FORSVARSMINISTERIET
MINISTRY OF DEFENCE

DET TALTE ORD GÆLDER

Taleseddel til FOU (alm. del) samrådsspørgsmål S, 11. maj 2017

Det russiske hackerangreb på Forsvaret

FOU samrådsspørgsmål S
Hvad kan ministeren oplyse om det russiske hackerangreb på Forsvaret? Hvordan vil regeringen reagere i forhold til Rusland, og hvordan vil regeringen styrke sikkerheden omkring forsvarets IT-systemer?

Spørgsmålet er stillet efter ønske fra Holger K. Nielsen (SF).

Besvarelse
Jeg vil indledningsvis godt takke udvalget for invitationen til at komme her i dag for at besvare spørgsmål om et meget aktuelt og vigtigt emne, nemlig Ruslands bekymrende adfærd.

Jeg vil også godt begynde med en forventningsafstemning, for det er sådan, at der kan være visse spørgsmål, jeg ikke kan besvare hverken helt eller delvist. Det kan fx være spørgsmål, der vedrører klassificerede oplysninger, som må håndteres i Kontroludvalget eller spørgsmål om sikkerhedsmæssige tiltag.

Selve hackerangrebet mod Forsvaret er beskrevet i en undersøgelsesrapport, som Center for Cybersikkerhed har offentliggjort med henblik på, at myndigheder og virksomheder kan drage nytte af erfaringerne fra hændelserne, og som indeholder forslag til tiltag, der kan hjælpe til at modvirke lignende angreb.

I 2015 og 2016 var Forsvaret udsat for en målrettet og vedholdende angrebskampagne. Kampagnen løb over lang tid, og der blev brugt forskellige metoder.

Som følge af kampagnen blev et af Forsvarets systemer til uklassificeret e-mail kompromitteret.

Det system, der blev angrebet, er det, der kaldes "mil.dk", altså e-mailadresser, der slutter på '@mil.dk'.

Det er lykkedes hackerne at stjæle passwords til visse brugeres e-mailkonti ved at lokke målpersoner til at indtaste deres loginoplysninger på falske loginsider. De falske loginsider lignede til forveksling den side, som brugerne af mil.dk normalt logger ind på. Der var fx oprettet en internetside, hvor den eneste forskel til den rigtige side var, at et enkelt punktum var skiftet ud med en bindestreg.

Hackerne har herefter kunnet anvende de login-oplysninger, som målpersonerne havde indtastet på de falske sider, til at kompromittere deres mailkonti.

Center for Cybersikkerhed vurderer, at et antal forsvarsansattes mailkonti på mil.dk har været kompromitterede i en længere periode.

Det vurderes, at indhold i de kompromitterede mailkonti er blevet kopieret af hackerne, i visse tilfælde ad flere omgange, i 2015 og 2016.

Det konstaterede angreb har sandsynligvis betydet, at uvedkommende har fået adgang til en større mængde information i form af mail-korrespondancer på de kompromitterede konti.

Mil.dk er en ikke-klassificeret mailtjeneste, men indhold i mails er generelt beskyttelsesværdigt.

Aktøren har også forsøgt at skaffe sig adgang til mil.dk konti ved at teste et meget stort antal mulige adgangskoder sammen med udvalgte brugernavne. Center for Cybersikkerhed har ikke set tegn på, at disse 'forceringsangreb' er lykkedes.

Samtidig med kompromitteringen af log-in oplysinger og e-mails fra mil.dk har der også været gennemført angreb med et større antal phishing-mails.

Via disse phishing-mails har aktøren forsøgt at installere malware på de ramte medarbejderes PC'ere, så aktøren kunne få adgang til og kontrol over dem.

Der er ikke set tegn på, at det er lykkedes for aktøren at installere malware på nogle maskiner og få kontrol over dem som følge af denne phishing-kampagne.

Jeg vil gerne understrege, at e-mailsystemet, der blev angrebet, som sagt er uklassificeret og derfor ikke har haft det samme høje sikkerhedsniveau, som Forsvarets mere sensitive systemer, som ikke er berørt.

Det ændrer dog ikke ved, at uvedkommende selvfølgelig ikke må få adgang til Forsvarets systemer.

Sikkerheden på mil.dk er derfor blevet hævet, og man er fortsat i gang med at opdatere det med væsentlig bedre sikkerhed. Så der er nu dæmmet op for angrebet, og systemet er ved at blive ændret for at mindske effekten af denne slags hændelser i fremtiden.

Og hvem var det så, der stod bag angrebet?

