RIGSPOLITIET

POLITI

24. august 2015 RIGSPOLITIET
J.nr. 2015-4252-202
Sagsbehandler: MSB005 Koncern IT

Datatilsynet
Borgergade 28, 5.
1300 København K

Redegørelse i forbindelse med Datatilsynets udtalelse af 31.07 2015

Dette notat er udarbejdet som svar på Datatilsynets udtalelse af 31. juli 2015.

Rigspolitiet skal indledningsvis bekiage, at Datatilsynet har haft oplevelsen af, at Rigspolitiet ikke har svaret tilstrækkeligt præcist eller hurtigt nok. Rigspolitiet tager kritikken fra Datatilsynet meget alvorligt og vil fremover sikre, at Datatilsynet rettidigt får præcise svar på deres spørgsmål.

Rigspolitiet har siden sikkerhedshændelsen iværksat en række sikkerhedsmæssige tiltag, dels foranlediget af den konkrete hændelse, dels foranlediget af anbefalinger fra Politiets Efterretningstjeneste (PET), Center for Cybersikkerhed (CfCS) og PWC.

Rigspolitiet vil i det følgende redegøre for:

1. Hvilke tekniske og processuelle tiltag Rigspolitiet har gennemført siden sikkerhedshændelsen i 2012 i forhold til adskillelse fra fx internettet – særligt med hensyn til isolation, adskillelse samt forsvar i dybden
2. Hvem der traf beslutning om, at webserveren skulle kunne tilgås fra internettet af brugere uden for CSC's lokalitet
3. Hvilke informationssystemer der blev driftet i Rigspolitiets logiske partitioner (LPARs) i Rigspolitiets mainframemiljø hos CSC
4. Hvorvidt Rigspolitiet har overvejet – eller vil overveje – at flytte informationssystemer, som Rigspolitiet er dataansvarlig for, ud af det omhandlede mainframemiljø

Ad 1.: Hvilke tekniske og processuelle tiltag Rigspolitiet har gennemført siden sikkerhedshændelsen i 2012 i forhold til adskillelse fra fx internettet – særligt med hensyn til isolation, adskillelse samt forsvar i dybden
Rigspolitiet har siden sikkerhedshændelsen iværksat en række tiltag med henblik på at højne sikkerheden og reducere sandsynligheden for et lignende angreb. Disse tiltag er iværksat på baggrund af de analyser og anbefalinger, der er udarbejdet af særligt PET og CfCS.

Nedenfor gennemgås forløbet efter sikkerhedshændelsen kronologisk. Gennemgangen efterfølges af en skematisk opsætning af de udførte tiltag vedrørende isolation, adskillelse og/eller forsvar i dybden.

I umiddelbar forlængelse af at Rigspolitiet konstaterede, at der havde været en sikkerhedshændelse i politiets systemer hos CSC, blev der iværksat en række tiltag med henblik på at sikre mainframeinstallationen mod lignende angreb. Disse tiltag omhandlede primært:

- Patchning af operativsystem og software
- Nedlukning af den kompromitterede webserver
- Indførelse af yderligere monitorering og logning
- Integritetskontrol af installationen
- Passwordskift på privilegerede brugerkonti

Såvel Rigspolitiet, PET som CfCS fremkom kort tid efter med rapporter vedrørende hændelsen, og CSC fik med ekstern bistand udarbejdet en rapport om hændelsesforløbet[1]. Som direkte konsekvens af rapporterne blev følgende tiltag iværksat:

- Gennemgang af mainframeinstallationen og kontrolleret nedlukning af alle webservere
- Begrænsning af indgående trafik gennem firewall
- Konfiguration af firewall indstillinger
- Begrænsninger i privilegerede rettigheder
- Sikring mod ændringer af systemfiler

Rigspolitiet, PET og CfCS nedsatte en arbejdsgruppe, der i samarbejde med en uafhængig it-revisor foretog en gennemgang og analyse af det fællesoffentlige mainframemiljø i samarbejde med CSC. Dette arbejde udmøntede sig i en række rapporter og udtalelser, som i vidt omfang er sammenfattet i *Rapport om sikkerhedsbrud hos CSC* (PET&CfCS august 2014), *Anbefalinger til styrkelse af sikkerheden i statens outsourcede it-drift* (CfCS august 2014), *Sikkerhedsanbefaling "Styrkelse af informationssikkerheden i mainframeinstallationer"* (CfCS januar 2015) samt i en revisionsrapport, der kom primo 2014.

