SAMBRUK MEDBORGARPC

Skapande av Säkerhetsövervakning

Maj 2023

MAGENTA aps

INNEHÅLLSFÖRTECKNING

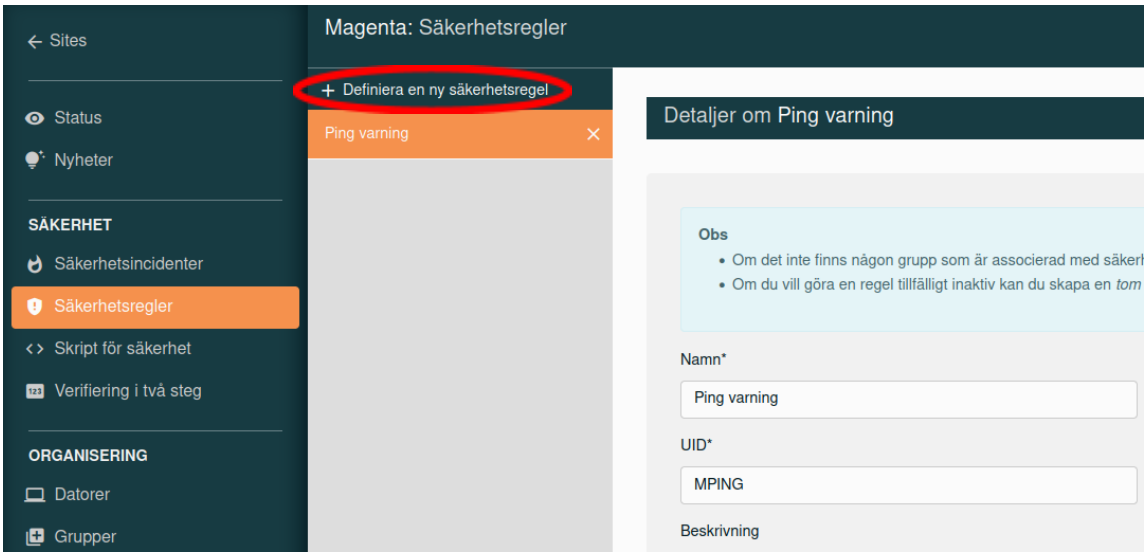
1 INTRODUKTION

Denna guide beskriver hur man ställer in säkerhetsövervakning på Sambruk MedborgarPC's administrationssystem.

Sambruk MedborgarPCs övervakningsmodul är inriktad på att övervaka keyloggers och försök att erhålla administratörsrättigheter på Sambruk MedborgarPC-klienterna. Övervakningsmodulen är utformad för att enkelt övervaka andra säkerhetshändelser än de som nämns.

2 INRÄTTA SÄKERHETSÖVERVAKNING

I Sambruk MedborgarPC's administrationsmodul hittar du i vänstermenyn en grupp menypunkter som handlar om säkerhet. För att ställa in en ny övervakning, klicka på menyn "Säkerhetsregler" och sedan "Definiera en ny säkerhetsregel" (Se Figur 1).



Figur 1

När du har klickat på "Definiera en ny säkerhetsregel" måste du ge regeln ett meningsfullt namn som beskriver vad som övervakas och eventuellt även vilken grupp av Sambruk MedborgarPC'er som övervakas (Se Figur 2).

