CENTER FOR CYBERSIKKERHED

Trusselsvurdering

Cybertruslen mod it-serviceudbydere

Indhold

CENTER FOR CYBERSIKKERHED

Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk

1. udgave november 2020

Trusselsvurdering: Cybertruslen mod it-serviceudbydere

Formålet med denne trusselsvurdering er at orientere danske myndigheder, virksomheder og beslutningstagere om cybertruslen mod it-serviceudbydere, herunder hostingudbydere og Managed Service Providers. Angreb mod it-serviceudbydere udgør en særlig alvorlig form for leverandørtrussel.

Hovedvurdering

- Cyberangreb mod it-serviceudbydere udgør en alvorlig og vedvarende trussel mod danske virksomheder og myndigheder.
- It-serviceudbyderes legitime, nødvendige og ofte særlige adgang til deres kunders it-systemer og netværk gør dem til attraktive mål for hackere.
- It-serviceudbydere bliver både ramt af målrettede og opportunistiske cyberangreb, hvor mange mål rammes samtidig.
- Hackere udfører cyberangreb mod it-serviceudbydere med forskellige formål. Truslen kommer bl.a. fra kriminelle hackere, der f.eks. udfører målrettede ransomware-angreb mod it-serviceudbydere.
- Statsstøttede hackere udfører også cyberspionage mod it-serviceudbydere. Hackerne går både efter virksomheders intellektuelle ejendom og myndigheders sensitive data.
- Derudover er der eksempler på, at it-serviceudbydere er blevet ramt af alvorligt forstyrrende angreb.

Analyse

Cyberangreb mod it-serviceudbydere udgør ikke bare en trussel mod virksomhederne selv, men også mod deres kunder.

Danske myndigheder og virksomheder er dermed udsat for en alvorlig trussel fra cyberangreb mod de it-serviceudbydere, såsom hostingudbydere og Managed Service Providers (MSP'er), som de er kunder hos. Det skyldes, at it-serviceudbydere har en legitim, nødvendig og ofte særlig adgang til deres kunders it-systemer, som hackere kan misbruge. Cyberangreb mod it-serviceudbydere udgør derfor en særlig alvorlig form for leverandørtrussel.

It-serviceudbyderes adgang gør dem til attraktive mål

It-serviceudbydere er attraktive mål for flere typer cyberaktører, særligt cyberkriminelle og statsstøttede hackere. Cyberangreb mod it-udbydere kan få betydelige konsekvenser, både i form af økonomiske tab, driftsforstyrrelser og for udbyderens renommé.

Ofte er det it-udbydernes adgang til deres kunders it-systemer og netværk, der tiltrækker hackerne. I cyberangreb mod it-serviceudbydere udnytter hackere den tillid og adgang, udbydere har hos deres kunder. Ved at angribe it-serviceudbydere kan hackere kompromittere mange af udbydernes kunder.

Eksempelvis blev it-systemer hos 22 offentlige administrationer i Texas inficeret med ransomwaren REvil via en it-serviceudbyder i august 2019. Angrebet skete ved, at MSP'en TSM Consulting blev kompromitteret, hvorefter deres fjernadgangsværktøj blev udnyttet af hackerne til at sprede malware i it-systemerne hos ofrene.

I et andet eksempel fra maj 2020 blev cloududbyderen Blackbaud udsat for et ransomware-angreb. Efterfølgende har en række amerikanske og britiske universiteter offentligt meddelt, at forskellige typer data, f.eks. personfølsomme oplysninger om deres ansatte og studerende, muligvis er blevet eksponeret som et resultat af kompromitteringen hos BlackBaud. Eksemplet illustrerer de konsekvenser, cyberangreb mod it-serviceudbydere kan få for udbydernes kunder.

Kriminelle hackere udfører også cyberangreb mod it-serviceudbydere, for senere at videresælge deres adgang til udbyderens it-systemer og i nogle tilfælde udbyderens kunders it-systemer. Den modus er en del af den samlede trussel for cyberkriminalitet og dermed ikke speciel i forhold til angreb mod it-serviceudbydere.

Forskellige typer it-serviceudbydere

It-serviceudbydere
It-serviceudbydere benyttes i denne trusselsvurdering som en samlet betegnelse for de forskellige typer virksomheder beskrevet nedenfor.

