



FOREBYG ONDSINDEDE ANGREB PÅ DIT NETVÆRK:

Gør alt udstyr i hjemmet sikkert

Det er ikke tilstrækkeligt at sikre sin pc og telefon mod angreb fra nettet. Alle enheder, der er forbundet til nettet, kan være i fare. Giv derfor alt udstyret et sikkerhedstjek i dag.



Giv dit hjem et sikkerhedstjek

Har du udstyr, der kan være i risiko for angreb fra nettet? I listen her kan du se eksempler på enheder, du bør sikre.

- **Sonos eller andre smarte højtalere**
- **Netværkskameraer**
- **Printer, der er forbundet til netværket**
- **TV-bokse som Google TV og Apple TV**
- **App-styrede stikkontakter**
- **Smart belysning**
- **Netværksharddiske (NAS)**
- **Smart-TV-apparater**
- **Trådløs router**
- **Gateways til fx gardiner, varmestyring eller lys**
- **Spillekonsoller**
- **Smart dørklokke**
- **Robotstøvsuger**
- **App-styret dørlås**
- **Hårde hvidevarer med indbygget Wi-Fi**
- **Vejrstation med netværksadgang**



Journalist
Henning Rasmussen

Det kan virke helt urimeligt at kassere elektronik, der stadig virker, og som du måske bruger i din hverdag. Men det kan være konsekvensen, hvis udstyret er forbundet til internettet, og det ikke længere modtager vigtige sikkerhedsopdateringer fra producenten.

Farlige sikkerhedshuller

Både sikkerhedseksperter og producenter – men også kriminelle – opdager nemlig løbende nye måder, man kan få uautoriseret adgang til udstyr, der er koblet til netværket i hjemmet. Sårbarhederne bliver ofte rettet ved at producenten udsender en firmware-opdatering til udstyr som smarte afbrydere, netværksharddiske og net-

værkskameraer. Men desværre er det de færreste producenter, der fortsætter med at opdatere usikkert udstyr, når alderen kommer over de fem år.

Måtte kassere dyrt kamera

Det måtte jeg selv sande på den smertelige måde. Jeg havde i mange år tre hundedyre netværkskameraer fra producenten D-Link installeret i mit hjem, og selv om alderen på dem havde passeret 10 år, virkede de fortsat fortrinligt. Men jeg opdagede inde på kameraernes styresider i browseren, at den seneste opdatering fra producenten var syv år gammel. Kriminelle havde med andre ord haft syv år til at finde et sikkerhedshul ved de tusinder af kameraer magen til mine. Derfor valgte jeg med tungt hjerte at kassere kameraerne, selv om de formentlig kunne have fungeret i en år-

række mere. Måske har du også udstyr af ældre dato stående i dit hjem?

Der er flere ting, du selv kan gøre for at sikre hjemmets enheder. Du bør starte med at tjekke, at adgangen til dem er sikret med en god kode, som du selv og ikke producenten har valgt. Derudover kan du sørge for, at der ikke er unødvendige porte åbne i din router, og at alt udstyret er opdateret med den seneste firmware.

Hvis du er i tvivl om, hvilket af dit udstyr i hjemmet, der er forbundet til netværket, kan du starte med at scanne netværket med programmet Advanced IP Scanner. Det afslører alle enheder på netværket, og her kan du også se udstyrets IP-adresse, som du skal bruge til at få adgang til det i din browser. Herefter er du klar til at følge vores enkle vejledninger til at sikre alt udstyret i dit hjem.



Advanced IP Scanner

Programmet scanner hele dit netværk, og viser dig alle de enheder, der er forbundet til netværket.

