CENTER FOR CYBERSIKKERHED

Undersøgelsesrapport

Én aktør, mange angreb

Undersøgelsesenheden ved Center for Cybersikkerhed

April 2017

Indhold

Opsummering

Denne rapport beskriver, hvordan en målrettet, vedholdende og ressourcestærk udenlandsk aktør har spioneret mod Danmark. Rapporten gennemgår, hvordan aktøren via forskellige former for cyberangreb har forsøgt at tiltvinge sig adgang til postkasser og maskiner under Forsvarets myndighedsområde og i Udenrigsministeriet. CFCS har fundet tegn på, at aktøren har haft adgang til en række e-mail-postkasser fra en ikke-klassificeret mail-service i Forsvaret og kopieret deres indhold. Der er ***ikke*** set tegn på, at maskiner eller data hos Udenrigsministeriet er blevet kompromitteret.

I 2015 og 2016 har CFCS observeret flere forsøg på at franarre e-mail-loginoplysninger, dvs. brugernavn og kodeord, fra medarbejdere under Forsvarsministeriets myndighedsområde ved hjælp af vellignende kopier af mail-servicens loginside (webmail.mil.dk). Målpersonerne er blevet forsøgt lokket til at indtaste deres loginoplysninger på de falske sider. Det er meget sandsynligt, at flere mil.dk-postkasser efterfølgende er blevet kompromitteret, og at postkassernes indhold er kommet i aktørens hænder over flere omgange i 2015 og 2016.

CFCS har afdækket to sideløbende bølger af phishing-e-mails med ondsindede links rettet mod Forsvarsministeriets myndighedsområde og Udenrigsministeriet. CFCS vurderer, at hensigten har været at få adgang til- og kontrol over modtagernes maskiner. Bølgerne har ramt i 2015 og involverer et større antal phishing-mails. Der er ikke set tegn på, at aktøren har fået adgang til nogen maskiner som følge af phishing-angrebene.

CFCS vurderer dertil, at samme aktør har forsøgt at tiltvinge sig adgang til mil.dk-postkasser og servere i Forsvaret via forceringsangreb i 2015 og 2016. Der er ikke set tegn på, at forceringsforsøgene er lykkedes.

Endeligt har CFCS set rekognosceringsaktivitet mod mailsystemer hos forskellige danske myndigheder, inklusiv under Forsvarsministeriets myndighedsområde. Aktiviteten er tegn på, at aktøren har en interesse for de rekognoscerede systemer, og der er derfor en øget risiko for, at de kan blive mål for cyberangreb.

CFCS vurderer, at det er meget sandsynligt, at aktøren APT28 (alias Fancy Bear, Sofacy, Pawn Storm, m.fl.) har franarret loginoplysninger til det internetvendte mailsystem mil.dk fra medarbejdere i Forsvaret. CFCS vurderer det sandsynligt, at samme aktør står bag de øvrige beskrevne hændelser. CFCS vurderer videre, at der er tale om en vedvarende trussel mod Forsvarsministeriets myndighedsområde og Udenrigsministeriet.

Rapporten indeholder forslag til tiltag, der med udgangspunkt i erfaringerne fra hændelserne kan hjælpe myndigheder og virksomheder til at modvirke lignende angreb.

Indledning

Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS) udgav i februar 2017 en trusselsvurdering, der bl.a. konkluderer at: "Cyberspionage mod offentlige og private mål udgør fortsat den alvorligste cyberstrussel mod Danmark. Der er tale om en meget aktiv trussel mod danske interesser. Truslen kommer især fra fremmede stater. Truslen fra cyberspionage mod danske myndigheder og virksomheder er **MEGET HØJ**"[1].

Denne undersøgelsesrapport omhandler et konkret eksempel på denne trussel. Den beskriver, hvordan en enkelt aktør udfører spionage mod Danmark ved hjælp af en række forskellige typer cyberangreb over to år.

Hændelserne understreger, at avancerede cyberangreb mod danske interesser oftest ikke bør betragtes som isolerede hændelser, men som fortløbende forbundne begivenheder. Cyberspionage er en konstant trussel, der kræver et konstant beredskab. Så længe ressourcestærke udenlandske aktører har en interesse i at stjæle følsomme oplysninger fra myndigheder i Danmark, kan lignende cyberangreb forventes.

Målgruppen for rapportens anbefalinger er ledelse og teknikere inden for it-drift og it-sikkerhed.

Som del af Forsvarets Efterretningstjeneste (FE) har CFCS adgang til særlig efterretningsbaseret viden. Af beskyttelseshensyn kan alle aspekter af sagen ikke beskrives i en offentlig rapport. Derfor er nogle detaljer om hændelserne, samt aspekter af CFCS' analyse, udeladt fra rapporten.

Alle relevante myndigheder er varslet i sagen.

CFCS's Netsikkerhedstjeneste

CFCS's Netsikkerhedstjeneste monitorerer løbende internettrafikken til og fra de myndigheder og virksomheder, der frivilligt er tilsluttet probenetværket. Når CFCS ser tegn på et muligt angreb, udfører centerets teknikere analyser af netværkstrafikken for at afgøre, om der er tale om et cyberangreb, og hvordan det kan stoppes. CFCS bistår tilsluttede kunder med blandt andet varslinger, analyser af kompromitterede maskiner og rådgivningstiltag.

