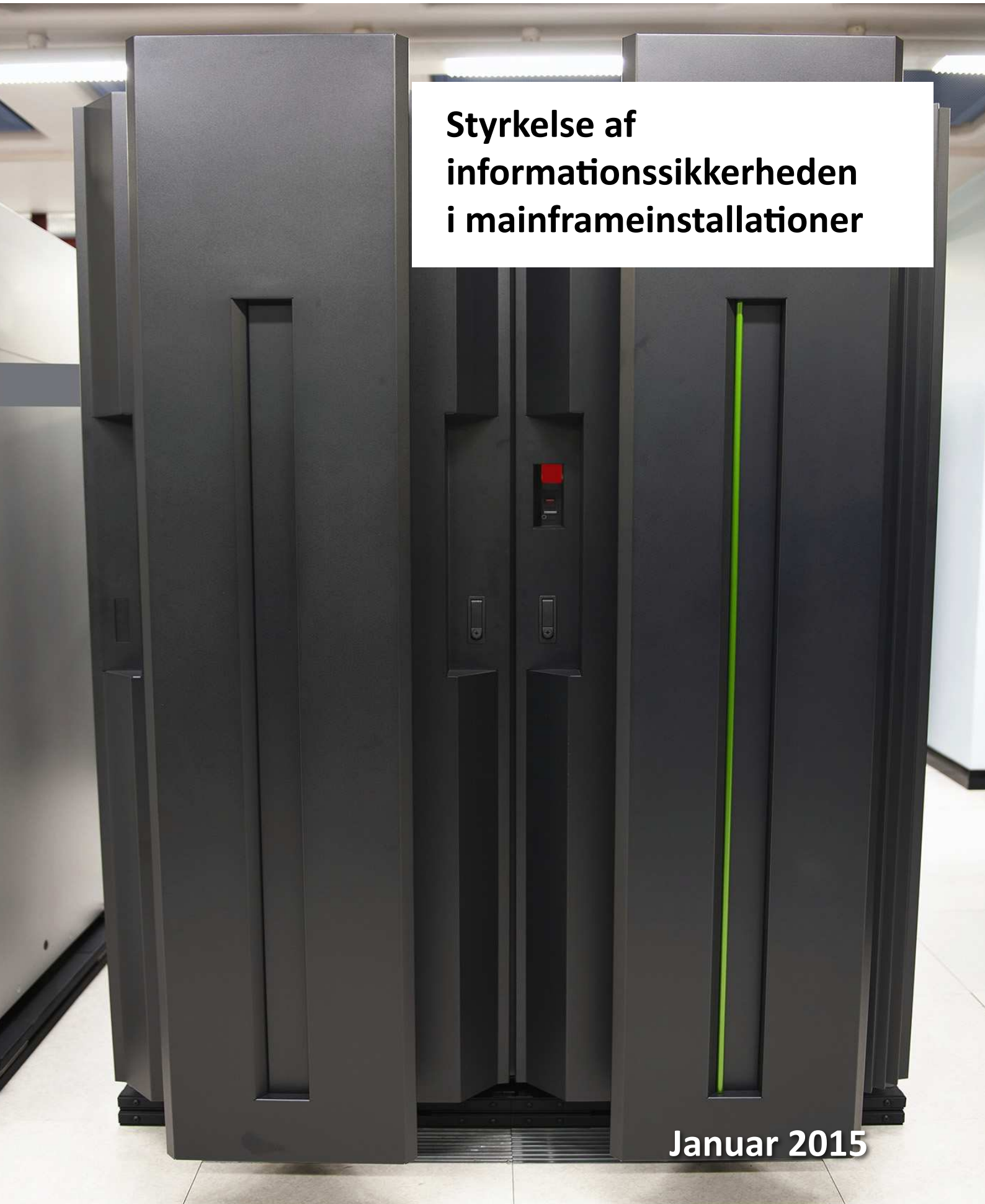
Sikkerhedsanbefaling

CENTER FOR CYBERSIKKERHED



Styrkelse af informationssikkerheden i mainframeinstallationer

Januar 2015

Indledning

Inden for de seneste år har flere mainframeinstallationer været udsat for hackerangreb. I Sverige og Danmark har hackerangreb med kompromittering til følge ramt mainframeinstallationer hos en række it-infrastrukturudbydere. Det har understreget behovet for at øge fokus på informationssikkerheden i mainframeinstallationer, da mange samfundsvigtige funktioner bliver udført ved hjælp af applikationer og systemer på mainframeinstallationer.