Sprog
Engelsk

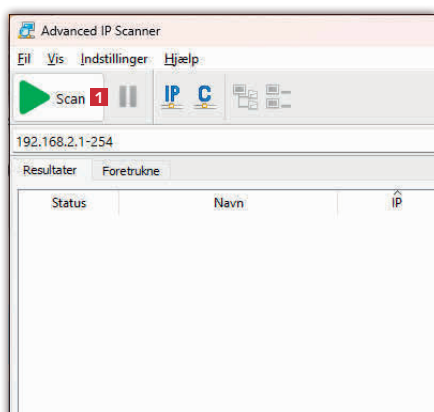
Virker med
Windows 10 og 11

Hent programmet på vores hjemmeside:
komputer.dk/2511

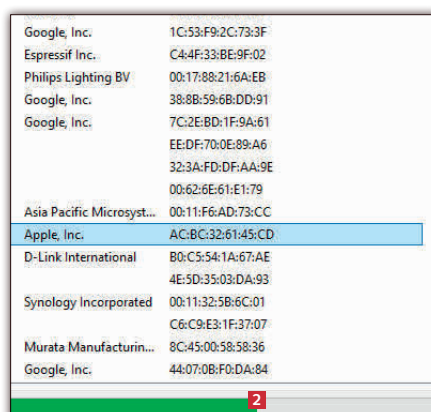


Start med at finde alle enheder på dit hjemmenetværk

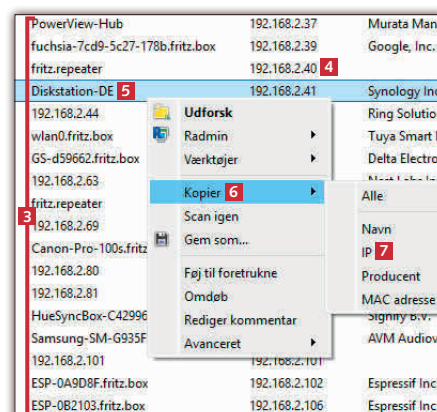
Du har brug for at kende IP-adresserne på dit udstyr, så du kan logge ind og tjekke sikkerheden. Adresserne finder du nemt med Advanced IP Scanner.



1 Hent Advanced IP Scanner på vores hjemmeside, og installer programmet. Når du starter det, skal du klikke på **Scan** **1** øverst til venstre.



2 Vent nu, mens hele netværket scannes igennem. Processen er færdig, når den grønne linje når hele vejen over bunden af vinduet **2**.

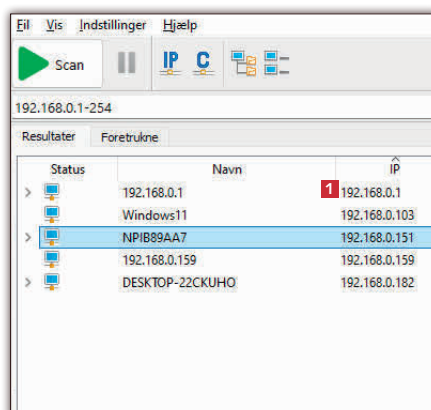


3 Enhederne **3** og deres IP-adresser **4** ses. Højreklik på en enhed **5**, vælg **Kopier** **6**, og **IP** **7**. Sæt adressen ind i browserens adressefelt.

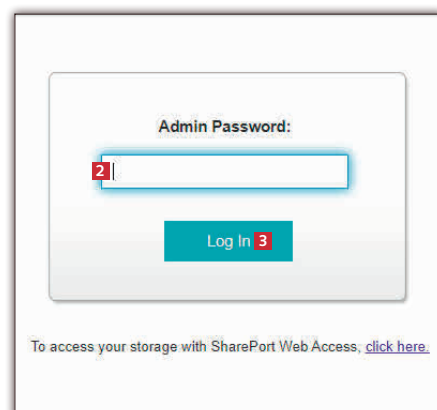


Opdater din router

Din trådløse router er direkte forbundet til internettet, og derfor er det vigtigt, at du sørger for at holde den opdateret med producentens seneste firmware.



1 Åbn Advanced IP Scanner-programmet, og scan pc'en. Øverst i listen over fundne enheder ser du din router og dens IP-adresse **1**. Den skal du bruge i næste trin.

