

Revision - Ofte Stillede Spørgsmål

- omkring OS2borgerPC og OS2borgerPC Kiosk

1. Kort introduktion af systemerne	2
2. Rettighedsstyring / Nedlåsning	2
3. Om rydning af data	7
Rydning af data - Browsers	8
Firefox	8
Chrome	8
4. Automatiske opdateringer	9
OS2borgerPC Kiosk	10
5. Overvågning af systemet - og keyloggers	10
6. Netværkssikkerhed generelt	11
7. End-point protection (anti-virus/anti-malware)	11
8. Øvrige spørgsmål	11
Kontakt Magenta	14

Indledning

Dokumentet er udarbejdet som svar på revisionsrelaterede spørgsmål til OS2borgerPC fra Magentas kommunale kunder.

ISO27001-certificeret

I 2023 blev Magenta certificeret i it-sikkerhedsstandard ISO 27001. Det betyder, at vores løsninger, herunder Os2borgerPC, er certificeret til den højeste internationale standard inden for it-sikkerhed.

Har du spørgsmål til dokumentet, vores ISO-certificering eller andet, så kontakt os. Dette er et levende dokument, som vi løbende opdaterer i takt med, at der kommer nye spørgsmål ind.

Kontaktoplysninger findes i bunden af dokumentet.

1. Kort introduktion af systemerne

Dette dokument omhandler de to beslægtede platforme **OS2borgerPC** og **OS2borgerPC Kiosk**.

OS2borgerPC benyttes primært til publikumsPC'er på biblioteker, daginstitutioner, borgerservice og jobcentre. Man har som udgangspunkt en fuld brugergrænseflade og kan vælge mellem at åbne forskellige programmer.

OS2borgerPC Kiosk har typisk enten ingen brugere, eller også er man begrænset til en enkelt webside i en browser. OS2borgerPC Kiosk benyttes til infoskærme, slideshows og til Kiosk-maskiner, i sidstnævnte tilfælde eksempelvis som komme-gå-skærme. Man er låst til at være inde i en browser, og man har ikke mulighed for at skifte væk fra den side, som browseren er konfigureret til at starte op på.

På grund af denne store forskel i anvendelse er fokus på sikkerhed på **OS2borgerPC** og **OS2borgerPC Kiosk** signifikant forskellig. Generelt kan man sige, at arbejdet med sikkerhed er langt mere omfattende på **OS2borgerPC**. Det skyldes hovedsageligt, at der fra disse maskiner kan blive logget ind på websteder, MitID, tjekket e-mail, tjekket netbank, downloadet private filer mv. Derfor er meget af sikkerheden på **OS2borgerPC** centreret omkring at sikre, at denne data ryddes op mellem de besøgende. Vi har desuden omfattende fokus på forskellige tiltag med henblik på overvågning og forhindring af keylogging.

En stor del af systemerne er konfigurerbare via de **scripts**, vi har udviklet til OS2borgerPC, så de præcise indstillinger kan variere fra kunde til kunde, lokation til lokation eller endda - i teorien, omend det sjældent er relevant - computer til computer. Derudover er hver enkelt kunde - kommunerne - selv administrator på maskinerne, så de kan reelt set lave alt om efter behov.

2. Rettighedsstyring / Nedlåsning

Denne sektion omhandler OS2borgerPC.

Der er en lokal administratorkonto på OS2borgerPC'erne, men det er ikke den konto, som borgerne logger ind på/har adgang til.

Besøgende logger ind på kontoen "**Borger**", der internt i systemet kaldes "**user**".

Administrator-kontoen hedder "**root**", og denne har ikke et kodeord sat, hvilket vil sige, at man ikke kan logge ind på den. Måden man kan få adgang til administratorkontoen er derfor via det system, der hedder "**sudo**", som kræver at ens bruger er medlem af en gruppe, der er tilføjet i filen "sudoers" som én, der har rettigheder til at køre kommandoer som **root**. "**superuser**" er medlem af **sudo**-gruppen; det er brugeren "**user**" ikke. Brugeren "**user**" har ikke rettigheder til at redigere filen "sudoers". Dermed er sikkerheden stærk.

