

SAMBRUK MEDBORGARPC

Skapande av Säkerhetsövervakning

Juli 2024

MAGENTA^{aps}

© Copyright 2024

INNEHÅLLSFÖRTECKNING

1 INTRODUKTION.....	3
2 INRÄTTA SÄKERHETSÖVERVAKNING.....	4
Globala säkerhetsskript.....	6
Detekter låst/udløbet Borger-bruger.....	6
Detekter nyttilsluttet keyboard.....	7
Detekter sudo-kørsel.....	8
Slutord.....	8

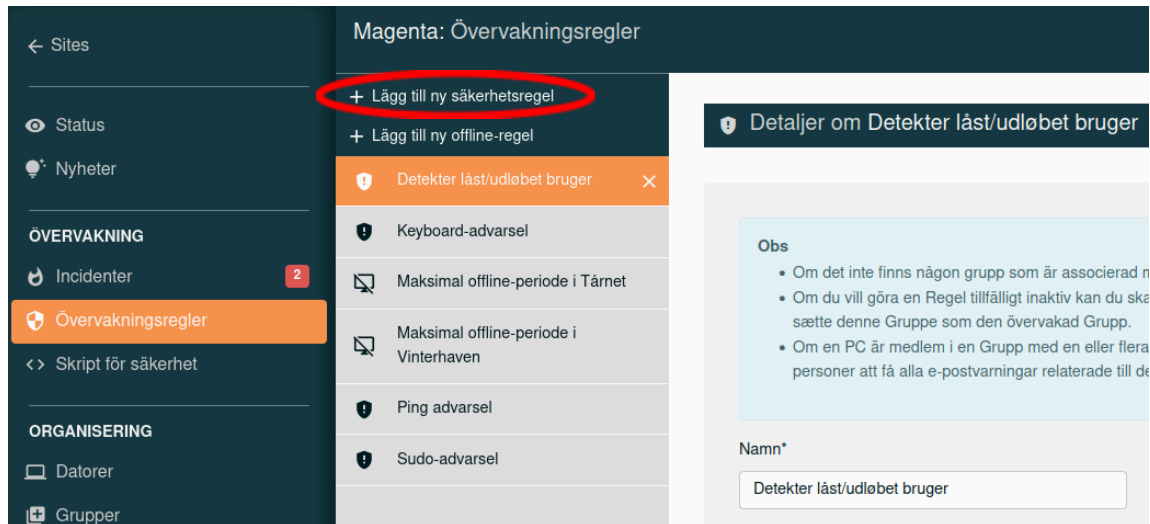
1 INTRODUKTION

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:erna. Övervakningsmodulen är utformad för att enkelt övervaka andra säkerhetshändelser än de som nämns.

2 INRÄTTA SÄKERHETSÖVERVAKNING

I Sambruk MedborgarPC:s administrationsmodul (adminsidan) hittar du i vänstermenyn en grupp meny punkter som handlar om övervakning. För att ställa in en ny säkerhetsövervakning, klicka på menyalternativet "Övervakningsregler" och sedan "Lägg till ny säkerhetsregel" (se Figur 1).



Figur 1

Efter att ha klickat på "Lägg till ny säkerhetsregel" måste du ge regeln ett namn, välja ett säkerhetsskript och välja en svårighetsgrad. Dessutom kan du ange en beskrivning och välja valfri "Övervakade grupper" och "Mottagare av e-postvarning" (se figur 2).

Det rekommenderas att du väljer ett beskrivande namn som beskriver vad som övervakas och eventuellt även vilka grupper av MedborgarPC:er som övervakas.

Säkerhetsskriptet bestämmer vad säkerhetsregeln faktiskt övervakar. Magenta har utvecklat tre globala säkerhetsskript som alla kunder har tillgång till. Dessa är "Detekter låst/udløbet Borger-bruger", "Detekter nytilsluttet keyboard" och "Detekter sudo-kørsel". Se avsnittet "Globala säkerhetsskript" för en detaljerad beskrivning av dessa säkerhetsskript.


Svårighetsgraden bestämmer svårighetsgraden av händelser relaterade till säkerhetsregeln. I de flesta fall är det lämpligt att använda "Hög" svårighetsgrad, som är vald som standard. Du kan också välja svårighetsgraden "Kritisk" om du anser att incidenter relaterade till säkerhetsregeln är mer kritiska än andra incidenter.

Svårighetsgraden "Normal" kan användas för säkerhetsregler om händelser inte utgör en säkerhetsrisk. Incidenter med svårighetsgraden "Normal" kommer som regel inte att visas i listan över incidenter.

Fältet "Beskrivning" är avsett för den eller de personer som ska hantera incidenter relaterade till säkerhetsregeln, om de inträffar. Fältet kan således användas för att ange ytterligare information som är relevant för hanteringen av de relaterade incidenterna.

Fältet "Övervakade grupper" används för att styra vilka datorer som säkerhetsregeln övervakar. Om fältet lämnas tomt kommer säkerhetsregeln att övervaka alla datorer på ens site. Om en eller flera grupper väljs kommer säkerhetsregeln att övervaka alla datorer i de valda grupperna.

