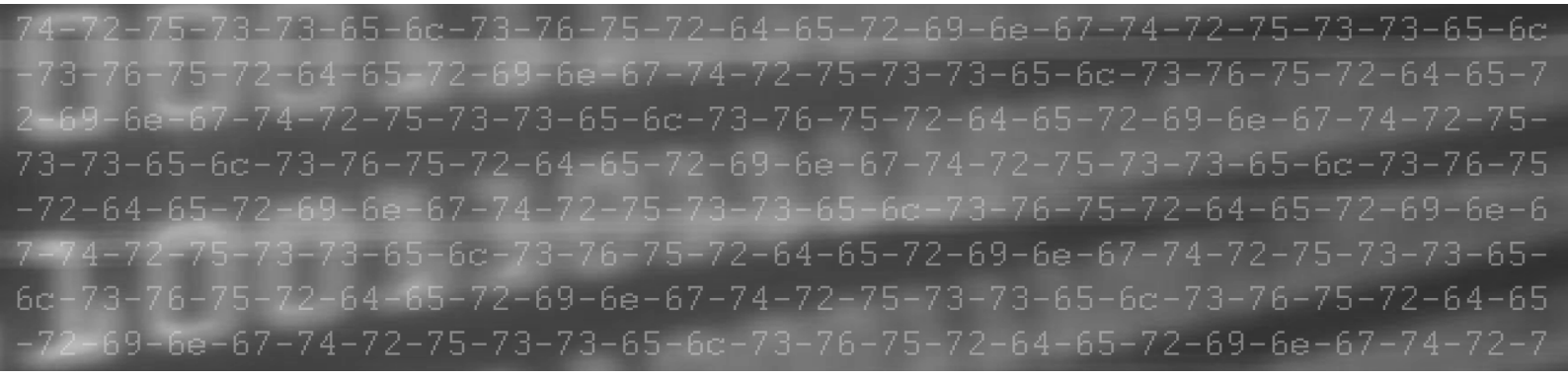
CENTER FOR CYBERSIKKERHED

Undersøgelsesrapport

Outsourcing – hvem har ansvaret?



Undersøgelsesenheden ved Center for Cybersikkerhed

Marts 2017

Outsourcing – hvem har ansvaret?

Indhold

Executive summary

This report describes a cyberattack against two Danish IT hosting companies in the period 2015-2016. We assess that a state or state-sponsored actor is behind the cyberattack, possibly in an effort to use the IT hosting companies as platforms to access information on clients' network or to spread malware for later exploitation. The report is prepared by the Security Analysis Branch under the Centre for Cyber Security (CFCS), and its aim is to accumulate data from the incident and provide accessible knowledge to counter future, similar incidents.

The incident was detected through a tip and the subsequent investigation concluded that one of the hosting companies had already been compromised in April 2015 via a client's website, which was hosted by one of the hosting companies' servers. A similar attack method was possibly employed against the second hosting company, though this cannot be confirmed or denied through the available data. The CFCS has detected several indications of malware activity on the compromised servers in 2015 and 2016, with the most recent activity registered in mid-2016. The attacker has used two different types of malware that may have been used to remote control compromised servers and to steal login information or other sensitive information.

It is possible that the actor has exploited the compromised servers or information to infect the local network or other hosting company clients, some of which also include public authorities. We cannot confirm nor deny whether sensitive information has been stolen from the hosting company's clients or whether the actor has exploited its access for alternative purposes.

Contemporary IT operations provide numerous possibilities to outsource services to IT hosting companies or to be part of various types of shared digital solutions at home and abroad. This report includes a series of considerations regarding security issues particularly associated with sharing or outsourcing IT, including how a hosting company may be compromised with the purpose of accessing a client's hosted server as a way of gaining access to the client's additional IT infrastructure.

Finally, based on lessons learned from these incidents, this report includes proposals for preventive measures aimed at helping private companies and state authorities resist future attacks. It is recommended that companies read the CFCS logging guidelines at www.cfcs.dk/publikationer to ensure that they have access to necessary information in case of compromise and need for restrictive measures to contain the security breach.

Opsummering

Denne rapport beskriver et cyberangreb mod to danske it-hostingfirmaer, som er blevet udført i perioden 2015-2016. Angrebet vurderes at være gennemført af en statslig eller statsstøttet aktør, muligvis med henblik på at anvende it-hostingfirmaerne som springbræt til informationer på kundernes netværk, eller på at sprede malware til senere misbrug. Rapporten er udarbejdet af Undersøgelsesenheden i Forsvarets Efterretningstjenestes Center for Cybersikkerhed (CFCS) med det formål at opsamle erfaringer fra hændelsen og stille viden til rådighed for at modvirke fremtidige, tilsvarende hændelser.

