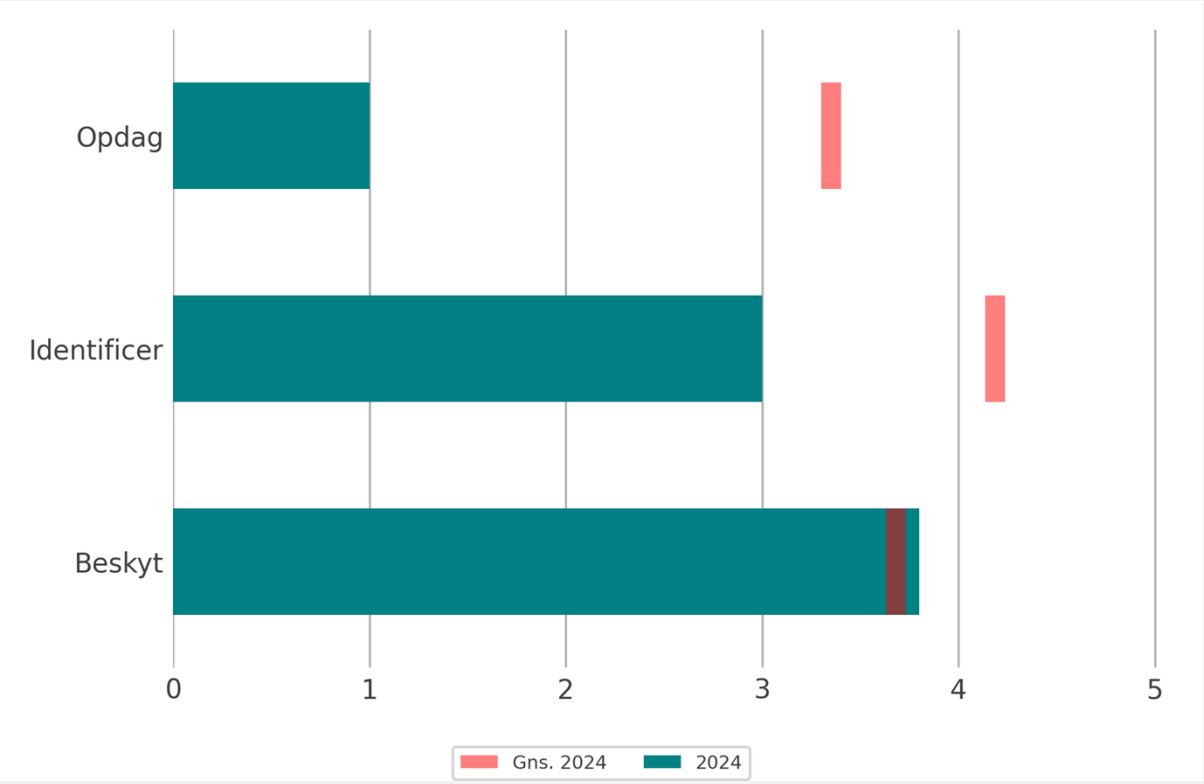
Ikke-kritiske tiltag med utilstrækkelig implementering

3 ikke-kritiske tiltag med lav implementering, hvor konsekvenser kan have stor betydning for sikkerheden.

Spørgsmål	Svar	Gns.	Type
Sikrer organisationen korrekt oprettelse og inddragelse af brugerrettigheder?	3.0	4.23	Beskyt
Stiller organisationen krav til passwords?	3.0	4.68	Beskyt
Er brugere med administratorrettigheder beskyttet med to-faktor-autentifikation og krypterede kanaler?	3.0	3.1	Beskyt

