

OS2BORGERPC

Oprettelse af Sikkerhedsovervågning

Oktober 2020

MAGENTA^{aps}

© Copyright 2020

INDHOLDSFORTEGNELSE

| | |
|---|----------|
| 1 Indledning | 3 |
| 2 Opsætning af Sikkerhedsovervågning | 4 |

1 INDLEDNING

Denne guide beskriver, hvordan man opsætter sikkerhedsovervågning på OS2borgerPC's administrationssystem.

OS2borgerPC's overvågningsmodul er målrettet overvågning af keyloggers og forsøg på at opnå administratorrettigheder på OS2borgerPC klienterne. Overvågningsmodulet er designet til nemt at kunne overvåge andre hændelser end de nævnte.

2 OPSÆTNING AF SIKKERHEDSOVERVÅGNING

I OS2borgerPC's administrationsmodul finder du i venstremenuen en gruppe af menupunkter, som omhandler sikkerhed. For at opsætte en ny overvågning skal man klikke på menuen "Regler" og herefter "definér nyt sikkerhedsproblem" (Se Figure 1).

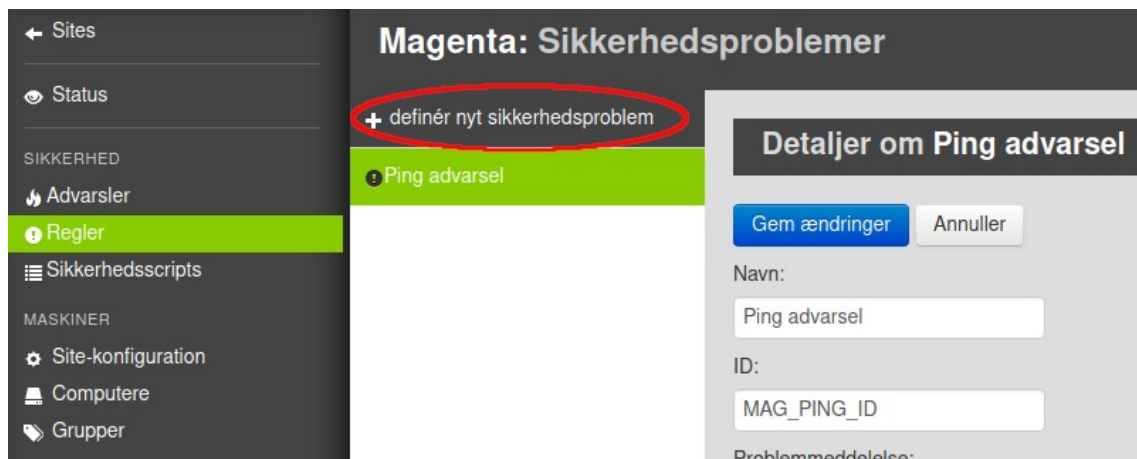


Figure 1

Når man har klikket på "definér nyt sikkerhedsproblem", skal man give problemet et sigende navn, som beskriver, hvad der overvåges og eventuelt også, hvilken gruppe af OS2borgerPC'er der overvåges (Se Figure 2).

Feltet "Id" er kun vigtigt for systemet og skal helst være unikt. Det må ikke indeholde mellemrum eller 'æøå'. Feltet "Problemmeddelelse" er henvendt til den eller de personer, som skal håndtere sikkerhedsproblemet, når det opstår. Så her skal der både være en uddybende beskrivelse af hændelsen og en beskrivelse af, hvordan hændelsen skal håndteres.

Feltet "Modtager(e) af email-advarsel" er de personer, der skal håndhæve sikkerhedsproblemerne, når de sker, og som derfor skal have en email omkring hændelsen.