Hændelsen blev opdaget gennem et tip, og den efterfølgende undersøgelse viste, at det ene hostingfirma blev ramt allerede i april 2015 via en kundes hjemmeside, som var hostet på en af hostingfirmaets servere. En lignende angrebsvinkel er muligvis blevet brugt mod hostingfirma nr. 2, men det kan ikke bekræftes af de tilgængelige data. CFCS har set flere tegn på malware-aktivitet på de kompromitterede maskiner i 2015 og 2016, hvor den seneste aktivitet er fra midten af 2016. Aktøren har brugt to forskellige typer malware i sit angreb, der bl.a. kan have været brugt til at fjernstyre kompromitterede maskiner og til at stjæle loginoplysninger eller anden følsom information.

Det er muligt, at aktøren har udnyttet de kompromitterede maskiner eller informationer fra dem til at sprede sig i det lokale netværk eller til andre af hostingfirmaets kunder, hvoraf også offentlige myndigheder indgår. Det kan hverken af- eller bekræftes, om der er stjålet følsomme oplysninger fra hostingfirmaets kunder eller om aktøren har udnyttet sin adgang på anden vis.

I moderne it-drift er der mange muligheder for at outsource til it-hostingfirmaer eller for at blive del af forskellige former for delte digitale løsninger i ind- eller udland. Rapporten indeholder en række betragtninger om de sikkerhedsproblemer, der knytter sig særligt til delt- og outsourcet it, herunder hvordan et hostingfirma kan kompromitteres med det formål at få adgang til en kundes løsning og derigennem få adgang til kundens øvrige infrastruktur.

Rapporten indeholder afslutningsvis forslag til tiltag, der, med udgangspunkt i erfaringerne fra hændelserne, kan hjælpe virksomheder og myndigheder til at modvirke fremtidige angreb. Her rådes blandt andet til at læse CFCS' logningsvejledning på www.cfcs.dk/publikationer med henblik på at sikre, at virksomheden har adgang til nødvendige informationer, når uheldet er ude, og sikkerhedsbruddet skal begrænses.

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 trussel 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 private virksomheder er **MEGET HØJ**."

Denne undersøgelse viser, hvordan angreb mod to danske hostingfirmaer har givet ondsindede aktører adgang til både systemer og informationer hos hostingfirmaerne og deres kunder. Undersøgelsen viste blandt andet, at aktøren havde installeret malware, der er set anvendt i perioden 2015 og 2016. På baggrund af angrebenes karakter indledte CFCS' udrykningshold et såkaldt incident response, hvor CFCS indgik et samarbejde med begge virksomheder om analyse og afhjælpning af angrebet. Det er resultaterne af disse to incident response-forløb, der danner grundlag for denne rapport.

I perioden 2015-2016 har CFCS set, at flere danske it-hostingfirmaer er blevet ramt af cyberangreb. Det har været mange forskellige typer angreb, og de kan ramme systemer, uanset om de er placeret på målets eget domicil, eller hostet hos eksterne leverandører.

Rapporten har til hensigt at oplyse og rådgive offentlige myndigheder og private virksomheder, så det er muligt at imødegå disse typer angreb og forbedre it-sikkerheden. Som led i dette beskrives nogle af de udfordringer med outsourcing, som CFCS har set hos virksomheder og myndigheder i sager, hvor udrykningsholdet har ydet støtte. I rapportens sidste kapitel findes forslag til tiltag, der med udgangspunkt i erfaringerne fra de hændelser, som er beskrevet her, kan hjælpe virksomheder og myndigheder til at forhindre fremtidige angreb.

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

Som del af Forsvarets Efterretningstjeneste har CFCS adgang til den særlige efterretningsbaserede viden, som FE råder over på cyberområdet. Af beskyttelseshensyn kan alle aspekter ikke beskrives i en offentlig rapport. Derfor er nogle informationer, inklusiv de involverede virksomheders navne og visse tekniske detaljer omkring sagens omfang og centerets kapaciteter, derfor udeladt fra denne rapport.

CFCS's Netsikkerhedstjeneste
CFCS's Netsikkerhedstjeneste har til opgave at opdage, analysere og bidrage til at imødegå cyber-angreb mod Forsvaret, virksomheder og statslige myndigheder. Fokus er på de avancerede angreb, der udføres af statslige eller statsstøttede aktører, kaldet "advanced persistent threats" eller APT.

CFCS analyserer løbende internettrafikken til og fra de myndigheder og virksomheder, der er tilsluttet CFCS's sensornetværk for at finde tegn på cyberangreb. Når CFCS observerer et muligt angreb mod en tilsluttet organisation, udfører centerets teknikere analyser af kundens ind- og udgående netværks-trafik, for at afgøre om der er tale om et cyberangreb. Hvis det er tilfældet, varsles myndigheden eller virksomheden. I visse tilfælde tilbyder CFCS at støtte med et teknisk udrykningshold, kaldet "incident response".