Kunder, der er tilsluttet Netsikkerhedstjenesten, opnår en styrket beskyttelse mod mere avancerede cyberangreb, der oftest udføres af statsstøttede aktører.

[1] Forsvarets Efterretningstjenestes Center for Cybersikkerhed: "Cybertruslen mod Danmark" (2017)

Sagen: En alsidig og vedholdende modstander

Afsnit 1 beskriver, hvordan aktøren har oprettet falske loginsider for Forsvarets ikke-klassificerede internetbrowser-baserede e-mailservice, og hvordan ansatte i Forsvaret er blevet manipuleret til at indtaste deres loginoplysninger på de falske loginsider.

Afsnit 2 beskriver to phishing-kampagner, der har ramt Forsvarsministeriets myndighedsområde samt Udenrigsministeriet. Via phishing-mails har aktøren forsøgt at installere malware på de ramte medarbejderes maskiner.

Afsnit 3 beskriver, hvordan aktøren har forsøgt at tiltvinge sig adgang til e-mail-konti og servere under Forsvarsministeriets myndighedsområde via forceringsangreb.

Afsnit 4 indeholder CFCS's vurdering af, hvem der står bag de beskrevne hændelser, og hvilken trussel aktøren udgør for Danmarks sikkerhed.

Afsnit 5 indeholder en opsamling af rapportens fund og betragtninger i sagen.

Afsnit 6 indeholder forslag til, hvordan lignende cyberangreb kan stoppes i fremtiden.

Tidslinje

2015, marts-juni:

a. Første phishing-kampagne. Et mindre antal phishing-e-mails blev sendt til specifikke medarbejdere under Forsvarsministeriets myndighedsområde og Udenrigsministeriet.

2015, april-juni:

b. Første forsøg på tyveri af loginoplysninger, her ved brug af en falsk loginside for webmail.mil.dk. Flere hundrede phishing-mails blev sendt til specifikke medarbejdere under Forsvarsministeriets myndighedsområde.

2015, juli-oktober:

a. Anden phishing-kampagne. Et mindre antal phishing-e-mails blev sendt til specifikke medarbejdere under Forsvarsministeriets myndighedsområde og Udenrigsministeriet.

2015, september-oktober:

a. Andet forsøg på tyveri af loginoplysninger, igen ved brug af en falsk loginside for webmail.mil.dk. Et par hundrede phishing-mails blev sendt til specifikke medarbejdere under Forsvarsministeriets myndighedsområde.
b. I samme periode er der også set forceringsforsøg mod flere mil.dk-konti.

2016, februar-april:

a. Rekognosceringsaktivitet mod mil.dk samt flere andre offentlige myndigheders mailsystemer.

2016, april:

a. Forceringsforsøg mod brugerkonti til SSH-fjernadgang til flere af Forsvarets it-systemer.

2016, oktober:

a. Tredje forsøg på tyveri af loginoplysninger fra aktøren, igen ved brug af en falsk log-inside for webmail.mil.dk. Omkring tusind phishing-mails blev sendt til specifikke medarbejdere under Forsvarsministeriets myndighedsområde.

Hackere med humor

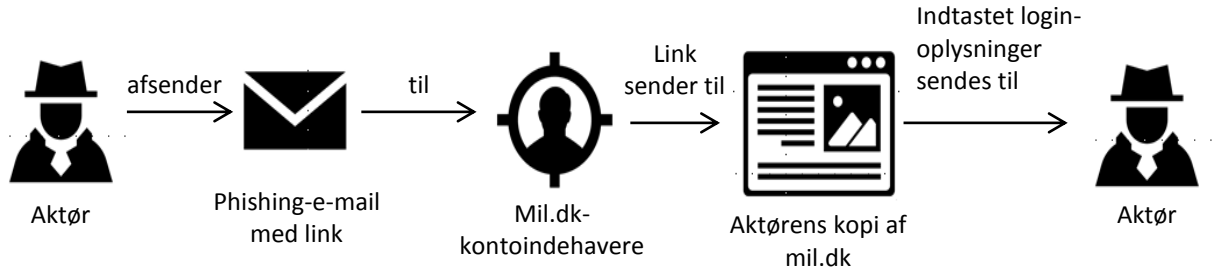
Ifølge offentlige hjemmesideregistrantoplysninger har registranten til en af de ondsindede hjemmesider foregivet at være bosiddende på Classensgade 38 (en andelsboligforening) i København. Telefonnummeret, som er angivet af registranten, er identisk med kontaktnummeret til FBI's lokalkontor i Newark, New Jersey.

1. Tyveri af loginoplysninger og kompromittering af email-konti

I foråret og efteråret 2015, samt efteråret 2016, har CFCS observeret forsøg på at franarre e-mail-loginoplysninger, det vil sige brugernavn og kodeord, fra medarbejdere under Forsvarsministeriets myndighedsområde via falske loginsider.

