



Rektor

Införande av webbfiler på Karolinska Institutet

KIs regler och riktlinjer, inom bland annat Informationssäkerhet, anger tydligt hur informationsresurser och IT-system får användas. IT-resurser så som Internet är ett arbetsredskap och ska nyttjas som sådant. Internet är idag den största spridningskanalen för skadlig kod och möjliggöraren för angrepp och stöld av informationstillgångar. Genom att införa ett filter skapas möjlighet att kontrollera och stoppa datakommunikationen till och från KI som kan medföra risker för informationsförlust för verksamheten.

Härmed beslutas enligt bilaga att fr.o.m. 2016-10-01 införa användningen av webbfiler vid Karolinska Institutet.

Beslut i detta ärende har fattats av vikarierande rektor Karin Dahlman-Wright i närvaro av universitetsdirektör Per Bengtsson, efter föredragning av IT-direktör Peter Book. Närvarande därutöver var bitr. universitetsdirektör Marie Tell, Medicinska föreningens ordförande Frida Hellström och IT-säkerhetsansvarig Fredrik Wallström.

Karin Dahlman-Wright

Peter Book

Bilaga:

- PM införande av webbfiler
- URL Hantering i KIs nya IPS



Universitetsförvaltningen
ITA
Fredrik Wallström

Införande av webbfiler på Karolinska Institutet

1. Inledning

Historiskt har nyttjandet av Informations- och IT-system inom KI fått ske under stort personligt ansvar, detta har även inkluderat användningen av resurser på Internet via den Internetanslutning som KI tillhandahåller via Sunet.

Internet, e-post och webben är idag de största spridningskanalerna och möjliggörarna av angrepp och spridning av virus och skadlig kod.

Under ett antal år har det funnits regler och riktlinjer inom KI som bland annat beskriver hur nyttjandet av Informations- och IT-system får ske, vilka informationssäkerhetsregler som gäller för KI som myndighet men även de etiska och moraliska skyldigheter alla verksamma inom KI ska efterleva.

ITA ser idag ett stort antal angreppsförsök mot våra IT-resurser och användare. Vi ser utbrott av virus och skadlig kod hos våra användare. Det sker utbrott av s.k. Ransomware, krypteringsvirus som beslagtar KIs information ute bland verksamheten.

Merparten av de användare och datorer som är anslutna till KIs nätverk är idag omanagerade, dvs. användaren är lokal administratör och hanterar sin egen dator själv efter bästa förmåga. Detta innebär att oftast saknas de skyddsfunktioner som krävs så som, uppdaterade och aktuella antivirusprogram, brandväggar, säkerhetsuppdateringar, programvaruuppdateringar och förmågan att säkerställa att ingen obehörig har åtkomst till informationen på datorn. Avsaknaden av dessa komponenter innebär stora risker för verksamheten inom KI. En smittad dator kan med enkelhet sprida smittan vidare till andra IT-resurser inom KI.

2. Införande av webbfiler

KI, som svensk myndighet, behöver ha skyddsfunktioner på plats för att säkerställa att skydd finns mot de risker och hot som en anslutning till Internet innebär. Myndigheten behöver också möjlighet att kontrollera att KIs regler och riktlinjer



inom bl.a. informationssäkerhet efterföljs men även att KIs etiska och moraliska värdegrund efterlevs.

KI inför från oktober 2016 ett webbfilter i KIs IPS-lösning för datakommunikation till och från KIs nätverk. Lösningen kontrollerar och där så behövs, blockerar anslutningsförsök till platser på Internet som bryter mot KIs regler och riktlinjer, som bedöms medföra risker för verksamheten på KI, att platsen inte anses innehålla arbetsrelaterad information eller att informationen bryter mot KIs etiska värdegrund.

För detaljerad information kring den tekniska implementationen, kategorier och hantering se bilaga 2.

Observera att detta är en skyddsfunktion av flera som behövs för att Informations- och IT-säkerheten inom KI ska komma till en acceptabel nivå.

1. Frågor

Frågor kring rektorsbeslutet besvaras av

Fredrik Wallström, fredrik.wallstrom@ki.se tel 524 8000 00