Tendenser og medfølgende sikkerhedsudfordringer ved it-styring og delt it

Som nævnt indledningsvis er der mange muligheder for at outsource eller blive del af forskellige former for delte digitale løsninger i moderne it-drift i ind- eller udland. I dag vil virksomheder og myndigheder ofte have systemer drevet af forskellige eksterne offentlige eller private leverandører. I staten findes flere forskellige it-fællesskaber, såsom Statens it, Sundhedsdatastyrelsen eller Kriminalforsorgens Koncern-IT. Derudover køber offentlige myndigheder også it-løsninger på det private marked. I den fællesoffentlige digitaliseringsstrategi 2016-2020[1] er outsourcet it, kaldet 'cloud computing', specifikt nævnt som en måde at skabe fleksibilitet og give potentielle besparelser i den offentlige it-drift.

Delt it-drift stiller særlige krav til sikkerheden, og der er desværre eksempler på, at disse krav ikke altid efterleves. Eksempelsvis har Rigsrevisionen fundet utilstrækkelig styring af it-sikkerheden i det fælles sundhedsdatanet[2], og CFCS har både fra denne sag og i lignende sager erfaret, at der kan være mangler i sikkerheden ved hændelser, der involverer delt it-drift.

Sagen: To it-hostingfirmaer kompromitteret

Begge de ramte hostingfirmaer er mellemstore forretninger i Danmark, der udbyder forskellige it-løsninger såsom hosting, konsulentbistand, udvikling og drift. Dette kapitel beskriver, hvordan aktøren bag angrebet er trængt ind i virksomhederne, hvilken ondsindet aktivitet CFCS har set, og hvilke mulige motiver, som kan være bag angrebet.

[1] Den fællesoffentlige digitaliseringsstrategi 2016-2020, Digitaliseringsstyrelsen, 2016
[2] Beretning om revisionen af statsregnskabet for 2015, Rigsrevisionen, 2016

CFCS har i samarbejde med de to berørte hostingfirmaer fundet og analyseret flere kompromitterede maskiner i deres netværk. Tidslinjen løber fra april 2015, hvor første tegn på kompromittering lokaliseredes hos hostingfirma 2. Først fire måneder efter ses tegn på kompromittering hos hostingfirma 1, og den ondsindede aktivitet fortsætter hos begge virksomheder frem mod sommeren 2016.

Der er fundet to typer APT-malware på de kompromitterede maskiner, og CFCS har kendskab til, at offentlige myndigheder er blandt de to virksomheders kunder.

Ud fra de analyserede data kan det hverken af- eller bekræftes, om der er stjålet følsomme oplysninger fra virksomhederne, eller om aktøren har udnyttet sin adgang på anden vis.

Hvordan opdages et cyberangreb?
CFCS kan blive opmærksom på et igangværende eller tidligere cyberangreb på flere måder. CFCS's sensornetværk, som bruges til at finde ondsindet ind- og udgående netværkstrafik hos centerets kunder, er ét sted. Centerets teknikere opdaterer løbende sensornetværket med informationer, der afslører tegn på cyberangreb. Mistanke om cyberangreb kan også komme via et tip fra en af Forsvares Efterretningstjenestes samarbejdspartnere. Endeligt kan data eller informationer fra offentligt tilgængelige kilder lede i retningen af aktivitet fra en APT-gruppe.

Angrebsteknik

CFCS har set tegn på, at kompromitteringen af hostingfirma 1 er sket via en hjemmeside hostet på en af hostingfirmaets servere, tilhørende en af hostingfirmaets kunder. Aktøren har sandsynligvis udnyttet en sårbarhed i hjemmesiden til at installere en bagdør direkte på en af hostingfirmaets servere, hvor hjemmesiden ligger. Ved hjælp af bagdøren har aktøren fået uautoriseret adgang til at installere malware på serveren. CFCS antager, at virksomhed 2 muligvis er blevet kompromitteret på en lignende facon, men har ikke oplysninger til rådighed, der kan underbygge dette.

Malware

Aktøren har brugt to forskellige typer malware i sit angreb hos de to hostingfirmaer.

Den ene type malware er et såkaldt remote access tool (RAT), der bl.a. giver operatøren adgang til at styre den kompromitterede maskine og få adgang til det indhold, der måtte være på den. Malwaren kan også bruges til at lave rekognoscering i det lokale netværk, hvis aktøren f.eks. ønsker at kompromittere endnu flere maskiner hos den ramte part.

Remote access tool (RAT)

Et "remote access tool", eller fjernstyringsværktøj, er et stykke software, der giver fjernadgang til en maskine. Sådanne værktøjer anvendes ofte helt legitimt i forbindelse med f.eks. it-support eller til opsætning af fjernarbejdspladser. Et RAT kan også være en del af et stykke malware, der i skjul giver en angriber uretmæssig adgang til en maskine eller netværk.

