FOLKETINGET
STATSREVISORERNE

FOLKETINGET
RIGSREVISIONEN

September 2025
– 24/2024

Rigsrevisionens beretning afgivet
til Folketinget med Statsrevisorernes
bemærkninger

Forsvarsministeriets beskyttelse af oplysninger om våben

24/2024

Beretning om

Forsvarsministeriets beskyttelse af oplysninger om våben

Statsrevisorerne fremsender denne beretning med deres bemærkninger til Folketinget og vedkommende minister, jf. § 3 i lov om statsrevisorerne og § 18, stk. 1, i lov om revisionen af statens regnskaber m.m.

København 2025

Denne beretning til Folketinget skal behandles ifølge lov om revisionen af statens regnskaber, § 18:

Statsrevisorerne fremsender med deres bemærkning Rigsrevisionens beretning til Folketinget og vedkommende minister.

Forsvarsministeren afgiver en redegørelse til beretningen.

Rigsrevisor afgiver et notat med bemærkninger til ministerens redegørelse.

På baggrund af ministerens redegørelse og rigsrevisors notat tager Statsrevisorerne endelig stilling til beretningen, hvilket forventes at ske i januar 2026.

Ministerens redegørelse, rigsrevisors bemærkninger og Statsrevisorernes eventuelle bemærkninger samles i Statsrevisorernes Endelig betænkning over statsregnskabet, som årligt afgives til Folketinget i februar måned – i dette tilfælde Endelig betænkning over statsregnskabet 2024, som afgives i februar 2026.

Statsrevisorernes bemærkning tager udgangspunkt i denne karakterskala:

Karakterskala	
Positiv kritik	• finder det meget/særdeles positivt • finder det positivt • finder det tilfredsstillende/er tilfredse med
Kritik under middel	• finder det ikke helt tilfredsstillende
Middel kritik	• finder det utilfredsstillende/er utilfredse med • påpeger/understreger/henstiller/forventer • beklager/finder det bekymrende/foruroligende
Skarp kritik	• kritiserer/finder det kritisabelt/kritiserer skarpt/indskærper • påtaler/påtaler skarpt
Skarpeste kritik	• påtaler skarpt og henleder særligt Folketingets opmærksomhed på

Henvendelse vedrørende denne publikation rettes til:
Statsrevisorerne
Folketinget
Christiansborg
1240 København K

Tlf.: 3337 5987
statsrevisorerne@ft.dk
www.ft.dk/statsrevisorerne

ISSN 2245-3008
ISBN online 978-87-7434-874-0

Statsrevisorernes bemærkning

Beretning om Forsvarsministeriets beskyttelse af oplysninger om våben

Forsvaret opbevarer våben mange steder, fx på deres kaserner, på depoter uden for kasernerne og hjemme hos frivillige i Hjemmeværnet. For at beskytte Forsvarets våben er det vigtigt, at Forsvarsministeriet kun giver deres ansatte adgang til oplysninger om våben i ministeriets it-systemer, hvis de har et arbejdsmæssigt behov for oplysningerne. Systemerne indeholder bl.a. oplysninger om, hvor mange og hvilke våben Forsvaret har, og hvor de opbevares. Forsvarsministeriet har to it-systemer, der indeholder oplysninger om våben. Systemerne bruges af ansatte på hele ministeriets område.

Formålet med undersøgelsen er at vurdere, om Forsvarsministeriet har sikret en tilstrækkelig beskyttelse af ansattes adgang til oplysninger om våben i ministeriets it-systemer.

Statsrevisorerne finder det kritisabelt, at Forsvarsministeriet har givet mange ansatte adgang til oplysninger om våben i ministeriets it-systemer uden at vurdere, om de har et arbejdsmæssigt behov herfor. Samtidig følger Forsvarsministeriet heller ikke tilstrækkeligt med i, hvem der tilgår oplysningerne i it-systemerne. Konsekvensen af dette er, at der er risiko for, at ansatte bevidst eller ubevidst videregiver oplysninger om Forsvarets våben, og at disse oplysninger kan bruges som led i spionage, sabotage og anden kriminalitet.