Angrebsteknik: falske loginsider og phishing-e-mails

Aktøren har brugt følgende metode til at franarre loginoplysningerne: Et stort antal phishing-e-mails afsendes til målpersoner, der har en særlig interesse for aktøren. Indeholdt i phishing-e-mailen er et link. Hvis linket følges, bliver vedkommende sendt til en meget vellignende kopi af loginsiden på webmail.mil[.]dk, der er opsat af aktøren. Indtaster målpersonen sine loginoplysninger på den ondsindede side, bliver disse registreret og gemt. Aktøren kan derefter bruge de franarrede oplysninger til at få adgang til målpersonens rigtige postkasse. Metoden er angivet i figur 1.



Figur 1: tyveri af loginoplysninger via falsk loginside

Sådan stopper du tyveri af loginoplysninger via falsk loginside

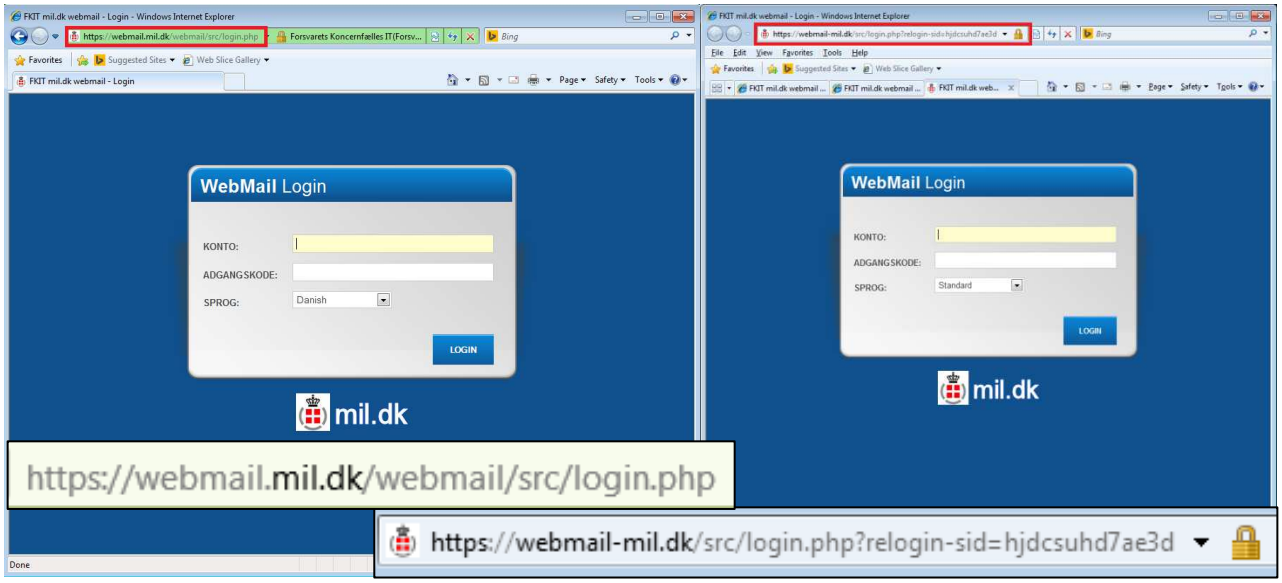
Brug af to-faktor-autentificering vil ofte forhindre denne angrebsmetode i at virke. Grunden er, at der ved to-faktorautentificering kræves et separat tidsbaseret kodeord for at logge på. Dette ekstra kodeord kan angriberen ikke opsnappe ved den metode, der er beskrevet her.

Manipulationsteknik

Aktøren har, ved hjælp af forskellige former for manipulation, forsøgt at få medarbejderne til at trykke på det indlejrede link i de afsendte phishing-e-mails. Manipulationen går på at få phishing-e-mailen til at se legitim ud, så målpersonen ikke fatter mistanke. Som eksempel kan nævnes brugen af en afsenderadresse, der foregiver at være en systemadministrator-konto. Visse emnefelter refererer til en systemopdatering.

I bilaget findes eksempler på de phishing-mails, der er fundet i sagen.

Når en målperson følger det indlejrede link i phishing-mailen, sendes personen til den falske udgave af loginsiden. Nedenfor, til højre i billede 2, ses et eksempel på den næsten identiske falske udgave af webmail.mil.dk anvendt i 1. angreb. Til venstre ses den ægte loginside til sammenligning:



Billede 1: Den falske e-mail-login-side sidestillet med den legitime side. De to URL'er er fremhævet nedenunder.

Bemærk bindestregen i stedet for punktummet i URL'en for den falske udgave.

Hvis målpersonen indtaster sine loginoplysninger, gemmes de, og personen videresendes til den officielle og korrekte loginside uden at være logget ind. Det eneste udsædvanlige offeret vil opleve under tyveriet er derfor, at et enkelt login ikke virker. Når login forsøges igen på den legitime side, får personen adgang til at læse sine mails som normalt.

Succesfuld kompromittering af e-mail-konti

Under afdækningen af sagen er der fundet eksempler på, at nogle modtagere af phishing-mails har besøgt de falske loginsider og indtastet deres loginoplysninger. Det er meget sandsynligt, at et antal mil.dk-postkasser er blevet kompromitteret og tilgået, og at deres indhold er blevet kopieret af aktøren ad flere omgange i 2015 og 2016.

