

A close-up photograph of a red Ethernet cable with a clear plastic RJ45 connector, plugged into a port on a blue network switch. The switch has a yellow label with numbers 6, 7, 8, and 9. In the foreground, there are blurred blue cables and another network port labeled '17'.

SIKRING AF DIT IT UDSTYR PÅ INTERNETTET

En guide fra
Prokumo

”ALTING” ER PÅ NETTET

Utrolig mange af de elektriske apparater der kan købes i dag, og som bruges både privat og til erhverv, er koblet direkte på internettet. Det kan være kameraer, harddiske, badevægten, køleskabet, telefoner, ure og meget andet.

Det kaldes ”Internet of things” og er et moderne begreb, der dækker over, at det ikke længere kun er computere, der er på internettet.

At bygge internetadgang i forbrugerelektronik til hjemmet, giver mange nye muligheder. Det medfører desværre også nye farer mod vores udstyr og ikke mindst privatliv.

Overvågningskameraet kan blive rettet mod os selv, vores informationer kan blive stjålet og kriminelle kan udnytte, at de har en ny mulighed for at få adgang til vores digitale liv og hjem.

Producenterne af elektriske apparater bør selvfølgelig tage ansvar for, at deres udstyr kan sikres godt nok. Det gør de fleste producenter også, men vi kan desværre ikke bare regne

med, at vores nye udstyr leveres med de bedste og mest sikre indstillinger fra fabrikken.

Derfor bliver vi nødt til at tage et personligt ansvar for at sikre den elektronik, vi tager med ind i vores hjem eller virksomhed.

Denne guide giver en række korte råd om, hvad du bør gøre for at beskytte dig selv, dit privatliv eller din forretning imod, at uvedkommende får adgang. Hvis du ikke selv har tid eller lyst til at rode med det, så få nogen til at hjælpe dig med at få det gjort. Alternativet kan være at dit hjem eller din virksomhed står åbent for alle og enhver med internetadgang ude i verden.

De sikreste hilsner

Prokumo

Jan Skinnerup



UDSTYR MED INTERNETADGANG



UDSTYR MED INTERNETADGANG

OVERVÅGNINGS- OG WEBKAMERAER

Kameraovervågning er blevet populært i Danmark. Hvad enten det er i hjemmet for at overvåge børneværelset, beskytte mod indbrudstyre eller holde øje med sommerhuset. Derudover kan der være kameraer installeret i meget af den elektronik, som vi selv tager med ind i hjemmet, såsom fjernsyn og computere.

Når du anskaffer dig overvågningsteknologi medfølger også risikoen for selv at blive overvåget. Udefrakommende kan i visse tilfælde få adgang til at kigge med i hjemmet, hvis dit udstyr ikke er beskyttet tilstrækkeligt. Standardopsætningen, når du køber udstyret, yder sjældent den fornødne beskyttelse.

Overvågning fra andre kan i sig selv være yderst ubehageligt, men det kan desværre også benyttes af indbrudstyre til at se, hvornår du forlader hjemmet. Så har overvågningskameraet pludselig den stik modsatte effekt af, hvad du havde regnet med.

NETVÆRKSHARDDISKE (NAS)

Harddiske til deling af filer i hjemmet og via nettet er blevet vildt populære. De er billige at anskaffe og de er langt hen ad vejen nemme at komme i gang med. Mange bruger NAS-bokse til at opbevare private billeder, dokumenter, musik og film, som så kan tilgås både i hjemmet, og når man er på farten.

Fordi NAS-bokse er så nemme at sætte op bliver de også brugt i mange mindre virksomheder i stedet for en filserver.

Udfordringerne ved NAS-bokse er stort set de samme som ved webkameraer. Man kan som almindelig bruger ikke bare antage, at standard-indstillingerne giver sikkerhed nok. Så undersøg det før hele verden kan se dine private billeder eller læse alle virksomhedens interne dokumenter.



SMART TV

Mange TV er i dag udformet som komplette mediecentre med harddiskoptager, internetadgang, mikrofon, kamera og mulighed for at installere applikationer.

Det giver naturligvis en masse muligheder, men samtidig giver det også mange af de samme udfordringer, som nævnt ovenfor. Der er risiko for sårbarheder, der kan udnyttes af kriminelle til at få adgang til TV'et, dets data, kamera, mikrofon og andre funktioner.

Du er derfor nødt til at tage dine forholdsregler i forbindelse med dit nye, smarte udstyr i hjemmet.

PHILIPS HUE

Smart lys i hjemmet er blevet vældig populært i form af specielt Philips Hue.

Dit Philips Hue lys er ikke som sådan direkte på internettet. Dine pærer kan ikke surfe efter kattevideoer på Facebook.

Men Philips Hue benytter det, der kaldes en bridge (en bro) i deres opsætning. Det er denne bridge, der kommunikerer med dit lys via et alternativt trådløst net, kaldet ZigBee.

Kommunikationen foregår altså ikke over dit normale trådløse net.

Selvom kommunikationen mellem bridge og dit Philips Hue lys er krypteret, så kan ZigBee nettet og enhederne derpå godt hackes. Det betyder at din nabo, eller andre i nærheden, vil kunne tænde og slukke for dit lys. Måske ikke en katastrofe som sådan, men dog alligevel ret irriterende.

Det skal dog nævnes, at muligheden for at du bliver hacket via dit ZigBee net er mindre end chancen for, at nogen kan hacke sig ind på dit normale trådløse net. Begge dele kræver også, at hackeren er i fysisk nærhed af dit netværk.