Hostingudbyder
Er en virksomhed, som ejer it-infrastruktur og udbyder it-ressourcer som hukommelse, lagerkapacitet og processorkraft til kunder. Er der tale om webhosting, udbyder virksomheden den it-infrastruktur og de it-værktøjer, som er nødvendige for at kunne oprette en hjemmeside og forbinde den til internettet.

Managed service provider (MSP)
Er en fællesbetegnelse for virksomheder, der leverer og forvalter forskellige typer it-services, som drift og support af kundens egen it-infrastruktur, herunder back-ups, patching og overvågning af it-netværket.

Cloududbyder
Er en virksomhed, som ejer it-infrastruktur, der ofte er distribueret geografisk. Via infrastrukturen tilbydes fjernadgang til dynamisk skalerbar serverkapacitet, software-applikationer som e-mail og kontorprogrammer eller en komplet udviklingsplatform, hvor kunden kan udvikle og køre sine egne applikationer og internettjenester.

Målrettede ransomware-angreb rammer også it-serviceudbydere

Både i Danmark og i udlandet er it-serviceudbydere blevet ramt af forskellige typer kriminelle cyberangreb gennem de seneste år.

I Danmark blev it-serviceudbyderen GlobalConnect ramt af et ransomware-angreb i efteråret 2019 og blev igen kompromitteret i april 2020. Det andet angreb ramte også it-systemer tilhørende en række af GlobalConnects kunder, herunder medicin-indkøberen Amgros.

Angreb på it-serviceudbydere kan påvirke kunders adgang til data

I 2019 blev flere udenlandske hostingudbydere ramt af ransomware-angreb, bl.a. SmarterASP.NET, der har mere end 440.000 kunder. Angrebet betød, at udbyderens kunder ikke havde adgang til deres data, for nogle kunder i flere dage.

Både i Danmark og udlandet er omfanget af målrettede ransomware-angreb steget de seneste år. I den type angreb afpresser kriminelle hackere virksomheder og myndigheder ved at kryptere centrale it-systemer. Den form for angreb rammer også it-serviceudbydere.

Ransomware-angreb mod it-serviceudbydere kan påvirke it-serviceudbyderes levering af ydelser og i værste fald afbryde leveringen af ydelser, såsom support og drift af it-infrastruktur, i længere perioder.

Hackere, der står bag målrettede ransomware-angreb, er siden slutningen af 2019 begyndt at lække følsomme data indsamlet fra ramte it-systemer, hvis ofre ikke betaler løsesummen. Ved angreb mod en it-serviceudbyder kan hackere potentielt få adgang til følsomme kundeoplysninger om virksomheder og myndigheder og bruge oplysningerne til at afpresse den ramte it-serviceudbyder.

Der er et samarbejde mellem de kriminelle, der udfører mere målrettede angreb, og de kriminelle, der rammer tusindvis af ofre gennem bl.a. phishing. Målrettede ransomware-angreb udføres ofte efter en indledende opportunistisk kompromittering af offeret med malware spredt gennem phishing eller via eksterne fjernadgangssystemer såsom Remote Desktop Protocol (RDP) og Virtual Private Network (VPN). Videregivelse og salg af disse indledende kompromitteringer kaldes for access-as-a-service.

Statsstøttede hackere angriber også it-serviceudbydere

Flere stater udfører cyberangreb mod både hostingudbydere og MSP'er. Ligesom det gælder for kriminelle, kan det være attraktivt for statsstøttede hackere at kompromittere selve it-serviceudbyderen eller bruge en kompromittering som et springbræt til at ramme specifikke mål blandt it-serviceudbyderens kunder. Ved at misbruge en it-serviceudbyders legitime adgang til kundens it-systemer og netværk kan hackerne omgå mange almindelige it-sikkerhedsforanstaltninger, såsom netværkssegmentering og kontrol med brugerrettigheder.

Flere eksempler på angreb mod danske it-serviceudbydere

I 2014-2015 blev et dansk it-hostingfirma samt en af virksomhedens kunder kompromitteret. CFCS vurderer, at angrebet blev udført af statsstøttede hackere og at formålet med angrebet var cyberspionage. Hændelsen er beskrevet i undersøgelsesrapporten "KingofPhantom – bagdør til hovedmålet" der er tilgængelig på CFCS' hjemmeside.