Den anden type malware er brugt som keylogger, dvs. til at registrere tastetryk på den kompromitterede maskine. Det kan f.eks. være indtastede brugernavne og kodeord til administrator-, og email-konti. Når malwaren har registreret informationen, sendes den tilbage til aktøren via internettet.

Begge typer malware er designet til at være svære at finde, når de kører på en kompromitteret maskine. Endvidere er dele af deres funktionalitet skjult for at gøre det svært at finde ud af præcis, hvordan de fungerer, hvis de skulle blive fundet alligevel.

På baggrund af de metoder og den malware, der er anvendt i angrebet, vurderer CFCS, at angrebet er udført af en statslig eller statsstøttet aktør. Ud over den APT-relaterede malware er der på de samme systemer også fundet flere typer malware, der bruges til almindelig berigelseskriminalitet eller andet misbrug.

Ondsindet aktivitet på kompromitterede maskiner

På grund af mangelfuld logning er der kun en begrænset dækning af hændelserne på de kompromitterede maskiner og netværk i angrebsperioden.

Keylogger-malwaren har i perioden været aktiv på maskiner hos begge hostingfirmaer og har registreret, hvad der er blevet indtastet på maskinerne. Der er også tegn på, at aktøren bag angrebet har kommunikeret med- og muligvis sendt kommandoer til RAT-malwaren på de samme maskiner.

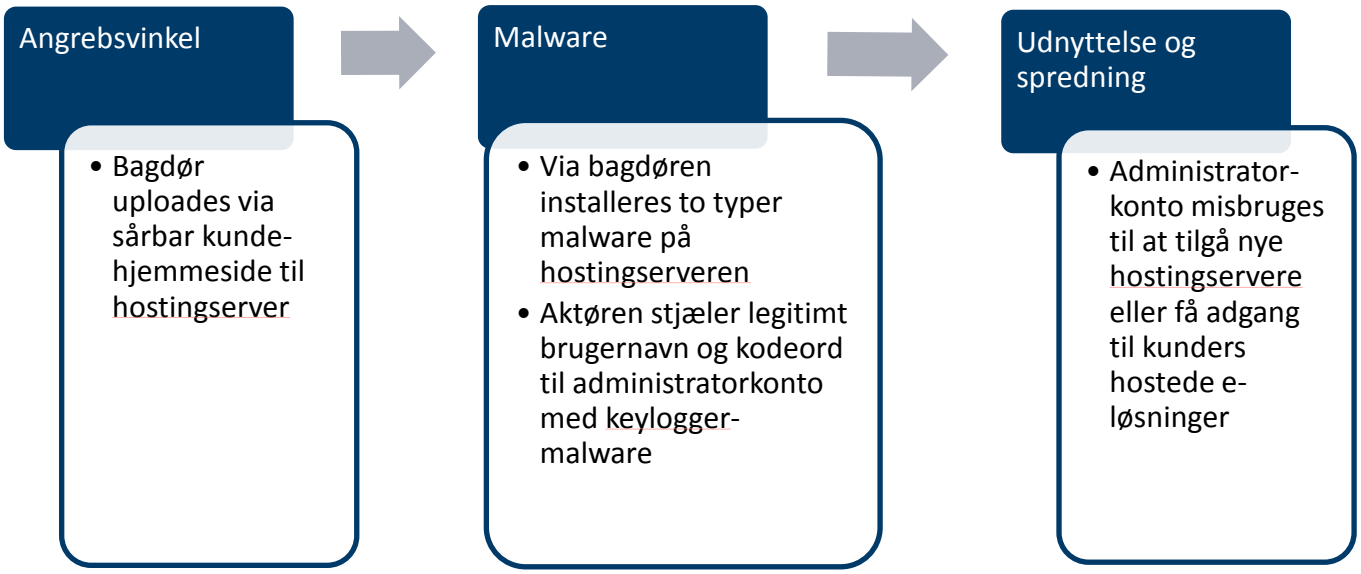
CFCS' analyse af de kompromitterede computere viser, at aktøren aktivt har forsøgt at skjule sin operation ved at forsøge at slette sine spor. Der er også fundet tegn på, at aktøren har overvåget de kompromitterede maskiner for at se, om angrebet blev opdaget.

Et muligt motiv

Det er muligt, at aktøren har udnyttet de kompromitterede maskiner eller informationer fra dem til at sprede sig i det lokale netværk eller til virksomhedens kunder. Selvom der ikke er tilstrækkelige informationer til at udpege aktørens konkrete mål, så kan sammenlignelige angrebskampagner vise, hvad aktøren sandsynligvis har været ude efter.