Borger-kontoen har kun skriverrettigheder til mapper, som bliver slettet ved hver logud. Ligeledes nulstilles ændringer i indstillinger i programmer efter logud. Vi foreslår derfor at slå kontinuerlig automatisk logud ved inaktivitet til via det relaterede script og at råde besøgende til at logge ud inden og efter brug.

Borgere kan downloade software, men ikke installere noget der forbliver på maskinen efter logud.

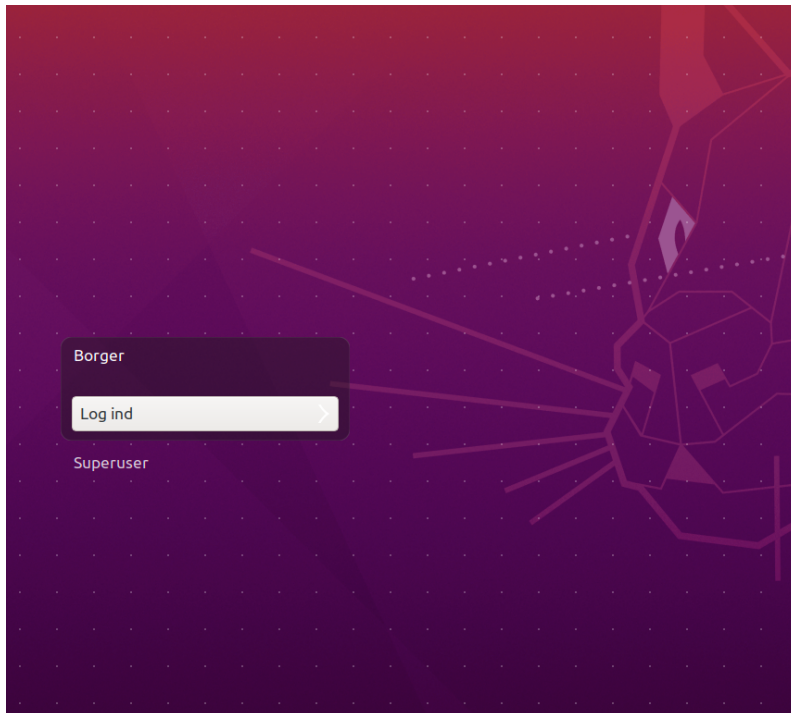
Derudover kan man fra adminsitet sætte sikkerhedsscripts op til at give advarsler ved alle forsøg på kørsler af **sudo**, hvis man ønsker det. Det gøres ved at oprette en sikkerhedsregel og tilknytte den til de grupper af maskiner, man ønsker overvåget. Mere om dette under sektionen "Overvågning af systemet - og keyloggers".

I versioner af OS2borgerPC installeret ud fra 5.0.0 imaget og nyere har vi desuden fjernet skriverrettighederne til Borgers skrivebord samt fjernet muligheden for at ændre i genvejene i menuen. Det betyder, at disse bliver nulstillet ved logud, men nu er det end ikke muligt at ændre dem midlertidigt.

Har man installeret fra en tidligere version af imaget, kan denne nedlåsning tilføjes via scripts.

Herunder vises et par screenshots for at dokumentere disse rettigheder:

Her ses det, at det er kontoen "Borger", som besøgende logger ind på.