Simultant med arbejdsgruppens analyse blev der iværksat en række af de tiltag, der blev behandlet af arbejdsgruppen. Det drejede sig særligt om:

- Udskiftning af slutbrugerpassword
- Sletning af brugerkonti
- Begrænsning af udgående trafik gennem firewall

[1] Indledende anbefalinger vedrørende politiets mainframesystem (PET, til tjenestebrug juli 2013), Indledende rapport om hackerangrebet på politiets IT-Systemer hos CSC (PET, fortrolig Juli 2013), Foreløbig rapport Sikkerhedsbrud hos CSC (CfCS, til tjenestebrug juli 2013).

- Differentiering af systembrugerrettigheder i forskellige forvaltnings- og driftsroller
- Integritetskontrol på systemfiler
- Udskiftning af SSH nøgler og SSL certifikater fra før hændelsen
- Flytning af FTP fra mainframe til separat server
- Verifikation af miljøopsætning i forhold til leverandørstandarder

Det er Rigspolitiets opfattelse, at de gennemførte tiltag adresserede de kritiske tekniske forhold, der er blevet identificeret i de nævnte rapporter, og at sikkerheden på den baggrund er højnet betydeligt. Det er således Rigspolitiets opfattelse, at der i dag er den fornødne adskillelse mellem internetadgange og Rigspolitiets informationssystemer.

Rigspolitiet har herudover iværksat et forhandlingsforløb med CSC, som bl.a. skal sikre en styrkelse af de nødvendige processer og styringsredskaber for it-sikkerhed, og at disse tydeliggøres i kontraktsgrundlaget.

De til dato udførte tiltag kan skematisk kategoriseres på følgende måde:

Isolation:
- Nedlukning af den kompromitterede webserver
- Gennemgang af mainframeinstallationen og kontrolleret nedlukning af alle webservere
- Begrænsning af trafik gennem firewall
- Flytning af FTP fra mainframe til separat server

Adskillelse:
- Passwordskift på privilegerede brugerkonti
- Begrænsninger i privilegerede rettigheder
- Differentiering af systembrugerrettigheder i forskellige forvaltnings- og driftsroller
- Monitorering af systemkontibrug
- Gennemgang, begrænsning af og kontrol med privilegerede rettigheder

Forsvar i dybden:
- Patchning af operativsystem og software
- Indførelse af yderligere monitorering og logning
- Integritetskontrol af installationen
- Sikring mod ændringer af systemfiler
- Udskiftning af slutbrugerpassword
- Konfiguration af firewall indstillinger
- Sletning af brugerkonti
- Begrænsning af udgående trafik gennem firewall
- Integritetskontrol på systemfiler
- Udskiftning af SSH nøgler og SSL certifikater fra før hændelsen
- Periodisk sikkerhedskontrol

- Oprydning i udfasede systemer og komponenter i miljøet
- Logkontroller og opbevaring af logmateriale
- Fast og fulgt procedure for ændringshåndtering
- Opdateringsproces ved særligt vigtige fejlrettelser
- Monitorering af trafik og systemadgange
- Gennemgang af processer
- Stram styring af netværkstrafik

I *Rapport om sikkerhedsbrud hos CSC* (PET&CfCS august 2014) er en del af ovennævnte tiltag prioriteret på følgende måde:

- Prioritet 1: Meget betydelige svagheder
- Prioritet 2: Betydelige svagheder

Af disse var alle prioritet 1 og de fleste prioritet 2 tiltag gennemført ultimo 2013, og CSC har bekræftet, at alle tiltag var fuldt gennemført i 2014.

Ad 2.: Hvem der traf beslutning om, at webserveren skulle kunne tilgås fra internettet af brugere uden for CSC's lokalitet

Mainframemiljøet hos CSC, som Rigspolitiet og andre myndigheder gør brug af, afvikler en række applikationer, hvoraf de ældste kan dateres til 1970'erne. Den teknologiske udvikling, der har præget it-industrien, herunder den stigende anvendelse af internettet fra 1990'erne, har løbende påvirket udviklingen af mainframemiljøet.