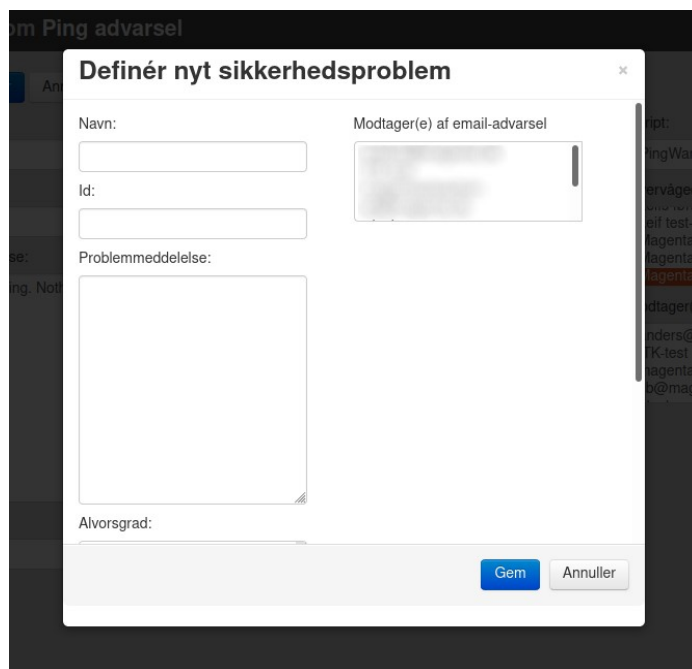


Figure 2

Når man scroller ned i oprettelsesvinduet, bliver man bedt om at tage stilling til alvorlighedsgraden af problemet. OS2borgerPC har to overvågningsscripts, som altid bør have alvorlighedsgraden "Kritisk", og det drejer sig om "Nyt Keyboard Detect" og "Detect sudo event".

Scriptet "Nyt Keyboard Detect" overvåger, om USB-keyboardet på OS2borgerPC klienten bliver taget ud og sat i igen. Dette udgør en sikkerhedsrisiko for borgerne, da keyloggers kan være sat imellem OS2borgerPC'en og tastaturet. Scriptet "Detect sudo event" holder øje med, om nogen forsøger at blive administrator på OS2borgerPC klienterne.

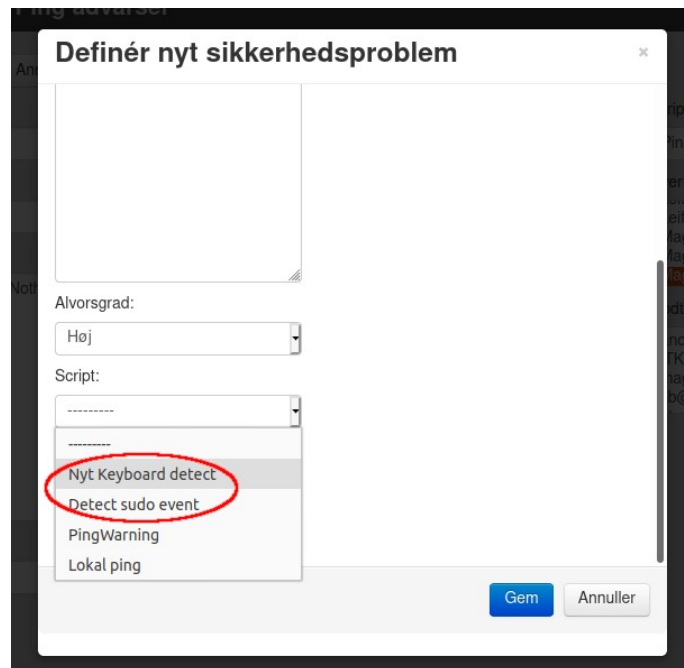


Figure 3

Det anbefales derfor kraftigt at have begge scripts til at overvåge samtlige borgerhenvendte OS2borgerPC'er.

Derfor anbefales det også at oprette to "Sikkerhedsproblemer". Et for "Nyt Keyboard Detect" og et for "Detect sudo event", som overvåger de grupper af OS2borgerPC'er, som bliver brugt af borgerne.

God fornøjelse og kontakt os endelig, hvis I skal have hjælp til at komme videre. På dette tidspunkt burde I have fået adgang til vores projektstyringssystem, Redmine, hvor I kan indrapportere fejl eller ændringsønsker (incidents eller service requests). Hvis der er større nedbrud eller fejl, hvor flere maskiner er påvirket, kan I ringe til os på vores hovednummer +45 33 36 96 96 eller skrive til os på support@magenta.dk

Se mere omkring support i kontrakten.

MAGENTA^{aps}

adresse

Pilestræde 43, 3. sal
1112 København K

email

info@magenta-aps.dk

telefon

(+45) 33 36 96 96