3 gode grunde til at holde jeres drivere opdaterede

CapaServices

Hvis en hacker får adgang til kernen i operativsystemet gennem en driver og kan deaktivere både antivirus og firewall, hvad hjælper det så at softwaren er opdateret ?

Introduktion
Mange af os har ikke indset vigtigheden af at holde drivere og firmware opdateret på vores computere. Vi opdaterer Windows, antivirus og firewall produkter, men drivere og firmware er ofte et overset element.

Der er flere årsager til, at det er vigtigt at holde drivere og firmware opdateret :

- Kritiske sikkerhedshuller lukkes
- Computeren kører mere stabilt
- Computeren yder bedre

Specielt den release cyklus som Microsoft anvender til Windows 10 kræver hyppig opdatering af drivere og firmware, hvis man vil have et system der kører stabilt. Drivere og firmware følger nemlig ofte Windows versionen.

Sikkerhed
Under den årlige hacker konference DEFCON, som blev afholdt i august 2019, præsenterede sikkerhedsfirmaet Eclypsium resultaterne af en undersøgelse, som dokumenterede sikkerhedshuller i over 40 drivere fra mindst 20 forskellige leverandører.

Hvis man kigger på de store computer producenters hjemmesider kan man se, at der hver måned frigives adskillige driver opdateringer, som skal lukke sikkerhedshuller.

Alene i foråret 2020, har de største producenter frigivet over 30 opdateringer til drivere med kritiske sikkerhedshuller.

De fleste sikkerhedshuller bliver lukket kort efter de er opdaget, bla. gik der kun få dage fra Eclypsium dokumenterede sikkerhedshullerne til producenterne havde frigivet en opdateret driver. Det viser med al tydelighed at producenter også er klar over vigtigheden af at prioritere sikkerhed ifm. drivere.

I perioden fra 2018 til 2019 er der sket en stigning i ransomware angreb på over 300% !
Selvom de fleste ransonware angreb ikke er direkte rettet mod sårbarheder i drivere, viser det, at behovet for at holde drivere og firmware opdateret ikke bliver mindre - tværtimod.

Eksempelvis blev myndighederne i Baltimore i foråret 2019 inficeret af ransomwaren RobbinHood, som netop udnytter en kritisk sårbarhed i en driver. Angrebet påvirkede over 10.000 computere og de samlede omkostninger vurderes til 120 millioner kroner.

CapaSystems
...because time matters

CapaSystems A/S
Roskildevej 342C
DK-2630 Taastrup

(+45) 70 10 70 55
sales@capasystems.com

RobbinHood udnytter en kritisk sårbarhed i en kernel driver fra Gigabyte, selvom driveren er godkendt og digitalt signeret af producenten af bundkortet.

(((TechAlert)))

Sårbarheden giver hackeren ubegrænset adgang til hele operativsystemet. Når ransomwaren har lukket sikkerhedsforanstaltninger som f.ex antivirus og firewall software ned, bliver bruger relaterede filer på computeren krypteret, så der ikke længere er adgang til dem.

Adgangen til filerne bliver kun genskabt, hvis brugeren betaler en "løsesum"

Funktionalitet

Mange IT-afdelinger har oplevet udfordringer med kombinationen af Thunderbolt docks og én eller flere eksterne computerskærme. Løsningen har i langt de fleste tilfælde været at opgradere firmware og drivere.

Ligeledes har mange IT-afdelinger oplevet udfordringer med blæseren i Microsoft Surface, som nærmest har kørt konstant. Ofte har løsningen også her været at opdatere firmware og drivere.

Ydeevne og Stabilitet

Drivere og firmware har stor indflydelse på en computers ydeevne og stabilitet, men det er svært at vurdere den helt konkrete effekt - opfattelsen er typisk at computeren "kører bedre"
Som et konkret eksempel frigav NVIDIA i sommeren 2019 deres Gamescom Game Ready Driver, som forbedrer ydeevnen på nogle af deres graffikkort med op til 23%

Løsninger

De fleste virksomheder opdaterer hardware drivere i forbindelse med installation af en ny computer, men der er sjældent fokus på at holde driverne opdateret efterfølgende.

Der findes nogle tredjeparts produkter på markedet som kan hjælpe med at holde driverne på en computer opdateret - men de primært rettet mod det private marked.

Mange af de store hardware producenter har deres eget software til at håndtere opdatering af drivere, men hvis en virksomhed har hardware fra flere forskellige producenter, kan det hurtigt blive indviklet at administrere.

Hos CapaSystems har vi udviklet en unik service, som er rettet mod erhvervsmarkedet og anvender teknologi der allerede er indbygget i Windows - vi kalder den **CapaDrivers** !

CapaSystems
...because time matters

CapaSystems A/S
Roskildevej 342C
DK-2630 Taastrup

(+45) 70 10 70 55
sales@capasystems.com