8: Fjernadgang til systemer

Status

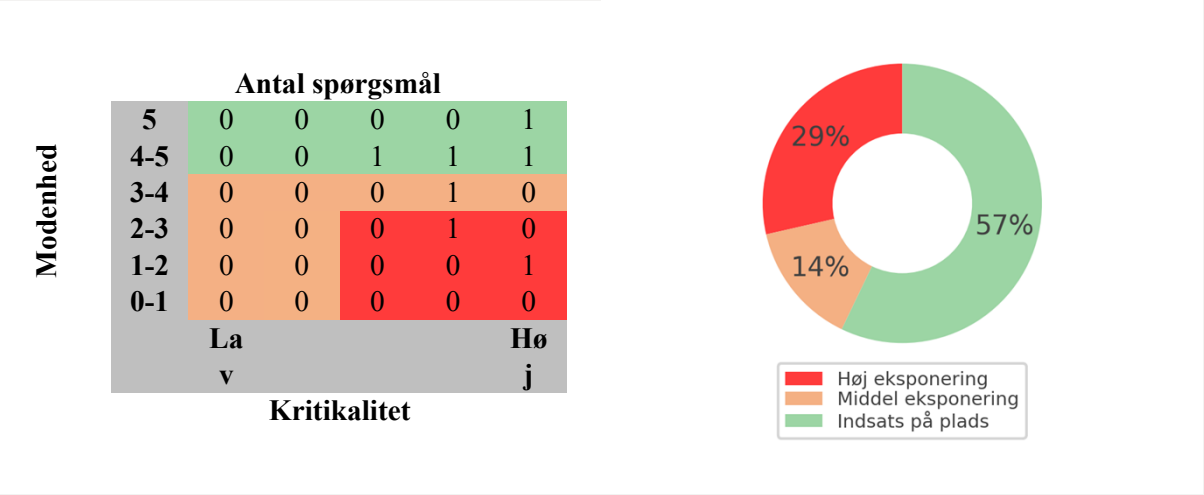


Grafen viser implementeringen af sikkerhedstiltag på sikkerhedsfunktioner. I tabellen herunder vises antallet af spørgsmål som organisationen har besvaret og hvor mange spørgsmål, der i alt afdækker organisationens indsatser fordelt på sikkerhedsfunktioner.

Sikkerhedsfunktion / Type	Spørgsmål besvaret	Spørgsmål i alt
Opdag	1	2
Identificer	1	1
Beskyt	5	9

Risiko

I tabellen herunder ses organisationens eksponering for cybertrusler som implementering af sikkerhedsindsatser (modenhed) ift. konsekvensen ved manglende indsats (kritikalitet).



Indsatsområder

Kritiske tiltag med utilstrækkelig implementering

2 kritiske tiltag med lavt svar, hvor konsekvenser kan have stor betydning for sikkerheden.

Spørgsmål	Svar	Gns.	Type
Udføres der regelmæssigt portscanninger for identifikation af uautoriserede porte?	1.0	3.47	Opdag
Er organisationens netværk segmenterede ift. datas følsomhed?	2.0	3.16	Beskyt