CFCS har tidligere set lignende kampagner, hvor hostingfirmaer er blevet kompromitteret med henblik på at få adgang til en kundes løsning og derigennem kundens infrastruktur. I et af disse tilfælde kunne det ses, hvordan angriberen først har skaffet sig adgang til en hostet webløsning, og herigennem kan få administrativ adgang til nogle af firmaets delte services, som databaseværktøjet SQL eller brugeradministrationsværktøjet Active Directory, og derfra kan springe videre til andre kunders løsninger. Der kan læses mere om denne type angreb i CFCS rapporten "King of Phantom – genvej til hovedmålet" på www.cfcs.dk/publikationer.

Når en maskine først er blevet kompromitteret, er der flere måder, hvorpå aktøren kan brede sig ud til andre systemer. I denne sag har CFCS set, at aktøren har brugt keylogger-malware, hvilket betyder, at aktøren kan stjæle loginoplysninger, så snart en bruger logger på. Loginoplysningerne er særligt værdifulde, hvis de tilhører en bruger med administrationsrettigheder, da de ofte har fuld adgang til alle maskiner og services på netværket. Alternativt kan aktøren bruge adgangen til at oprette sin egen brugerkonto med administrationsrettigheder. Dette gør det muligt for aktøren at fastholde sin adgang til netværket, selvom den oprindelige administratorkonto får skiftet password eller lukkes.



Figur 1: Tegningen viser, at det, der begynder som en simpel kompromittering af en mindre kundes hjemmeside, potentielt kan sprede sig til kritisk infrastruktur eller medføre tyveri af store mængder data.

I det omfang en stjålen administratorkonto kan tilgå data eller services for hostede kunder, kan kontoen også misbruges til at stjæle oplysninger eller sprede malware samme steder. Som nævnt indledningsvis kan et hostingfirma således fungere som et springbræt til at få adgang til kundernes infrastruktur, personfølsomme oplysninger eller lignende.

Det er også muligt, at angrebet har haft til hensigt at kompromittere maskiner til senere misbrug. Motivet kan så være at opbygge kapacitet til at udføre cyberangreb ved at inkludere et stort antal kompromitterede maskiner i en ondsindet infrastruktur. Denne form for cyberangreb er nærmere beskrevet i den tidligere undersøgelsesrapport "Når Danmark sover - fjendtlig opmarch på usikre servere, 2016" på www.cfcs.dk/publikationer.

Når skaden sker

Hvis en virksomheds eller myndigheds data stjæles, har det som regel alvorlige konsekvenser. For en privat virksomhed kan konsekvenserne f.eks. være tab af markedsandele, produktionstab, tab af viden, negativ branding, fald i tillid hos kunder med videre.

For at opgøre de præcise skader, er det en forudsætning, at der er opsamlet forskellige logs til at belyse dette. Det har derfor i de konkrete tilfælde været vanskeligt at fastslå skadesvirkningerne hos hostingfirmaerne eller de kunder, der måtte være berørt af angrebet. Dette skyldes, at der ikke var opsamlet eller gemt logningsmateriale i tilstrækkelig grad. CFCS er ofte ude for, at logningsoplysningerne mangler eller er utilstrækkelige. Dette udgør et stort problem i forhold til at analysere angrebene – både i forhold til at forstå angrebets omfang og angribernes modus og teknikker, men også i forhold til den efterfølgende udbedring og genopbygning. Typisk vil ramte virksomheder og myndigheder dog have udgifter til både egne analyser og mitigerende tiltag, ligesom udgifter til nyt hardware og geninstallation af servere og systemer koster tid og penge, herunder udgifter til eventuelle sikkerhedsfirmaer.

Typiske problemstillinger hos kunder

CFCS har til opgave at styrke det danske forsvar mod cyberangreb. En af måderne denne opgave løses på, er ved at støtte virksomheder og myndigheder, som er mistænkt for at være kompromitteret med APT-relateret malware. Når en mistanke opstår, tager CFCS kontakt til den berørte virksomhed og myndighed med et tilbud om støtte til at finde og eventuelt fjerne den malware, der måtte være. I visse alvorligere tilfælde tilbyder CFCS at sende et incident response team til at bistå lokalt med opklaringsarbejdet, hvis virksomheden eller myndigheden ønsker det. For virksomheden eller myndigheden kan samarbejdet hjælpe til at få svar på, hvordan angrebet er foregået, hvad der er hændt på kompromitterede maskiner og netværk, og hvilken malware, der præcist er tale om. Informationerne er gode at have, når der efterfølgende skal ryddes op, og eventuelle sikkerhedshuller skal lukkes.

For at CFCS kan yde en optimal hjælp, er det vigtigt, at virksomheden eller myndigheden er moden til det. Det er CFCS's erfaring, at der er stor forskel på virksomheders og myndigheders modenhed, når det gælder IT-sikkerhed. Modenhed kan i denne sammenhæng defineres på flere måder. Teknisk modenhed og forståelse for nødvendigheden af anvendelsen af forskellige sikkerhedsteknologier er én faktor. En anden er den måde kunde og hostingfirma/it-fællesskab kommunikerer, og i det hele taget har aftalt

deres gensidige forpligtelser. Uklare aftaler og forventninger mellem leverandør og kunde kan i sidste ende resultere i, at ingen gør noget i tilfælde af et cyberangreb.

