STYRELSEN FOR
PATIENTSIKKERHED

Udvikling og Systemer

Dato 01-09-2016
Sagsnr. 16/9992
Sagsbeh. Jph

Redegørelse for brud på sikkerheden i.f.m. sagkyndigs behandling af klagesager

Ved behandling af klager, sendes sager med sagsoplysninger til sagkyndige konsulenter til vurdering. Dette sker inden for et lukket Citrix miljø. Den sagkyndige skriver sin vurdering i samme miljø og sender denne tilbage til styrelsen.

En sagkyndig har imidlertid ved vurdering af 4 sager sendt sager ud af det lukkede Citrix miljø.

Konkret er der fra den 20. august 2016 og frem til og med d.d. konstateret følgende:

Lørdag d. 20. august:

- Den sagkyndige konstaterer, at han har et problem med at åbne de PDF-filer indeholdende det samlede sagsmateriale han har fået tilsendt og skal behandle inden for det sikre Citrix-miljø. Han sender en mail herom til supporten, som imidlertid ikke er åben i weekenden.
- I fraværet af en hurtig løsning på sikker åbning af filerne vælger den sagkyndige at sende materialet til sin private [redacted] konto. Dette er den sagkyndige bekendt med er et sikkerhedsbrud.
- Kort efter at den sagkyndige har sendt de fire mails med de 4 sager, konstaterer han, at han ikke modtager noget på sin [redacted] og opdager derefter, at han i stedet for "[redacted]" har skrevet "[redacted]".
- Den sagkyndige skriver igen til supporten, at han har begået et alvorligt sikkerhedsbrud, da han ikke modtager en fejlmeddelelse og de 4 mails derfor må antages at være modtaget af en forkert modtager. Han angiver endvidere, at en ven har oplyst at det domæne han har sendt til, formentlig er sat op til at modtage al post uanset hvad der står foran @[redacted].

Søndag d. 21. august:

- Den sagkyndiges mails til supporten læses af en supporter, som straks kontakter ham. Sammen konstaterer de, at det er et sikkerhedsbrud og at det antageligt er et firma der har modtaget de 4 mails.
- Supporteren kontakter IT-chefen og da det er kendt, at Google og de øvrige store spillere på markedet i årevis har kæmpet mod den form for såkaldte "typo-domæner[1]" er den umiddelbare antagelse at modtageren er et lødigt firma, som dagen efter vil kunne kontaktes mhp. at sikre at data slettes.
- STPS's medlem af det koncernfælles informationssikkerhedsudvalg, VD Steffen Egesborg Hansen (SEH), orienteres om sagen, og det aftales at vende tilbage til den mandag.

Mandag d. 22. august:

- Sikkerhedsbruddet rapporteres til den koncernfælles informationssikkerheds-enhed i SDS.
- Registranten/ejeren af domænet forsøges forgæves kontaktet per telefon. Derefter undersøges domænet nærmere, og det konstateres, at der er risiko for, at det er et domæne, som bevidst er etableret med det formål at høste data, der ved en fejl måtte blive sendt til domænet.

Tirsdag d. 23. august:

- Interne undersøgelser viser, at det med stor sikkerhed er et såkaldt "malicious" domæne, idet webtrafik eksempelvis sender brugeren videre til websider med malware.
- Den sagkyndige kontaktes af IT-chefen og forlægges, at sikkerhedsbruddet er en realitet og indeholder to elementer: Selve udsendelsen til et eksternt domæne og at det konkrete domæne må anses for "malicious". Den sagkyndige viser, at han er klar over sagens alvor.
- Sagen drøftes på et møde og der besluttes en opgaveliste og –fordeling mellem SEH, cheferne i styrelsens klagecenter og IT chefen..
- Den sagkyndiges behandling af STPS sager sættes i bero og de 4 sager blev trukket tilbage fra den sagkyndige.. Dette kommunikeres til den sagkyndige af en chef i klagecentret.
- Det besluttes omgående at spærre de sagkyndiges mailsystems mulighed for at sende til andre domæner end sst.dk, patientombuddet.dk samt stps.dk, hvorved en præcis gentagelse af sikkerhedsbruddet er umuliggjort.

[1] Domænenavne der udnytter typiske slåfejl til at tiltrække trafik.

- Det besluttes at skærpe vejledninger og udarbejde en awareness-kampagne over for såvel de sagkyndige som de interne medarbejdere.
- Det vurderes, at der endnu ikke er tilstrækkelig viden til en anmeldelse til Datatilsynet eller til orientering af personerne hvis data er omfattet af sikkerhedsbruddet.
- SDS anmodes om bistand til efterforskning, men SDS havde ikke mulighed for at bistå.
- Det private sikkerhedsfirma CSIS kontaktes mhp. på hjælp til teknisk efterforskning og undersøgelse/vurdering af mulighederne for at gøre noget for at sikre de data, der er sendt til uvedkommende adresse. Tirsdag aften indgås aftale med CSIS og de gives de nødvendige (ikke-følsomme) oplysninger til deres opgaveløsning.

