# IP-adresser og brug i Danmark
# for Advokatgruppen.dk

| | |
|---|---|
| Kunde: | Advokat Dan M. Dahl Rahimian fra Advokatgruppen.dk |
| Forfatter: | Henrik Lund Kramshøj |
| Version | 1.0 |
| Dato: | 2019-08-29 |
| Dokument id: | 2019082201 |
| Fortrolighedsniveau: | Offentligt - Uklassificeret |

# Indhold

# Revision History

| Revision | Date | Author(s) | Description |
|---|---|---|---|
| 1.0-create | 2019-08-10 | HLK | Oprettet |
| 1.0 | 2019-08-29 | HLK | Kunde version |

Dette projekt udført af Zencurity ApS i perioden August 2019.

## Fortrolighedsniveau

Dette projekt er klassificeret som: Offentligt - Uklassificeret

Rapporten kan frit bruges af kunden, og udleveres til andre.

## Copyright

# Kapitel 1

# Indledning

Dette dokument er oprindeligt skrevet af cand.scient Henrik Lund Kramshøj, hlk@zencurity.com direktør og ejer af Zencurity ApS . Dokumentet er oprettet i sommeren 2019 og foreligger nu i en foreløbig første version.

Dokumentet er tiltænkt brug hos advokater i retsager i Danmark og indeholder informationer om internet-termer som IP-adresse, router, protokoller m.v. Projektet er foregået i samarbejde med Dan M. Dahl Rahimian fra Advokagruppen.dk

Beskrivelsen tager udgangspunkt i mangeårig og detaljeret baggrundsviden om hvordan internet og it-sikkerhed indenfor samme fungerer.

Alle må komme med input til dette dokument og det er hermed publiceret under en åben licens. Licensen tillader deling og videre forarbejdning af dokumentet kommercielt og ikke-kommercielt efter licenstypen, BSD 3-Clause License.

Primær kontakt for dette dokument er Henrik Lund Kramshøj .

## Om Zencurity ApS

Zencurity ApS er et mindre IT-sikkerhedsfirma med kunder i Danmark, Europa og andre steder. Typiske kunder er mellemstore til store virksomheder med erkendt behov for rådgivning indenfor IT-sikkerhedsområdet.

Typiske opgaver for Zencurity ApS er:

- Opbygning af IT infrastruktur, netværk, routere, firewalls
- Sikkerhedsrådgivning indenfor internet og netværksteknologier
- Sikkerhedstest herunder pentest, DDoS test, gennemgang af kode og aktiv test

- Undervisning og foredragsvirksomhed
- Tilslutning af virksomheder til internet gennem registrering af internetadresser, indkøb af internetforbindelser, indkøb og konfiguration af hardware

Firmaet ejes og drives af Henrik Lund Kramshøj og er videreførelse af egen virksomhed siden 2003.

Firmaet er medlem hos RIPE NCC som LIR, dk.zencurity og driver blandt andet eget netværk med AS nummer AS57860.

## Forfatterens baggrund

Mit navn er Henrik Lund Kramshøj, uddannet cand.scient fra Datalogisk Institut ved Københavns Universitet (DIKU). Jeg har siden start 1990erne arbejdet med internetteknologier og opnået ekspertviden indenfor netværk og it-sikkerhed.

Jeg er certificeret CISSP siden 2003 og tidligere haft certificeringer som CEH, Juniper Service Provider Routing and Switching, Specialist (JNCIS-SP) (udløb 2019) m.fl.

Jeg har arbejdet professionelt med it-sikkerhed og netværk siden midt 1990erne.

# Kapitel 2

# Konklusion

Emnet for dette dokument er at beskrive IP-adresser og udvalgte emner omkring routersikkerhed, trådløs sikkerhed og malware i forbindelse med private forbrugeres niveau af samme.