2. Forsøg på inficering af maskiner med malware

Samtidig med tyveriet af loginoplysinger og e-mails afsender samme aktør to bølger af phishing-e-mails mod Forsvarsministeriets myndighedsområde og Udenrigsministeriet. CFCS har fundet et større antal phishing-mails sendt til et tocifret antal e-mail-konti, der alle indeholder ondsindede links. Formålet er at installere malware på målets maskine, så der opnås adgang til- og kontrol over den. Hensigten kan være at få adgang til følsomme oplysninger, der måtte ligge på den ramte maskine eller i det lokale netværk.

Første phishing-kampagne: marts-juni 2015

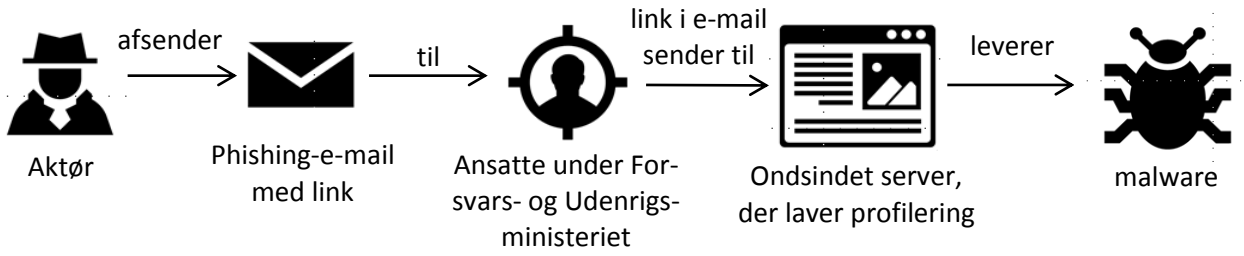
Første phishing-kampagne varer i mere end tre måneder, fra marts 2015 til juni 2015. CFCS har fundet et antal e-mails sendt til et tocifret antal konti.

Anden phishing-kampagne: juli-oktober 2015

Anden phishing-kampagne kører fra juli 2015 til oktober 2015. CFCS har også her fundet et antal e-mails sendt til et tocifret antal konti.

Angrebsteknik: hvordan opnår aktøren kontrol over en maskine?

Før aktøren kan få adgang til- og styre maskinen, skal det lykkes at gennemføre tre trin: manipulation → Profilering → Udnyttelse og Kompromittering. Nedenfor er angrebsteknikken illustreret.



1. trin: manipulation

De afsendte Phishing-mails imiterer nyhedsbreve fra en række nyhedsmedier, udenrigsministerier og tjenester samt internationale organisationer. Hensigten er at få de fremsendte phishing-mails til at se legitime og interessante ud, så modtagerne klikker på det indlagte link. Både afsenderadressen, emnefeltet, teksten i mailen og det indlejrede link er designet til at få modtageren til at tro, at der er tale om en ganske almindelig nyheds-e-mail.

Aktøren har imiteret legitime hjemmesider og organisationer, og har valgt et internationalt og sikkerhedspolitisk tema. Dette tema er sandsynligvis valgt af aktøren i den forventning, at det vil have særlig appel for målpersonerne og øge chancen for, at en phishing-e-mail bliver åbnet og linket fulgt.

Emnerne er i visse tilfælde kopieret fra reelle, aktuelle nyheder, enten i form af selve overskriften, eller som et uddrag af den indledende brødtekst. Phishing-mailen er i de tilfælde afsendt samme dag som nyheden er offentliggjort, hvilket betyder, at aktøren har designet mailen umiddelbart inden den er blevet afsendt.

De afsendte phishing-mails indeholder alle et link, der synes at pege på en legitim hjemmeside.

2. trin: profilering og identificering af sårbarheder i målets maskine

Hvis målpersonen manipuleres til at følge linket, begynder maskinen at kommunikere med en ondsindet server på internettet. Serveren gennemfører en profilering af målpersonens maskine via et script, der sendes til offerets maskine. Scriptet danner og sender en lille tekstfil tilbage til angriberne med informationer om offerets maskine. Det kan være oplysninger om, hvilket styresystem, browser, plugins og programmer offeret anvender med tilhørende versionsnumre. På baggrund af profileringen foretager den ondsindede server automatisk en vurdering af sårbarheder på maskinen, der kan udnyttes til at installere malware. Dette kan f.eks. være en internet-browser, der ikke er opdateret til nyeste version.

3. trin: udnyttelse af sårbarheder i målets maskine og installation af malware

Hvis serveren identificerer en brugbar sårbarhed, udnyttes den til at installere malware på målets maskine.

Uanset om der findes en passende sårbarhed, videresendes offeret efterfølgende til den legitime hjemmeside, som linket i phishing-mailen refererer til, i den tro, at intet unormalt er hændt. Hele processen er automatisk og er overstået så hurtigt, at målet aldrig opdager kommunikationen med den ondsindede server. Nogle gange vil forsøget på at inficere maskinen dog medføre sikkerhedsmeddelelser eller popup-bokse, der kræver en godkendelse på målpersonens skærm.

Sådan stopper du forsøg på inficering af maskiner med malware

Et af top fire-rådene i CFCS's vejledning "Cyberforsvar der virker" er at holde alle programmer opdateret. I dette tilfælde ses konkret, hvordan opdaterede programmer kan have en afgørende betydning for at stoppe et cyberangreb.

