EN LISTIG LØSNING:

Sæt en fælde for hackerne

Hvis din computer rammes af ransomware, bliver dine filer låst og helt ubrugelige. Men med det smarte værktøj Data Sentinel kan du snyde hackerne og sikre dine filer.

Journalist
Niklas Ernst

Normalt er det dig, der går i fælden, når de it-kriminelle og hackerne lægger skumle planer og får dig til at installere malware, virus eller ransomware på din computer. Men med programmet NeuShield Data Sentinel er det i stedet dig, der sætter en fælde op for hackerne.

Grundlæggende beskytter programmet dig mod ransomware, som er den type skadelig software, der kan låse dine filer, og hvor bagmændene efterfølgende opkræver en løsesum for at låse dine filer op, så du igen kan bruge dem. Med Data Sentinel på din computer behøver du dog ikke betale en rød reje, da programmet hjælper dig med at redde dine filer ud af hackernes kraftfulde kryptering. Ja, faktisk redder programmet ikke dine filer, det skjuler dem i stedet, så hackerne tror, at de har fået fingre i dine filer – men i virkeligheden er historien en ganske anden.

Sådan virker programmet

Det fungerer på følgende måde: Du skal forestille dig et stort whiteboard, hvor der står noget tekst. Teksten er dine filer. Forestil dig så, at der bliver lagt en stor glasplade hen over whiteboardet. Glaspladen er usynlig, men skaber dog en barriere. Når nogen prøver at ændre din tekst, ser det ud som om, at de har skrevet oven på den. Men i virkeligheden har de blot skrevet på pladen, som let kan viskes ren. – og under pladen er teksten stadig intakt og præcis som før.

På samme måde laver Data Sentinel et sæt falske versioner af dine filer, som hackerne *tror* er ægte filer, og som de ved hjælp af ransomware krypterer. Men dine rigtige filer går fri, og kan nemt fiskes frem efter et ransomware-angreb, da hackerne og deres ransomware kun har fået fat i de falske lokkemadsfiler. Hackerne får en lang næse – og du får lov at have dine filer i fred og ro.

Kryptering

Når man krypterer data eller kommunikation, gøres indholdet ulæseligt gennem en matematisk metode, der kræver en nøgle (som typisk er et kodeord) for at gøre materialet læseligt igen.

Ransomware

Ransomware er et program, som krypterer og dermed låser dine filer. Derefter vil bagmændene opkræve en løsesum fra dig for at dekryptere filerne, så du kan få adgang til dem igen.

NeuShield Data Sentinel

Pas godt på dine filer og sørg for, at hverken hackere eller it-kriminelle kan få held til at kryptere dem.