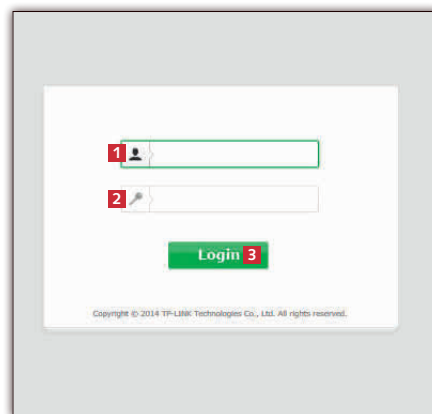


2 Åbn din browser, og indtast din routers adresse i adressefeltet. Tryk på **Enter**. Indtast adgangskoden til din router **2**. Den er valgt af dig selv eller producenten. Klik på **Log In** **3**.

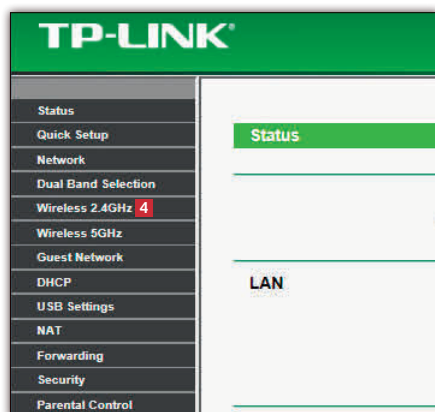


Vælg den stærkeste kryptering

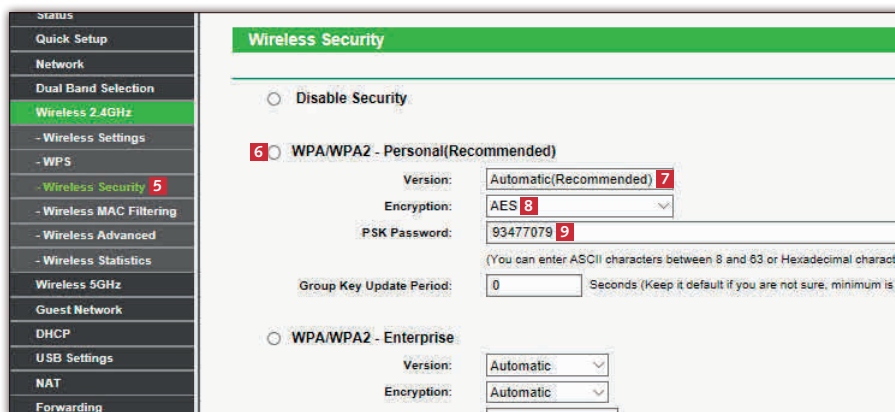
Den trådløse forbindelse mellem dit udstyr og din router er sikret med en kryptering, der findes i forskellige udgaver. Sørg for, at vælge den nyeste og sikreste standard.



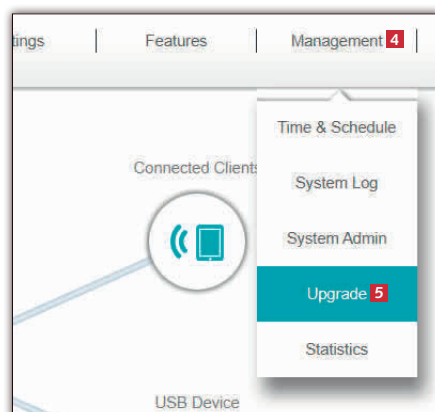
1 Åbn din browser, og indtast adressen til routeren i adressefeltet. Tryk på **Enter**. Indtast brugernavn **1** og adgangskode **2** til routeren (står i manualen). Klik på **Login 3**.