Her ses det at "Borger"-kontoen internt i systemet hedder "user"

```

Abn  [icon]  passwd
/etc


1 root:x:0:0:root:/root:/bin/bash
2 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
3 bin:x:2:2:bin:/bin:/usr/sbin/nologin
4 sys:x:3:3:sys:/dev:/usr/sbin/nologin
5 sync:x:4:65534:sync:/bin:/bin/sync
6 games:x:5:60:games:/usr/games:/usr/sbin/nologin
7 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
8 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
9 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
10 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
11 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
12 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
13 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
14 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
15 list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin
16 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
17 gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
18 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
19 systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
20 systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
21 systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
22 messagebus:x:103:106:/nonexistent:/usr/sbin/nologin
23 syslog:x:104:110:/home/syslog:/usr/sbin/nologin
24 _apt:x:105:65534:/nonexistent:/usr/sbin/nologin
25 tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
26 uidd:x:107:114:/run/uidd:/usr/sbin/nologin
27 tcpdump:x:108:115:/nonexistent:/usr/sbin/nologin
28 avahi-autoipd:x:109:116:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
29 usbmux:x:110:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
30 rtkit:x:111:117:RealtimeKit,,,:/proc:/usr/sbin/nologin
31 dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
32 cups-pk-helper:x:113:120:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
33 speech-dispatcher:x:114:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
34 avahi:x:115:121:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/usr/sbin/nologin
35 kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin
36 saned:x:117:123:/var/lib/saned:/usr/sbin/nologin
37 nm-openvpn:x:118:124:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
38 hplip:x:119:7:HPLIP system user,,,:/run/hplip:/bin/false
39 whoopsie:x:120:125:/nonexistent:/bin/false
40 colord:x:121:126:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
41 geoclue:x:122:127:/var/lib/geoclue:/usr/sbin/nologin
42 pulse:x:123:128:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
43 gnome-initial-setup:x:124:65534:/run/gnome-initial-setup:/bin/false
44 gdm:x:125:130:Gnome Display Manager:/var/lib/gdm3:/bin/false
45 sssd:x:126:131:SSSD system user,,,:/var/lib/sss:/usr/sbin/nologin
46 user:x:1000:1001:Borger,,,:/home/user:/usr/bin/bash
47 superuser:x:1001:1002:Superuser,,,:/home/superuser:/bin/bash
48 lightdm:x:127:133:Light Display Manager:/var/lib/lightdm:/bin/false
49 systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
50 fwupd-refresh:x:128:134:fwupd-refresh user,,,:/run/systemd:/usr/sbin/nologin