Det er nødvendigt, at private virksomheder og offentlige myndigheder sørger for at understøtte et højt niveau for informationssikkerhed på mainframesystemer. Og det er afgørende, at deres arbejde med informationssikkerhed tager udgangspunkt i en klar forståelse af risikobilledet og af, hvordan konkrete trusler kan imødegås.

Sikkerhedsanbefalingen henvender sig primært til de it-sikkerhedstekniske medarbejdere, der til dagligt håndterer mainframeinstallationer i deres organisation, men den kan også med fordel læses af organisationernes ledelse. Erfaringen er således, at god informationssikkerhed forudsætter forankring hos topledelsen.

I sikkerhedsanbefalingen beskriver Center for Cybersikkerhed en række konkrete tiltag til hvordan myndigheder og virksomheder kan mindske risikoen for hackerangreb, der anvender de samme fremgangsmåder, som tidligere er set ved angreb mod mainframeinstallationer i Danmark og Sverige, herunder det meget omtalte hackerangreb mod CSC.

Center for Cybersikkerhed fokuserer i sikkerhedsanbefalingen på at bidrage til at sætte mainframeejere og -administratorer i stand til at identificere sårbarheder og implementere passende sikkerhedstiltag, så hackerangreb i højere grad bliver imødegået og konsekvenserne mindsket.

Også kunder til mainframeydelser kan med fordel læse sikkerhedsanbefalingen. Kunderne kan med sikkerhedsanbefalingen i hånden indlede dialog med deres leverandør om passende sikringstiltag. Der vil typisk være behov for, at der bliver udarbejdet tillæg til de eksisterende kontrakter, drifts- og samarbejdsaftaler.

Center for Cybersikkerheds sikkerhedsanbefaling koncentrerer sig om interne forhold i mainframen samt forebyggelse af hackerangreb fra internettet. Øvrige aspekter af arbejdet med informationssikkerhed, som f.eks. risikovurdering, opbygning af robust it-arkitektur og ledelsesinddragelse i øvrigt, bliver ikke berørt specifikt. Også i informationssikkerhedsarbejde med mainframeinstallationer, der ikke er koblet til internettet, vil en række af anbefalingerne være relevante.

Center for Cybersikkerhed og Digitaliseringsstyrelsen har udgivet et sæt overordnede sikkerhedsanbefalinger, herunder til ledelsesinddragelse og kontraktstyring, i rapporten ”Anbefalinger til styrkelse af sikkerheden i statens outsourcede it-drift”, som kan findes på cfcs.dk.

Beskrivelse af mainframeinstallationer

Mainframeinstallationer er computere med stor regnekraft og kapacitet til mange samtidige transaktioner. Deres regnekraft, lagerkapacitet m.m. deles af mange brugere.

Adgangen til data og systemer på mainframeinstallationer kontrolleres med et tilvalgt system for sikkerhedsadministration. Det drejer sig som oftest om Ressource Access Control Facility (RACF) fra IBM eller Computer Associates' Access Control Facility (ACF2).

Systemet for sikkerhedsadministration er typisk en database, der indeholder alle oplysninger om brugernavne, passwords (krypteret), beskrivelse af data og andre systemressourcer samt de enkelte brugeres og systemers rettigheder til samme.

Flere af de mainframeinstallationer, som har været udsat angreb, har alle haft hardware fra IBM med operativsystemet z/OS og adgangskontrol via RACF. Denne sammensætning er den mest udbredte installationstype blandt mainframes i Danmark.