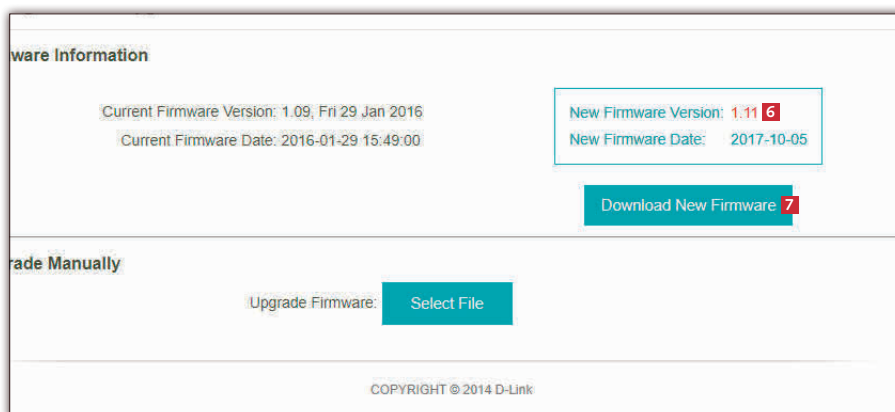
2 Klik på **Wireless 2.4GHz 4** i menuen for at ændre indstillingerne for det trådløse 2,4 GHz-netværk.



3 Klik på **Wireless Security 5**. Markér **WPA/WPA2 Personal 6**, eller WPA3, hvis det er tilgængeligt. Vælg **Automatic 7**, **AES 8**, og skriv en kode, som ikke umiddelbart kan gættes af andre **9**. Klik på **Save**. Nu genstarter din router, og når den kører igen, skal du logge på netværket igen fra alle dine enheder. Gentag processen for dit 5 GHz-netværk.



3 På denne router-model skal man klikke på **Management 4** og vælge **Upgrade 5**. Det kan fx også hedde **Advanced** eller **Firmwareupgrade** på andre modeller.



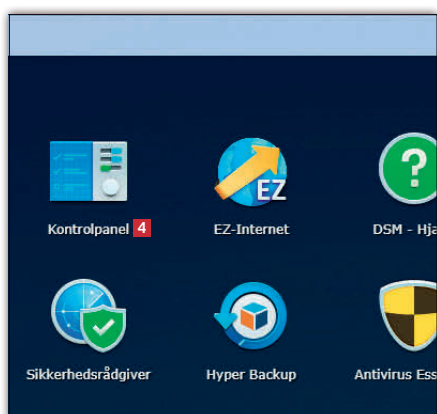
4 Her vil du kunne se, hvis der er en ny udgave af firmwaren til din router **6**. Klik på **Download New Firmware 7** for at hente og installere den. Tjek efter installationen igen, om du har den seneste firmware.



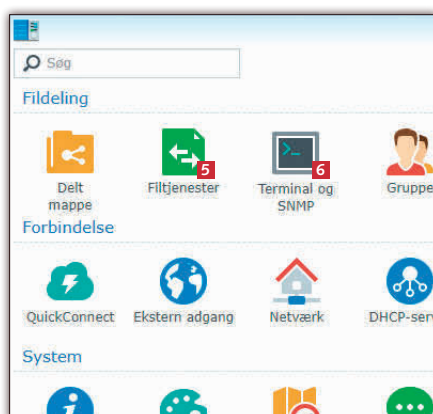


Luk de åbne porte i din NAS

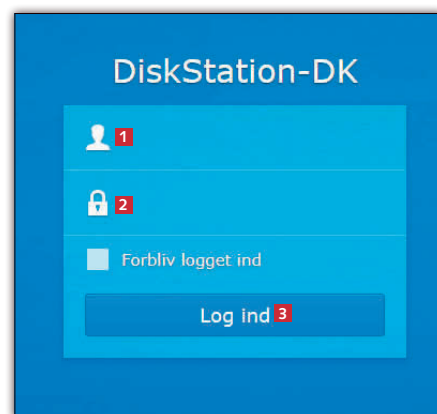
En moderne netværksharddisk (NAS) har masser af funktioner udover lagring af dine filer. Derfor skal du tjekke, om portene til NAS'ens serverfunktioner er lukkede, hvis du ikke bruger mulighederne.