Rigspolitiet har ved sin behandling af sagen ikke fundet konkret information om, hvem der traf beslutning om etablering af den pågældende webserver. Det fremgår af de svar, som CSC har fremsendt i forbindelse med Datatilsynets undersøgelse, at webserveren er etableret for en anden statslig kunde. Det er sket på et tidspunkt, hvor der ikke har været anvendt de standardiserede processer for etablering og kontrol af leverandørservices, som anvendes i dag.

Rigspolitiet har overfor CSC understreget, at Rigspolitiet fremadrettet skal inddrages, når CSC foretager ændringer, der kan påvirke Rigspolitiets it-miljø hos CSC.

Ad 3.: Hvilke informationssystemer der blev driftet i Rigspolitiets logiske partitioner (LPARs) i Rigspolitiets mainframemiljø hos CSC

Rigspolitiets LPAR´s er et redundant par. Den ene er placeret i det primære driftscenter hos CSC, mens den anden er placeret i det sekundære driftscenter på en anden lokation hos CSC.

Denne opsætning er implementeret for at sikre, at den sekundære LPAR kan overtage den aktive driftsrolle, hvis den primære LPAR går ned. De installerede informationssystemer på de to LPAR's er derfor identiske.

De to LPAR's anvender i udgangspunktet det samme storagesystem på den primære lokation, hvor der findes en aktiv kopi (et spejl) af pågældende informationssystemer på den sekundære lokation i det tilfælde, at både den primære mainframe og storagesystemet fejler samtidigt.

Følgende systemer blev på hændelsestidspunktet afviklet på Rigspolitiets LPAR's:

- Anmeldelsesregistret (ANM)
- Det Centrale Cykelregister (KOS)
- Efterlyste Køretøjer (EK)
- Index 1 (IX1)
- Det Centrale Kørekortregister (CRK)
- Kriminalregistret (KR)
- Centralregistret for Motorkøretøjer (CRM)
- Parkeringsafgifter (CRP)
- Det Centrale Pasregister (PAS)
- Schengen Information System (SIS)
- Det Centrale Katastroferegister (KAT)
- Rettighedsregistret (RET)

Ad 4.: Hvorvidt Rigspolitiet har overvejet – eller vil overveje – at flytte informationssystemer, som Rigspolitiet er dataansvarlig for, ud af det omhandlede mainframemiljø

Det er Rigspolitiets vurdering, at den tekniske arkitektur for det omhandlede mainframemiljø ikke i sig selv er en hindring for implementering af anerkendte principper for sikkerhed – en vurdering som også fremgår af sikkerhedsanbefalingen fra CfCS vedrørende styrkelse af informationssikkerheden i mainframeinstallationer (Januar 2015).

Konkret har LPAR-arkitekturen på mainframemiljøet opnået en sikkerhedscertificering på sikkerhedsniveau (EAL5+). Rigspolitiet har derfor ikke på baggrund af det konkrete sikkerhedsbrud og de gennemførte sikkerhedstiltag fundet det nødvendigt at adskille systemerne fysisk.

Rigspolitiet vil fremover definere sikkerhedsniveauet og kontrollere efterlevelsen deraf i henhold til anbefalinger fra bl.a. CfCS, PET samt den gældende sikkerhedsstandard (ISO27001). Rigspolitiet vil samtidig følge den teknologiske udvikling med henblik på løbende at iværksætte relevante forebyggende tiltag i forhold til det aktuelle risikobillede.

Afslutningsvis kan Rigspolitiet oplyse, at Rigspolitiet løbende overvejer mulighederne for at flytte hele eller dele af systemerne væk fra mainframemiljøet med henblik på at realisere forretnings- og driftsmæssige gevinster. Dette sker som et led i Rigspolitiets generelle overvejelser om modernisering af systemerne og er ikke direkte afledt af sikkerhedsmæssige årsager.

Med venlig hilsen

John Vestergaard

Kst. IT direktør