Sprog
Engelsk

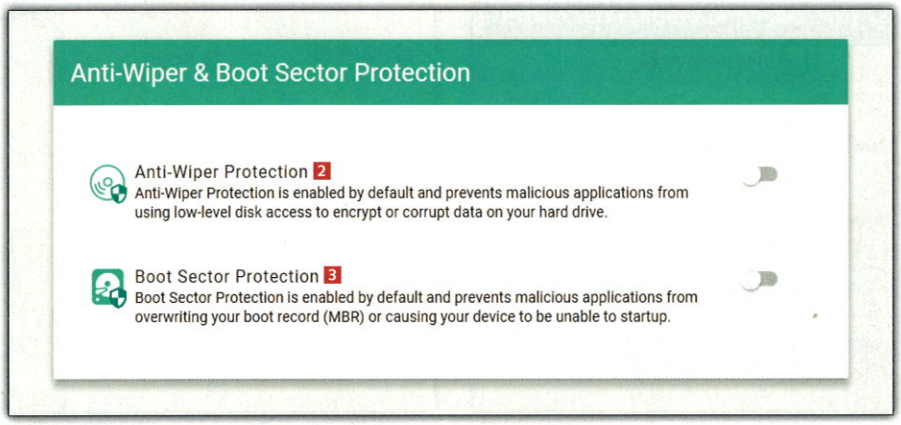
Virker med
Windows 10 og 11

Hent programmet på vores hjemmeside:
komputer.dk/2419

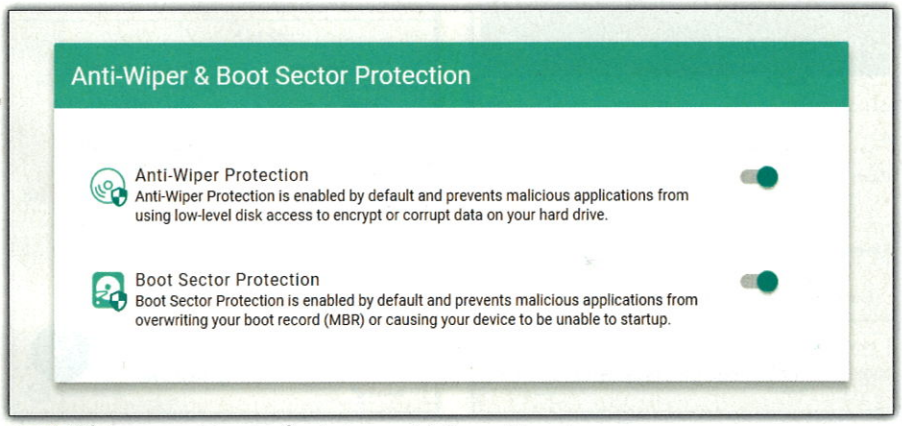
Vælg de bedste indstillinger

For at få NeuShield Data Sentinel til at virke optimalt, så dine filer forbliver sikre, er der et par indstillinger, du skal slå til. Dem gennemgår vi her.

1 Åbn programmet og kig i venstre side. Her skal du klikke på **Anti-Wiperware** 1.



2 Du bliver præsenteret for to begreber: **Anti-Wiper Protection** 2 og **Boot Sector Protection** 3. De to værktøjer gør det ekstra besværligt for hackerne at få adgang til din computer, så dem skal du slå til, hvis de ikke allerede er aktiveret.



3 Sådan ser det ud, når de to værktøjer er blevet aktiveret i programmet. Herefter er du klar til at lære om de andre funktioner i værktøjet.

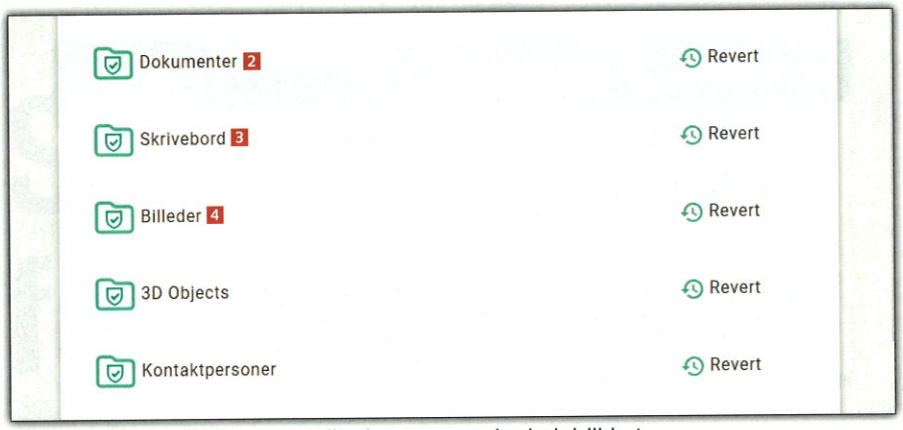
4 Klik til sidst på **Overview** 4 for at gå tilbage til hovedmenuen i programmet.

Foto: Filshyna/Shutterstock.com

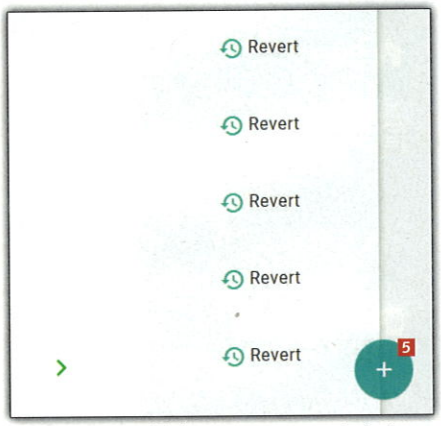
Udpeg de mapper, der skal beskyttes

Du er nu klar til at vælge de mapper, der skal sikres mod ransomware-angreb. Programmet vælger en række mapper som standard, men du kan nemt tilføje flere.

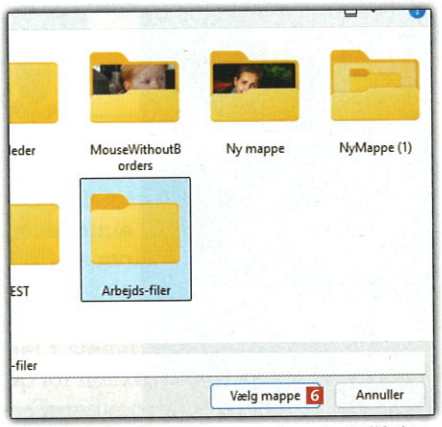
1 Klik på **Anti-Ransomware** 1 i venstre side af programmet.