Statsrevisorerne

8. september 2025

Mette Abildgaard
Leif Lahn Jensen
Serdal Benli
Mikkel Irminger Sarbo
Lars Christian Lilleholt
Mohammad Rona

Statsrevisorerne bemærker:

- At en del af de ansatte, der har adgang til it-systemerne, har adgang til detaljerede oplysninger om våben, herunder fx antallet af våben, typer af våben og våbnenes placering.
- At Forsvarsministeriet ikke lever op til flere af kravene i den internationale standard for informationssikkerhed og flere af kravene i ministeriets egne sikkerhedsbestemmelser.
- At Forsvarsministeriet ikke har vurderet, om de ansatte har et arbejdsmæssigt behov for våbenoplysningerne.
- At Forsvarsministeriet finder, at adgangen til oplysninger om våben skal ses i sammenhæng med beskyttelsen af de militære områder, hvor Forsvaret opbevarer våben. Rigsrevisionens beretning om Forsvarsministeriets beskyttelse af militære områder viser dog, at ministeriets beskyttelse af områderne er kritisabel.

Statsrevisorerne er enige med Rigsrevisionen i, at Forsvarsministeriet bør tage stilling til, om ansatte med adgang til oplysninger om Forsvarets våben har et arbejdsmæssigt behov for oplysningerne, uanset om de ansatte er blevet sikkerhedsgodkendt, og uanset om de militære områder er tilstrækkeligt beskyttet.

Statsrevisorerne konstaterer, at Forsvarsministeriet har oplyst, at de vil iværksætte tiltag til at styrke it-sikkerheden og beskyttelsen af de militære områder.

Indholdsfortegnelse

Rigsrevisionen har selv taget initiativ til denne undersøgelse og afgiver derfor beretningen til Statsrevisorerne i henhold til § 17, stk. 2, i rigsrevisorloven, jf. lovbekendtgørelse nr. 101 af 19. januar 2012.

Rigsrevisionens mandat til at gennemføre undersøgelsen følger af rigsrevisorlovens § 2, stk. 1, nr. 1.

Beretningen vedrører finanslovens § 12. Forsvarsministeriet.

I undersøgelsesperioden august 2024 - april 2025 har der været følgende minister:

Troels Lund Poulsen: februar 2023 -

Beretningen har i udkast været forelagt Forsvarsministeriet, hvis bemærkninger i videst muligt omfang er afspejlet i beretningen.

1. Indledning

1.1. Formål og konklusion

1. Denne beretning handler om beskyttelsen af de oplysninger om våben, ammunition og eksplosiver, som Forsvarsministeriets ansatte har adgang til i ministeriets it-systemer. Vi omtaler herefter våben, ammunition og eksplosiver som våben.

Oplysninger om våben er oplysninger om, hvor mange og hvilke våben Forsvaret har, samt hvor de opbevares. Forsvaret opbevarer våben mange steder, fx på deres kaserner, på depoter uden for kasernerne og hjemme hos frivillige i Hjemmeværnet.

2. Våben har betydning for Forsvarets mulighed for at udføre deres opgaver og kan få fatale følger i de forkerte hænder. Derfor skal våben ifølge Forsvarsministeriets egne sikkerhedsbestemmelser være særligt beskyttet.

For at beskytte Forsvarets våben er det vigtigt, at ministeriet kun giver deres ansatte adgang til oplysninger om våben i ministeriets it-systemer, hvis de har et arbejdsmæssigt behov for oplysningerne. Det er også vigtigt, at ministeriet følger med i, hvilke oplysninger de ansatte tilgår i systemerne, så ministeriet kan opdage mistænkelig aktivitet. Hvis ministeriet ikke beskytter oplysningerne om våben godt nok, er der risiko for, at oplysningerne ender hos uvedkommende personer og fx bruges som led i spionage, sabotage eller anden kriminalitet.