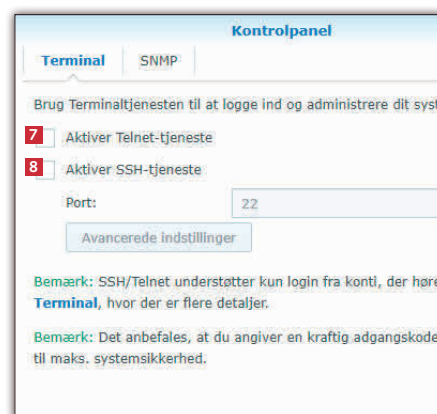
2 Find NAS'ens **Kontrolpanel** **4**. Det vil se forskelligt ud og hedde noget forskelligt afhængig af NAS'ens model og mærke. Her er det Synology.



3 Åbne porte i din NAS kan typisk findes under **Filtjenester** **5** eller **Terminal og SNMP** **6**.



1 Find adressen til din NAS med Advanced IP Scanner. Åbn din browser, og indtast adressen. Tast **Enter**. Indtast dit brugernavn **1** og adgangskode **2**. Klik på **Log ind** **3**.



4 Sørg for at fjerne fluebenene ved **Aktiver Telnet-tjeneste** **7** og **Aktiver SSH-tjeneste** **8**, hvis det ikke er noget, du aktivt bruger. Klik på **Anvend**. Nu er risikoen elimineret.



Gør dine adgangskoder stærkere

Når du køber nyt udstyr, er det som regel sikret med en standardkode fra producenten. Den bør du ændre til en god og stærk kode, som du selv har valgt. Her viser vi hele processen med et IP-kamera.

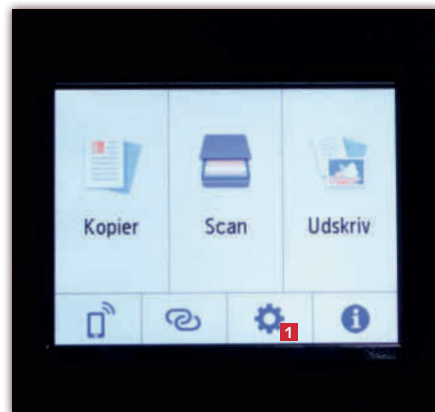


1 Find adressen til dit netværkskamera i Advanced IP Scanner, og indtast det i din browsers adressefelt. Tryk på **Enter**. Indtast brugernavn **1** og kode **2**. Klik på **OK** **3**.



Opdater alt dit udstyr

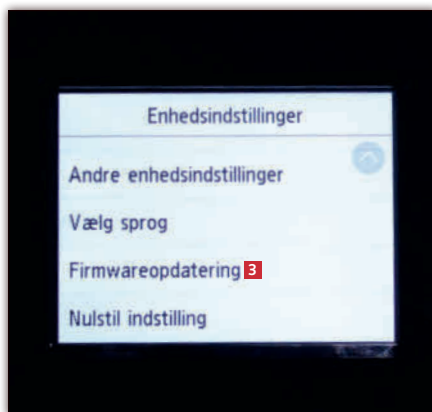
Det er ikke alt udstyr, som automatisk og løbende opdateres af producenten. Derfor bør du selv med jævne mellemrum tjekke, om der er nye opdateringer tilgængelige. Det gælder fx også din printer, hvis den er forbundet til netværket.



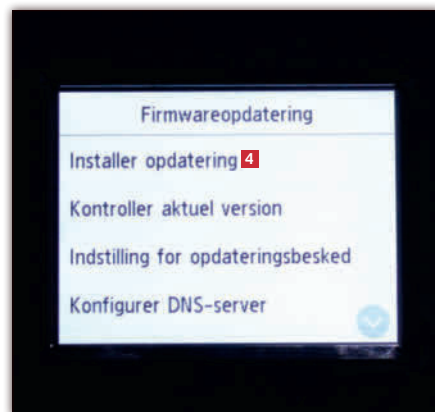
1 På en nyere Canon-printer med trådløs adgang til internettet ser hovedmenuen på printerens lille skærm sådan ud. Her skal du trykke på tandhjulet **1**.



