Transportministeriet

MINISTEREN

Dato 15. januar 2016
J. nr. 2015 - 4766

Frederiksholms Kanal 27 F
1220 København K

Telefon 41 71 27 00

Statsrevisorenes sekretariat
Folketinget
Christiansborg
1240 København K

Ministerredegørelse om beretning nr. 1/2015 til Statsrevisorerne om adgangen til IT-systemer der understøtter samfundsvigtige opgaver.

Statsrevisorerne har fremsendt ovennævnte beretning og har bedt om en redegørelse for de foranstaltninger og overvejelser, som beretningen har givet anledning til.

Revisionen omhandlede seks institutioner, hvoraf Banedanmark indgår i undersøgelsen på Transport- og Bygningsministeriets område. Revisionens resultater er præsenteret i anonymiseret form. De overordnede temaer er styring, logning og kontrol af udvidede administratorrettigheder for henholdsvis betroede it-medarbejdere og for system og –servicekonti.

Rigsrevisionen finder samlet set, at alle institutionerne udsætter sig selv for alvorlige it-sikkerhedsmæssige risici, og ikke i tilstrækkelig grad følger alment kendte anbefalinger for god praksis for at sikre og beskytte adgangen til IT systemer og data, som understøtter samfundsvigtige opgaver.

I forhold til Banedanmark er det indledningsvist vigtigt at være opmærksom på, at der indenfor jernbaneområdet er væsentlig forskel på de administrative og tekniske systemer. De systemer, som den foreliggende revision dækker over, har ikke indflydelse på de sikkerhedsmæssige aspekter i forhold til afviklingen af den daglige togtrafik.

Jernbanedriften består af tekniske og lukkede anlæg, og ingen af de sikkerhedsbærende jernbanesystemer er knyttet til brugeradministrationssystemet Active Directory (AD) der styrer adgangen til IT systemer. En hacker kan i værste tilfælde kun forstyrre jernbanedriften i minimal grad, f. eks. i form af forstyrrelse af højtalerudkald, trafikinformation eller lignende.

Rigsrevisionen anbefaler en række tiltag i forhold til begrænsning af antallet af personer eller konti med udvidede administratorrettigheder, håndtering og kompleksitet af passwords, samt muligheden for at kunne tilgå netværket fra lokale arbejdsstationer i virksomheden.

Banedanmark tager revisionens anbefalinger til efterretning og har begrænset såvel antallet af betroede it-medarbejder med udvidede administratorrettigheder, som antallet af system- og servicekonti med udvidede administratorrettigheder. Endvidere vil Banedanmark tilpasse personlige passwords og systempasswords som anbefalet. Herudover vil Banedanmark sikre, at system- og servicekonti med udvidede brugerrettigheder ikke kan tilgå netværket fra loka-

le arbejdsstationer samt, at passwords udskiftes når betroede medarbejdere fratræder deres stilling.

Rigsrevisionen har endvidere en række anbefalinger i forhold til logning af udvidede administratorrettigheder og overvågning af anomalier. Banedanmark har forud for revisionen igangsat tiltag der skal medvirke til at forbedre opfølgningen på logning af AD aktiviteter bl. a. gennem etablering af logmanagementsystemer. Endvidere er Banedanmark tilknyttet Center for Cybersikkerheds overvågning af al ind- og udgående datatrafik, hvor der scannes for unormale aktiviteter. På baggrund af revisionens anbefalinger, vil Banedanmark igangsætte tiltag, der skal medvirke til yderligere at forbedre de eksisterende rutiner for at opfange anomalier.

Kopi af denne redegørelse er sendt til Rigsrevisionen, rr@rigsrevsionen.dk

Med venlig hilsen

Hans Christian Schmidt