Fältet "Mottagare av e-postvarning" används för att ange den eller de användare på ens site som ska få ett e-postmeddelande om incidenter relaterade till säkerhetsregeln. Observera att det även är möjligt att ange en eller flera "Ansvariga för gruppen" för en given grupp. Om en dator är medlem i en grupp som har en eller flera ansvariga kommer dessa ansvariga att få alla e-postmeddelanden om eventuella händelser relaterade till den datorn istället för de e-postmottagare som valts i säkerhetsregeln. Det är givetvis endast möjligt att skicka e-postmeddelanden till användare som har angett sin e-postadress på adminsidan.

 Ny säkerhetsregel

Obs

- Om det inte finns någon grupp som är associerad med Regeln kommer Regeln att gälla **alla** Datorer.
- Om du vill göra en Regel tillfälligt inaktiv kan du skapa en *tom* Gruppe (dvs. en Gruppe uden Computere) og sætte denne Gruppe som den overvakte Gruppe.
- Om en PC är medlem i en Grupp med en eller flera ansvariga personer, då kommer dessa ansvariga personer att få alla e-postvarningar relaterade till det PC istället för de mottagare som valts här.

Namn*

Säkerhetsskript*

Svårighetsgrad*

Hög

Beskrivning

Övervakade grupper

+ Lägg till en grupp för övervakning

Ingen vald

Mottagare av e-postvarning

+ Lägg till e-postmottagare

Ingen vald

Spara ändringar

Avbryt

Figur 2

Globala säkerhetsskript

Detekter låst/udløbet Borger-bruger

Säkerhetsskriptet "Detekter låst/udløbet Borger-bruger" övervakar om Medborgare-användaren har låsts. Medborgare-användaren kan låsas med skriptet

["Sikkerhed - Bloker for login ved USB-event"](#) eller skriptet ["Sikkerhed - Bloker for login ved hård nedlukning"](#) om ett eller båda skripten har körts på datorn.

Skriptet "Sikkerhed - Bloker for login ved USB-event" kommer att låsa Medborgare-användaren om någon USB-enhet sätts in eller tas bort (detta inkluderar mus eller tangentbord). Skriptet kan dock bara vara aktivt medan datorn är på, varför skriptet "Sikkerhed - Bloker for login ved hård nedlukning", som låser Medborgare-användaren om datorn tappar ström, kopplas ur eller stängs av vid knappen, existerar. Medborgare-användaren kan som utgångspunkt inte stänga av datorn via menyn, så tillsammans förhindrar de två skripten att en USB-enhet sätts in eller tas bort utan att Medborgare-användaren låses ute.

Kombinationen av "Sikkerhed - Bloker for login ved USB-event", "Sikkerhed - Bloker for login ved hård nedlukning" och en säkerhetsregel med säkerhetsskriptet "Detekter låst/udløbet Borger-bruger" kan alltså användas om du vill förhindra insättningen eller en USB-enhet tas bort från datorn utan att upptäckas. Datorn kan sedan kontrolleras innan Medborgare-användaren låses upp för att säkerställa att en keylogger inte har satts in.

Medborgare-användaren kan låsas upp genom att köra skriptet ["Sikkerhed - Sæt Borger som aktiv efter blokeret login \(lås op\)"](#) eller via genvägen på superusers skrivbord som lagts till av skriptet ["Sikkerhed: Genvej til at låse Borger-konto op fra superusers skrivebord"](#).

Detekter nyttilsluttet keyboard

Säkerhetsskriptet "Detekter nyttilsluttet keyboard" övervakar om ett tangentbord är anslutet till datorn. Säkerhetsskriptet kommer också att svara om det aktuella tangentbordet tas bort och återansluts. Datorn bör sedan kontrolleras för att säkerställa att en keylogger inte har satts in mellan datorn och tangentbordet.

Om vanliga medborgare har tillgång till datorns USB-ingångar rekommenderas att du antingen övervakar datorn med en säkerhetsregel med säkerhetsskriptet "Detekter nyttilsluttet keyboard" eller kombinationen av "Sikkerhed - Bloker for login ved USB-event", "Sikkerhed - Bloker for login ved hård nedlukning" och en säkerhetsregel med säkerhetsskriptet "Detekter låst/udløbet Borger-bruger". Kombinationen med säkerhetsskriptet "Detekter låst/udløbet Borger-bruger" utgör en mer strikt och fullständig övervakning av USB-enheterna, men säkerhetsskriptet "Detekter nyttilsluttet keyboard" kan t.ex. användas om det är tänkt att medborgarna ska kunna sätta in vanliga USB-enheter i datorn.

Om datorn är inlåst i en bur som hindrar vanliga medborgare från att komma åt datorns USB-ingångar behöver man normalt sett inte använda "Detekter nyttilsluttet keyboard"

eller kombinationen med "Detekter låst/udløbet Borger-bruger".

Detekter sudo-kørsel

Säkerhetsskriptet "Detekter sudo-kørsel" övervakar om försök görs att köra kommandon med "sudo", som används för att få administrativa rättigheter på datorn. Det bör dock noteras att ett försök att köra "sudo" inte automatiskt är en säkerhetsrisk, eftersom Medborgare-användaren inte har rättigheter att köra "sudo". Alla försök att köra "sudo" som Medborgare-användare kommer alltså automatiskt att avvisas, men säkerhetsskriptet "Detekter sudo-kørsel" kommer fortfarande att svara på sådana försök.

Slutord

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 säkerhetsproblem eller förfrågningar om support/felkorrigering (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

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