Logning: analysegrundlaget

Når CFCS skal bistå en virksomhed eller myndighed med at afdække, om der har været et cyberangreb, og fastlægge dets eventuelle omfang, er det helt afgørende, at der er foretaget logning af aktiviteten på relevante systemer og relevant netværkstrafik. Det er bl.a. gennem disse logs, at CFCS kan undersøge, hvad der er hændt på de netværk og maskiner, hvor der er en mistanke om en kompromittering. I mange tilfælde er der ikke logs tilgængelige, eller også er de mangelfulde. Det kan være i forhold til antal systemer, der er loggede, hvor lang en periode de dækker, og hvor længe de gemmes. Ofte mangler logs af den simple årsag, at det kan opfattes som dyrt og besværligt at gemme.

CFCS vurderer, at de manglende logs ofte skyldes uklare aftaler og forventninger mellem kunde og leverandør. Har kunden ikke stillet specifikke krav om logning, vil de sjældent blive opsamlet. Ønsker kunden adgang til logs, kan dette arrangeres mod en merbetaling. Hvis kundens egen modenhed i forhold til forståelse af it-sikkerhed er lav, er det dog ikke sikkert, at kunden tænker på, at logs er nødvendige, hvorfor dette ikke bestilles. CFCS har i en række tilfælde erfaret, at en leverandør tilmed har undladt at informere kunden om hensigtsmæssigheden ved at opsamle logs.

Opsamling

Fordi hostingfirmaer i stigende grad bliver brugt som indgang til endelige mål af ondsindede aktører, er det særligt vigtigt at have kontrol med de aftaler, der indgås med eksterne it-leverandører. Undersøgelsen af denne hændelse viste så store mangler i logningsoplysninger – både i forhold til periode og indhold, at konsekvenserne og omfanget af angrebet ikke fuldt ud kunne afdækkes. CFCS vurderer, at manglen på logning ofte bunder i uklare kommunikationsveje og ansvarsfordeling mellem hostingfirmaet og deres kunder.

Nedenstående afsnit beskriver nogle procesmæssige tiltag og anbefalinger, der kan være med til at sikre en bedre samarbejdsaftale mellem kunde og hostingsfirma med henblik på styrket it-sikkerhed ved outsourcet it-drift.

Anbefalinger

På baggrund af de to beskrevne hændelser anbefaler CFCS, at topledelsen i alle organisationer erkender de risici, der er forbundet med anvendelsen af outsourcet it-drift og anvendelse af eksterne it-services. Der er mange forhold vedrørende styring af informationssikkerhed, der skal tages i betragtning, når hele eller dele af en organisations it-drift skal outsources. Området er for stort til, at det hele kan dækkes her, men der er en række anbefalinger, der knytter sig til de forhold, der har karakteriseret de to sager beskrevet ovenfor.

Ethvert kunde-leverandørforhold gennemlever en livscyklus, der kan inddeles i flere faser, og for hver fase er der særlige aspekter vedrørende informationssikkerhed, der skal adresseres i forholdet mellem kunde og leverandør.

Planlægningsfasen

Inden en organisation påbegynder outsourcing af it-drift eller services, bør den sikre sig, at den er i besiddelse af et godt, solidt og retvisende billede af egen it-arkitektur; hvilke informationer, systemer, netværk, datastrømme m.m. har organisationen? Hvis dette overblik mangler, er det meget vanskeligt at tage de rette beslutninger på informationssikkerhedsområdet i forhold til at outsource.

Når en organisation har besluttet sig for at outsource it-drift eller anvende eksterne it-services, skal det afdækkes, hvilke informationssikkerhedsmæssige risici, det vil medføre. Det kan være risici i forhold til at beskytte informationernes fortrolighed, integritet eller tilgængelighed. Når en organisation indgår i et samarbejde om it-drift, ændrer det organisationens risikobillede, fordi outsourcing både kan introducere nye risici, såvel som skabe muligheder for at forbedre sikkerheden. I planlægningsfasen skal organisationen beslutte sig for de overordnede krav til informationssikkerhed, der skal stilles til kommende samarbejdspartnere, og det skal afklares, hvilke opgaver man selv vil udføre, og hvilke opgaver leverandøren skal udføre. De overordnede krav bør være udarbejdet, før man går i gang med at udvælge leverandører.

