UDENRIGSMINISTERIET

Statsrevisorernes Sekretariat
Folketinget
Christiansborg
1240 København K

Asiatisk Plads 2
DK-1448 København K
Telefon +45 33 92 00 00
Telefax +45 32 54 05 33
E-mail: um@um.dk
http://www.um.dk

Bilag	Sag/ID Nr.	Enhed	Dato
	2017 - 14718	Controller	23. april 2018

Udenrigsministerens redegørelse vedr. Statsrevisorernes beretning nr. 11/2017 om beskyttelse mod ransomwareangreb

Udenrigsministeriet har den 21. februar 2018 modtaget Statsrevisorernes bemærkninger til Rigsrevisionens beretning nr. 11/2017 om beskyttelse mod ransomwareangreb. Beretningen omhandler Rigsrevisionens undersøgelse af hvorvidt Sundhedsdatastyrelsen, Udenrigsministeriet, Banedanmark og Beredskabsstyrelsen har en tilfredsstillende beskyttelse mod ransomwareangreb.

Jeg er overordnet enige med Rigsrevisionen i, at ministeriets beskyttelse mod ransomware på nogle områder på revisionstidspunktet kunne styrkes yderligere – særligt set i lyset af en stadig stigende trusselsvurdering i forhold til cyberangreb. Rigsrevisionens overordnede vurdering af Udenrigsministeriets beskyttelse, som værende ikke tilfredsstillende på linje med de tre andre undersøgte institutioner, synes dog hård, ikke mindst når den underliggende vurdering af parametre tages i betragtning. Dette er der gjort opmærksomt på i skriftligt svar til Rigsrevisionen, hvor det særligt bemærkes, at Udenrigsministeriet på de indre, tekniske sikringstiltag får "grøn" på alle parametre bortset fra en enkelt "gul". Udenrigsministeriet vurderer netop de indre, tekniske sikringstiltag som meget væsentlige i forhold til at sikkerheden overfor angreb.

I forhold til den mere detaljerede bedømmelse er fem ud af samlet 20 parametre, som Rigsrevisionen anvender i beretningen, "røde". For fire af disse gælder, at Udenrigsministeriet enten allerede har, eller planlægger, at gennemføre tiltag i overensstemmelse med Rigsrevisionens anbefalinger.

Status på gennemforte tiltag:

- 2-Faktor login ved webmail losninger er implementeret ultimo 2017
- Ny backup politik er blevet udviklet og ledelsessanktioneret (orientering til UMs IT-bestyrelse på mode 19. april 2018)
- Tilpassede procedurer, der optimerer opdatering af tredjepartsprodukter mest muligt er iværksat ultimo 2017
- Systematisk back up på et uafhængigt (offline) tape-medie er implementeret ultimo 2017
- Afdækning af procedurer for systematisk aftestning af genetablering af systemer og data er iværksat primo 2018

I forhold til en af de "rode" kategorier (forhindre adgang til brug af f.eks. hotmail/gmail) er det Udenrigsministeriets vurdering, at en blokering af disse redskaber vil medfore en uhensigtsmæssig tung byrde i forhold til ministeriets arbejdsrytme og den fleksibilitet, der forudsættes hos Udenrigstjenestens medarbejdere. Udenrigsministeriet har derfor, som også tidligere svaret Rigsrevisionen, introduceret en række tiltag, der forhindrer brugere i at kunne downloade og eksekvere skadelige filer og kode.

Jeg vil gerne benytte lejligheden til at takke for den grundige undersøgelse af området. Jeg lægger især stor vægt på, at der arbejdes målrettet på at styrke it-sikkerheden, hvilket vi i Udenrigsministeriet har et særligt fokus på. Ministeriet arbejder således målrettet og kontinuerligt på at styrke it-sikkerheden i både ude- og hjemmetjenesten, både når det angår ransomware, men også mod andre former for cyberangreb.

Kopi af redegørelsen er samtidig sendt til Rigsrevisionen.

Med venlig hilsen

Anders Samuelsen
Udenrigsminister