```

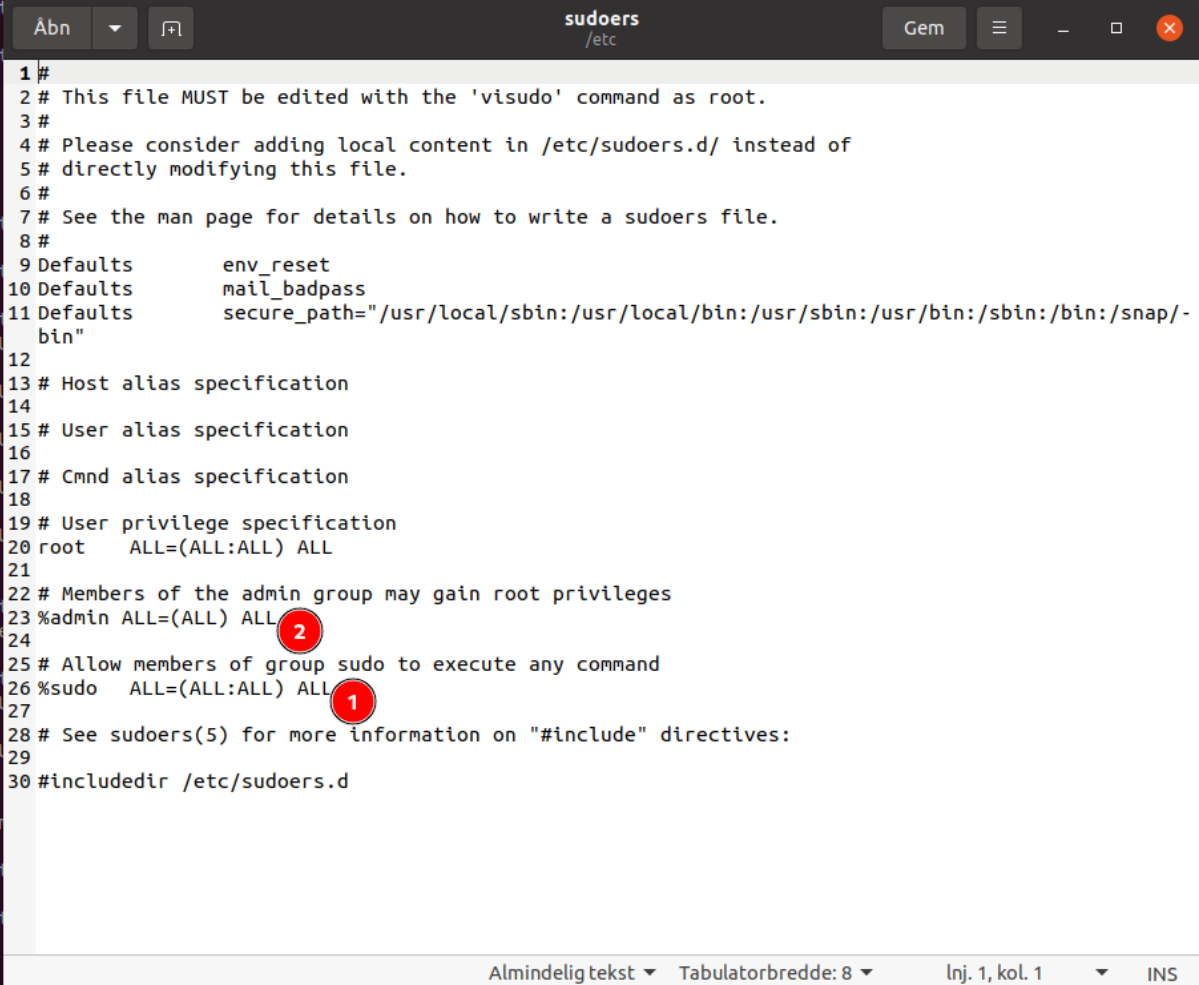
I filen /etc/group ses en liste over "grupperne" i systemet og hvilke brugere, der er medlem heraf. Her ser man ud fra gruppen "sudo", at kun brugeren "superuser" og ikke "user" er medlem heraf. Brugeren "user" har ikke rettigheder til at redigere denne fil.

```
Abn ▼ [+]
```

```
1 root:x:0:
2 daemon:x:1:
3 bin:x:2:
4 sys:x:3:
5 adm:x:4:syslog
6 tty:x:5:syslog
7 disk:x:6:
8 lp:x:7:
9 mail:x:8:
10 news:x:9:
11 uucp:x:10:
12 man:x:12:
13 proxy:x:13:
14 kmem:x:15:
15 dialout:x:20:
16 fax:x:21:
17 voice:x:22:
18 cdrom:x:24:
19 floppy:x:25:
20 tape:x:26:
21 sudo:x:27:superuser
22 audio:x:29:pulse
23 dip:x:30:
24 www-data:x:33:
25 backup:x:34:
26 operator:x:37:
27 list:x:38:
28 irc:x:39:
29 src:x:40:
30 gnats:x:41:
31 shadow:x:42:
32 utmp:x:43:
33 video:x:44:
34 sasl:x:45:
35 plugdev:x:46:
36 staff:x:50:
37 games:x:60:
38 users:x:100:
39 nogroup:x:65534:
40 systemd-journal:x:101:
41 systemd-network:x:102:
42 systemd-resolve:x:103:
43 systemd-timesync:x:104:
44 crontab:x:105:
45 messagebus:x:106:
46 input:x:107:
47 kvm:x:108:
48 render:x:109:
49 syslog:x:110:
50 tss:x:111:
51 bluetooth:x:112:
```



