OS2BORGERPC

Oprettelse af Sikkerhedsovervågning

Juli 2024

MAGENTA aps

INDHOLDSFORTEGNELSE

1 INDLEDNING 3
2 OPSÆTNING AF SIKKERHEDSOVERVÅGNING 4
Globale sikkerhedsscripts 6
Detekter låst/udløbet Borger-bruger 6
Detekter nytilsluttet keyboard 7
Detekter sudo-kørsel 8
Afsluttende bemærkninger 8

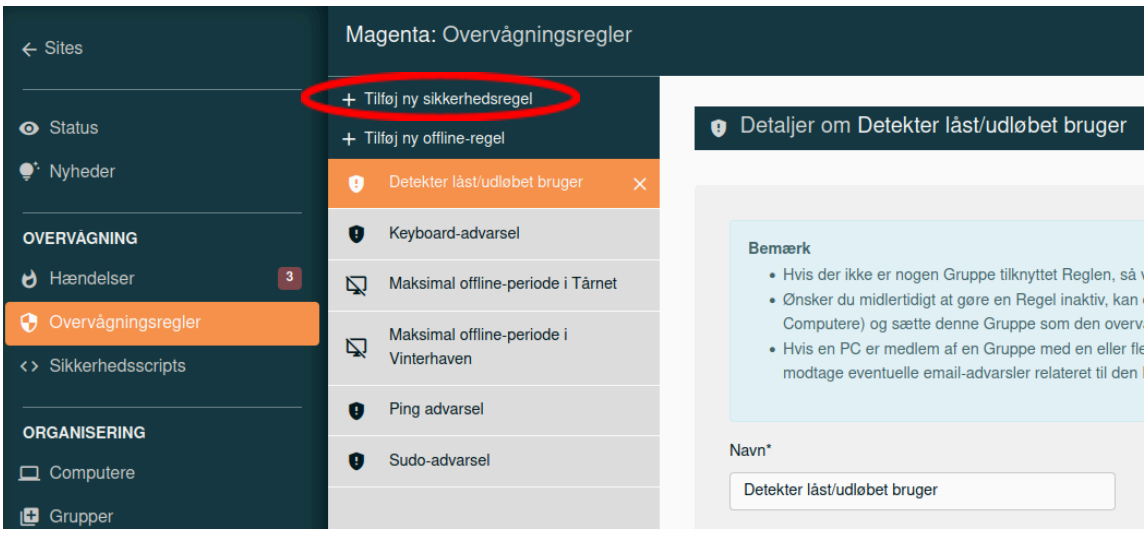
1 INDLEDNING

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'erne. Overvågningsmodulet er designet til nemt at kunne overvåge andre sikkerhedshændelser end de nævnte.

2 OPSÆTNING AF SIKKERHEDSOVERVÅGNING

I OS2borgerPC's administrationsmodul (admin-sitet) finder du i venstremenuen en gruppe af menupunkter, som omhandler overvågning. For at opsætte en ny sikkerhedsovervågning skal man klikke på menupunktet "Overvågningsregler" og derefter "Tilføj ny sikkerhedsregel" (Se Figur 1).



Figur 1

Når man har klikket på "Tilføj ny sikkerhedsregel", skal man give reglen et navn, vælge et sikkerhedsscript og vælge alvorlighedsgrad. Derudover kan man angive en beskrivelse samt vælge eventuelle "Overvågede grupper" og "Modtager(e) af e-mail-advarsel" (Se Figur 2).

Det anbefales, at man vælger et sigende navn, som beskriver, hvad der overvåges og eventuelt også hvilke(n) gruppe(r) af OS2borgerPC'er, som overvåges.

Sikkerhedsscriptet bestemmer, hvad sikkerhedsreglen reelt overvåger. Magenta har udviklet tre globale sikkerhedsscripts, som alle kunder har adgang til. Disse er "Detekter låst/udløbet Borger-bruger", "Detekter nytilsluttet keyboard" og "Detekter sudo-kørsel". Se afsnittet "Globale sikkerhedsscripts" for en detaljeret beskrivelse af disse sikkerhedsscripts.