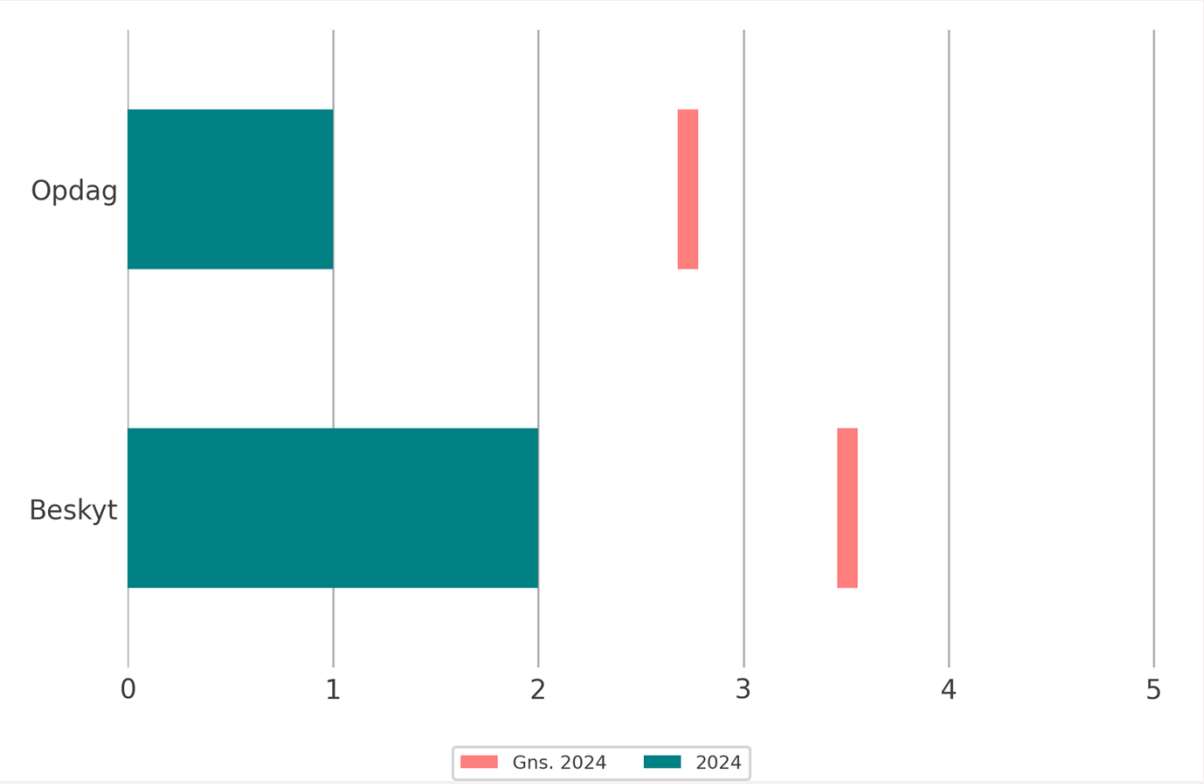
Ikke-kritiske tiltag med utilstrækkelig implementering

1 ikke-kritiske tiltag med lav implementering, hvor konsekvenser kan have stor betydning for sikkerheden.

Spørgsmål	Svar	Gns.	Type
Anvender og vedligeholder organisationen en fortegnelse over alle netværksgrænser?	3.0	4.24	Identificer

9: Awareness

Status

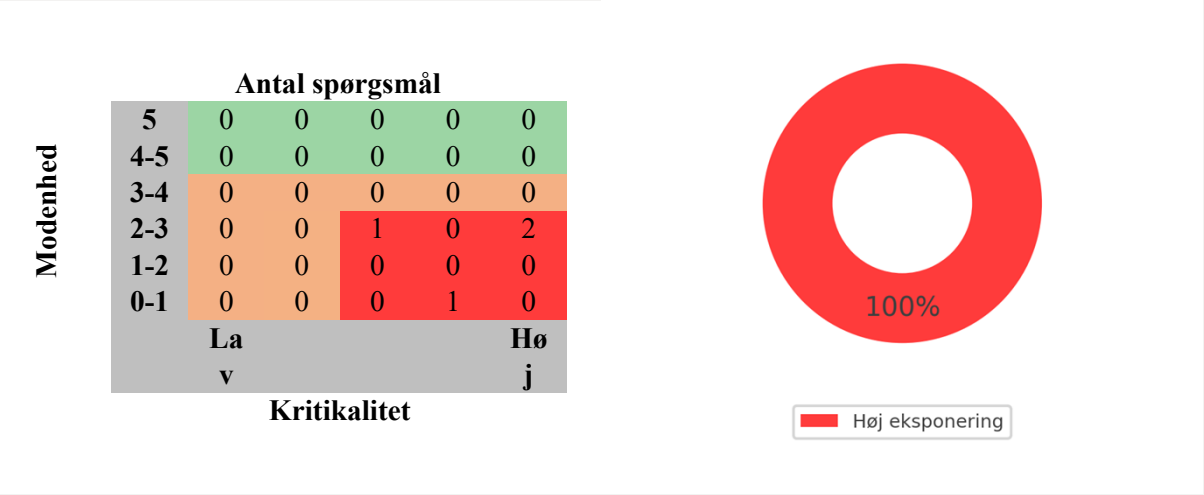


Grafen viser implementeringen af sikkerhedstiltag på sikkerhedsfunktioner. I tabellen herunder vises antallet af spørgsmål som organisationen har besvaret og hvor mange spørgsmål, der i alt afdækker organisationens indsatser fordelt på sikkerhedsfunktioner.