Indenfor dette emne er der nogle konklusioner:

- Emnet IT-sikkerhed er komplekst og private forbrugere ønsker ikke at beskæftige sig med emnet
- Udstyr der udleveres af internetudbydere til brug hos private er af en ringe kvalitet sikkerhedsmæssigt og det er sandsynligt at der er kendte og ukendte sikkerhedshuller som kan udnyttes af kriminelle
- Computere som benyttes af private er i høj grad ofte utidssvarende, ikke opdaterede, inficeret med malware i variende grad og må betragtes som værende usikre. Dette inkluderer bærbare computere, tablets, telefoner samt internetopkoblede enheder som kameraer, smart TV, smarte højtalere (Internet of Things) mv.
- Sikring af netværk kræver dyb teknisk indsigt og ved undervisning gennem mere end 15 år primært til IT-professionelle er det tydeligt at selv blandt disse er der meget få som har det fulde overblik over IT-sikkerhed og viden om at opretholde et højt sikkerhedsniveau

Når sikkerheden således hos forbrugere generelt er ringe skal man være varsom med at stole for meget på data der peger på en bestemt internetforbindelse som oprindelse for bestemte typer trafik.

Selv professionelle IT-brugere har svært ved at designe og implementere sikre netværk med professionelt udstyr, og har ligeledes problemer med sikring af enheder der tilsluttes.

Derfor vil professionelle IT-sikkerhedsfolk være vidende om at angreb, spam, og andre typer skadelig trafik ofte er iværksat af andre end ejere af enheder, og forbindelser.

# Kapitel 3

# Internet

Internet er allestedsnærværende og mange danskere har idag smart phones og andre enheder som benytter internet mange gange dagligt.

Ordets oprindelse findes i internetworking, som er en beskrivelse af den logiske opbygning, kommunikation mellem netværk. Et internet er således et netværk af netværk. Det store verdensomspændende Internet skrives indimellem med stort forbogstav for at skelne mellem et generelt internet og Internet.

Det specielle ved Internet er at ingen entitet ejer dette. Internet kan ses som et løst samarbejde mellem netværksoperatører som på tværs af landegrænser. Ud fra relativt simple kontrakter aftales samarbejde om at overholde visse spilleregler. Primært aftales at der udveksles og videresendes traffik på lige fod, også kaldet netneutralitet. Dette område gennemgås ikke.

Der er derfor ingen enkelt organisation som kontrollerer internet, kan lukke for dele, eller tvinge deltagende netværk til at følge bestemte regler.

På dette Internet benyttes TCP/IP som er forkortelse for IP-protokollerne, som er standarder for pakkebaseret elektronisk kommunikation som deltagende netværk forventes at overholde. Forkortelsen indeholder ligeledes en af de mest benyttede, TCP. Denne protokol benyttes blandt andet til email, browsing og andre formål. På de laveste niveauer, tæt på hardware sendes data som pakker, der kan sammenlignes med postkort. De sendes med modtager og afsender, og overholder et simpelt format.

Der kan læses mere om disse protokoller på eksempelvis Wikipedia:
`https://en.wikipedia.org/wiki/Internet_protocol_suite`

# Kapitel 4

# IP-adresser

Et centralt koncept i Internetkommunikation er at der kommunikeres mellem IP-adresser. Ligesom en telefonsamtale mellem to personer er der oftes kommunikation mellem to computere, ofte kaldes klient og server.

Når klienten skal kommunikere med servere ved brug af TCP/IP benyttes IP-adresse som endepunktet for kommunikationen.

Konkret er IP-adresser et 32-bit tal, som har en værdi mellem 1 og 4294967296, men som oftest skrives de som oktetter med punktum imellem. Disse tal bestyres af internetorganisationer som RIPE NCC
`https://www.ripe.net/`. RIPE NCC er den Regional Internet Registry (RIR) for Danmark, der er 5 sådanne som dækker adresserne for hele verden. De andre er: AfriNIC, LACNIC, APNIC og ARIN.

Eksempler på IP-adreser er

- 127.0.0.1 en speciel adresse som findes på alle computere. Det tillader eksempelvis webudvikling på en lokal bærbar computer hvor klient og server er på samme adresse
- 192.168.1.1 en meget brugt privat IP-adresse hos forbrugere. Den lokale router som skaber adgang til internet har denne adresse. Klienter indenfor netværket har derefter adresser som 192.168.1.10, 192.168.1.123.
- 192.0.2.1 - 192.0.2.255 er specielle adresser som kan benyttes til dokumentation. Det anbefales at man altid og udelukkende benytter sådanne *documentation prefixes* når man skriver eksempler i generelle dokumenter. Specielt bør man ikke blot tage en adresse tilfældigt da man derved kan komme til at pege på en organisation som idag benytter disse adresser på Internet.