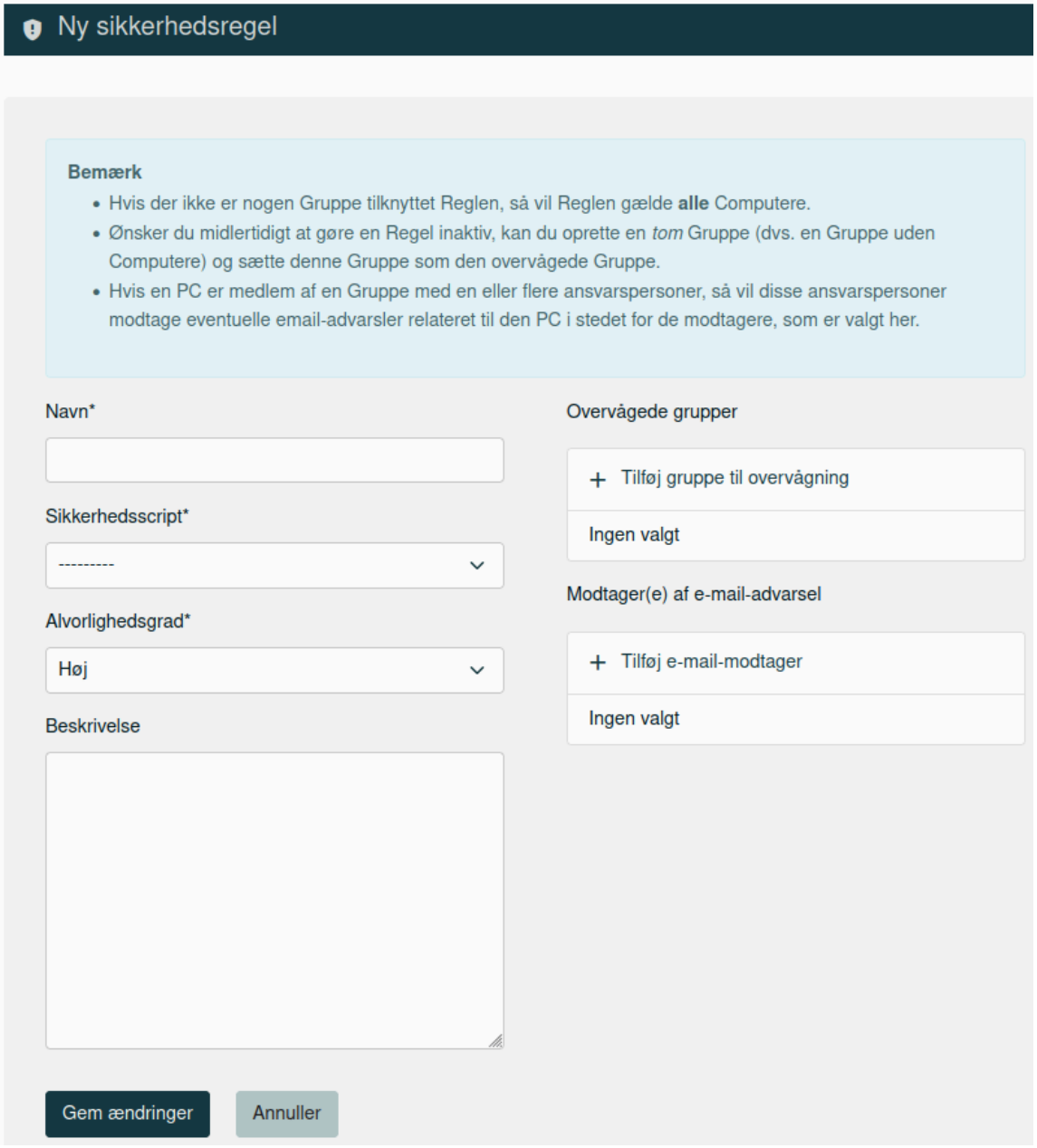
Alvorlighedsgraden bestemmer alvorlighedsgraden af hændelser relateret til sikkerhedsreglen. I de fleste tilfælde vil det være passende at bruge alvorlighedsgraden "Høj", som er valgt som standard. Man kan også vælge alvorlighedsgraden "Kritisk", hvis

man mener, at hændelser relateret til sikkerhedsreglen er mere kritiske end andre hændelser. Alvorlighedsgraden "Normal" kan bruges til sikkerhedsregler, hvis hændelser ikke udgør en sikkerhedsrisiko. Hændelser med alvorlighedsgraden "Normal" vil ikke som udgangspunkt blive vist på listen over hændelser.

Feltet "Beskrivelse" er henvendt til den eller de personer, som skal håndtere hændelser relateret til sikkerhedsreglen, hvis de opstår. Feltet kan således bruges til at angive ekstra information, som er relevant for håndteringen af de relaterede hændelser.

Feltet "Overvågede grupper" bruges til at styre hvilke computere, som sikkerhedsreglen overvåger. Hvis feltet efterlades tomt, vil sikkerhedsreglen overvåge alle computere på ens site. Hvis der vælges en eller flere grupper, vil sikkerhedsreglen overvåge alle computere i de valgte grupper.

Feltet "Modtager(e) af e-mail-advarsel" bruges til at angive den eller de brugere på ens site, som skal have en email om hændelser relateret til sikkerhedsreglen. Bemærk at det også er muligt at angive en eller flere "Ansvarspersoner" for en given gruppe. Hvis en computer er medlem af en gruppe, som har en eller flere ansvarspersoner, vil disse ansvarspersoner modtage alle emails om eventuelle hændelser relateret til den computer i stedet for de email-modtagere, som er valgt på sikkerhedsreglen. Det er naturligvis kun muligt at sende emails til brugere, som har angivet deres email på admin-sitet.



