Danmarks nationalbank hacket som led i ‘verdens mest sofistikerede hackerangreb’

version2.dk/artikel/danmarks-nationalbank-hacket-led-verdens-mest-sofistikerede-hackerangreb-1092886

June 29, 2021

Statshackere har haft muligheden for at kompromittere dele af Nationalbankens it-setup med et udspekuleret, internationalt setup.

Mads Lorenzen
Journalist

Reportage29. juni 2021 kl. 03:45

errorÆldre end 30 dage

42 kommentarer. Hop til debatten

Mads Lorenzen
Journalist

Manglende links i teksten kan sandsynligvis findes i bunden af artiklen.

Nogle af verdens mest sofistikerede hackere har haft en it-bagdør i Nationalbanken i syv måneder. Nationalbanken selv kan ikke udelukke, at de formodede russiske statshackere har misbrugt bagdøren til at kompromittere Nationalbanken yderligere.

Det viser en aktindsigt, Version2 har fået i sagen. Aktindsigten slår fast, at Danmarks Nationalbank, der driver hele Danmarks centrale finansielle infrastruktur, blev ramt af det verdensomspændende Solarwinds-hackerangreb tilbage i december 2020.

Uanset hvad statshackerne har brugt adgangen til, har de haft en enestående mulighed, vurderer Jan Lemnitzer, der er ekstern lektor i it-sikkerhed på CBS.

»Nationalbanken ligger inde med en masse spændende informationer om Danmark og danske virksomheder. Men vi ved også, at det er et strategisk mål for russerne at destabilisere Vesten. Russerne har altså en interesse i at skabe forvirring, og det vil man bestemt opnå, hvis man sætter Nationalbanken ud af spillet,« siger Jan Lemnitzer.

Opdaget ved en tilfældighed

Solarwinds-bagdøren stod i Nationalbankens tilfælde åben i syv måneder, inden angrebet blev opdaget ved en tilfældighed af det amerikanske sikkerhedsfirma Fire Eye.

Nationalbankens leverandør af det kompromitterede program, Solarwinds Orion, vurderer det derfor som en ‘umulig opgave at bevise udeblivelsen af IOC’er (Indications of Compromise, *red.*)’, skriver leverandøren i en intern mail til Nationalbanken.

En bagdør er et it-sikkerhedshul, der tillader angribere at komme ind i systemer, når de vil, og denne konkrete bagdør blev i al hemmelighed installeret i det ellers troværdige Solarwinds-program, der styrer komplicerede netværks-systemer. Derfor er Solarwinds den perfekte måde at angribe et selskabs eller en organisations servere på.

»Hvis man har adgang til Solarwinds er det generelt set ret nemt at køre ting på alle servere, Solarwinds har adgang til. Hvis du har et program, du vil inficere systemet med, kan Solarwinds installere det overalt med ét klik fra dem, der styrer Solarwinds,« forklarer Lucas Lundgreen, der som white hat hacker hos virksomheden Banshie lever af at teste virksomheders sikkerhed. Inden da arbejdede han blandt andet med opsætning af Solarwinds-servere.

Danmarks finansielle hjerte

Hver bankdag flyder 639 milliarder kroner gennem Danmarks finansielle infrastruktur, og alle betalinger mellem banker går direkte gennem systemet Kronos2, der køres af Nationalbanken.

Kronos2 fungerer desuden som platform for alle valutahandler, detailbetalinger og værdipapirhandler. Derfor er den danske nationalbank et yderst attraktivt mål for russerne, vurderer to it-sikkerhedsforskere, Version2 har snakket med.

»Hvis man kan stoppe transaktionerne, nationalbanken laver, og programmerne, der sørger for dem, bryder helvede løs. Nationalbanken er et mega spændende mål for hackere,« siger Carsten Schürmann, der er it-sikkerhedsprofessor på ITU.

Sendte verdens it-afdelinger på overarbejde

Umiddelbart er der dog intet, der tyder på, at Nationalbanken er berørt dybere end den såkaldte Stage1-kompromittering, fremgår det af aktindsigten. Stage1-kompromittering betyder kort fortalt, at en lille kodestump i Nationalbankens it-system har informeret hackerne om, at bagdøren er klar til at blive åbnet for dem.

Men kodestumpen har ligget klar i mere end syv måneder inden Nationalbanken, og de 18.000 andre berørte selskaber og organisationer, fik nys om den. Derfor er det meget svært at udelukke, at de formodede russiske bagmænd ikke har kompromitteret systemet dybere - og fjernet sporene igen.

Det gjorde den formodede russiske hackergruppen netop, da den udnyttede samme trick, Nationalbanken i god tro er faldet for, da hackerne blandt andet kompromitterede det amerikanske forsvarsministerium, Microsoft – og indirekte også den amerikanske nationalbank, Federal Reserve.

Ønsker ikke at stille op til interview

Danmarks Nationalbank ønsker ikke at stille op til interview, men skriver i en mail til Version2:

»SolarWinds-angrebet ramte også den finansielle infrastruktur i Danmark. De relevante systemer blev inddæmmet og analyseret, så snart kompromitteringen af SolarWinds Orion blev kendt. Der blev grebet konsekvent og hurtigt ind på en tilfredsstillende måde, og ifølge de udførte analyser var der ingen tegn på, at angrebet har haft reelle konsekvenser.«

Version2 har fået delvis indsigt i opklaringsarbejdet efter Nationalbanken blev bekendt med kompromitteringen. Flere bekymrede forskere og it-sikkerhedseksperter stiller spørgsmålstegn ved Nationalbankens håndtering af sagen i Version2's mere tekniske, opfølgende artikel, der udkommer i eftermiddag.