Ingen tegn på kompromitteringer med malware

CFCS har ikke set tegn på, at det er lykkedes for aktøren at installere malware på nogle maskiner og få kontrol over dem som en følge af de to phishing-kampager.

3. Forceringsangreb mod e-mail-konti og servere

Sideløbende med forsøgene på at franarre loginoplysninger og phishing-kampagnerne, har CFCS set forsøg fra aktørens side på at forcere kodeord på en række udvalgte mil.dk-e-mailkonti og servere under Forsvarets myndighedsområde i efteråret 2015 og foråret 2016.

Hensigten er at få adgang til de ramte e-mail-konti for at kopiere deres indhold og få adgang til at styre og tilgå de ramte servere.

Angrebsteknik: automatiseret loginforsøg
I forceringsangrebet i 2015 har aktøren forsøgt at logge ind på mil.dk-e-mail-konti ved automatiseret at teste et meget stort antal mulige adgangskoder sammen med udvalgte brugernavne. Målet er at "gætte" den korrekte kode, og derved få adgang til postkassens indhold. Forceringsforsøget er gjort både på mil.dk-loginsiden og direkte til mailserveren. Der er tegn på, at brugernavnene på de konti, der er forsøgt forceret, er kendt af aktøren i forvejen.

I angrebet i 2016 prøver aktøren at forcere flere brugerkonti for fjernadgange (SSH) på servere i forskellige dele af Forsvaret. SSH—fjernadgange bruges typisk til server-administration. Hvis en sådan konto kompromitteres, kan aktøren potentielt få adgang til at tilgå og styre den ramte server.

Sådan stopper du forceringsangreb

Sikkerhedspolitikker, som eksempelvis at kræve komplekse kodeord og automatisk timeout ved for mange forkerte loginforsøg, vil typisk gøre sådanne forceringsforsøg tidsmæssigt urentable.

Ingen tegn på succesfulde forceringsforsøg
CFCS har ikke set tegn på, at forceringsangrebene er lykkedes.

4. Tilskrivning

CFCS vurderer, at det er meget sandsynligt, at aktøren APT28 står bag kompromitteringen af det internetvendte mailsystem mil.dk ved at franarre loginoplysninger fra et antal brugere. CFCS vurderer det sandsynligt, at samme aktør står bag de øvrige beskrevne hændelser. Vurderingen bygger på en række faktorer, hvoraf ikke alle er beskrevet i denne rapport.

APT28 er beskrevet af flere private sikkerhedsfirmaer. Se blandt andet: "APT28: At the Center of the Storm" (2017) af FireEye samt "Operation Pawn Storm: Using Decoys to Evade Detection" (2014) og "How Cyberpropaganda Influenced Politics in 2016" (2017) af Trend Micro.

Truslen

Aktører, der udfører cyberspionage, gør meget for at skjule både deres aktivitet og identitet. Det er derfor altid behæftet med en vis usikkerhed at tilskrive cyberspionage til specifikke organisationer. CFCS vurderer dog, at et andet lands efterretningstjeneste står bag de gentagende forsøg på cyberspionage mod Udenrigsministeriet og Forsvarsministeriets myndighedsområde.

CFCS vurderer, at angribernes udvælgelse af myndigheder og medarbejdere i de to ministerier afspejler langsigtede efterretningsbehov hos aktøren angående dansk sikkerheds- og udenrigspolitik og dansk forsvar. CFCS vurderer, at der er tale om en vedvarende trussel mod de to ministerier.

Cyberspionage mod offentlige myndigheder og private virksomheder udgør fortsat den alvorligste cybertrussel mod Danmark og danske sikkerhedspolitiske og økonomiske interesser. Der er tale om en særdeles aktiv trussel, og som denne rapport illustrerer, er danske myndigheder og virksomheder løbende udsat for forsøg på cyberspionage.

Truslen mod offentlige myndigheder er især rettet mod myndigheder af betydning for dansk udenrigs- og sikkerhedspolitik, herunder Udenrigsministeriet og Forsvarsministeriets myndighedsområder. Flere lande har stået bag forsøg på cyberspionage mod de to ministerier inden for de seneste år. Der eksisterer ligeledes en tilsvarende trussel mod det internationale sikkerhedssamarbejde Danmark deltager i, bl.a. mod NATO.

5. Opsamling

Rapporten viser, at Forsvarsministeriets myndighedsområde og Udenrigsministeriet i 2015 og 2016 har været mål for en større spionage-indsats fra en udenlandsk aktør. CFCS har afdækket flere forsøg på at franarre loginoplysninger, phishing-kampagner og forceringsangreb. Aktøren bag har haft delvist held med angrebene.