I /etc/sudoers ses det, at det er "sudo", der afgør, hvem der har adgang til at køre noget som root/administrator. Gruppen "admin" eksisterer ikke, og det kræver administrator-rettigheder både at oprette en gruppe og at justere medlemmer heraf. Brugeren "user" har som nævnt ikke rettigheder til at redigere denne fil.



```
1 #
2 # This file MUST be edited with the 'visudo' command as root.
3 #
4 # Please consider adding local content in /etc/sudoers.d/ instead of
5 # directly modifying this file.
6 #
7 # See the man page for details on how to write a sudoers file.
8 #
9 Defaults                env_reset
10 Defaults                mail_badpass
11 Defaults                secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"
12
13 # Host alias specification
14
15 # User alias specification
16
17 # Cmnd alias specification
18
19 # User privilege specification
20 root    ALL=(ALL:ALL) ALL
21
22 # Members of the admin group may gain root privileges
23 %admin   ALL=(ALL) ALL
24
25 # Allow members of group sudo to execute any command
26 %sudo   ALL=(ALL:ALL) ALL
27
28 # See sudoers(5) for more information on "#include" directives:
29
30 #includedir /etc/sudoers.d
```

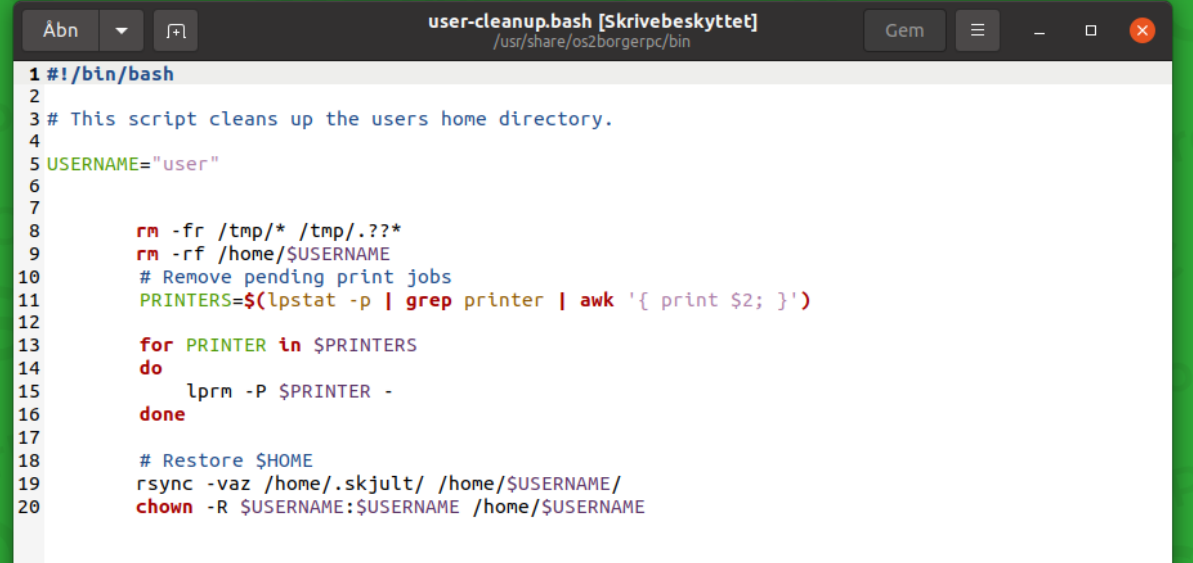
3. Om rydning af data

Denne sektion omhandler: OS2borgerPC

Alle besøgende logger ind som Borger-kontoen på OS2borgerPC.

Borger har ikke administrator-adgang, så programmer kørt af Borger kan kun skrive til hjemmemappen (/home/user) og til mapper for midlertidige filer. Disse mapper ryddes ved logud.

Følgende script sørger for denne oprydning ved logud. Brugeren "user" har ikke rettigheder til at redigere dette script:



```
1 #!/bin/bash
2
3 # This script cleans up the users home directory.
4
5 USERNAME="user"
6
7
8 rm -fr /tmp/* /tmp/.*
9 rm -rf /home/$USERNAME
10 # Remove pending print jobs
11 PRINTERS=$(lpstat -p | grep printer | awk '{ print $2; }')
12
13 for PRINTER in $PRINTERS
14 do
15     lprm -P $PRINTER -
16 done
17
18 # Restore $HOME
19 rsync -vaz /home/.skjult/ /home/$USERNAME/
20 chown -R $USERNAME:$USERNAME /home/$USERNAME
```

Disse PC'er er derudover designet til ikke at opbevare data af værdi, som skal beskyttes, så angreb som ransomware ville ikke påvirke dem. De kan inden for en time geninstalleres og gendannes til samme konfiguration, som de havde inden.