Private og offentlige adresser er to begreber som bruges om IP-adresser. En offentlig IP-adresse kan bruges på Internet, hvor netværksoperatører sørger for at pakker med en offentlig modtageradresse fremsendes i retning af netværksdestinationen.

En pakke vil typisk krydse flere netværk, mindst to, men oftere 3-5 og indimellem op til 10 - uden at der er en øvre grænse.

I de netværk der sendes fra og de netværk der modtages vil man ofte benytte en oversættelse mellem de offentlige IP-adresser og interne - private - adresser. De private adresser benyttes grundet en generel mangel på IP-adresser.

En analogi for offentlige og private IP-adresser kan være telefoncentraler med lokalnumre. Indenfor et hus kan ringes med kort lokalnummer, men skal der ringes ud af huset sker det med vores sædvanlige 8-cifrede telefonnumre.

Det bemærkes at kommunikation på internet udelukkende benytter IP-adresserne til kommunikationen. Protokoller i lag ovenfor som eksempelvis HTTP der benytes til hjemmesider skal derfor have oversat navne til IP-adresser inden kommunikationen kan begynde.

En klient der vil besøge en hjemmeside skal altså slå adresser op i en telefonbog, som i internetsammenhæng er Domain Name System (DNS). Denne service tillader opslag fra navne som www.example.com til adresser som 192.0.2.100.

En internet kommunikation kan således opsummeret foregå på følgende måde:

En bruger der vil besøge Folketingets hjemmeside http://www.ft.dk vil forårsage følgende, opsummeret og forsimplet:

1. Indtastningen af adressen **www.ft.dk** i en browser
2. Klientens software beder om adressen bagved navnet www.ft.dk hos en navneserver lokalt, enten på samme computer eller hos internetudbyderen
3. Navneserversoftware vil gennem en rekursiv process finde informationer om andre navneserver i dette hierarki .dk, ft.dk og til sidst vil der blive forspurgt på navnet www.ft.dk
4. Svaret på dette opslag sendes til klienten, www.ft.dk har addressen **152.115.53.69**
5. Web browseren vil åbne en TCP forbindelse mellem egen adresse eksempelvis 192.168.1.22 ud til hjemmesiden på adressen 152.115.53.69. Derved sendes data gennem den lokale router 192.168.1.1
6. Hjemmesiden modtages i et antal IP-pakker og vises på skærmen

Bemærkninger. Da klienten har en privat adresse som ikke kan benyttes på Internet vil den lokale router erstatte afsenderadressen med sin egen offentlige adresse. Det kunne være 185.129.62.2 Denne process kaldes for Network Adress Translation (NAT) og benyttes af langt de fleste internetudbydere i Danmark.

Uddelingen af IPv4 adresser har nået et omfang så der nu er ikke er flere offentlige adresser og de sidste ressourcer bestyres meget restriktivt.

Det gør at forbrugere idag oplever at deres router i hjemme har private adresser og kun kan tilgå internet gennem NAT løsningen hos udbydere. De såkaldte Carrier Grade NAT. I sådanne løsninger deler tusindvis af forbrugere samme offentlige adresser.

Disse delte løsninger skaber problemer for efterforskning og der kan eksempelvis læses mere om dette emne hos Europol:

https://www.europol.europa.eu/newsroom/news/are-you-sharing-same-ip-address-criminal-law-enforcement-call-for-end

En tilsvarende dansk artikel kan findes på Version2.dk / Ingeniøren

https://www.version2.dk/artikel/europol-carrier-grade-nat-giver-massive-efterforskningsmaessige-problemer-968396

# Kapitel 5

# IP-adresse opsummeret

1. Hvad er en IP-adresse. En IP-adresse er et nummer som bruges som afsender og modtager på IP-pakker, data der sendes over Internet. Det skrives oftest med punktum eksempelvis som 192.0.2.1. Al kommunikation på internet er mellem IP-adresse. Navne oversættes til IP-adresser med navnesystemet (Domain Name System (DNS).