Skydeøvelse i Forsvaret. **Foto:** Henning Bagger /Ritzau Scanpix

Forsvarsministeriet har to it-systemer, der indeholder oplysninger om våben. Systemerne bruges af ansatte på hele ministeriets område. De ansatte, der har adgang til oplysningerne, kan se en betydelig del af Forsvarets våbenbeholdning.

3. Forsvarets Efterretningstjeneste (FE) vurderede i 2024, at truslen mod Danmark er blevet mere alvorlig. Vurderingen er bl.a. baseret på, "*at Rusland optræder mere og mere risikovilligt og blandt andet har gennemført sabotageaktioner i flere europæiske lande*". Ifølge FE spionerer fremmede stater, især Rusland og Kina, mod Danmark. FE vurderer, at "*både Rusland og Kina særligt forsøger at skaffe sig adgang til oplysninger om politiske processer, udenrigs-, sikkerheds- og forsvarspolitik og militære kapaciteter*".

Ifølge Center for Cybersikkerhed udgør ansatte en potentiel vej ind i enhver organisation, da de enten bevidst eller ubevidst kan sprede, skade eller ændre informationer. Ansatte, der ubevidst handler skadeligt, er ifølge Center for Cybersikkerhed involveret i op mod halvdelen af sikkerhedshændelserne i en organisation.

Det er offentligt kendt, at der tidligere har været hændelser, hvor Forsvarets våben er blevet stjålet og er endt i kriminelle grupper eller brugt til kriminelle formål.

4. Formålet med undersøgelsen er at vurdere, om Forsvarsministeriet har sikret en tilstrækkelig beskyttelse af ansattes adgang til oplysninger om våben i ministeriets it-systemer.

Rigsrevisionen har selv taget initiativ til undersøgelsen i august 2024.

5. Forsvarsministeriet har oplyst, at våben kræver særlig beskyttelse. Oplysninger om våben er klassificerede, men er ifølge ministeriet almindeligt forekommende i Forsvaret og kræver ikke særlig beskyttelse. Dermed behandler ministeriet ikke oplysninger om våben anderledes end oplysninger om andre genstande som fx sokker og uniformer.

Rigsrevisionen konstaterer, at det følger af sikkerhedscirkulæret og Forsvarsministeriets sikkerhedsbestemmelser, at ministeriet skal beskytte klassificerede oplysninger – herunder oplysninger om våben. Fx skal ministeriet kun give ansatte indsigt i oplysningerne, hvis de ansatte har et arbejdsmæssigt behov. Kravene i ministeriets sikkerhedsbestemmelser har bl.a. til formål at beskytte ministeriets it-systemer mod spionage, sabotage og anden kriminalitet.

6. Forsvarsministeriet har vurderet, at nogle af de problemer, som Rigsrevisionen har afdækket i denne undersøgelse, ikke kan offentliggøres. Det skyldes ifølge ministeriet, at der er tale om sikkerhedsforhold, der vedrører ministeriets it-systemer, og at Rigsrevisionens beskrivelser af problemerne kan gøre det lettere at begå kriminalitet. Rigsrevisionen har imødekommet ministeriets ønske om fortrolighed. Beretningen, der er baseret på omfattende og detaljeret materiale, indeholder derfor kun overordnede og summariske beskrivelser af problemerne.

Konklusion

Forsvarsministeriets beskyttelse af ansattes adgang til oplysninger om våben er meget utilfredsstillende. Ministeriet har givet mange ansatte adgang til oplysninger om våben i ministeriets it-systemer uden at vurdere, om de har et arbejdsmæssigt behov herfor. Ministeriet følger heller ikke tilstrækkeligt med i, hvem der tilgår oplysningerne. Forsvarsministeriet lever dermed ikke op til flere af kravene i den internationale standard for informationssikkerhed og flere af kravene i ministeriets egne sikkerhedsbestemmelser.

Konsekvensen er, at der er en øget risiko for, at ansatte bevidst eller ubevidst videregiver oplysninger om Forsvarets våben, som kan bruges som led i spionage, sabotage og anden kriminalitet.

