CENTER FOR CYBERSIKKERHED

Trusselsvurdering

Cyberangreb mod leverandører

CENTER FOR CYBERSIKKERHED

Trusselsvurdering: Cyberangreb mod leverandører

Forsvarets Efterretningstjeneste
Kastellet 30
2100 København Ø

Tlf.: 33 32 55 80
E-mail: cfcs@cfcs.dk
www.cfcs.dk

1. udgave oktober 2019

Fremmede stater og kriminelle angriber ofte deres mål gennem forsyningskæden ved at kompromittere leverandører. Denne trusselsvurdering kan bruges af virksomheder og myndigheder til at sætte fokus på cybertruslen mod forsyningskæden.

Hovedvurdering

- Nogle leverandører er attraktive mål for hackere, fordi de kan give adgang til mange mål og data på én gang.
- Der er hackergrupper med kapacitet til og intention om at angribe leverandører, som udbyder centrale services og infrastruktur til virksomheder og myndigheder i Danmark.
- CFCS vurderer, at angrebsmetoden både benyttes af fremmede stater og cyberkriminelle.

Analyse

Cyberangreb mod leverandører af centrale services til danske virksomheder og myndigheder udgør en cybertrussel, herunder mod samfundsvigtige sektorer.

Cyberangreb mod forsyningskæden er en angrebsmetode, hvor hackere angriber en organisation for at benytte denne som springbræt til at kompromittere organisationens kunder. Dermed kan hackerne udnytte en organisation til at få adgang til informationer eller systemer, der tilhører hackernes egentlige mål.

Cyberangreb kan motiveres af forskellige ting, såsom bl.a. spionage eller økonomisk vinding.

Leverandører
Leverandører i denne trusselsvurdering er enhver organisation, der leverer it-services, software eller hardware. Det kan også være organisationer, der opbevarer data for kunder eller har adgang til kunders data. Leverandører outsourcer også opgaver videre til underleverandører. Der skelnes i trusselsvurderingen ikke mellem leverandører og underleverandører.

Leverandører er attraktive mål for hackere
Angrebsmetoden er effektiv, fordi kompromittering af en leverandør på én gang kan give adgang til mange mål, til indhentning af leverandørens kundedata eller adgang til væsentlige dele af en sektors infrastruktur.

Leverandører har ofte uhindret adgang til mange af deres kunders netværk og data. Ved blot at kompromittere én leverandør kan en aktør potentielt få mulighed for at bevæge sig uhindret på tværs af adskillige kunders netværk og data.

Aktører forsøger også at kompromittere leverandører på tværs af landegrænser. Det kan f.eks. være, at der er en lavere cybersikkerhed i en leverandørs underafdeling i et givent land, som gør det lettere at kompromittere leverandørens øvrige systemer. Hvis ikke leverandørens netværk er segmenterede på tværs af afdelinger, kan det give en aktør mulighed for at bevæge sig horisontalt i netværk på tværs af landegrænser.

Flere store internationale leverandører er gennem de seneste år blevet kompromitteret eller forsøgt kompromitteret. Nogle af disse leverandører udbyder også deres tjenester til myndigheder og virksomheder i Danmark. Ifølge åbne kilder blev elektronikgiganten ASUS hacket i løbet af 2018. ASUS' officielle software, ASUS Live Update tool, blev inficeret med malware. Det betød at brugere, som opdaterede programmet, downloadede en kompromitteret udgave af ASUS' software, der kunne give hackerne adgang til computerne.

Cyberangreb mod norske Visma
Den norske softwareleverandør Visma offentliggjorde i februar 2019, at den var blevet kompromitteret. Ifølge åbne kilder var formålet at få adgang til Vismas kunders data. Visma er en større international leverandør, som blandt andet leverer cloud-software til virksomheders regnskab og forretning. Selskabet har også afdelinger i Danmark.

Enkelte statsstøttede hackergrupper har de seneste år specifikt rettet deres opmærksomhed mod leverandører, der tilbyder cloud-løsninger og datalagertjenester til kunder i hele verden. Ved at kompromittere disse leverandører har aktørerne haft fjernadgang direkte ind i kundernes netværk, hvorfra de har kunnet stjæle informationer. Fordi hackerne misbrugte leverandørernes betroede netværk og brugte legitime brugernavne og kodeord, har det været vanskeligt for ofret at skelne mellem legitim og illegitim aktivitet. I visse tilfælde har aktørerne også haft adgang til de kundedata, der lå på leverandørernes egne servere.

Andre statsstøttede hackergrupper er specifikt gået efter større vestlige advokat- og rådgivningsfirmaer for derved at få adgang til relevante og ofte følsomme oplysninger fra virksomhederne selv og deres kunder. Revisionsfirmaer kan også være mål, da de ligeledes besidder følsomme informationer om deres kunder.

Der er også set cyberangreb mod computerproducenter og softwareleverandører, hvor leverandørernes softwareopdateringer blev inficeret med malware, som kunderne efterfølgende downloadede. NotPetya-angrebet, der bl.a. ramte Mærsk i juni 2017, er et af de mest kendte eksempler på et sådan angreb på en software leverandør.

Cyberangreb mod cloud-leverandører
Flere cloud-leverandører har ifølge åbne kilder været mål for et omfattende cyberangreb i en kampagne, som er døbt Cloud Hopper. Kampagnen var, ifølge åbne kilder, rettet mod nogle af de største internationale leverandører, herunder sandsynligvis deres kunder.

