

København 04.06.2024

OPSUMMERING AF PRESSEMØDE VEDR. ØGET TRUSSELSNIVEAU

Hvad er nyt? Center for Cybersikkerhed (CFCS) hæver deres trusselsniveau for destruktive cyberangreb fra lavt til middel.

Hvorfor er det relevant? Set i lyset af den stigende trussel fra Rusland italesætter forsvarsministeren nu behovet for, at danske myndigheder, virksomheder og borgere er bedre forberedt i tilfælde af angreb fra Rusland.

Hvad sker der nu? CFCS har fremlagt en række anbefalinger til, hvordan virksomheder skal håndtere dette, og regeringen lover samtidig at udarbejde et borgerberedskab inden for de næste to uger.

Materialer

- Du finder pressemeddelelsen her: [LINK](#)
- Du finder anbefalingerne fra CFCS her: [LINK](#)

Lidt mere kontekst

På baggrund af den øgede trussel fra Rusland hæver Center for Cybersikkerhed (CFCS) deres trusselsniveau for destruktive cyberangreb fra lavt til middel. Der er stadig to højere trusselsniveauer, og der er derfor ikke tale om en konkret trussel netop nu.

Meldingen er i særdeleshed henvendt til virksomheder og myndigheder, men der opfordres også til, at borgere skal være særligt opmærksomme på russisk påvirkning. Derudover lover regeringen at komme med et såkaldt borgerberedskab indenfor 14 dage.

Vigtige nedslagspunkter

- Trusselsniveauet for destruktive cyberangreb fra Rusland hæves fra lavt til middel.
- Det er særligt henvendt til virksomheder og myndigheder, der bør genbesøge deres cyberberedskaber.
- Forsvarsministeren finder det nødvendigt at orientere den danske befolkning om det øgede trusselsniveau og vil udarbejde et borgerberedskab.
- Der er ikke tale om en konkret trussel, men trusselbilledet kan ændre sig fra dag til dag og uden varsel.

Referat af pressemøde

- CFCS hæver trusselsniveauet for destruktive cyberangreb fra lavt til middel.
- Dette er på baggrund af trusler fra Rusland.
- Truslen kan komme til udtryk som angreb mod elforsyning, vandforsyning eller lignende.
- Rusland er blevet mere risikovillige til at bruge den slags angreb mod vestlige lande, herunder Danmark.
- Destruktive cyberangreb er designet til at skabe ravage og til at ødelægge ting eller systemer.

- Manipulation af operationelle systemer, som kan medføre strømsvigt, er der stadig lav sandsynlighed for.
- Det er vigtigt, at myndigheder og styrelser får styr på deres cyberberedskaber med det samme.
- Det anbefales, at virksomheder og myndigheder genbesøger deres foranstaltninger mod cyberangreb.
- CFCS har lavet en række råd til virksomheder, som ligger på deres hjemmeside.
- *Hvad forventer forsvarsministeren og CFCS, at borgerne gør nu? Det tegner et billede af, at vi bevæger os ind i en alvorlig situation. Der er ikke en konkret trussel, men situationen er alvorlig, og det er essentielt, at danskerne bliver orienteret. Hævelsen af trusselsniveauet er mestendels henvendt til virksomheder og myndigheder, men borgere skal være opmærksom på, at man kan blive påvirket udefra. Danskerne skal læse denne melding som et pejlemærke om, at man skal forberede sig til et nyt trusselsbillede. Regeringen fremlægger et borgerberedskab, der skal kommunikere, hvordan borgerne skal forholde sig til dette.*
- Forsvarsministeren vil ikke komme med konkrete tal som i Norge, hvor befolkningen er blevet anbefalet at kunne klare sig i syv dage, men siger, at det er klogt at vise rettidig omhu.
- Truslen er stadig kun middel, men kan ændre sig uden varsel. Rusland har midlerne til at udføre angreb, så det handler udelukkende om intentionerne.