Sikkerhedsfunktion / Type	Spørgsmål besvaret	Spørgsmål i alt
Opdag	2	2
Beskyt	2	3

Risiko

I tabellen herunder ses organisationens eksponering for cybertrusler som implementering af sikkerhedsindsatser (modenhed) ift. konsekvensen ved manglende indsats (kritikalitet).



Indsatsområder

Kritiske tiltag med utilstrækkelig implementering

4 kritiske tiltag med lavt svar, hvor konsekvenser kan have stor betydning for sikkerheden.

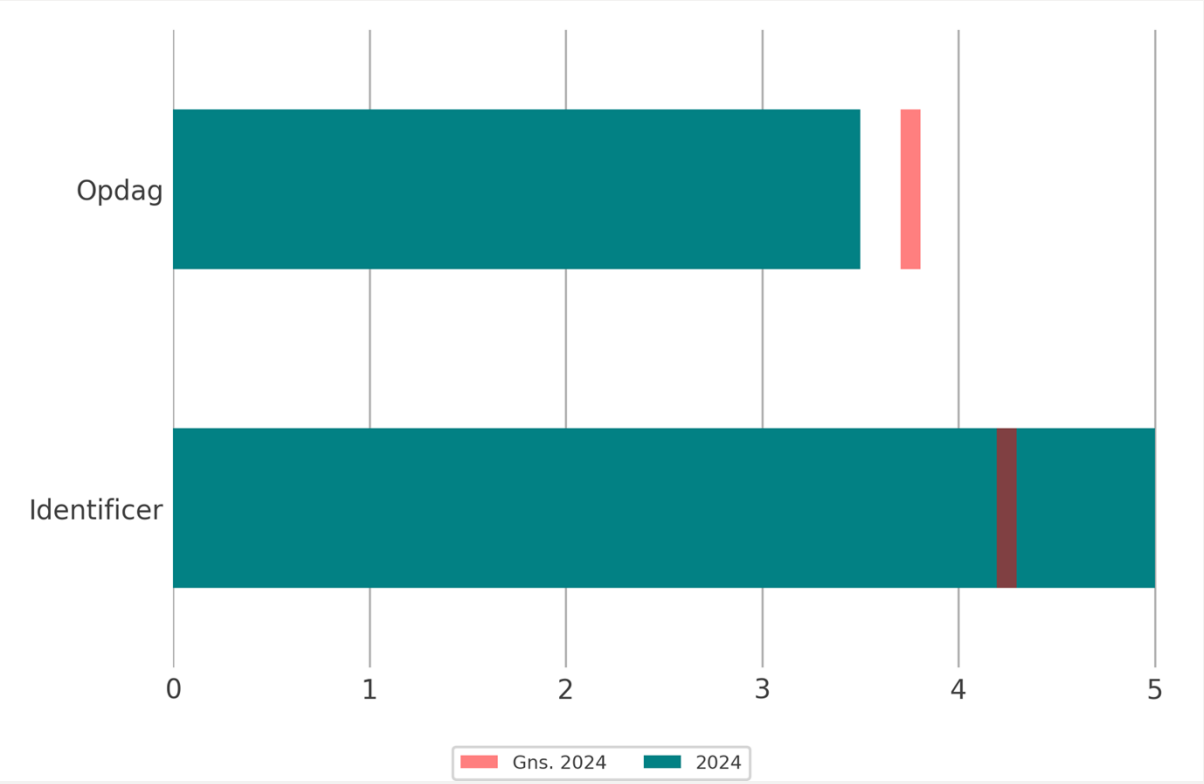
Spørgsmål	Svar	Gns.	Type
Uddannes medarbejdere i informationssikkerhed?	2.0	3.42	Opdag
Får alle nyansatte særlig introduktion i informationssikkerhed?	2.0	3.37	Beskyt
Gennemgår alle medarbejdere regelmæssigt videreuddannelse i informationssikkerhed?	2.0	2.97	Beskyt
Måles medarbejdernes viden om informationssikkerhedspolitikken eller dens retningslinjer?	0.0	2.14	Opdag