På baggrund af hændelserne kan følgende fremhæves:

- Som beskrevet i kapitel 1 er et antal e-mail-konti tilhørende ansatte under Forsvarsministeriets myndighedsområde blevet kompromitteret og deres indhold kopieret. Der er ikke set kompromitteringer i forbindelse med phishing-kampagnerne og forceringsangrebene som beskrevet i kapitel 2 og 3. Der er ikke set tegn på, at maskiner eller data hos Udenrigsministeriet har været kompromitteret.
- Forsvarets mil.dk mail-service er beregnet til ikke-klassificeret kommunikation. Derfor er mil.dk-mail-servicen ikke underlagt de samme sikkerhedskrav, som de systemer der håndterer klassificeret information. I takt med, at mil.dk-mail-servicen bliver brugt i stadig større omfang i Forsvarsministeriets myndighedsområde, har dens anvendelsesområde udvidet sig. Selvom trusselsbilledet løbende har ændret sig, har der ikke været iværksat nye sikkerhedsforanstaltninger for at imødegå disse ændringer. Én konsekvens af det er, at konti, der burde have været spærret eller underlagt tvungen passwords-skifte, stod åbne for aktøren efter loginoplysningerne blev franarret. Det gjorde det muligt for aktøren at kopiere indholdet af flere konti efter angrebet blev kendt. En række nye sikkerhedstiltag er implementeret i Forsvarets webmail-løsning, på baggrund af erfaringerne fra hændelserne, der er beskrevet her.
- Kompromitteringen af mil.dk-e-mail-konti udgør en sikkerhedsrisiko, selvom der er tale om en ikke-klassificeret e-mail-løsning. Fra et cybersikkerheds-perspektiv kan informationerne anvendes til blandt andet at skræddersy phishing-mails, og kompromitterede konti kan misbruges som afsenderadresser for flere phishing-mails. Informationer taget fra ansatte under Forsvarsministeriets myndighedsområdes e-mail-indbakker kan også være værdifulde ud fra et klassisk efterretningsperspektiv. De kan f.eks. omhandle møde- og rejseaktivitet, kontaktoplysninger eller private forhold. Informationerne kan misbruges til forsøg på rekruttering, afpresning eller til planlægning af yderligere spionage.

6. Anbefalinger

På baggrund af de konkrete hændelser har CFCS opstillet følgende anbefalinger vedrørende cyberforsvar som forretningen, dvs. myndigheder, virksomheder og organisationer bør følge. Forretningen skal i denne sammenhæng forstås som den ene part i et kunde-it-leverandør-forhold, hvor it-leverandøren kan være en intern driftsorganisation.

- Ansvaret for informationssikkerhed, og herunder forretningens cyberforsvar, er som udgangspunkt placeret hos topledelsen, men konkrete opgaver bør uddelegeres, herunder det forretningsmæssige ansvar for specifikke it-løsninger som mail-service mv. Herved kan man sikre, at cyberforsvaret i relation til specifikke it-anvendelser ikke overses.
- Overblik over forretningens it-anvendelse er en forudsætning for, at der kan etableres et fuldt dækkende cyberforsvar.
- Opdaterede risikovurderinger er grundlaget for forretningens cyberforsvar. Risikovurderingerne bør tage udgangspunkt i det aktuelle trusselbillede for forretningen, samt erkendte sårbarheder i såvel it-infrastrukturen som i de arbejdsgange, der er knyttet til it-anvendelsen. Overblik over sårbarheder bør leveres af leverandøren. Find evt. opdaterede trusselvurderinger på www.cfcs.dk.
- Ved at åbne for adgang til interne it-tjenester via Internettet har forretningen også eksponeret sig selv for en række nye trusler. Traditionelle identifikations- og autentifikationsmetoder som brug af bruger-id og traditionelt password kan ikke længere anses for at være sikre i forbindelse med en sådan adgang. Alternative metoder, herunder to-faktor autentifikation, kan derfor bidrage til et bedre cyberforsvar på dette område.
- Generel anvendelse af internetbærende tjenester, herunder e-mail og internetbrowsing, forudsætter, at den enkelte medarbejder i forretningen og hos leverandøren er bevidst om de risici, der er forbundet hermed. En vigtig brik i den forbindelse er løbende afholdelse af awareness-kampagner og øvelser for alle medarbejdergrupper. Det kan ofte være særdeles vanskeligt for den enkelte medarbejder at gennemskue, hvornår en e-mail eller hjemmeside er autentisk eller falsk.
- Hvis uheldet sker, er det yderst vigtigt, at forretningen med støtte fra leverandøren er i stand til at reagere hensigtsmæssigt, således at angrebet stoppes og eventuelle sikkerhedshuller om muligt lukkes øjeblikkeligt, herunder spærring af kompromitterede konti eller ændring af passwords, m.m..
- En af forudsætningerne for, at forretningen eller leverandøren kan opdage og reagere korrekt på angreb og sikkerhedshuller, er at der foretages en løbende overvågning og logning af relevante netværk og systemer.