2. Hvad kan udledes af en IP-adresse. IP-adresser registreres centralt og tildeles til brugere af internetudbydere. Dette sker via 5 Regional Internet Registries (RIRs). Ud fra en IP-adresse kan man i Whois databaser slå op hvilket netværk der har lov til at benytte denne.

NB: Der foregår ofte afsendelse af data med forfalskede afsenderadresser, eksempelvis ifb DDoS angreb. De data der kan slås op i Whois systemet indeholder bl.a: netværksnavnet, kontaktinformationer på organisationen, herunder hjemmehørende land.

Eksempel på opslag

```
inetnum:        185.129.60.0 - 185.129.60.255
netname:        SERVICE-NET2
descr:          Various Zencurity internal and public facing services
country:        DK
admin-c:        HK5541-RIPE
tech-c:         HK5541-RIPE
status:         ASSIGNED PA
mnt-by:         dk-zencurity-1-mnt
created:        2018-10-17T07:33:20Z
last-modified:  2018-10-17T07:33:20Z
source:         RIPE
```

3. Vil man kunne se hvilket elektronisk udstyr, hvilken person eller hvor dette geografisk har befundet sig. Mange data om computere og internet er flygtige, og det vil sjældent være muligt efterfølgende at finde informationerne og udtale konkrete konklusioner. Hvis man under en efterforskning straks slår op vil det være muligt med nogen usikkerhed at sige hvilken vej gennem netværk der er benyttet. Hvis man har rådata vil man indimellem kunne udtale mere konkret hvilken type operativsystem eller producent der formentlig er benyttet.

4. Hvad vil man reelt kunne udlede af programmer som opsnapper IP-adresser i P2P netværk. I torrentsammenhæng virker protokollerne ved at klienterne fortæller at de tilbyder data - filer - til netværket. Disse informationer skal andre klienter modtage og det vil derfor være en indikation at der er en torrentklient som er villig til at udsende de data. Såfremt man kun opsamler trackinginformationen vil det ikke være givet at data findes, kun ved en opsamling af data - download - eller dele af data vil det være muligt at konkludere hvilke data der var tilgængelige.

5. Hvad ville ske, hvis en person som har et P2P program på computeren og enten bevidst/ubevidst logger på en internetforbindelse Hvis man har et P2P program installeret og forbinder til et netværk vil programmet begynde at kommunikere med delingsnetværket. Dette sker på samme måde som emailprogrammer der med mellemrum checker for ny post, programmer der spørger efter opdateringer, hjemmesider der forbinder til servere i baggrunden, chatfunktioner som melder sig online osv.

6. Hvordan foregår delingen i et P2P netværk?. Peer-to-peer er et begreb man benytter om kommunikation mellem klienter, hvor disse også fungerer som servere. Et peer-to-peer program kan således kommunikere med et andet af samme type, og både sende og modtage data. Metoden er mere effektiv end centraliseret server arkitektur, idet en central server med data kun kan understøtte et vist antal klienter, hvor en peer-to-peer arkitektur skalerer med antallet af klienter der tilbyder data.

En af de mest populære teknologier indenfor peer-to-peer er BitTorrent som benytter en tracker struktur. Denne tracker er en server som assisterer klienterne i at finde hinanden og de ønskede data. Klienter som vil downloade vil således først kommunikere deres eksistens til trackeren, og der få viden om andre klienter - hvorefter kommunikationen og data går direkte mellem klienterne.

Kilder `https://en.wikipedia.org/wiki/Peer-to-peer` `https://en.wikipedia.org/wiki/BitTorrent` `https://en.wikipedia.org/wiki/BitTorrent_tracker`

7. Hvad er Swarmsize, se kolonne P i vedlagte pdf bilag 7.

Swarm er et begreb der bruges om de peers der indgår i delingen af en bestemt torrent, en eller flere filer. Hvis der således er 10 klienter som har dele af data, eller er ved at hente data, vil swarm size være 10. NB: processen med deling af data via torrent er meget dynamisk og dette tal vil derfor være behæftet med en vis usikkerhed.