I 2015 blev en dansk it-serviceudbyder, der bl.a. leverer hosting til offentlige kunder, kompromitteret. CFCS vurderer, at formålet med angrebet var at opbygge et netværk bestående af kompromitterede maskiner til brug i flere cyberangreb. Angrebet var en del af en større kampagne, der er beskrevet i undersøgelsesrapporten "Når Danmark sover – fjendtlig opmarch på usikre servere", som er tilgængelig på CFCS' hjemmeside.

Det kan være sværere at afgøre, hvordan en virksomhed er blevet kompromitteret, hvis angrebet er blevet udført via en it-serviceudbyder. Det kan medvirke til at gøre it-serviceudbydere til attraktive mål for statsstøttede hackere, der ønsker at skjule deres aktiviteter.

Statsstøttede hackere fra flere lande har igennem de seneste år udført cyberspionagekampagner mod og via it-serviceudbydere. Hackerne er både gået efter virksomheders intellektuelle ejendom og myndigheders sensitive data. Eksempelvis har statsstøttede hackere flere gange angrebet it-serviceudbydere, der leverer services til regeringer og andre myndigheder i udlandet.

Eksempelvis er flere leverandører af it- og cloudløsninger blevet hacket som en del af en cyberspionagekampagne kaldet 'Cloudhopper'. Hackerne har både haft adgang til data fra it-serviceudbyderne selv, og de har også haft adgang til udbydernes kunder. I flere medier er det f.eks. beskrevet, at Hewlett Packard Enterprise Co (HPE) og IBM blev kompromitteret af hackergruppen kendt som APT10. Den 20. december 2018 anklagede det amerikanske justitsministerium og FBI to kinesiske statsborgere for at være tilknyttet hackergruppen.

Den norske virksomhed Visma, der bl.a. leverer cloudsoftware, blev også kompromitteret i 2019. Visma har også afdelinger i Danmark.

Udover cyberspionage kan statsstøttede hackere også udføre forstyrrende cyberangreb mod it-serviceudbydere.

Det skete eksempelvis i efteråret 2019, hvor både amerikanske og britiske myndigheder offentligt anklagede russiske statsstøttede hackere for at stå bag et alvorligt forstyrrende angreb mod den georgiske web-hostingudbyder Pro Service d. 28. september 2019. I bl.a. de britiske myndigheders offentlige udtalelser om angrebet blev det anført, at angrebet blev udført for at skabe ustabilitet og underminere Georgiens suverænitet.

Cyberangrebet mod Pro Service førte til, at over 2000 georgiske hjemmesider blev udsat for såkaldte defacement-angreb. Hjemmesiderne tilhørte bl.a. den georgiske regering, præsidentkontoret, civile domstole, lokale byråd, banker, NGO'er samt større virksomheder og nyhedsmedier i Georgien. Det originale indhold på de mange hjemmesider blev erstattet af et foto af Georgiens tidligere præsident, Mikheil Saakashvili, med teksten "I'll be back", før hackerne lukkede hjemmesiderne ned. Alle hjemmesiderne var dog oppe igen efter 24 timer.

Mere viden om cybertruslen mod it-serviceudbydere

Center for Cybersikkerhed (CFCS) udgiver løbende vejledninger og trusselsvurderinger. Nedenfor er fremhævet en række produkter af særlig relevans for håndteringen af truslen mod it-serviceudbydere. Alle produkterne er tilgængelige på CFCS' hjemmeside.

Vejledning om leverandørstyring
Vejledningen "Informationssikkerhed i leverandørforhold" indeholder en række forslag til, hvordan styringen af forholdet mellem organisationer og leverandører kan varetages.

Trusselsvurdering om truslen med leverandører
Trusselsvurderingen "Cyberangreb mod leverandører" beskriver generelt cybertruslen mod leverandører.

Vejledning til anvendelse af cloudservices
"Vejledning til anvendelsen af cloudservices" beskriver de principielle problemstillinger, cloudservices introducerer og giver konkrete anvisninger til at vurdere anvendelsen af cloudservices.

FE bruger denne skala for sandsynligheder i analyser

Usandsynligt	Mindre sandsynligt	Muligt	Sandsynligt	Meget sandsynligt

"FE vurderer" svarer til "Sandsynligt", medmindre en anden sandsynlighed er angivet.