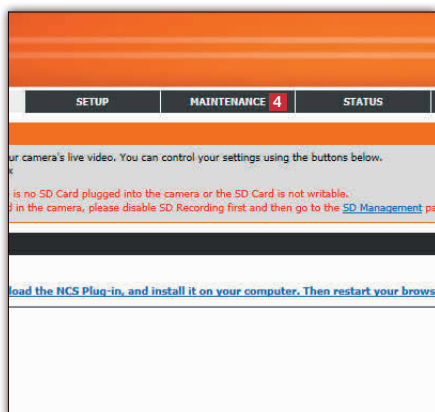
2 Vælg punktet **Enhedsindstillinger** **2**.



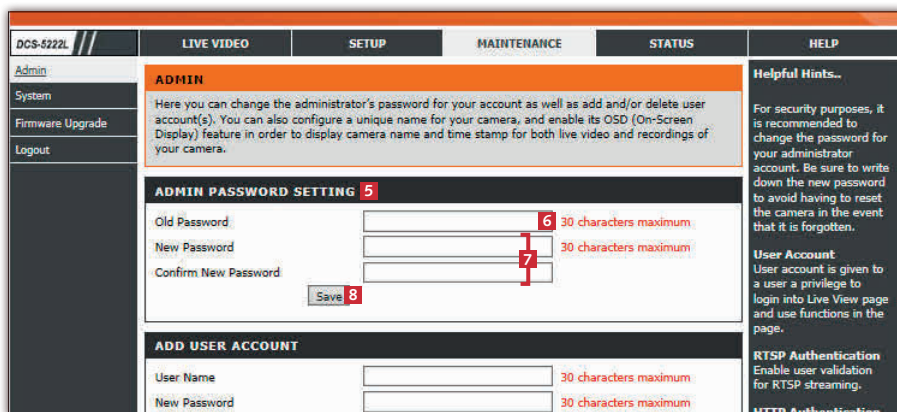
3 Rul ned i bunden af menuen og tryk på **Firmwareopdatering** **3**.



4 Tryk på **Installer opdatering** **4**, og følg nu guiden, der opdaterer din printer med den seneste firmware. Så har du minimeret risikoen for angreb på din printer fra nettet.



2 Her er vi inde på et IP-kamera fra D-Link. Siderne ser forskellige ud fra producent til producent. Ved D-Links udstyr skal man først klikke på **Maintenance** **4**.



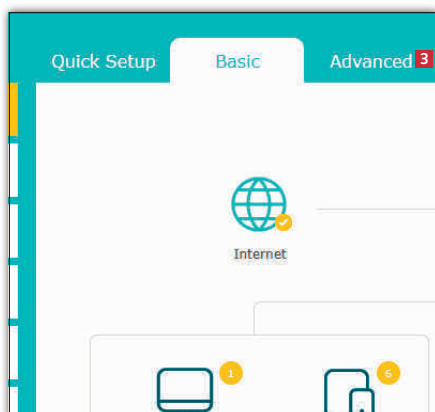
3 Under **Admin password setting** **5** skal du indtaste den gamle adgangskode til udstyret **6**. Skriv derefter den nye kode to gange **7**. Klik på **Save** **8** for at gemme indstillingerne. Nu har du gjort det sværere at bryde ind på dit udstyr.



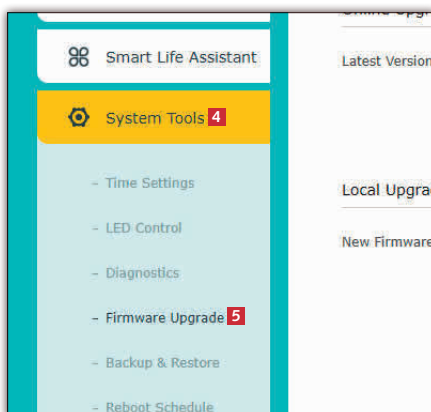


Opdateres dine enheder ikke mere?