# Kapitel 6

# Wifi-forbindelse

De fleste private i Danmark har idag håndholdte enheder og bærbare computere der forbinder til Internet via trådløse teknologier, populært kaldet Wi-Fi.

Når vi som privatforbrugere har en internetforbindelse, så åbnes således en vej for os til Internet. Desværre åbnes ofte også adgang til vores hjem og vores interne netværk.

Vores forbindelse er baseret på en hjemmerouter, ofte kaldet CPE-router for Customer Premises Equipment. Denne er typisk udstyret med trådløst internet og forbinder vores hjem med internetudbydere.

Sikkerheden på trådløse netværk hos private er typisk en af følgende

* Ingen sikkerhed, åbent trådløst netværk. Dette ses også hos mange konferencecentre, barer, cafeer m.fl. Det er ikke i Danmark ulovligt at have et åbent netværk som andre kan benytte. * WEP En ældre krypteringsstandard som betragtes som værende usikker. Den kan brydes i praksis på sekunder og anbefales derfor ikke. * WPA og WPA2 Personal. Krypteringsmetoder hvor der benyttes et kodeord til det trådløse netværk. Koden er ofte tildelt af internetudbyderen, men kan ændres og bliver det ofte for at lette adgangen til netværket for familie og venner. Det anbefales at benytte den opdaterede WPA version 2.

Hos virksomheder vil en mere avanceret WPA Enterprise benyttes som giver individuel autentificering.

1. Hvordan er mulighederne for at bryde et kodeord for en WIFI forbindelse med WPA2? Sikkerheden afhænger primært af kodeordets styrke, så et kortere kodeord vil være nemmere at knække. De kodeord som genereres af internetudbydere er idag ofte omkring 10 tegn, men kun bogstaver og tal - for at undgå en større supportbyrde. De kodeord som indtastes af privatpersoner må antages at være af ringere kvalitet.

Samtidig skiftes WPA kodeord yderst sjældent og der vil derfor typisk være adgang i længere tid, måneder til år, såfremt et kodeord gættes.

Der findes værktøjer som benytter grafikkort til at forsøge at knække WPA koder, og disse vil

2. Er du bekendt med nogle sikkerhedsbrister for WPA2?

Der har været akademiske problemer i WPA2, men det mest praktiske angreb er til teknologien Wi-Fi Protected Setup (WPS) som benyttes til at lette adgang for brugerne til netværket. Teknologien blev introduceret omkring 2006 og er idag stadig aktiv mange steder, grundet manglende opdatering af software på hjemmeroutere.

Denne teknologi har haft alvorlige sikkerhedsbrister som gør at WPA koden til netværket kunne findes på 4-10 timer såfremt denne teknologi er aktiveret. Idag indeholder routersoftware ofte tiltag der forsinker angrebet, men det er stadig muligt - idet antallet af forsøg på tilkobling *kun er ca. 11.000 forsøg*

Et værktøj til at udnytte dette hedder Reaver og kan benyttes af enhver med meget lidt træning.

Eksempel artikel `https://www.pwnieexpress.com/blog/wps-cracking-with-reaver`

3. Hvordan vil en privatperson kunne beskytte sig fuldstændig mod uautoriseret adgang til ens WIFI forbindelse? En privatperson vil have svært ved at beskytte imod uautoriseret adgang, idet beskyttelsen ofte vil kræve højere vidensniveau og kontinuerlig overvågning.

Samtidig benyttes trådløse netværk ofte af andre, herunder gæster.

Koden til netværket er ofte angivet under routeren, så blot kort tid vil give mulighed for at aflæse denne.

Koder er samtidig gemt på enheder som kan være udsat for hacking. Mange koder som internetbrugere er ligeledes lækket på Internet i store databaser. Se yderligere kapitel 7

4. Hvor langt væk vil du vurdere en standard router vil kunne tilgås fra? Jeg vil vurdere at en standard router ville kunne nås fra en afstand af mindst 50-100m med en god retningsbestemt antenne.