Fredag d. 26. august:
- Alle vejledninger gennemgås og ordlyden ensrettes og præciseres i alle vejledninger.
- Plan aftalt for sikring, af at tekniske, forretningsmæssige og sikkerhedsmæssige vejledninger samlet dækker det nødvendige og at disse sikres kendt af alle også efter justeringer eller udgivelse af nye versioner.

Søndag d. 28. august:
- Rapporten fra CSIS modtages kl. 22.29.

Mandag d. 29. august:
- CSIS rapporten og den interne opgaveliste i forbindelse med sikkerhedsbruddet behandles på et møde.
- Konklusionen er at data er kompromitteret og ikke kan sikres. Der gives desuden en række anbefalinger, heraf er den vigtigste tekniske anbefaling allerede implementeret. De øvrige anbefalinger undersøges nærmere, idet der skal ske en afklaring af, om og hvordan de kan implementeres i STPS konkrete miljø.
- CSIS anbefaling om id-tyveriforsikring til de berørte og spørgsmålet om rådgivning til de berørte borgere tilsendes SDS, idet disse ses som områder, der skal tages stilling til centralt.
- Klagecentret oplyser, at der ved gennemgang af det kompromitterede materiale er fundet personfølsomme data på syv personer.
- Det besluttedes, at der midt i ugen sker mundtlig orientering af de berørte borgere. Den mundtlige følges af en skriftlig redegørelse. Afklaringen af rådgivningsmuligheden og spørgsmålet om tegning af id-forsikring for borgerne søges afklaret, inden disse kontaktes.
- Det besluttedes at udarbejde en foreløbig anmeldelse sikkerhedsbruddet til Datatilsynet, som derefter kan følges af en opfølgende og mere omfattende redegørelse af, hvad der er sket og hvilke aktioner der er taget for at hindre gentagelse.
- Det besluttedes at den normale praksis med at minimere konsekvenserne at et datatab ved at søge data slettet gennem kontakt med dem, der uberettiget er kommet i besiddelse af dem, ikke kan finde anvendelse i denne sag. Årsagen er, at modtageren uden for enhver tvivl må antages at være kriminel, hvorfor enhver yderligere kontakt medfører en blottelse for angreb på vores mailservere, IP-adresser mv. og samtidig bringer en uheldig opmærksomhed på deres adgang til data de eventuelt ikke kender værdien af. Eksempelvis må det forventes, at et primært fokus hos kriminelle er på kreditkortdata og at det ikke er sikkert, at deres systemer registrerer danske CPR-numre indeholdt i de vedhæftede PDF-filer. Forsøg på kontakt vil derfor på uheldig vis henlede deres opmærksomhed på de data de allerede har modtaget fra STPS, men uden at der kan forventes en positiv sikkerhedsmæssig effekt af det, snarere tværtimod
- Øvrige anbefalinger fra CSIS undersøges og vurderes.

Onsdag d. 31. august
- Spørgsmål omkring forsikring, erstatning og rådgivning af de berørte borgere er i samarbejde med SDS undersøgt nærmere. SDS anbefaler en række "spørgsmål/svar", som STPS sikrer bliver medtaget i orienteringen af de berørte patienter, idet en mindre del bruges som svarberedskab på evt. opfølgende spørgsmål fra dem. Kammeradvokaten inddrages af SDS i relation til spørgsmålene om erstatningsansvar. Svar herfra ventes senest mandag d. 5. september..

- De mest nødvendige faktuelle oplysninger for en orientering af de berørte borgere er d.d. nedfældet, og der er udarbejdet et internt beredskab til relevante chefer og et talepapir til brug for telefonsamtalerne med borgerne.
- Departementet udbeder sig oplysninger om uddybelse af, hvilke foranstaltninger, der er truffet over for de berørte borgere, herunder at de er informereret. Nærværende redegørelse opdateres med de aktuelle informationer og den opdaterede version, en aktuel status samt talesedlen til brug for orienteringen af patienterne tilsendes departementet pr. mail.
- Det besluttes, at der ringes til de berørte patienter fra kl. 08.30 torsdag, hvorefter der gives besked til departementet, når alle er kontaktet.
- Sagen anmeldes til Datatilsynet torsdag. d. 1. september 2016.
- Nye oplysninger fra klagecentret betyder, at antallet af berørte patienter skal rettes til 7.

Sagen har fuld ledelsesmæssig fokus, og nærværende redegørelse samt en mere detaljeret log ajourføres i takt med at de næste aktioner tages.