En del af de ansatte, der har adgang til de undersøgte it-systemer, har adgang til detaljerede oplysninger om våben. Oplysningerne er fx antallet af våben, typer af våben og våbnenes placering. Ministeriet har ikke vurderet, om de ansatte har et arbejdsmæssigt behov for oplysningerne. Ministeriet følger heller ikke tilstrækkeligt med i, hvem der søger på oplysningerne i it-systemerne, og hvilke oplysninger der søges på.

Militære områder
Militære områder er arealer og bygninger, som benyttes af myndigheder under Forsvarsministeriet. Militære områder omfatter bl.a. kaserner, flådestationer, flyvestationer, øvelsesområder og skydeterræner.

Forsvarsministeriet har oplyst, at alle ansatte med adgang til it-systemerne er sikkerhedsgodkendt. Ministeriet har også oplyst, at adgangen til oplysninger om våben i it-systemerne ikke kan ses isoleret, men skal ses i sammenhæng med beskyttelsen af de militære områder, hvor Forsvaret opbevarer våben. Det skyldes, at uvedkommende personer kun kan skaffe sig adgang til våbnene ved også at tvinge sig adgang til områderne. Rigsrevisionens beretning om Forsvarsministeriets beskyttelse af militære områder viser, at ministeriets beskyttelse af områderne er kritisabel.

Rigsrevisionen vurderer, at Forsvarsministeriet bør tage stilling til, om ansatte med adgang til oplysninger om Forsvarets våben har et arbejdsmæssigt behov for oplysningerne. Det gælder, uanset om de ansatte er blevet sikkerhedsgodkendt, og uanset om de militære områder er tilstrækkeligt beskyttet. Rigsrevisionen lægger vægt på, at oplysninger om våben i sig selv eller i kombination med andre kilder kan bruges som led i bl.a. spionage, sabotage og anden kriminalitet og derfor er oplysninger, som bør beskyttes.

Forsvarsministeriet har oplyst, at de vil iværksætte tiltag til at styrke it-sikkerheden og beskyttelsen af de militære områder.

1.2. Vurderingskriterier, metode og afgrænsning

Vurderingskriterier

7. Vores undersøgelse er baseret på 19 vurderingskriterier, som følger af den internationale standard for informationssikkerhed (ISO 27001) og af Forsvarsministeriets "Bestemmelser for den Militære Sikkerhedstjeneste". Det har siden 2016 været obligatorisk for statslige myndigheder at følge ISO 27001. Standarden beskriver bl.a., hvordan myndighederne skal beskytte deres informationer.

Forsvarsministeriets bestemmelser for militær sikkerhed er ministeriets egne krav til, hvordan ministeriets myndighedsområde skal beskyttes. Bestemmelserne er bl.a. baseret på sikkerhedscirkulæret, NATO's sikkerhedsbestemmelser, Forsvarsministeriets direktiv for den militære sikkerhedstjeneste, ISO 27001 og Forsvarsministeriets bestemmelser om informationssikkerhed.

Formålet med bestemmelserne for militær sikkerhed er bl.a. at beskytte mod trusler rettet mod Forsvarets informationer og it-systemer. Det fremgår af bestemmelserne, at Forsvarsministeriet skal tage højde for de ansattes arbejdsmæssige behov, når de giver de ansatte adgang til oplysninger i systemerne.

Forsvarets Efterretningstjeneste har udarbejdet bestemmelserne, og forsvarschefen har godkendt dem. Forsvarsministeriet har det overordnede ansvar for, at informationssikkerheden lever op til bestemmelserne. Kravene om informationssikkerhed i bestemmelserne er mindstekrav.

Vores vurderingskriterier baserer sig på de krav, der vedrører adgangsstyring, logning og beskyttelse af registreringer. Det skyldes, at disse krav er afgørende for ministeriets beskyttelse af oplysninger om våben. Vi har dermed ikke undersøgt alle krav i ISO 27001 eller alle krav i ministeriets bestemmelser.

Metode

8. Undersøgelsen baserer sig på dokumentgennemgang og besøg hos Forsvarsministeriets myndigheder samt på demonstrationer og gennemgange af de it-systemer, der indeholder oplysninger om våben.

