Kort fortalt

It-sikkerheden på Statens It's servere

Konklusion

Statens It under Finansministeriet har ikke sikret, at alle Statens It's servere kan sikkerhedsopdateres. Det skyldes dels, at Statens It ikke har opgraderet eller nedlagt servere, der ikke længere kan sikkerhedsopdateres, dels at de har et ufuldstændigt overblik over myndighedernes servere. Dette finder Rigsrevisionen utilfredsstillende. Konsekvensen er, at der er risiko for, at hackere kan få adgang til følsomme personoplysninger og forretningskritiske data, og at disse oplysninger og data kan blive misbrugt eller ødelagt.

Statsrevisorerne udtaler

"Center for Cybersikkerhed under Forsvarets Efterretningstjeneste vurderer, at truslen i Danmark fra cyberkriminalitet og cyberspionage er meget høj, og at truslen fra cyberaktivime er høj. Statsrevisorerne finder det utilfredsstillende, at Statens It ikke har sikret, at alle Statens It's servere kan sikkerhedsopdateres. Statsrevisorerne finder det bekymrende, at Statens It's utilstrækkelige sikkerhedsopdateringer og utilstrækkelige kompenserende foranstaltninger indebærer risiko for, at borgeres og virksomheders personoplysninger og forretningskritiske data kan blive misbrugt eller ødelagt. Statsrevisorerne finder det også bekymrende, at borgeres og virksomheders tillid til offentlige myndigheder kan blive svækket som følge deraf".

Væsentligste resultater af undersøgelsen

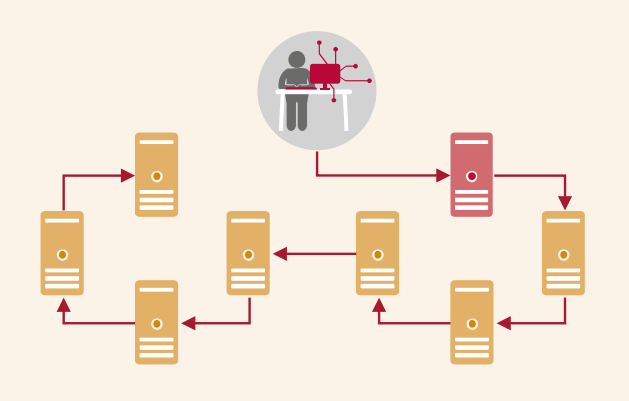
- Statens It har ikke opgraderet eller nedlagt servere, inden leverandøren er ophørt med at udvikle sikkerhedsopdateringer.
- Statens It har ikke gennemført tilstrækkelige kompenserende foranstaltninger for de servere, der ikke længere kan sikkerhedsopdateres.
- Statens It har ikke procedurer, der sikrer, at de løbende og rettidigt kan opgradere eller nedlægge servere, der ikke længere kan sikkerhedsopdateres.

Baggrund og formål med undersøgelsen

Formålet med undersøgelsen er at vurdere, om Statens It under Finansministeriet har sikret, at Statens It's servere kan sikkerhedsopdateres, så følsomme personoplysninger og forretningskritiske data ikke udsættes for en unødig risiko for kompromittering. Danmark er et af de mest digitaliserede lande i verden, og cybertrusler er derfor et grundvilkår for danske myndigheder. Cyberangreb kan medføre, at statens it-systemer og data bliver ødelagt eller gjort utilgængelige, samt at oplysninger om danske borgere og virksomheder bliver misbrugt eller ødelagt.

Det er en grundlæggende del af en god it-sikkerhed at holde servere opdaterede. En server har en begrænset levetid, hvor leverandøren forpligter sig til at udvikle sikkerhedsopdateringer, i takt med at sårbarheder opdages. Når levetiden ophører, vil serveren ikke længere kunne sikkerhedsopdateres.

Spredning af et cyberangreb mellem servere i et fiktivt åbent netværk



Statens It har ansvaret for it-drift og it-sikkerhed for de 46 myndigheder, der indgår i undersøgelsen. Statens It har ansvaret for serverne og deres sikkerhed, mens myndighederne i de fleste tilfælde har ansvaret for driften af de fagsystemer, som ligger på serverne. Statens It har oplyst, at de ikke kan opgradere eller nedlægge serverne, fordi myndighederne ikke har opfyldt deres ansvar for at sikre, at myndighedernes fagsystemer er kompatible med nye servere. Rigsrevisionen konstaterer, at det nuværende setup ikke er tilstrækkeligt til at løse problemet, og anbefaler derfor, at Finansministeriet tager stilling til, om der er den rigtige arbejds- og ansvarsfordeling mellem Statens It og myndighederne i forhold til serverne, så Statens It kan løfte deres ansvar for it-sikkerheden i statens it-infrastruktur.

Læs hele rapporten på www.rigsrevisionen.dk. Kontakt Rigsrevisionens pressechef Lisbeth Sørensen på tlf. 33 92 85 06/ls@rigsrevisionen.dk eller Statsrevisorernes sekretariatschef Gitte Korff på tlf. 33 37 59 85/ gitte.korff@ft.dk for yderligere information.

FOLKETINGET STATSREVISORERNE
FOLKETINGET RIGSREVISIONEN