De fysiske forhold gør at dette er behæftet med stor usikkerhed. I et villaområdet med enkeltfamilienhuse vil det kunne være over 100m, mens etageejendomme med mange trådløse netværk gør det besværligere at kommunikere med et af disse over større afstand.

I en etageejendom vil det derfor ofte være nemmere at få signal fra en genbo som kan ses fra altanen, end to etager over eller under.

Den trådløse forbindelse kan således som beskrevet i dette kapitel være en mulighed for at fremmede kan gøre brug af vores forbindelse.

Opsummeret er IT-sikkerheden på trådløse netværk i vores hjem altså svag, typisk grundet en af følgende årsager:

- Ingen kode på trådløse internet. Det er lovligt at dele internet, og det er indimellem standardindstilling for enheder
- Dårlige koder, private vælger ofte almindelige ord eller korte koder som en angriber vil kunne knække

- Dårlige standarder, som eksempelvis Wi-Fi Protected Setup (WPS) - en fejlbehæftet funktion som en angriber kan bruge til at skaffe sig adgang til netværket. Denne kan ofte ikke slåes fra.
- Ældre standard som Wired Equivalent Privacy (WEP) - ligesom WPS er denne utilstrækkelig til at sikre et moderne netværk. På visse enheder kan WPS og WEP funktioner slåes fra, men det er ikke noget en almindelig privatforbruger forventes at kunne gøre.

Kilder til mere information: `https://en.wikipedia.org/wiki/Wi-Fi`

# Kapitel 7

# Hacking af computere

Der er også andre måder at få tilgang til IP-adresse og et netværk på.

Private forbrugere har ofte ikke styr på IT-sikkerhed. Det er et komplekst emne som selv virksomheder i Danmark stadig kæmper med. Emnet omtales ofte som malware, virus og orme.

1. Vil du beskrive hvad Malware er, herunder hvordan man kan få dem? Malware står for malicious software og er software med skadelig logik.

Definitionen nedenfor er fra bogen *Computer Security: Art and Science*, Matt Bishop ISBN: 9780321712332:

**Definition 23-1** *Malicious logic*, more commonly called *malware*, is a set of instructions that cause a site's security policy to be violated.

**Definition 23-2** A *Trojan horse* is a program with an overt (documented or known) purpose and a covert (undocumented or unexpected) purpose.

Malware kan inficere en brugers computer gennem websider og browsere, via email med links, via dokumenter som makrovirus og andre filer - eksempelvis MP3 afspillere og USB drev.

Det er meget almindeligt at private computere er inficeret med malware. Det drejer sig om eksempelis 114.000 inficeret af en type i 2014,
`https://www.computerworld.dk/art/229672/saa-mange-danske-maskiner-er-fanget-i-et-botnet`

Det bemærkes at netop den manglende sikkerhed på computere hos private er årsagen til indførelse af NemID baseret på *papkortet*.

2. Vil du beskrive hvad et router angreb er?

Routerangreb er når ydersiden af netværket - routeren som skaber forbindelse til internet angribes. Disse har typisk kendte sikkerhedsfejl og generelt dårlig software. Kriminelle kan således angribe disse enheder og efterfølgende tilgå det interne netværk, eller sende skadelig trafik til internet - herunder DDoS angreb og spam.

3. Vil du beskrive om der findes andre måder, at kunne få adgang til at benytte IP-adressen? (Malware og router angreb)

Udover at bryde ind i routeren er der mange enheder som tilbyder funktioner til at åbne forbindelser. En af disse er UPnProxy som giver angribere mulighed for at benytte andres internetforbindelser.

Når denne type funktion misbruges vil det se ud som om trafikken kommer fra forbrugerens enhed, men reelt er det en proxy funktion der blot videresender via denne forbindelse.