9. Undersøgelsens metode er uddybet i bilag 1.

10. Revisionen er udført i overensstemmelse med standarderne for offentlig revision, jf. bilag 1.

Afgrænsning

11. Undersøgelsen er afgrænset til at omfatte de dele af Forsvarsministeriets it-systemer, der indeholder oplysninger om våben. Undersøgelsen omfatter dermed ikke andre oplysninger i systemerne.

Undersøgelsen vedrører ministeriets ansattes adgang til oplysninger om våben. Ansatte dækker medarbejdere på Forsvarsministeriets område samt it-leverandører og konsulenter ansat af ministeriet. Vi har ikke undersøgt ministeriets beskyttelse af it-systemer mod hackerangreb fra eksterne, ligesom vi ikke har undersøgt ministeriets it-beredskab.

12. Rigsrevisionen har i en selvstændig beretning fra september 2025 undersøgt, om Forsvarsministeriet har sikret en tilstrækkelig beskyttelse af militære områder. Denne beretning omfatter derfor ikke denne problemstilling.

13. Undersøgelsen er afgrænset til perioden august 2024 - april 2025. Undersøgelsen omhandler det sikkerhedsbillede, der var aktuelt på dette tidspunkt, og omfatter ikke eventuelle initiativer, som Forsvarsministeriet efterfølgende har gennemført.

2. Beskyttelse af oplysninger om våben

14. Dette kapitel handler om, hvorvidt Forsvarsministeriet har sikret en tilstrækkelig beskyttelse af ansattes adgang til oplysninger om våben i ministeriets it-systemer.

Undersøgelsen viser, at Forsvarsministeriet ikke har sikret en tilstrækkelig beskyttelse af ansattes adgang til oplysninger om våben i ministeriets it-systemer. Forsvarsministeriet lever dermed ikke op til flere af kravene i den internationale standard for informationssikkerhed og flere af kravene i ministeriets egne sikkerhedsbestemmelser.

Vi omtaler af sikkerhedsmæssige hensyn de to undersøgte it-systemer som system A og system B.

15. Vores undersøgelse er baseret på 19 vurderingskriterier, hvoraf 9 omhandler system A, og 10 omhandler system B. Den samlede oversigt over vurderingskriterierne fremgår af tabel 1.

Tabel 1
Antal vurderingskriterier fordelt på emner for de to it-systemer

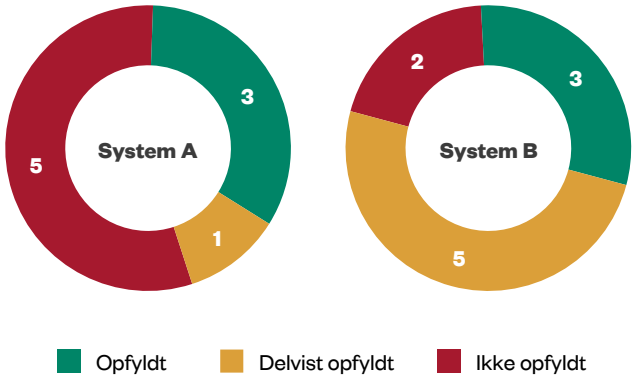
Emne		Kriterier for system A	Kriterier for system B
Adgang til oplysninger om våben	Vurdering af adgange	3	4
	Regelmæssig gennemgang af adgange	2	1
Logning af opslag om våben	Logning og beskyttelse af loggen	2	3
Beskyttelse af registreringer af oplysninger om våben	Kvalitetssikring af oplysninger	1	1
	Beskyttelse mod uautoriseret ændring og sletning af oplysninger	1	0
	Sikkerhedsopdatering og supportering	0	1
Vurderingskriterier i alt		**9**	**10**

Note: Vi har ikke undersøgt vurderingskriterier relateret til emnet "Sikkerhedsopdatering og supportering" for system A, da vi tidligere har afrapporteret disse i anden sammenhæng. Vi har ikke undersøgt vurderingskriterier relateret til emnet "Beskyttelse mod uautoriseret ændring og sletning af oplysninger" for system B, da it-systemet ikke indeholder stamdata. Stamdata kan fx være serienummer på et våben.