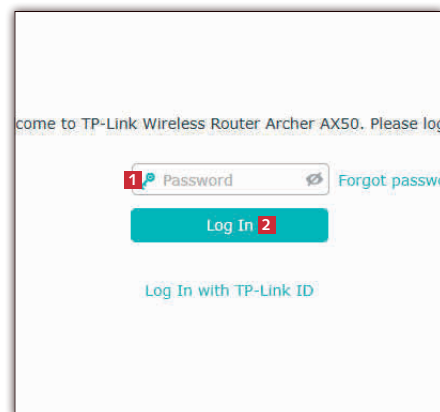
Inde i dine enheders styresider kan du som regel se, hvornår den seneste firmware er installeret. Er det mere end fem år siden, bør du kraftigt overveje at udskifte udstyret for at eliminere risikoen for angreb. Her bruger vi en router fra TP-Link som eksempel.



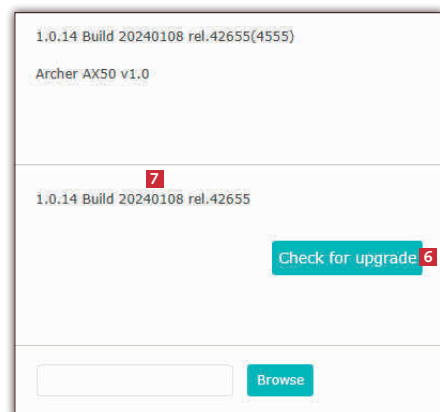
2 På noget udstyr skal du først klikke på **Advanced** **3**, før du kan se detaljer om den installerede firmware.



3 Klik på **System Tools** **4** eller lignende, og vælg **Firmware Upgrade** **5**.



1 Find adressen til udstyret i Advanced IP Scanner – her er det en router. Skriv adressen i browserens adressefelt og tast **Enter**. Skriv koden til udstyret **1** og klik på **Log in** **2**.



4 Klik på **Check for upgrade** **6**. Du kan ofte se datoen for den senest installerede firmware **7**. Er datoen før 2020, er det ikke sandsynligt, at dit udstyr modtager flere opdateringer.

Overvej at kassere ældre udstyr

Det er efterhånden 10-15 år siden, at smarte enheder til blandt andet overvågning og styring af lys og varme begyndte at dukke op, og derfor har meget udstyr i dag nået en alder, hvor producenten ikke længere opdaterer det. Det er måske også tilfældet for de enheder, du har i dit hjem, hvis du har ejet dem i

en årrække. Desværre er mange sårbarheder så dybtliggende, at kun en helt ny firmware fra producenten kan løse det. Derfor opdateres især nyere mærkevaregøj ofte hver gang, der er fundet nye sårbarheder. Anderledes forholder det sig med udstyr af ældre dato eller importerede Kina-produkter. Derfor har du reelt kun to muligheder, hvis nogle af dine enheder ikke længere modtager opdateringer: Du

kan smide udstyret ud og købe noget nyt, eller koble enheden fra dit netværk/internet og bruge den lokalt i hjemmet, hvis det er en mulighed.



Mange netværkskameraer som dette fra D-Link modtager ikke længere firmware-opdateringer. Dermed rettes eventuelle sikkerhedshuller ikke mere.

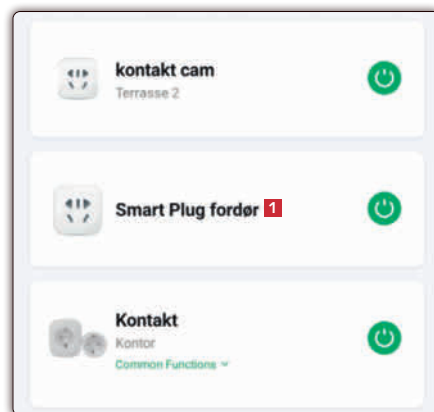


Har du en smart højttaler, kan du opleve, at det for længst er slut med at hente nye sikkerhedsrettelser til den.