Rydning af data - Browsere

I nyere versioner af OS2borgerPC imaget - version 5.0.0 og nyere - har vi lavet en del forbedringer i forhold til nedlåsning af browserne og yderligere rydning af browser-data uden behov for logud. Af browsere er Firefox installeret som standard, og mange kommuner vælger pt. derudover at installere Chrome.

Har man et ældre image, kan denne oprydning tilvælges via scripts.

Firefox

Følgende data slettes når browseren lukkes (dvs. inden logud):

- Cache
- Cookies
- Formulardata
- Historik
- Sessioner
- Sideindstillinger
- Offline apps

Chrome

Browserdata slettes i Chrome, så snart browseren lukkes.

Ved browserlukning slettes al data.

Følgende browserdata slettes desuden automatisk af Chrome hver time, selv hvis browseren ikke har været lukket:

- Auto-udfyld
- Browserhistorik
- Cashede billeder og filer
- Downloadhistorik
- App data
- Sideindstillinger.

4. Automatiske opdateringer

Denne sektion omhandler: OS2borgerPC og OS2borgerPC Kiosk

På OS2borgerPC er automatiske sikkerhedsopdateringer slået til som standard.

Sikkerhedsopdateringer kommer fra virksomheden Canonical, der står bag Ubuntu.

Man kan via et script (**Script System - Aktivér automatiske opdateringer fra Ubuntu**) valgfrit slå det til, så øvrige program-opdateringer til Ubuntu også hentes og installeres automatisk, eller man kan opdatere manuelt via scriptet **System - Opdater alt**.

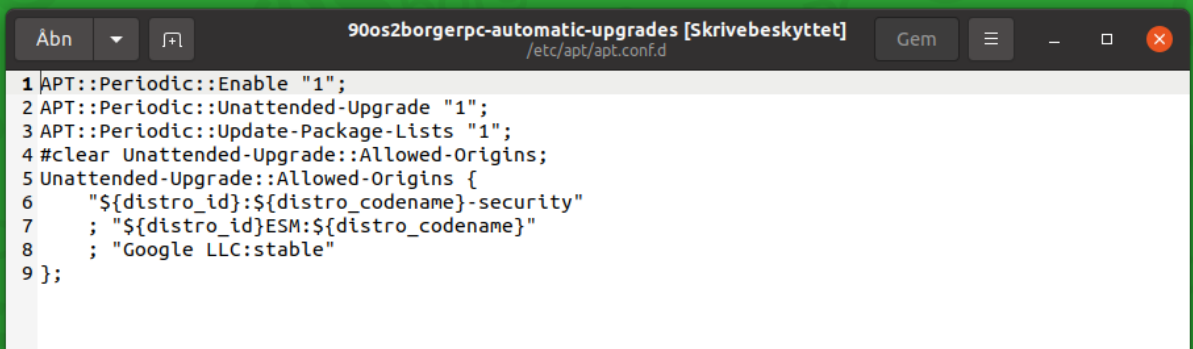
Vi anbefaler at udrulle de ikke-sikkerhedsmæssige opdateringer manuelt, eksempelvis en gang om måneden, og så kan man bagefter tjekke, at alt er som det skal være, frem for at der er en lille risiko for at noget ikke længere virker hensigtsmæssigt, og det ikke opdages med det samme.

Sikkerhedsopdateringerne rulles ud løbende og enkeltvist og er ikke en del af større "releases", og der er derfor ikke en liste over dem. Vi kan dog skrive et script til at liste opdateringshistorikken for en specifik maskine, hvis det ønskes, da denne information gemmes i filen `/var/log/apt/history.log`

Hvad angår frekvensen for opdateringer, så tjekker hver enkelt PC efter opdateringer 1-2 gange dagligt, og det er på vilkårlige tidspunkter for ikke at overbelaste Ubuntu's pakke-servere.