Kilde: Rigsrevisionen.

Det samlede resultat af undersøgelsens 19 vurderingskriterier fremgår af figur 1. Vi har i figuren fordelt vurderingskriterierne på de to it-systemer.

Figur 1
Opfyldelsen af vurderingskriterier i system A og i system B



Kilde: Rigsrevisionen på baggrund af oplysninger fra Forsvarsministeriet.

Figur 1 viser, at beskyttelsen af oplysninger om våben i system A ikke er opfyldt for 5 af vurderingskriterierne, er delvist opfyldt for 1 af kriterierne og opfyldt for 3 af kriterierne. For system B er 2 af kriterierne ikke opfyldt, 5 af kriterierne er delvist opfyldt, og 3 af kriterierne er opfyldt.

Rigsrevisionen konstaterer, at der er flest svagheder i system A, som også er det it-system, der indeholder de mest kritiske oplysninger om våben.

I de følgende afsnit uddyber vi undersøgelsens resultater i forhold til de enkelte vurderingskriterier.

2.1. Adgang til oplysninger om våben

Vurdering af adgange

16. Forsvarsministeriet skal vurdere og beskrive, hvilke adgange ansatte skal have i ministeriets it-systemer. Vurderingen skal foretages på baggrund af de ansattes arbejdsmæssige behov og på baggrund af, hvor sensitive og vitale oplysningerne er. Dette følger af den internationale standard for informationssikkerhed og af ministeriets egne sikkerhedsbestemmelser.

17. Vores undersøgelse viser, at Forsvarsministeriet har givet mange ansatte adgang til oplysninger om våben i system A uden at beskrive og vurdere, om de har et arbejdsmæssigt behov for oplysningerne. Vi kan af hensyn til fortrolighed ikke oplyse det præcise antal ansatte. Der er forskel på, hvor detaljerede oplysninger de ansatte kan se, men fælles for dem er, at de kan se én eller flere oplysninger relateret til våben.

Næsten halvdelen af de ansatte, der har adgang til oplysningerne om våben i system A, kan se detaljerede oplysninger om våben. Det kan være oplysninger om antallet af våben, typer af våben og våbnenes placering. Forsvarsministeriet har ikke vurderet og beskrevet, om de har et arbejdsmæssigt behov for oplysningerne.

Typer af våben
Typer af våben er oplysninger, der viser, hvilke typer af våben Forsvaret opbevarer. Det er fx pistoler, maskingeværer, ammunition, håndgranater og miner.

De fleste af de ansatte, der har adgang til oplysningerne i system A, kan se, hvilke typer af Forsvarets våben der er i transit. Våben i transit er våben, der bliver flyttet eller skal flyttes fra én placering til en anden med fx lastbil. Når våben er i transit, er de taget ud af et depot, pakket ned i en kasse og enten: 1) klar til at blive sendt, 2) sendt afsted i transport eller 3) ankommet til et andet depot.

Forsvarsministeriet har oplyst, at ministeriet beskytter våben, der er i transit. Vi har ikke efterprøvet, om dette er korrekt.

18. Vores undersøgelse viser også, at Forsvarsministeriet har givet en række ansatte adgang til oplysninger om våben i system B uden at foretage en vurdering af, om de har et arbejdsmæssigt behov for oplysningerne. Med adgangen kan de ansatte se detaljerede oplysninger om de våben, der er registreret i systemet. Der er derfor risiko for, at oplysningerne kan ses af ansatte, som ikke har arbejdsmæssigt behov.

19. Forsvarsministeriet har oplyst, at størstedelen af de ansatte, der har adgang til oplysninger om våben i system A og system B, er ansat steder i Forsvaret, hvor der ofte vil være behov for at kunne tilgå oplysninger om våben. Herudover har ministeriet oplyst, at alle ansatte skal være sikkerhedsgodkendt for at få adgang til systemerne.