CFCS har udarbejdet et antal vejledninger, der med fordel kan bidrage til forretningens generelle viden om et godt cyberforsvar. Følgende kan nævnes i denne sammenhæng:

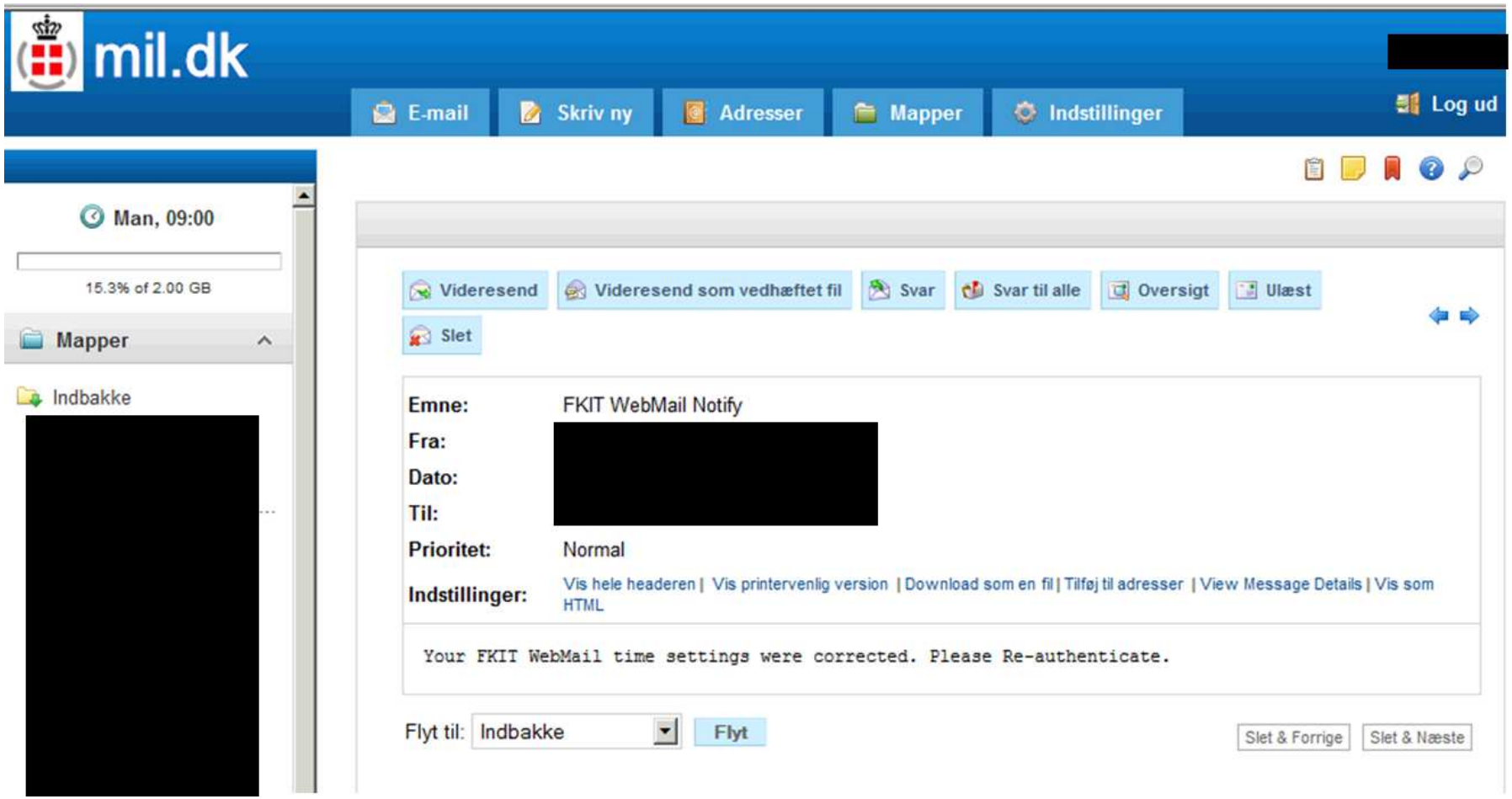
- Cyberforsvar der virker
- Spear-phishing – et voksende problem
- Logning – en del af et godt cyberforsvar
- Passwordvejledning

Vejledningerne kan findes på CFCS hjemmeside under følgende link www.cfcs.dk/publikationer.