Ønsker man at tjekke efter opdateringer oftere, ville vi relativt hurtigt kunne udvikle et script til at ændre dét.

De automatiske opdateringer styres af konfigurationsfilen, der ses nedenfor. Brugeren "user" har ikke rettigheder til at redigere denne fil:



```
Abn 90os2borgerpc-automatic-upgrades [Skrivebeskyttet] Gem  
/etc/apt/apt.conf.d  
1 APT::Periodic::Enable "1";  
2 APT::Periodic::Unattended-Upgrade "1";  
3 APT::Periodic::Update-Package-Lists "1";  
4 #clear Unattended-Upgrade::Allowed-Origins;  
5 Unattended-Upgrade::Allowed-Origins {  
6     "${distro_id}:${distro_codename}-security"  
7     ; "${distro_id}ESM:${distro_codename}"  
8     ; "Google LLC:stable"  
9 };
```

Opdatering af OS2borgerPC Klienten

Den del af PC'en, der kommunikerer med adminsitet - OS2borgerPC-klienten - opdaterer sig selv automatisk, når vi frigiver en ny version. Man kan finde dens frigivelses-historik her:

<https://github.com/OS2borgerPC/os2borgerpc-client/blob/master/NEWS.rst>

Brugeren "user" har ikke rettigheder til at redigere klienten.

OS2borgerPC Kiosk

OS2borgerPC Kiosk-maskiner henter, i modsætning til OS2borgerPC, ingen opdateringer automatisk, da disse maskiner primært anvendes som infoskærme uden tilknyttede tastaturer. Der er således ikke samme risici som med en OS2borgerPC.

Kiosk-PC'erne kan dog stadig opdateres manuelt via scripts. Man kan også slå automatiske opdateringer til, så de som BorgerPC'er automatisk henter opdateringer, via de samme scripts som bruges til BorgerPC, der nævnes ovenfor.

5. Overvågning af systemet - og keyloggers

Denne sektion omhandler: OS2borgerPC

Man har mulighed for følgende overvågning på OS2borgerPC via det, der i løsningen benævnes **Sikkerhedsscripts**:

- Man kan få en advarsel, når en person forsøger at køre noget som administrator på maskinen. (Detekter sudo-kørsel). Det skal dog siges, at Borger slet ikke har rettigheder til at køre kommandoer som administrator, men dette kan give en advarsel, hvis nogen ikke desto mindre skulle forsøge at gøre det.
- Man kan få en advarsel, hvis der indsættes et nyt keyboard (Detekter nyt keyboard)
- Man kan lave en opsætning, så Borger logges ud øjeblikkeligt, og Borger låses for login, hvis en USB-enhed tilføjes eller fjernes

- Man kan opsætte det således, at login til Borger låses, hvis strømskiftet hives ud eller maskinen slukkes på knappen.

Vores anbefalinger

Hvis en maskine er placeret nær personalet på et bibliotek eller i borgerservice, og der ikke er perioder med selvbetjening uden personale, anbefaler vi, at man på disse maskiner kører med mere "løs" sikkerhed, og at indsætning af USB-sticks eksempelvis kan være tilladt på PC'erne.

Hvis en maskine **ikke** er under opsyn, eller hvis den er tilgængelig ved selvbetjening og uden der er overvågning, anbefaler vi hårdere sikkerhed på maskinen, såsom ikke at tillade indsættelse af USB-enheder.

6. Netværkssikkerhed generelt

Denne sektion omhandler: OS2borgerPC og OS2borgerPC Kiosk

Netværkssikkerhed håndteres ikke af OS2borgerPC som udgangspunkt, men bestemmes i stedet af, hvordan man vælger at sætte det netværk op, som borgerPC'erne kører på. På denne måde vælger man selv det sikkerhedsniveau, man ønsker på dette område, og man kan definere det hele ét sted (i routeren) frem for på den enkelte computer. Vi anbefaler, at man laver et særskilt netværk til publikumsmaskiner.