Rigsrevisionen konstaterer, at Forsvarsministeriet ifølge ministeriets egne bestemmelser skal vurdere, om ansatte har et arbejdsmæssigt behov for adgangen til oplysningerne, uanset hvor de arbejder, og uanset om de er sikkerhedsgodkendt.

Regelmæssig gennemgang af adgange

20. Forsvarsministeriet skal regelmæssigt gennemgå ansattes adgange til oplysninger i it-systemer for at sikre, at de ansatte fortsat har et arbejdsmæssigt behov for oplysningerne. Ministeriet skal også sikre, at de ansatte ikke har adgang til flere eller andre oplysninger end de oplysninger, ministeriet har besluttet at give dem adgang til.

21. Vores undersøgelse viser, at Forsvarsministeriet ikke regelmæssigt gennemgår, om ansatte fortsat har behov for oplysninger om våben for at udføre deres arbejde. Ministeriet gennemgår heller ikke, om de ansatte i praksis kan se flere eller mere sensitive oplysninger end dem, ministeriet har besluttet at give dem adgang til. Dermed er der risiko for, at nogle ansatte fx kan se placeringen af våben, uden at ministeriet har taget stilling til, om de har et arbejdsmæssigt behov.

2.2. Logning af opslag om våben

Logning og beskyttelse af loggen

22. Forsvarsministeriet skal ifølge den internationale standard for informationssikkerhed og egne bestemmelser tage stilling til, hvilke hændelser i ministeriets it-systemer der skal logges. Ministeriet skal også logge alle sikkerhedsbetydende hændelser. Logning betyder, at man registrerer, hvem der opretter, tilgår og ændrer oplysninger i et it-system, og gemmer en oversigt over hændelser i systemet. Ministeriet skal også regelmæssigt gennemgå loggen, overvåge relevante hændelser og beskytte loggen mod ændring og sletning fra uvedkommende personer.

23. Vores undersøgelse viser, at Forsvarsministeriet ikke følger tilstrækkeligt med i, hvem der søger på oplysninger om våben i system A og system B. Ministeriet logger ikke, hvilke oplysninger de ansatte søger på i systemerne, fx hvis de søger på bestemte typer af våben. Vores undersøgelse viser, at Forsvarsministeriet har beskyttet de logger, som ministeriet har for systemerne, mod ændring og sletning fra uvedkommende personer. Ansatte kan derfor ikke slette eller ændre i loggerne for at sløre eventuelle ændringer, som de har lavet i oplysninger om våben.

2.3. Beskyttelse af registreringer af oplysninger om våben

Kvalitetssikring af oplysninger

24. Forsvarsministeriet skal beskytte oplysninger, så de er brugbare til den planlagte anvendelse. Det betyder, at ministeriet skal sikre, at oplysningerne er korrekte og retvisende.

25. Vores undersøgelse viser, at ministeriet har sikret, at registreringer af oplysninger om våben i system A er korrekte. Ministeriet kvalitetssikrer oplysninger om våben i systemet. Det kan fx være oplysninger om våben, som transporteres mellem ministeriets depoter, og som udleveres til frivillige i Hjemmeværnet.

26. Vores undersøgelse viser også, at ministeriet har sikret, at der er procedurer for kvalitetssikring af registreringer af oplysninger om våben i system B. Der er dermed lav risiko for, at der optræder forkerte oplysninger om våben i it-systemet. Det skyldes, at ansatte kun kan registrere oplysninger om et våben i systemet, hvis de har udfyldt en række felter, og hvis en sagsbehandler manuelt har kontrolleret informationerne.

Beskyttelse mod uautoriseret ændring og sletning af oplysninger

27. Forsvarsministeriet skal beskytte oplysninger tilstrækkeligt, fx mod at de slettes eller ændres uden godkendelse.

28. Vores undersøgelse viser, at ministeriet beskytter stamdata om våben i system A mod, at de slettes eller ændres uden grund. Stamdata i systemet er bl.a. våbnenes serienumre.

29. Vi har ikke undersøgt, om ministeriet beskytter stamdata om våben i system B, da it-systemet ikke indeholder stamdata.