Udvælgelse af leverandører

Når der opstilles tildelingskriterier for valg af leverandører, skal det overvejes, i hvilken grad kravene til informationssikkerhed skal vægte, herunder om fortrolighed, integritet og tilgængelighed er lige væsentlige parametre for valg af leverandør i forhold til den konkrete leverance. Økonomi er som regel et væsentligt parameter, når det kommer til valg af leverandør, og i forhold til sikkerhed bør det vurderes, om de sikkerhedsforanstaltninger, leverandøren forpligter sig til at levere, står i et rimeligt og realistisk forhold til prisen. Nogle leverandører vil måske slække på sikkerhedsforanstaltningerne for at kunne give et bedre bud på prisen. Det kan være en fordel at stille krav om, at prisen på leverancen af sikkerhed specificeres i udbud og kontrakt, således at leverandøren har et økonomisk incitament til at levere det aftalte sikkerhedsniveau.

Andre forhold, der kan have betydning for valg af leverandør ud fra et sikkerhedsmæssigt perspektiv, er f.eks. leverandørens markedsposition. Hvorvidt det er en stor spiller eller en mindre spiller kan have såvel negativ som positiv indflydelse på den leverede informationssikkerhed. Et andet forhold som bør medtages i overvejelserne, er lock-in-problematikken: Vælger man en leverandør, der leverer en meget unik ydelse, kan det være svært senere at skifte til en anden leverandør.

Aftalen

Ved udarbejdelse af aftalegrundlaget skal man være opmærksom på, at det er aftalegrundlaget, der fremadrettet regulerer den sikkerhed, leverandøren er forpligtet til at levere. Men det anbefales også, at der gennem aftalen etableres en formaliseret proces til håndtering af dialogen mellem kunden og leverandøren vedrørende leverancen, både i det daglige, men også i tilfælde af, at der opstår utilsigtede hændelser i form af f.eks. et cyberangreb. I de to konkrete sager var det tydeligt, at der manglede klare aftaler om ansvarsfordeling og kommunikationsveje.

Det anbefales, at man som kunde nøje overvejer, hvilke styringsmuligheder vedkommende vil have i forhold til tilpasning af sikkerheden i leverancen. Forhold hos både kunden og leverandøren kan hele tiden ændre sig, ligesom trusselsbilledet også er foranderligt. Derfor bør aftalen rumme muligheder for løbende at kunne justere på sikkerheden inden for rammerne af aftalen.

Aftalen skal indeholde de informationssikkerhedskrav, som leverandøren skal leve op til og regulere, som minimum på følgende områder:

- Opgaver, roller og ansvarsfordeling hos både kunden og leverandøren.
- De aftalte sikkerhedsforanstaltninger, herunder:
  - Leverandørens adgang til kundens informationer, adgangsstyring og brug af administrative konti.
  - Leverandørens forpligtelser i forhold til underleverandører.
  - Håndtering af ændringer, enten på foranledning af kunden eller leverandøren. Det forhold, at andre kunder hos leverandøren kan have ønsker om ændringer, kan påvirke sikkerheden for egen organisation og bør tages i betragtning. Håndtering af ændringer i form af opdateringer kan også skabe udfordringer, når man deler it-platform med andre organisationer.
  - Håndtering af informationssikkerhedshændelser, herunder hændelser som potentielt kan have uønskede konsekvenser. Opgaver og ansvar skal være klart placeret. I tilfælde af en hændelse skal der ofte handles hurtigt, og der er derfor ikke tid til at afklare opgaver og ansvar. Et af de forhold, der bør afklares i aftalen, er hvem, der har kompetence til at lukke services, kommunikationslinjer, systemer m.m. Procedure for afprøvning af beredskabsplaner bør ligeledes indgå i aftalen.

- Adskillelse af kundens informationer eller systemer fra andre kunders informationer eller systemer. Kunden skal overveje relevante risici ved, at egne informationer er "blandet" med andre kunders informationer på fælles servere. I efterforskningsmæssig sammenhæng kan det være vanskeligt at undersøge computerudstyr, hvis det indeholder informationer fra andre organisationer. Evnen til at tage hurtige beslutninger om f.eks. lukning af netadgang hæmmes, hvis det også berører andre.
- Leverandørens forpligtelse til at oplyse kunden om informationssikkerhedshændelser.
- Monitorering af sikkerheden, herunder krav til, hvad der skal logges, og hvor længe logs skal opbevares, før de må slettes. CFCS' logningsvejledning kan findes på www.cfcs.dk/publikationer.
- Kundens ret og muligheder for at følge op på sikkerhedstilstanden af leverancen. Mulighed for at foretage revision og gennemføre sikkerhedstest, enten af kunden selv eller af tredjepart, bør indgå i aftalen.
- Procedure for, hvordan der skal handles i tilfælde af, at aftalen skal ophøre – enten frivilligt eller som følge af en tvist mellem parterne. Det skal afklares, hvordan kunden får sine informationer tilbage eller overleveret til en ny leverandør, hvor hurtigt det skal gøres, i hvilket format, m.m.