Ikke-kritiske tiltag med utilstrækkelig implementering

0 ikke-kritiske tiltag med lav implementering, hvor konsekvenser kan have stor betydning for sikkerheden.

10: Leverandørstyring

Status

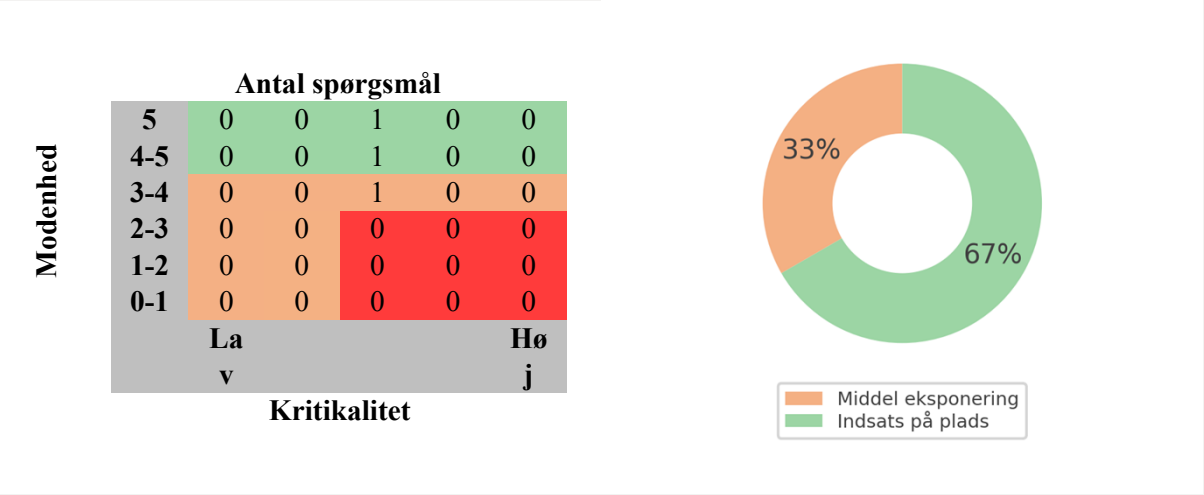


Grafen viser implementeringen af sikkerhedstiltag på sikkerhedsfunktioner. I tabellen herunder vises antallet af spørgsmål som organisationen har besvaret og hvor mange spørgsmål, der i alt afdækker organisationens indsatser fordelt på sikkerhedsfunktioner.

Sikkerhedsfunktion / Type	Spørgsmål besvaret	Spørgsmål i alt
Opdag	2	3
Identificer	1	1

Risiko

I tabellen herunder ses organisationens eksponering for cybertrusler som implementering af sikkerhedsindsatser (modenhed) ift. konsekvensen ved manglende indsats (kritikalitet).



Indsatsområder

Kritiske tiltag med utilstrækkelig implementering

0 kritiske tiltag med lavt svar, hvor konsekvenser kan have stor betydning for sikkerheden.

Ikke-kritiske tiltag med utilstrækkelig implementering

1 ikke-kritiske tiltag med lav implementering, hvor konsekvenser kan have stor betydning for sikkerheden.

Spørgsmål	Svar	Gns.	Type
Dokumenteres organisationens krav til sikkerheden hos leverandører i serviceaftaler (SLA) eller databehandleraftaler?	3.0	4.24	Opdag