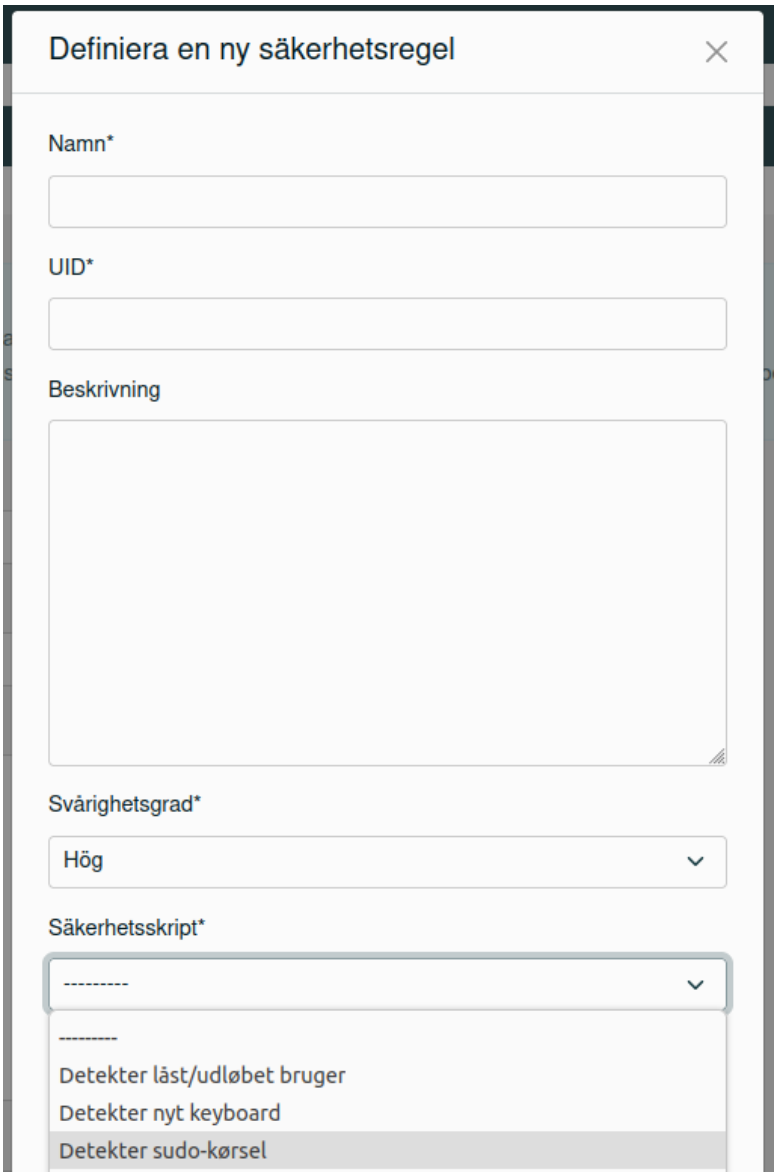
Fältet "UID" är bara viktigt för systemet och ska helst vara unikt. Den får inte innehålla mellanslag eller 'ööå'. Fältet "Beskrivning" är avsett för den eller de som ska hantera säkerhetsregeln när den inträffar. Så här ska det finnas både en detaljerad beskrivning av händelsen och en beskrivning av hur händelsen ska hanteras.

Fältet "Mottagare av e-postvarning" är de personer som ska upprätthålla säkerhetsincidenterna när de inträffar, och som därför måste få ett mejl om incidenten.

Figur 2

När du rullar ner i skapandefönstret ombeds du att bestämma hur allvarlig problemet är. Sambruk MedborgarPC's administrationsmodul har två säkerhetsskript som alltid ska ha svårighetsgraden "Kritisk", och dessa är "Detekter nyt keyboard" och "Detekter sudo-kørsel".

Säkerhetsskriptet "Detekter nyt keyboard" övervakar om USB-tangentbordet på Sambruk MedborgarPC-klienten tas bort och sätts in igen. Detta utgör en säkerhetsrisk för medborgarna, eftersom keyloggers kan placeras mellan Sambruk MedborgarPC och tangentbordet. Säkerhetsskriptet "Detekter sudo-kørsel" håller ett öga på om någon försöker bli administratör på Sambruk MedborgarPC-klienterna.



Figur 3

Det rekommenderas därför starkt att ha båda säkerhetsskripten för att övervaka alla Sambruk MedborgarPC'er som vänder sig till medborgare.

Därför rekommenderas det också att skapa två "Säkerhetsregler". En för "Detekter nyt keyboard" och en för "Detekter sudo-kørsel", som övervakar grupperna av Sambruk MedborgarPC'er som används av medborgare.

Ha det så kul och kontakta oss slutligen om du behöver hjälp att komma vidare. Vid det här laget bör du ha fått tillgång till vårt projektledningssystem, Redmine, där du kan rapportera fel eller ändringsförfrågningar (incidents eller service requests). Om det är större haverier eller fel där flera maskiner är drabbade kan du ringa oss på vårt huvudnummer +45 33 36 96 96 eller skriva till oss på support@magenta.dk

Se mer om support i kontraktet.

MAGENTA aps

adresser
Pilestræde 43, 3. sal
1112 København K

Skt. Johannes Allé 2
DK-8000 Aarhus C

Imaneq 32 A
3900 Nuuk, Grønland

e-post
info@magenta-aps.dk
telefon
(+45) 33 36 96 96