2 Du får nu en liste over alle de mapper, der i øjeblikket er beskyttet af programmet. Altså her eksempelvis **Dokumenter** 2, **Skrivebord** 3, **Billeder** 4 og så videre.



3 For at tilføje en mappe, skal du klikke på krydset 5 i bunden af programmet.



4 Vælg den mappe, der skal tilføjes til programmet og beskyttes. Klik på **Vælg mappe** 6.

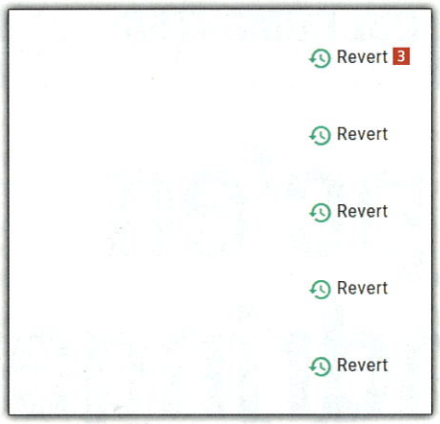
5 Nu er mappen 7 tilføjet til programmet og dermed beskyttet i tilfælde af angreb. Vil du tilføje flere mapper, gentager du blot processen.

Gendan en beskadiget fil

Nu er dine udvalgte mapper og filer beskyttet. Hvis du på et tidspunkt kommer ud for, at en fil bliver låst af ransomware, kan du bruge NeuShield Data Sentinel til at få den tilbage, uanset om filen er låst, ændret eller helt væk.

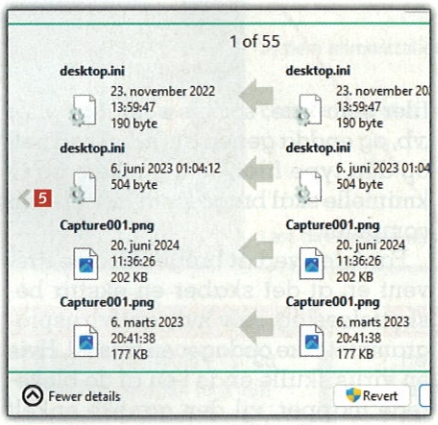
1 Åbn NeuShield Data Sentinel og klik på **Anti-Ransomware** 1 i venstre side af programmet.

2 Identificer så den mappe, som den pågældende fil var gemt i. I dette tilfælde var der tale om en fil i mappen **Dokumenter** 2.

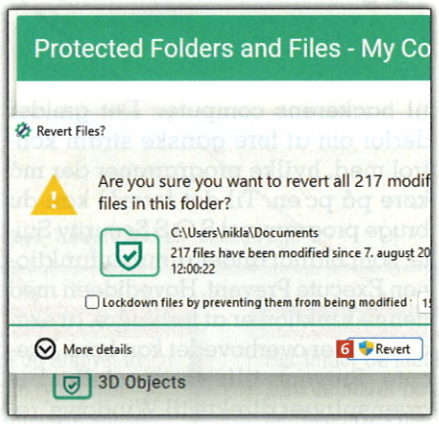


3 Klik på knappen **Revert** 3 ud for mappens navn for at starte processen med at få filen eller filerne tilbage i uskadt tilstand.

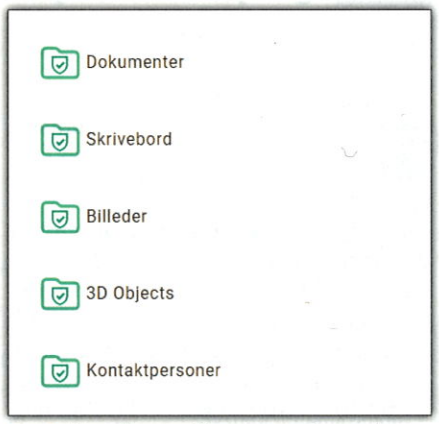
4 I vinduet, der åbner, skal du klikke på **More details** 4 for at få en oversigt over de filer, som kan ændres tilbage.



5 Du kan nu se de filer, hvor der er registreret ændringer. Klik på pilene 5 i siderne for at navigere mellem dem.



6 Klik på **Revert** 6 for at få filerne tilbage i deres oprindelige tilstand fra før ransomware-angrebet. Klik på **Ja** i vinduet, der åbner.



7 Herefter er filerne gendannet, og du kan igen finde dem på de placeringer, hvor de oprindeligt var.