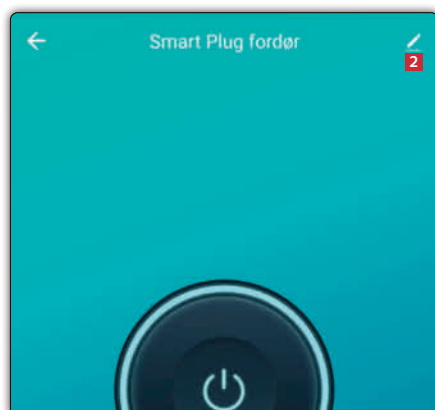


Opdater dit udstyr via en app

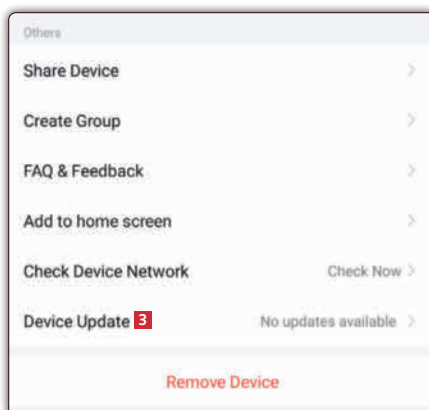
En stor del af det smart home-udstyr, der sælges i dag, kan kun styres fra en app på din telefon. Derfor kan det også være fra denne app, du skal søge efter og installere opdateringer til udstyret.



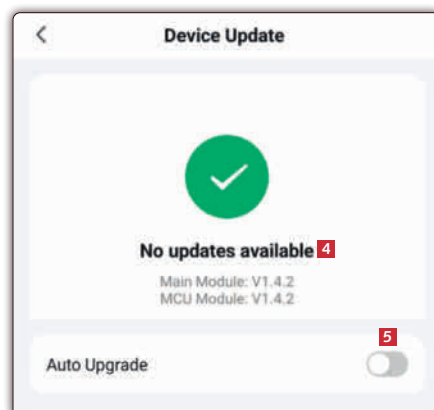
1 Hvis dit udstyr kun kan styres med en app, skal du åbne den tilhørende app. Hvis appen styrer mere end én enhed, skal du trykke ind på den relevante enhed i oversigten **1**.



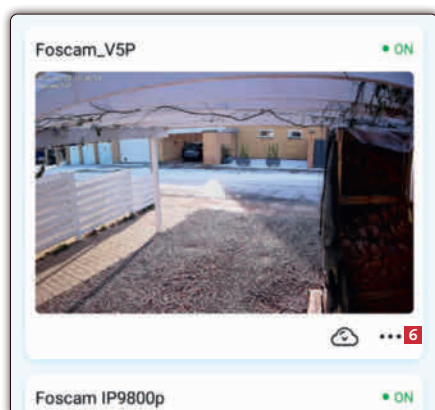
2 Tryk nu videre ind til enhedens indstillinger **2**.



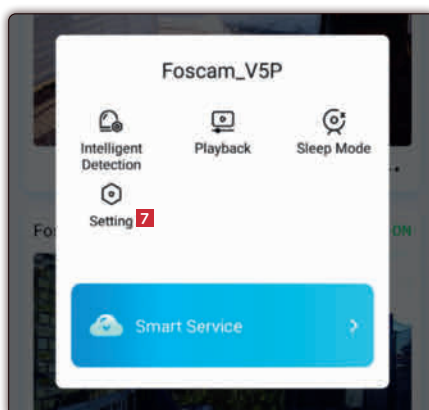
3 Tryk på **Device Update** **3** eller lignende.



4 Her kan du se, om der er nye opdateringer til din enhed **4**. Du kan også ofte markere, at enheden fremover automatisk skal hente nye opdateringer **5**.



5 Hvis dit udstyr er et app-styret netværkskamera, skal du typisk klikke på de tre prikker under kamera-billedet **6**. Her er mærket Foscam.



6 Klik så på **Setting** **7**.



7 Vælg menuen **Firmware Upgrade** **8**. Herfra kan du både opdatere kameraet og tjekke, hvornår den seneste opdatering er installeret.