Kendte angrebsmetoder mod mainframeinstallationer

Dette afsnit omhandler de teknikker, som bl.a. blev anvendt ved hackerangrebet mod CSC til at omgå RACF. De udgør grundlaget for beskrivelsen af de modforanstaltninger, som de it-sikkerhedsansvarlige for landets mainframeinstallationer bør overveje.

Den væsentligste årsag til, at det lykkedes for hackere at opnå adgang til data på mainframes, er at de kunne udnytte den såkaldte Authorized Program Facility autorisation (APF-autorisation[1]).

Angrebene er udført ved, at der uopdaget er blevet anvendt uautoriserede APF-programmer i styresystemet USS/Unix, hvorfra der er udstedt TSO-kommandoer (time sharing option)[2] mod z/OS ved brug af en hacket USS-systembruger. Risikoen for misbrug er tilsvarende stor, hvis det er muligt at installere uautoriserede APF-programmer direkte i z/OS. Det skyldes, at APF-programmer giver det udførende program autorisation som en del af operativsystemet med stort set ubegrænsede beføjelser

Ved at udnytte APF-autorisationen har det været muligt at eskalere niveauet af systemrettigheder for den hackede systembruger til et niveau, der normalt kun tildeles operativsystemet selv. Med de eskalerede rettigheder har det været muligt at omgå RACF-adgangskontrollen og opnå adgang til alle data på de berørte z/OS-platforme.

Hackerne har dermed haft mulighed for en omfattende kompromittering af fortroligheden og har haft mulighed for at forårsage nedbrud, slette eller forvanske data, som det ofte ville være særdeles vanskeligt at genskabe/genindsamle.

De ændrede brugerrettigheder har kun været gældende for den aktive (kørende) brugersession, hvorfor der ikke har været efterladt spor efter ændringerne, hverken i

[1] APF-autorisation giver det udførende program autorisation som en del af operativsystemet med stort set ubegrænsede beføjelser.

[2] TSO betyder, at mange personer kan få adgang til et styresystem samtidigt. Den enkelte er dog uvidende om, at andre også har adgang til operativsystemet på samme tid. For en TSO-bruger ser det altså ud som om, at vedkommende er den eneste bruger på systemet. TSO anvendes primært af mainframe-systemadministratorer og -programmører.

RACF-databasen eller SMF-loggen (Service Management Facility på z/OS). Da der ikke har været nogen umiddelbar indikation af den uautoriserede indtrængen i øvrigt, har angrebene kunnet foregå uopdaget over længere perioder.

Anbefalinger

Det er Center for Cybersikkerheds erfaring, at det blandt mange mainframeejere og -administratorer har været den fremherskende opfattelse, at mainframeinstallationernes tekniske kompleksitet i sig selv udgjorde en beskyttelse mod angreb. De kendte angreb mod mainframeinstallationer har imidlertid vist, at angribere har tilstrækkelig teknisk indsigt og vilje til at angribe mainframesystemer. En tommelfingerregel i vurderingen af, om informationssikkerhedsniveauet er passende, er at det skal være på et niveau, der vil forhindre uautoriseret adgang fra den mest erfarne systemprogrammør. Mainframeejere og -administratorer kan altså ikke forlade sig på den tekniske kompleksitet som en sikkerhedsfaktor.

Center for Cybersikkerhed ønsker også at understrege, at det er afgørende, at ikke blot mainframeejere og -administratorer, men også kunder er bevidste om de mange informationssikkerhedsaspekter, der knytter sig til mainframeinstallationer. Derfor giver Center for Cybersikkerhed en række anbefalinger, som mainframeejere, leverandører af mainframetjenester samt mainframekunder bør kende.

Der er ikke tale om forslag til en sikkerheds- og funktionalitetsløsning, der berører samtlige de informationssikkerhedsaspekter, som knytter sig til mainframeinstallationer, men om en række konkrete anbefalinger, der vil være til gavn for mange mainframeejere, leverandører af mainframetjenester samt mainframekunder

Center for Cybersikkerhed anbefaler:

– At mainframeejerne nøje gennemgår deres APF-sikkerhedsopsætning. Der bør kun benyttes godkendte APF-programmer, og opdateringsadgang til APF-biblioteker[3] skal styres restriktivt.