Figur 2

Globale sikkerhedsscripts

Detekter låst/udløbet Borger-bruger

Sikkerhedsscriptet "Detekter låst/udløbet Borger-bruger" overvåger, om

Borger-brugeren er blevet låst. Borger-brugeren kan blive låst af scriptet "Sikkerhed - Bloker for login ved USB-event" eller scriptet "Sikkerhed - Bloker for login ved hård nedlukning", hvis et eller begge scripts er blevet kørt på computeren.

Scriptet "Sikkerhed - Bloker for login ved USB-event" vil låse Borger-brugeren, hvis der indsættes eller fjernes en vilkårlig USB-enhed (dette inkluderer mus eller keyboard). Scriptet kan dog kun være aktivt, mens computeren er tændt, hvilket er grunden til at scriptet "Sikkerhed - Bloker for login ved hård nedlukning", som låser Borger-brugeren, hvis computeren mister strømmen, får trukket stikket eller slukkes på knappen, eksisterer. Borger-brugeren kan som udgangspunkt ikke slukke computeren via menuen på nyere versioner af OS2borgerPC, så tilsammen forhindrer de to scripts, at der indsættes eller fjernes en USB-enhed, uden at Borger-brugeren bliver låst.

Kombinationen af "Sikkerhed - Bloker for login ved USB-event", "Sikkerhed - Bloker for login ved hård nedlukning" og en sikkerhedsregel med sikkerhedsscriptet "Detekter låst/udløbet Borger-bruger" kan således benyttes, hvis man vil forhindre, at der indsættes eller fjernes en USB-enhed fra computeren, uden at det opdages. Computeren kan derefter kontrolleres, inden Borger-brugeren låses op for at sikre, at der ikke er blevet indsat en keylogger.

Borger-brugeren kan låses op ved at køre scriptet "Sikkerhed - Sæt Borger som aktiv efter blokeret login (lås op)" eller via den genvej på superusers skrivebord som tilføjes af scriptet "Sikkerhed: Genvej til at låse Borger-konto op fra superusers skrivebord".

Detekter nytilsluttet keyboard

Sikkerhedsscriptet "Detekter nytilsluttet keyboard" overvåger, om der tilsluttes et keyboard til computeren. Sikkerhedsscriptet vil også reagere, hvis det nuværende keyboard fjernes og tilsluttes igen. Computeren bør så kontrolleres for at sikre, at der ikke er blevet indsat en keylogger mellem computeren og keyboardet.

Hvis almindelige borgere har adgang til computerens USB-indgange, anbefales det, at man enten overvåger computeren med en sikkerhedsregel med sikkerhedsscriptet "Detekter nytilsluttet keyboard" eller kombinationen af "Sikkerhed - Bloker for login ved USB-event", "Sikkerhed - Bloker for login ved hård nedlukning" og en sikkerhedsregel med sikkerhedsscriptet "Detekter låst/udløbet Borger-bruger". Kombinationen med sikkerhedsscriptet "Detekter låst/udløbet Borger-bruger" udgør en mere striks og fuldstændig overvågning af USB-enhederne, men sikkerhedsscriptet "Detekter nytilsluttet keyboard" kan f.eks. benyttes, hvis det er meningen, at borgere skal kunne indsætte almindelige USB-enheder i computeren.

Hvis computeren er låst inde i et bur, som forhindrer almindelige borgere i at tilgå

computerens USB-indgange, vil det normalt ikke være nødvendigt at benytte "Detekter nytilsluttet keyboard" eller kombinationen med "Detekter låst/udløbet Borger-bruger".

Detekter sudo-kørsel

Sikkerhedsscriptet "Detekter sudo-kørsel" overvåger, om der bliver gjort forsøg på at køre kommandoer med "sudo", som bruges til at opnå administratorrettigheder på computeren. Det bør dog bemærkes, at et forsøg på at køre "sudo" ikke automatisk er en sikkerhedsrisiko, da Borger-brugeren ikke har rettigheder til at køre "sudo". Alle forsøg på at køre "sudo" som Borger-brugeren vil således automatisk blive afvist, men sikkerhedsscriptet "Detekter sudo-kørsel" vil stadig reagere på sådanne forsøg.

Afsluttende bemærkninger

God fornøjelse og kontakt os endelig, hvis I skal hjælp til at komme videre. På dette tidspunkt burde I have fået adgang til vores projektstyringssystem, Redmine, hvor I kan indrapportere sikkerhedsproblemer eller ønsker om support/fejlrettelse (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
Titanhus, Titangade 13
2200 København

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