

OS2BORGERPC

Oprettelse af Sikkerhedsovervågning

Oktober 2021

MAGENTA^{aps}

© Copyright 2021

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 sikkerhedshændelser 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 "Sikkerhedsregler" og herefter "definér ny sikkerhedsregel" (Se Figure 1).

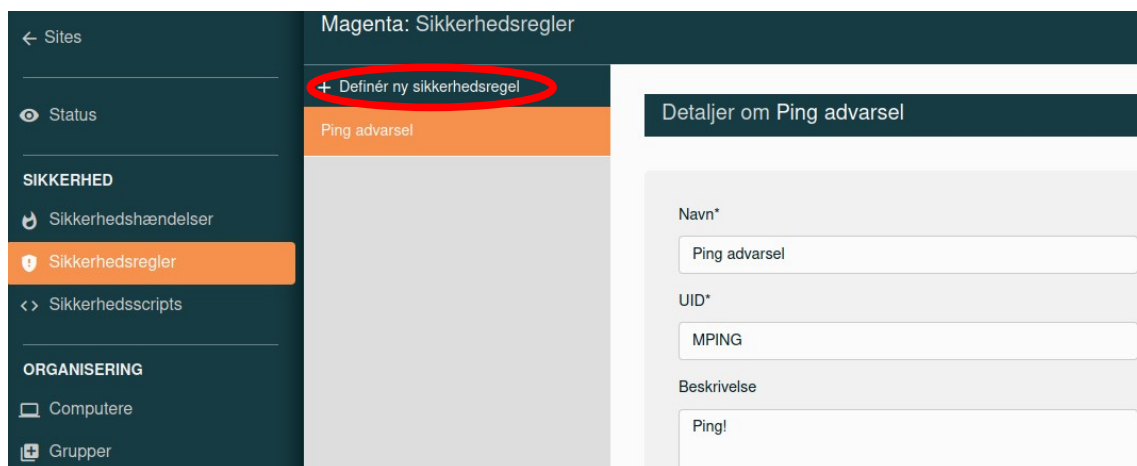
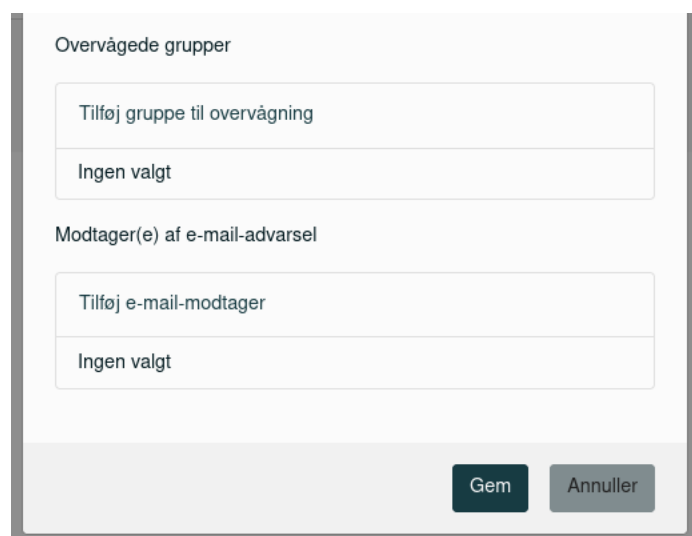


Figure 1

Når man har klikket på "definér ny sikkerhedsregel", skal man give reglen 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 "Beskrivelse" er henvendt til den eller de personer, som skal håndtere sikkerhedsreglen, 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 sikkerhedshændelserne, når de sker, og som derfor skal have en email omkring hændelsen.



The screenshot shows a web form with two main sections. The first section is titled "Overvågede grupper" and contains a text input field with the placeholder "Tilføj gruppe til overvågning" and a dropdown menu currently showing "Ingen valgt". The second section is titled "Modtager(e) af e-mail-advarsel" and contains a text input field with the placeholder "Tilføj e-mail-modtager" and a dropdown menu currently showing "Ingen valgt". At the bottom right of the form are two buttons: "Gem" (Save) and "Annuller" (Cancel).

Figure 2

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

Sikkerhedsscriptet "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. Sikkerhedsscriptet "Detect sudo event" holder øje med, om nogen forsøger at blive administrator på OS2borgerPC-klienterne.

Definér ny sikkerhedsregel

Navn*

UID*

Beskrivelse

Alvorlighedsgrad*

Kritisk

Sikkerhedsscript*

Nyt Keyboard detect

Detect sudo event

Nyt Keyboard detect

Figure 3

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

Derfor anbefales det også at oprette to "Sikkerhedsregler". 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}

adresser

Pilestræde 43, 3. sal
1112 København K

Skt. Johannes Allé 2
DK-8000 Aarhus C

Imaneq 32 A
3900 Nuuk, Grønland

email

info@magenta-aps.dk

telefon

(+45) 33 36 96 96