

Riktlinjer för administratörsrättigheter på egen dator

Publicerad: 2020-05-08

Beslutsfattare: Helena Wallskog

Handläggare: Marcus Sällstedt

Beslutsdatum: 2020-05-08

Giltighetstid: Tillsvidare

Ansvarig för förvaltning: Riktlinjerna förvaltas av infrastrukturavdelningen.

Sammanfattning: Syftet med riktlinjerna är att upprätthålla en god säkerhet inom Mittuniversitetets IT-miljö. Detta för att undvika dataförlust, data stöld, intrång, sabotage och liknande. Riktlinjerna syftar vidare till att vara en del av skyddet mot att Mittuniversitetets datorer används för attacker mot universitetet men även mot andra parter.

Innehållsförteckning

Riktlinjer för administratörsrättigheter på egen dator	3
Bakgrund och syfte	3
Egeninstallerade program.....	4
Licenser	4
Exponering av datorn.....	4
Backup	4
Support och rättigheter	5

Riktlinjer

2020-06-11

DNR: MIUN 2020/1045

Riktlinjer för administratörsrättigheter på egen dator

Bakgrund och syfte

Syftet med riktlinjerna är att upprätthålla en god säkerhet inom Mittuniversitetets IT-miljö. Detta för att undvika dataförlust, data stöld, intrång, sabotage och liknande. Riktlinjerna syftar vidare till att vara en del av skyddet mot att Mittuniversitetets datorer används för attacker mot universitetet men även mot andra parter.

Av dessa säkerhetsskäl har användare på Mittuniversitetet normalt sett inga administrationsrättigheter på sin dator. Vid särskilda behov kan dessa rättigheter komma att aktiveras.

För att ansöka om administratörsrättigheter på enskild dator ansöker användare om detta genom en blankett. Denna blankett ska skrivas under av användaren samt prefekt/avdelningschef. Administratören ansvarar för att datorn och egeninstallerade program alltid sköts enligt denna riktlinje.

Administratörsrättigheter får endast användas för de ansökta behoven angivna i blanketten. Detta kan exempelvis vara installation eller konfiguration av specifika program på grund av att användningen kräver stor kontroll över hela datormiljön eller mycket specialkunskap.

Viktigt att notera är att vara administratör på sin dator innebär ofta merarbete och merkostnader för organisationen. Dels måste administratörerna lägga tid på kontinuerlig kunskapsinhämtning och administrativt arbete för att hålla datorn inklusive programvaror i gott skick. Dels kan merarbete uppstå för övriga organisationen i form av komplicerade supportärenden, utredningar av datorintrång, intrång som även drabbar andra system, användare som är oklara över supportnivå och säkerhetsnivå på de olika programmen eller förlust av data. Det krävs arbetstid av datorsystemets administratörer för att hålla datorsystemet i gott skick och för att hålla sig vederbörligt informerade. Dessutom kan det krävas plötsliga arbetsinsatser t ex vid upptäckt av säkerhetshål eller vid intrång. Användare och prefekt/avdelningschef ska vara väl medveten om detta så att den arbetstid som krävs finns tillgänglig för administratörerna.

Denna riktlinje beskriver hur egenadministrerade datorsystem ska kunna drivas på ett för alla parter så smidigt och säkert sätt som möjligt.

Regler

2020-06-11

DNR: MIUN 2020/1045

Egeninstallerade program

Som administratör på din dator ansvarar du själv för att hålla egeninstallerade program uppdaterade. Detta för att undvika säkerhetshål som kan kompromettera operativsystemet eller övriga delar av Mittuniversitetets IT-miljö.

Innan ett program installeras ska en bedömning av programmets behov och risker genomföras så att man både initialt och fortlöpande kan vidta de åtgärder som krävs för att driva systemet med erforderlig stabilitet och god säkerhetsnivå. T ex ska programmets behov av säkerhetskopiering (backup), åtkomstbegränsning, risker för användare, risker för intrång, etc. analyseras.

Programmen ska alltid vara uppdaterade i god ordning för att undvika säkerhetshål och liknande. Detta ska ske utan onödig fördröjning. Även om automatiska uppdateringsfunktioner används måste man fortlöpande övervaka att de fungerar. Om programmet inte längre är möjligt att uppdatera, t ex pga. produktens ålder, ska det tas ur drift eller isoleras från datornätet och andra program.

Administratörer ska fortlöpande hålla sig informerade om säkerhetsproblem, produktens upphörande etc. Detta gäller även för andra program och system som programmet bygger på.

Licenser

Alla program du installerar själv måste ha en giltig licens. Program som levereras som shareware måste följa leverantörens licensvillkor. Administratören själv ansvarar för att eventuella nödvändiga licenser för egen införskaffad och installerad hård- och mjukvara finns och att villkoren för dessa uppfylls. Alla licenser beställs och administreras av infrastrukturavdelningen.

Exponering av datorn

Om du har behov av att installera program som gör datorn publikt tillgänglig på internet, speciellt om det är tjänster med inloggning för andra användare, måste du anmäla detta till Helpdesk, helpdesk@miun.se. På så sätt kan du få råd ifall det är ett program med kända säkerhetshål eller konfigurationsdetaljer man av säkerhetsskäl bör tänka på. Det kommer även att vara hjälpsamt för att fånga upp behov som eventuellt bör tillhandahållas centralt.

Backup

Om programmet innehåller data av värde ska regelbunden säkerhetskopiering (backup) genomföras. Om säkerhetskopiering inte sker ska alla inblandade parter vara väl medvetna om detta och konsekvenserna av detta.

Regler

2020-06-11

DNR: MIUN 2020/1045

Support och rättigheter

Det är viktigt att du är medveten om att din dator kan komma att stängas av för utredning vid intrång eller liknande incidenter.

En dator kan helt eller delvis isoleras, stängas av eller beslagtas för utredning om Infrastrukturavdelningen bedömer att det är påkallat. Några exempel på när detta kan bli aktuellt är:

- Datorsystemet har utsatts för intrång.
- Datorsystemet bedöms vara säkerhetsmässigt sårbart.
- Datorsystemet stör annan verksamhet.
- Datorsystemet har använts på ett sätt som är oförenligt med lagar och förordningar eller med regelverk.

Det är inte ovanligt att ett intrång är en del i ett större sammanhang där flera intrång och även andra brott kan ha begåtts. Utredningar kan därför bli tidskrävande och därför kan datorer och program förbli helt eller delvis otillgängligt under en längre tid.

En dator som utsatts för intrång får inte anslutas till datornätet eller tas i drift förrän intrånget är utrett samt intrångssäkerhet upprättad. Det kan vara mycket svårt att hitta alla dolda bakdörrar varför det ofta är enklast och säkrast med en komplett ominstallation och endast återställa ett minimum av data från säkerhetskopia.

Om man upptäcker ett intrång ska detta skyndsamt anmälas till HelpDesk, helpdesk@miun.se. Detta så att man gemensamt kan bedöma skadans storlek och om flera användare och/eller andra system är berörda.

I det fall punkterna i denna riktlinje inte efterföljs kan administratören bli fråntagen sina administratörsrättigheter.