Hvis det ønskes, kan vi dog udvikle scripts til konfiguration af eksempelvis firewalls på den enkelte maskine.

7. End-point protection (anti-virus/anti-malware)

Denne sektion omhandler: OS2borgerPC og OS2borgerPC Kiosk

Der er som udgangspunkt ikke antivirus/antimalware software på OS2borgerPC. Vi mener at Ubuntu's sikkerhedsmodel, deres hyppige sikkerhedsopdateringer og vores egne sikkerhedstiltag overflødig gør dette. Som beskrevet ovenfor logger alle besøgende ind med den stærkt begrænsede Borger-konto. Alle data slettes efter logud, og vi har scripts til automatisk udlogging ved inaktivitet. Vi har derudover scripts til at overvåge sudo-kørsler og indsættelse af keyboards samt ved alle former for ændringer i USB-enheder.

8. Øvrige spørgsmål

Denne sektion omhandler: OS2borgerPC og OS2borgerPC Kiosk

Spørgsmål: Kan maskinerne fjernstyres og i givet fald hvordan?

Svar: Maskinerne kan fjernstyres via det adminsitet, vi i Magenta udvikler og "hoster", og som ansatte i jeres kommune har fået adgang til, når I benytter løsningen. Medarbejderne kan selv oprette og slette brugere efter behov.

Adressen på adminsitet er: <https://os2borgerpc-admin.magenta.dk>

Spørgsmål: Hvad er styresystemet og versionen heraf?

Svar: Det kan variere fra maskine til maskine, men har man installeret fra Magentas images, er der typisk enten tale om Ubuntu 20.04 eller Ubuntu 22.04.

Begge er såkaldte "Long Term Support" udgivelser og får derfor opdateringer i 5 år efter frigivelsen. 20.04 betyder, at versionen er frigivet i april 2020.

Se nærmere info her: <https://ubuntu.com/about/release-cycle>

I kan henvende jer til os, hvis I ønsker hjælp til at svare på dette spørgsmål for jeres specifikke PC'er.

Spørgsmål: Hvor ofte logges der automatisk ud?

Svar: Det konfigurerer hver enkelt kunde per gruppe af computere eller enkelte computer. Der kan også logges ud manuelt.

Man kan dog typisk se disse oplysninger ved at kigge på en gruppes tilknyttede scripts eller med endnu større sikkerhed ved at køre et script ud på computeren for at få den til at vise dens konfiguration heraf.

I kan henvende jer til os, hvis I ønsker hjælp til at svare på dette spørgsmål for jeres specifikke PC'er.

Spørgsmål: Er der blokeret for MitIDs og NemIDs RA-portaler?

Svar:

Der er som udgangspunkt ikke blokeret for nogen form for netværkstrafik fra maskinerne.

I forhold til MitIDs og NemIDs RA-portaler vil vi anbefale at løse dette i netværksinfrastrukturen, eks. via et separat VLAN til BorgerPC'erne, som har blokeret for de relevante sider i firewall-opsætningen. Det anbefaler vi af disse grunde:

1. For at have én central konfiguration frem for, at det er spredt på de enkelte maskiner.
Derved er der ikke risiko for, at man glemmer at sætte det op på en maskine eller to i miljøet.
2. For at det er sværere at omgå. Eksempelvis kan det ikke omgås ved at sætte sin egen PC til netkablet i stedet.

Hvis det ønskes, kan vi udvikle et script til blokering af de relevante domæner og IP-adresser på de enkelte BorgerPC'er.

Kontakt Magenta

Har du andre spørgsmål end ovenstående?
Kontakt os via nedenstående oplysninger:

Mail

support@magenta.dk

København

Pilestræde 43, 3. sal
DK-1112 København K
+45 3336 9696

Aarhus

Silkeborgvej 260
DK-8230 Åbyhøj
+45 3336 9699

Nuuk

Imaneq 32 A
3900 Nuuk, Grønland
+299 556675