Center for Cybersikkerhed vurderer, at angrebene stammer fra en statsstøttet aktør – den såkaldte Fancy Bear gruppe, eller APT28, som også er kendt under en række andre navne. Det er samme aktør, som ifølge de amerikanske myndigheder stod bag angrebet mod det demokratiske parti i USA.

Det er en aktør, der i det hele taget er meget aktiv over hele verden. Det kan man bl.a. læse i en rapport, som et større it-sikkerhedsfirma, Trend Micro, har offentliggjort. Af rapporten fremgår det, at sikkerhedsfirmaet har kendskab til, at aktøren bl.a. har udført angrebskampagner, som dem vi har oplevet, mod et meget stort antal ministerier, offentlige myndigheder og private virksomheder over hele verden. Aktøren er især gået efter militære myndigheder, forsvars- og udenrigsministerier og forsvarsindustrien.

Men aktøren har også rettet angreb mod politiske partier og institutioner og internationale organisationere og NGO'er.

Lad mig understrege, at det, Forsvaret har været udsat for, er efterretningsindhentning eller spionage og ikke et destruktivt cyberangreb. Det er jo ikke overraskende, at russerne prøver at spionere mod os, og de er jo heller ikke ene om at udføre efterretningsvirksomhed.

Men når jeg har valgt at gå ud at fortælle, hvad der er sket, er det fordi russernes cyberkampagner i stigende grad er blevet et centralt element i en meget bekymrende udvikling. Ruslands adfærd viser nemlig, at deres hacking ikke kun finder sted med et efterretningsmæssigt formål.

Hacking, og oplysninger opnået via hacking, bruges til aktivt at undergrave vestlige samfund og demokratiske institutioner gennem påvirknings- og misinformationskampagner. Som vi har set det i USA, og som det fx også er blevet omtalt i forbindelse med den franske præsidentvalgkamp.

Det er vigtigt, at vi er opmærksomme på denne trussel, og derfor har det efter min mening været vigtigt at tale offentligt om angrebet.

Jeg gør mig ingen illusioner om, at russerne indrømmer angrebet – det gør de jo aldrig, og jeg ser ikke noget formål med en diplomatisk reaktion. Men jeg synes, det er vigtigt at få truslerne frem i lyset, så vi kan blive bedre til at tage vores forholdsregler.

Rusland har tværtimod forsøgt at aflede opmærksomheden fra sig selv ved at påstå, at der slet ikke har været et angreb, og at vi skulle have fabrikeret oplysningerne for at tale truslen op.

I forhold til den fremadrettede sikkerhed vil jeg begynde med at sige, at jo mindre fremmede stater og andre med fjendtlige hensigter ved om, hvad vi konkret gør for at sikre informationssikkerheden omkring Forsvarets it-systemer, des bedre.

Derfor håber jeg, der er forståelse for, at jeg ikke kan fortælle i detaljer om de konkrete tiltag, der er iværksat og hvilke specifikke tiltag, der i øvrigt planlægges gennemført i fremtiden. Der er allerede gjort noget, og mere vil blive gjort fremover. Det omfatter både tekniske tiltag samt yderligere information til brugerne om trusler og beskyttelse.

Systemet, der blev hacket, er som sagt et mailsystem til uklassificeret post. Der er tale om et ældre system, og analyser har vist, at der kunne være bedre sikkerhedsforanstaltninger.

Truslen fra cyberspionage mod danske myndigheder og virksomheder vurderes som meget høj.

Det er derfor nødvendigt løbende at forholde sig til det trusselsbillede og på den baggrund justere informationssikkerheden og forbedre den, hvis det er nødvendigt.

Som forsvarsminister er jeg naturligvis optaget af, at Forsvarsministeriets it-systemer har et ordentligt sikkerhedsniveau, og at det løbende bliver vurderet, ikke mindst når truslen ændres.

Det ligger mig naturligvis også på sinde, at der er et passende sikkerhedsniveau i alle offentlige myndigheder så vel som hos private

virksomheder og hos borgerne. I den forbindelse er udbredelse af viden om sikkerhedsbrud vigtig. Viden giver bedre mulighed for at beskytte sig. Offentliggørelsen af rapporten om angrebet på Forsvaret skal også ses i det lys.

Jeg forventer, at en styrkelse af indsatsen på cyberområdet bliver en del af udspillet til et kommende forsvarsforlig og har noteret mig blandt reaktionerne på denne sag, at det synes der at være bred forståelse for.

Tak for ordet.