Cyberangreb mod ukrainsk leverandør
Leverandører i Ukraine er tidligere blevet udnyttet i cyberangreb, der også har berørt danske virksomheder. NotPetya-angrebet havde sit udspring hos en kompromitteret ukrainsk softwarevirksomhed, som har udviklet softwaren M.E.Doc. Hackere leverede malware til virksomheder gennem en softwareopdatering til M.E.Doc. Malwaren var en såkaldt orm, der efterfølgende hurtigt spredte sig til øvrige dele af de berørte virksomheders it-infrastruktur samt til andre virksomheder.

Der kan være tilfælde, hvor en leverandør ikke længere er i stand til at udsende sikkerhedsopdateringer. Det pågældende produkt vil over tid udgøre et stadig stigende sikkerhedsproblem. Som eksempel har det amerikanske Bureau of Industry and Security (BIS) i maj 2019 udsendt en liste over selskaber, som amerikanske virksomheder, efter en given dato, ikke må eksportere til uden en særlig tilladelse. Kinesiske Huawei er blandt andet nævnt på listen. Hvis forbuddet effektueres, kan det betyde, at Huawei på kort sigt ikke vil være i stand til at levere nye produkter og sikkerhedsopdateringer, som indeholder hardwaredele eller software fra amerikanske selskaber.

Danske organisationer benytter i høj grad leverandører
Mange virksomheder og myndigheder i Danmark benytter leverandører til digitale tjenester eller services, som de outsourcer til. Det er typisk cloud-løsninger, datalagertjenester og it-serviceydelser. Mange af leverandørerne, som der outsources til, er udenlandske globale udbydere.

Outsourcing kan på mange måder give god mening ud fra et forretningsmæssigt synspunkt, da det kan optimere flere arbejdsgange, og virksomheden eller myndigheden kan fokusere sine ressourcer.

Anvendelse af en anerkendt ekstern outsourcing-leverandør vil ofte også give sikkerhedsmæssige fordele i kraft af de store leverandørers stadig stigende professionelle indsats for at modgå både simple og mere avancerede cybertrusler. Det kan dog også give sikkerhedsmæssige udfordringer, hvis man ikke stiller relevante sikkerhedskrav og opnår tilstrækkelig indsigt i og kontrol med løsningen. Ved outsourcing overlader man reelt beskyttelsen af data og it-systemer til leverandøren, selvom ansvaret for et tilstrækkeligt sikkerhedsniveau forbliver i virksomheden eller myndigheden.

Outsourcing af services til leverandører øger koncentrationsrisikoen fra cybertruslen, da aktører kan kompromittere mange ofre eller væsentlig infrastruktur på én gang ved at kompromittere en leverandør, såfremt der ikke er etableret relevante og dækkende sikkerhedsforanstaltninger.

Kompromitteringer i forsyningskæden er svære at opdage
Det kan være vanskeligt at opdage kompromitteringer eller få indsigt i forsøg på kompromittering i forsyningskæden, fordi det ikke er virksomhederne eller myndighederne, som bliver kompromitteret men derimod deres leverandør.

Cyberkriminelle angriber leverandører i Business Email Compromise (BEC)
Cyberkriminelle har angrebet forsyningskæden ved at kompromittere leverandørers e-mail-konti. Aktørerne udnytter f.eks. de kompromitterede e-mail-konti til at opsnappe fakturaer og forfalske kontooplysninger på fakturaerne, som efterfølgende sendes til leverandørens kunder. Netop fordi kunden forventer at modtage en faktura for den service, som leverandøren har ydet, kan det være meget vanskeligt at opdage forfalskningen.

Af samme årsag kan det være svært for virksomheder og myndigheder at risikostyre cybertruslen mod forsyningskæden. Når en service outsources til en leverandør, outsources cybersikkerhed og adgang til data også. Leverandørens niveau for cybersikkerhed, omfang af beredskab m.m. bliver automatisk til en delmængde af virksomhedens eller myndighedens eget i forhold til at beskytte sig mod cybertrusler. Det kan være en udfordring for virksomheder og myndigheder at få tilstrækkeligt indblik, kontrol og indflydelse i disse procedurer hos leverandører.

Leverandører outsourcer også opgaver videre til underleverandører. Det kan gøre risikostyringen af cybertruslen endnu vanskeligere.

Vejledning om leverandørstyring
CFCS har udgivet vejledningen ”Informationssikkerhed i leverandørforhold”, som indeholder en række forslag til, hvordan styringen af forholdet mellem organisationer og leverandører kan varetages. Vejledningen kan læses på CFCS’ hjemmeside.

Trusselsniveauer
Forsvarets Efterretningstjeneste bruger følgende trusselsniveauer.

INGEN	Der er ingen indikationer på en trussel. Der er ikke erkendt kapacitet eller hensigt. Angreb/skadevoldende aktivitet er usandsynlig.
LAV	Der er en potentiel trussel. Der er en begrænset kapacitet og/eller hensigt. Angreb/skadevoldende aktivitet er mindre sandsynlig.
MIDDEL	Der er en generel trussel. Der er kapacitet og/eller hensigt og mulig planlægning. Angreb/skadevoldende aktivitet er mulig.
HØJ	Der er en erkendt trussel. Der er kapacitet, hensigt og planlægning. Angreb/skadevoldende aktivitet er sandsynlig.
MEGET HØJ	Der er en specifik trussel. Der er kapacitet, hensigt, planlægning og mulig iværksættelse. Angreb/skadevoldende aktivitet er meget sandsynlig.

FE bruger denne skala for sandsynligheder i analyser