SECURE CLOUD NETWORK

TAG DINE FORHOLDSREGLER



TAG DINE FORHOLDSREGLER

SKIFT DIT KODEORD

Når du får nyt udstyr har det som regel enten et blankt eller et foruddefineret standard password. F.eks. en "admin" bruger med password "1234". Disse standard passwords fremgår af producentens brugervejledninger, og de er derfor meget nemme at finde frem til på nettet, hvis ikke man bare kan gætte sig til dem.

Med andre ord, så er dit nye udstyr på ingen måde reelt beskyttet når du modtager det. Vi anbefaler på det kraftigste, at du skifter password med det samme, når du installerer nyt udstyr.

Et godt password skal være på 12-16 tegn eller mere, så det er svært at gætte. Har du brug for inspiration til et godt password, så læs eventuelt mit [blogindlæg](#) om passwordsikkerhed eller søg på nettet. Der findes masser af gode guides til hvordan du laver et godt og sikkert password, som samtidigt er nemt at huske.

HOLD DIT UDSTYR OPDATERET

Dit nye udstyr kan indeholde sårbarheder, der kan udnyttes af uvedkommende. Sårbarhederne kan f.eks. gøre, at man kan tilgå dit udstyr, selv om du har fulgt rådet ovenfor og ændret dit kodeord.

Check regelmæssigt efter opdateringer til dit udstyr på leverandørens hjemmeside. I mange tilfælde har udstyret en funktion til at tjekke for opdateringer direkte fra producenten. Du finder denne funktion der hvor du typisk konfigurerer dit udstyr. Hvis du er rigtig heldig, så har dit udstyr endda muligheden for at tjekke for opdateringer, og automatisk selv installere dem regelmæssigt. Så bliver det ikke nemmere. Hvis dit udstyr har en sådan funktion, så slå den til.

Især hvad angår Philips Hue, så er der ikke noget password du kan opdatere, og der er ikke nogen sikkerhedsindstillinger, som du kan slå til eller fra. Her gælder det om at få installeret de opdateringer der kommer fra Philips.

BENYT EN FIREWALL

Langt de fleste moderne internet-routere, som du får fra din teleudbyder, indeholder en firewall. Den sikrer, at uvedkommende ikke kan få adgang til dit netværk.

Du skal sikre dig, at der er lukket for alt uvedkommende trafik, med mindre du specifikt ønsker at have noget åbent udefra. Det bliver hurtigt teknisk når man roder med en firewall. Er du i tvivl, så læs manualen, få hjælp fra nogen du kender eller kontakt din teleudbyder for vejledning.

Stort set alle routere/firewalls der sælges til private kommer som standard konfigureret således, at der er lukket for uvedkommende trafik udefra. Men køber du en større og mere avanceret model – typisk til brug i din virksomhed – så kan du på ingen måde regne med, at den er konfigureret på forhånd. Så skal du selv i gang med at sikre dig, at alting er som du vil have det.

DEAKTIVER DET DU IKKE BRUGER

Rigtigt meget udstyr har langt flere funktioner end der bruges eller er behov for. De funktioner du ikke bruger bør du deaktivere. Det kan f.eks. være FTP funktionen i din NAS.

Funktioner der er deaktiveret minimerer risikoen for utilsigtet overvågning i hjemmet eller, at fremmede får adgang til dine private dokumenter.

Jeg anbefaler derfor, at du slår overvågnings- og betjeningsfunktioner fra, som du ikke behøver. Alternativt, hvis du er lavpraktisk, kan du sætte et stykke tape over de kameraer, du ikke har behov for. Det er en nem og billig løsning, og umulig at hacke udefra.

DEAKTIVER UPnP

En del udstyr med internetadgang understøtter UPnP (Universal Plug And Play). UPnP er lavet for at udstyr meget nemt kan forbinde sig uden at du som forbruger skal have en masse teknisk viden. Det er utrolig nemt at bruge, men det er det også for dem, som har lyssky formål.

Jeg anbefaler derfor kraftigt, at du slår UPnP fra i dit udstyr, hvis du ikke specifikt har behov for det. Ellers risikerer du nemt, at der pludselig er åbne porte i din internet-router, således udstyret kan tilgås udefra.

OPSUMMERING

Vi er således kommet frem til afslutningen og de tre keypoints du skal tage med fra denne guide er:

- Sørg for at have sikre passwords.
- Sørg for at holde dit udstyr opdateret.
- Overvej hvilke funktioner du rent faktisk vil bruge, og luk ned for resten.

Garanteret alt sammen noget, du har hørt før. Jeg håber du med denne guide har fået en reminder om, at få det gjort. De evigt tilbagevendende avisforsider med danskere, der har fået deres privatliv "invaderet" af fremmede vidner om, at

der stadig er rigtig mange, som netop ikke får gjort disse ting. Lad det ikke være dig, der bliver den næste artikel i Ekstrabladet. ☺

Tak fordi du har downloadet min guide. Vil du vide mere så kig endelig forbi min blog på www.prokumo.dk/blog/ og følg gerne med på de sociale medier for mere inspiration:



Om Prokumo

Prokumo er den lille virksomheds IT afdeling. Vi hjælper små virksomheder med at udnytte de mange muligheder der eksisterer med cloud computing. Samtidig slipper I for at skulle bøvle med det tekniske. Prokumo tager hånd om begge dele.

Spørgsmål eller forslag til denne guide kan rettes til info@prokumo.dk