Sikkerhedsopdatering og supportering

30. Forsvarsministeriet skal sikre, at databaser og servere bliver sikkerhedsopdateret og supporteret.

31. Vores undersøgelse viser, at ministeriet har sikret, at databasen og serverne for system B er blevet sikkerhedsopdateret. Dermed er databasen og serverne beskyttet mod, at de ansatte kan udnytte kendte sårbarheder til at få adgang til oplysninger om våben og dermed foretage uautoriserede ændringer i oplysningerne.

32. Vi har ikke undersøgt sikkerhedsopdatering og supportering for system A, da vi tidligere har afrapporteret dette i anden sammenhæng. Vores afrapportering viste, at ministeriet havde sikret dette.

Rigsrevisionen, den 28. august 2025

Birgitte Hansen

/Kristian Brink og Vicky la Cour

Bilag 1. Metodisk tilgang

Undersøgelsen bygger på en gennemgang af dokumenter, inspektion af systemer og møder med udvalgte medarbejdere fra Forsvarsministeriet og Forsvarsministeriets Materiel- og Indkøbsstyrelse. Undersøgelsen er desuden på udvalgte områder kvalitetssikret ved demonstrationer af og udtræk fra it-systemerne, der fx viser oprettede brugere. Formålet har været at efterprøve den information, vi har fået.

Beretningen omfatter perioden august 2024 - april 2025.

Vurderingskriterier

Undersøgelsens 19 vurderingskriterier baserer sig på den internationale standard for informationssikkerhed (ISO 27001) og på Forsvarsministeriets "Bestemmelser for den Militære Sikkerhedstjeneste" (FKOBST 358-1). Vurderingskriterierne er baseret på de foranstaltninger i ISO 27001 og de krav i ministeriets bestemmelser, der vedrører adgangsstyring, logning og beskyttelse af registreringer. Det skyldes, at disse krav er afgørende for ministeriets beskyttelse af oplysninger om våben. Vi har dermed ikke undersøgt alle foranstaltninger i ISO 27001 eller alle krav i ministeriets bestemmelser.

De 19 vurderingskriterier fordeler sig overordnet set på tre emner: adgang til oplysninger om våben, logning af opslag om våben og beskyttelse af registreringer af oplysninger om våben.

Væsentlige dokumenter

Vi har gennemgået en række dokumenter, herunder:

- ISO 27001 fra 2022
- Bestemmelser for den Militære Sikkerhedstjeneste (FKOBST 358-1)
- vejledninger til system A
- vejledning til system B
- politik for adgangsstyring, herunder oprettelse af brugere og rettighedsstyring
- oversigt over brugerroller og rettigheder
- oversigt over brugerkonti
- politik for logning og overvågning
- politik for sikkerhedsopdateringer.

Formålet med gennemgangen af dokumenterne har været at undersøge Forsvarsministeriets adgangsstyring, logning og beskyttelse af registreringer af oplysninger i de dele af it-systemerne, der vedrører oplysninger om våben.

Møder

Vi har holdt møder med Forsvarsministeriet og Forsvarsministeriets Materiel- og Indkøbsstyrelse for at få indsigt i området og for at få gennemgået, valideret og uddybet det materiale, vi har modtaget i forbindelse med gennemgangen af hvert vurderingskriterie. Møderne danner ikke i sig selv grundlag for undersøgelsens resultater.

Kvalitetssikring

Undersøgelsen er kvalitetssikret via vores interne procedurer for kvalitetssikring, som omfatter høring hos den reviderede samt ledelsesbehandling og sparring med chefer og medarbejdere i Rigsrevisionen. Dokumentgennemgangen er foretaget af mindst to medarbejdere for at kvalitetssikre resultaterne.

Standarderne for offentlig revision

Revisionen er udført i overensstemmelse med standarderne for offentlig revision, herunder standarderne for større undersøgelser (SOR 3). Standarderne fastlægger, hvad brugerne og offentligheden kan forvente af revisionen, for at der er tale om en god faglig ydelse. Standarderne er baseret på de grundlæggende revisionsprincipper i rigsrevisionernes internationale standarder (ISSAI 100-999).