– At mainframeejerne sikrer og fastholder en ufravigelig change-procedure for alle elementer af z/OS-operativsystemer.

– At mainframeejerne begrænser adgangen til at ændre i APF-opsætningen. Det kan bl.a. gøres ved kun at give adgang i forbindelse med godkendt change, og kun så længe ændringen gør det nødvendigt.

– At mainframeejerne sikrer løbende overvågning af ændringer (eller forsøg på ændringer) i z/OS-operativsystemet, med henblik på at afdække svagheder i changeproceduren.

– At mainframeejerne sikrer kontrol af og opfølgning på operatør- og RACF-kommandoer, der kan ændre opsætning af APF, SMF etc. (”SETPROG”, ”SET PROG” m.fl.).

– At mainframeejerne sikrer, at der sker daglig opfølgning på ændringer i specielle autorisationer, der dækker styringsniveauet over RACF. Det vil sige adgange, der er givet i kraft af brugerens særstilling (sikkerhedsadministrator, databaseadministrator, systemoperatør etc.), i modsætning til adgange, som er givet via en bevilling i RACF.

[3] For USS/OMVS-adgangskontrol med opdatering af APF-bit (READ adgang til RACF FACILITY class, profil ”BPX.FILEATTR.APF”).

– At mainframeejerne lukker al unødvendig adgang til vitale operativsystemdata, herunder operativsystemets sikkerhedsopsætning, sikkerhedssystemdata (f.eks. RACF-databasen) og eventuelle kopier af disse data (f.eks. backup).

– At mainframeejerne supplerer ovennævnte tiltag med en løbende vurdering af den generelle sikkerhedsopsætning i z/OS.

– At mainframeejerne sikrer housekeeping i operativsystemet. Det vil bl.a. sige oprydning i udfasede komponenter, overflødige system-users etc.

– At mainframeejerne holder sig opdaterede med udviklingen i kendte trusler mod mainframesystemer herunder gennem IBM's "Security Bulletins".

– At mainframeejerne løbende bør vurdere relevansen af samtlige de adgange, som er blevet givet "udenom" sikkerhedssystemet. Det gælder f.eks. adgang som RACF attribute PRIVILEDGED, -TRUSTED, - OPERATIONS, DB2 SYSADM og alle lignende adgangsmekanismer, der giver adgang på et overordnet niveau.

– At mainframeejerne altid har opdateret de centrale web-servere sikkerhedsmæssigt og sammenholdt sikkerhedsforholdene med mulige intelligente netværkskomponenter som eksempelvis IPS/IDS-løsninger. Det samme gør sig gældende for alle andre Internetvendte applikationsløsninger og services på mainframeinstallationer.

– At mainframeejerene overvejer nedlukning og eller flytning af primære internet vendte web-servere og internetvendte applikationsløsninger under både USS og z/OS til rene og isolerede platforme, eksempelvis en decentral Linux-platform.

– At mainframekunder går i dialog med deres leverandør om sikkerhedsniveauet i den købte løsning med henblik på at kunne foretage en risikovurdering, sikre ansvarsfordeling og vurdere behovet for tilkøb af relevante sikkerhedsløsninger. Center for Cybersikkerheds og Digitaliseringsstyrelsens rapport "Anbefalinger til styrkelse af sikkerheden i statens outsourcede it-drift" indeholder nærmere herom. Den kan findes på cfcs.dk

Center for Cybersikkerhed

Center for Cybersikkerhed er statens kompetencecenter på cybersikkerhedsområdet og fokuserer på beskyttelse af samfundsvigtige funktioner mod avancerede cyberangreb. Det sker bl.a. ved, at Center for Cybersikkerhed varsler om cyberangreb, og ved at centeret efter nærmere vurdering bistår angrebne organisationer med at imødegå og afhjælpe cyberangreb.

På Center for Cybersikkerheds hjemmeside, cfcs.dk, er der yderligere information om cybertrusler og cybersikkerhed, herunder trusselsvurderinger, vejledninger samt en årlig risikovurdering.