Et forhold, der kan tages med i aftalen, er misligholdelse. Her er det værd at overveje, om der er sikkerhedsmæssige krav, der er så væsentlige, at manglende overholdelse vil medføre opsigelse af aftalen. Men det er samtidigt vigtigt at være opmærksom på, at netop opsigelse af en aftale kan medføre uønskede sikkerhedsmæssige udfordringer.

Styring af informationssikkerheden i drift

Når aftalen er indgået, skal kunden sikre sig, at leverandøren er helt klar over de forpligtelser, vedkommende har påtaget sig. I nogle tilfælde er forhandlingerne om aftalen ført mellem en indkøbsafdeling hos kunden og en salgsafdeling hos leverandøren. Derfor kan det være meget givtigt, at de medarbejdere, der skal udføre informationssikkerhedsopgaverne på begge sider i dagligdagen, får aftalt de nærmere procedurer for arbejdet.

Efterfølgende skal kunden løbende sikre sig, at de indgåede aftaler om informationssikkerhed overholdes, eksempelvis at den aftalte adgangs- og ændringsstyringsproces fungerer. Dette kan bl.a. gennemføres ved tilsynsbesøg.

Derudover skal kunden være opmærksom på forhold, der kan påvirke informationssikkerheden i leverancen, som ikke er dækket af almindelig ændringsstyring. Det kan være ændringer i:

- Leverandørens forretningsmål, mission eller omgivelser.

- Leverandørens økonomiske forhold.
- Leverandørens ejerforhold, sammenlægninger el.lign.
- Leverandørens fysiske og geografiske placering (flytter de evt. til et andet land).
- Leverandørens informationssikkerhed generelt.
- Leverandørens evne til at agere i tilfælde af sikkerhedshændelser.
- Relevante love, reguleringer eller kontraktlige forhold kunden er underlagt.

Der bør med jævne mellemrum udarbejdes risikovurderinger af leverancen i samarbejde mellem kunde og leverandør. På baggrund af vurderingen aftales handleplaner for risikohåndtering, som kunden efterfølgende skal holde øje med opfyldelsen af.

Afslutning af leverandør-kundeforholdet

Når aftalen mellem kunde og leverandør ophører – af den ene eller anden grund – skal de processer, der er beskrevet i aftalen, gennemføres. Ud over, at kunden skal have overført sine informationer, data og eventuelt software til sig selv eller en anden leverandør, skal det sikres, at data hos leverandøren destrueres i det omfang, det er beskrevet i aftalen.

At styre outsourcede it-løsninger kan være ganske omfattende, og organisationer skal derfor sikre sig, at de rette kompetencer og ressourcer er til rådighed i organisationen til denne opgave.

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 2014:

"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 – f.eks. Digitaliseringsstyrelsen og PET – inkluderes afhængig af hændelsen. Enheden etableres i 1. kvartal 2015."

Henvisninger

- KingofPhantom – bagdør til hovedmålet: www.cfcs.dk/publikationer
- Når Danmark Sover – Fjendtlig opmarch på usikre servere: www.cfcs.dk/publikationer
- Cyberforsvar der virker: www.cfcs.dk/publikationer
- Logning – en del af et godt cyberforsvar: www.cfcs.dk/publikationer
- Den fællesoffentlige digitaliseringsstrategi 2016-2020, Digitaliseringsstyrelsen, 2016: www.digst.dk
- Beretning om revisionen af statsregnskabet for 2015, Rigsrevisionen, 2016: www.rigsrevisionen.dk

Bilag 1 – Malwareoversigt

Oversigt over malware fundet på tre udvalgte hosts. Der er medtaget både crime-relateret malware samt APT-relateret malware.

Firma	Malware	Type
Hostingfirma 1	Gh0st (BRemotes)	RAT
Hostingfirma 1	Gh0st (IEHelper)	RAT
Hostingfirma 1	RAT 1 ZXShell	APT-relateret RAT
Hostingfirma 1	RAT 2 PlugX	APT-relateret RAT
Hostingfirma 1	Packed, old cmd.exe	Tool
Hostingfirma 1	cmd.exe	Tool
Hostingfirma 1	Gh0st (IEHelper)	RAT
Hostingfirma 1	Gh0st (DarkAngel)	RAT
Hostingfirma 1	Gh0st (Proxy/cc3)	RAT
Hostingfirma 1	IIS 6 – Local Priv Esc	Exploit
Hostingfirma 1	Packed, old cmd.exe	Værktøj
Hostingfirma 1	Mimikatz – Password	Værktøj
Hostingfirma 1	Pass.com – Password	Værktøj
Hostingfirma 1	ELF1.4 – Gem filer	Værktøj
Hostingfirma 1	Email2DBServer	Værktøj
Hostingfirma 1	ASPX – Web proxy	Værktøj
Hostingfirma 2	RAT 1 ZXShell	APT-relateret RAT
Hostingfirma 2	RAT 2 PlugX	APT-relateret RAT