`https://www.akamai.com/us/en/multimedia/documents/white-paper/upnproxy-blackhat-proxies-via-nat-injections-white-p`
`pdf`

Billede fra samme paper:


Figure 16: APT groups use UPnProxy chains to hide their origin

4. Hvor sandsygt vil du sige det er, at almindelige private har computere, som er inficerede af Malware?

Det er meget sandsynligt at private computere som har været brugt til almindelig hjemmebrug har skadelig software. Mange private benytter enten ingen eller gratis anti-malware software til beskyttelse, som er utilstrækkelig.

5. Findes der nogen statistikker på hvor mange computere som enten er eller potentielt kan være inficeret af malware eller lignende?

Der er jævnligt statistikker for bestemte *familier* af malware som har inficeret mellem 100.000s og millionvis af computere.

# Kapitel 8

# Router sikkerhed

Når man køber adgang til internet leveres typisk til privatbrugere en router-enhed. Denne enhed benytter udbyderens valgte teknologi, ADSL kobber, Fiber eller coax-antennekabel.

Disse enheder forbindes til internet men er i mange tilfælde ikke sikre. Enhederne skal være billige på grund af stor konkurrence mellem udbydere, og kunderne vil ikke betale en høj oprettelsespris.

Derfor er kvaliteten ikke god nok. Værre endnu kommer der ofte ingen opdateringer, og eventuelle opdateringer lægges ikke automatisk på enhederne.

De nyeste tal og statistikker fra en undersøgelse publiceret i august 2019 fortæller at set over 15 år har kvaliteten været for nedadgående.

> A survey of more than 6,000 firmware images spanning more than a decade finds no improvement in firmware security and lax security standards for the software running connected devices by Linksys, Netgear and other major vendors.*

`https://securityledger.com/2019/08/huge-survey-of-firmware-finds-no-security-gains-in-15-years/`

Det betyder at kriminelle har næsten uhindret adgang til 100.000-vis af router-enheder over hele verden.

Eksempelvis kunne et botnet, Mirai botnet fra 2016 inficere omkring 900.000 enheder hos Deutsche Telekom.
`https://en.wikipedia.org/wiki/Mirai_(malware)`

Almindelige forbrugere har ikke selv mulighed for at beskytte sig, og må forlade sig på den sikkerhed som udbyderen har valgt - ved valg af enhederne.

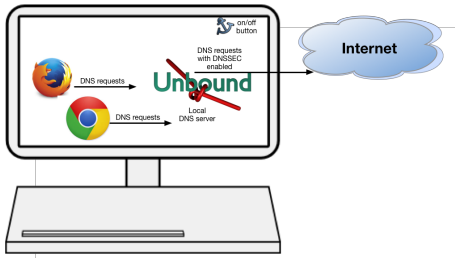
Kilder:
`https://the-parallax.com/2019/01/24/wi-fi-router-security-worse-citl-shmoocon/`

# Kapitel 9

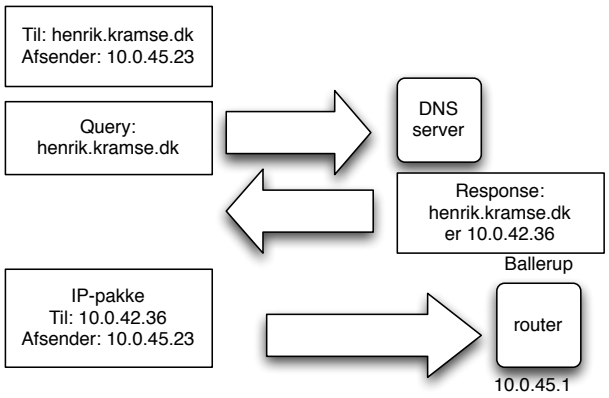
# DNS Eksempel

Et eksempel på Domain Name Service (DNS) opslag vises nedenfor.

Hvis en bruger sidder med en computer og vil tilgå en hjemmeside sker det oftest ved brug af en browser. Det kunne være Firefox eller Chrome som vist på tegningen:




Når der indtastes et navn, eksempelvis `henrik.kramse.dk` vil DNS på klienten forespørge:




I dette eksempel bruges således navnet `henrik.kramse.dk` og via DNS findes addressen `10.0.42.36`

Når dette er sket vil en browser som Firefox eller Chrome kunne tilgå den pågældende hjemmeside.