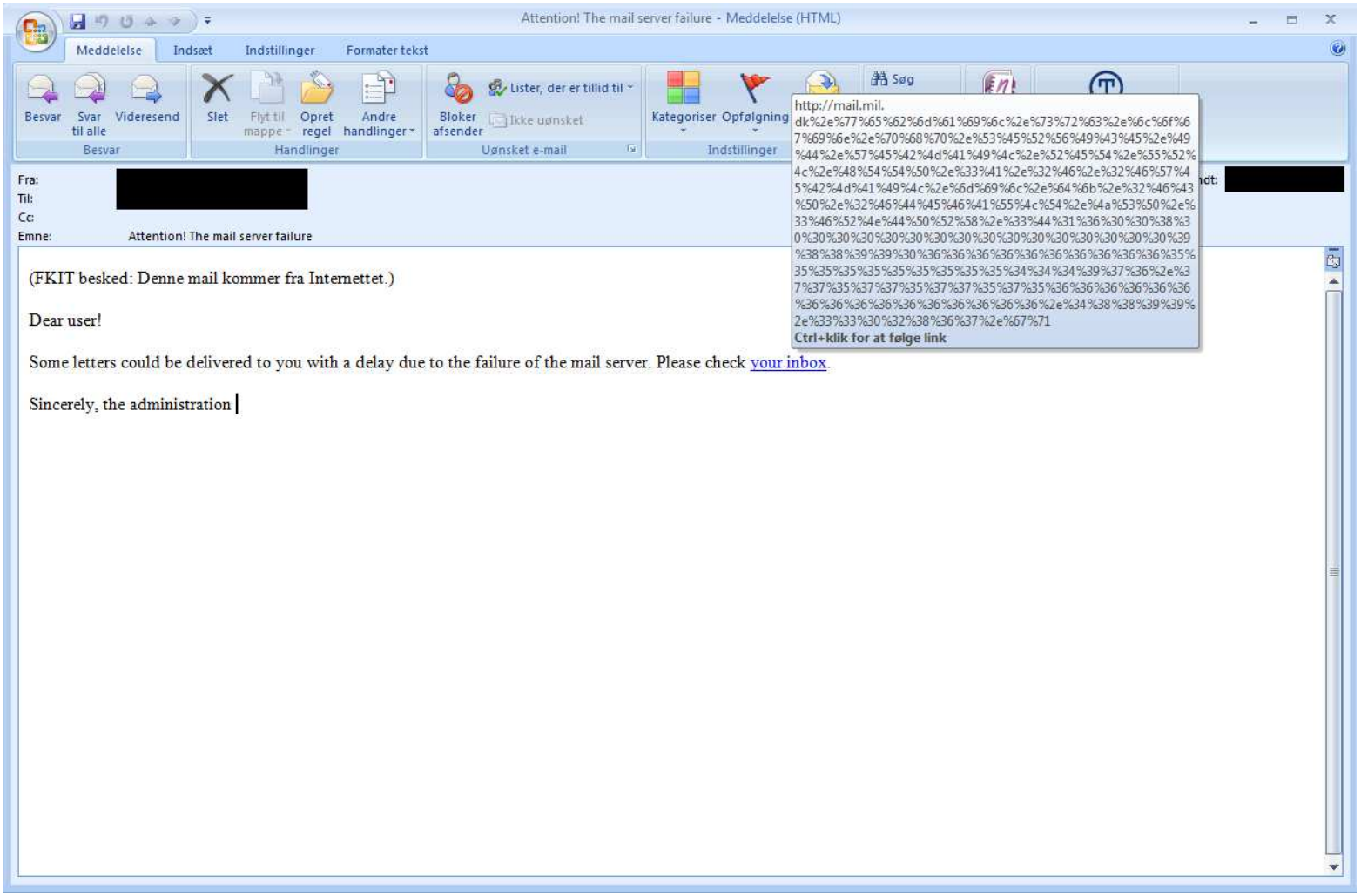
Bilag

Webmail.mil.dk og FIIN

Mil.dk er en mail-service, der anvendes på tværs af Forsvaret. Mil.dk-postkasser kan tilgås over nettet via en internetbrowser, og kan derfor anvendes hjemmefra eller under rejser. Politikken for brugen af mil.dk-mailservicen er, at den ikke må anvendes til klassificeret information af nogen art. FIIN er Forsvarets mailservice beregnet til sensitivt materiale og er separeret fra internettet. Det er altså ikke muligt at tilgå FIIN fra internettet, som man kan med mil.dk. Kompromitteringen af mil.dk-konti udgør ikke en direkte risiko for det sensitive materiale, der ligger på FIIN.



Phishing-mail anvendt i 2. angreb. Medarbejderen bliver bedt om at klikke på et link og logge ind på sin mil.dk-konto da ”time settings were corrected”.



Phishing-mail anvendt i 3. angreb. Medarbejderen bliver bedt om at følge et link og logge ind på sin mil.dk-konto da der muligvis er mails der er leveret med forsinkelse. Link-adressen man sendes til skjult via en teknik kaldet obfuskering. Som det ses på billedet viser link-adressen: "http://mail.mil.dk" efterfulgt af en lang række tegn. Følges linket bliver man sendt til en falsk loginside.

CFCS's Undersøgelsesenhed

I december 2014 udkom den første nationale strategi for cyber- og informationssikkerhed. Et af initiativerne i strategien blev at etablere en særlig Undersøgelsesenhed i CFCS, vis opgave det er at undersøge og afdække større cyberhændelser. På baggrund af disse udredninger udsender CFCS rapporter, så myndigheder og virksomheder kan drage nytte af erfaringerne fra tidligere hændelser og beskytte sig bedre.

Uddrag fra National strategi for cyber- og informationsstrategi:

"Regeringen har indført, at alle statslige myndigheder skal underrette Center for Cybersikkerhed ved større cybersikkerhedshændelser. Blandt de cybersikkerhedshændelser, som indrapporteres, vil der være hændelser, der er særlige alvorlige. Regeringen ønsker, at der sker relevant udredning og analyse af sådanne hændelser. Samtidig skal det sikres, at erfaringerne fra hændelserne opsamles og i størst muligt omfang stilles til rådighed for andre myndigheder og virksomheder, således at erfaringerne kan anvendes aktivt i arbejdet med at forebygge fremtidige hændelser. Derfor vil Center for Cybersikkerhed: etablere en enhed til undersøgelse af større cybersikkerhedshændelser. Enheden består som udgangspunkt af medarbejdere fra Center for Cybersikkerhed. Andre myndigheder – fx Digitaliseringsstyrelsen og PET – inkluderes afhængig af hændelsen. Enheden etableres i 1. kvartal 2015."