

IT-sikkerhed: Security headers

Indholdsfortegnelse

1. Problemstilling	2
2. Problemformulering.....	2
3. Metodeovervejelser og metodevalg.....	3
4. Definitioner	3
4.1 Definition af Security headers.....	3
4.2 Definitioner af seks specifikke Security headers.....	4
5. Analyse	4
5.1 Implementeringsart og -omfang	4
5.1.1 Mest besøgte danske hjemmesider	4
5.1.2 Mest besøgte hjemmesider globalt set	8
5.2 Grunde til implementeringsart og -omfang.....	9
6. Konklusion.....	11
7. Litteraturliste	13
7.1 URL'er.....	13
8. Bilag.....	14
8.1 Bilag 1: De 50 hjemmesider, der er mest besøgt af danske brugere.....	14
8.2 Bilag 2: Oversigt over implementeringen af Security headers på de af danske brugere mest besøgte danske hjemmesider og et udpluk af øvrige danske hjemmesider pr. d. 26. marts 2020..	16
8.3 Bilag 3: Virksomheders svar på 3 spørgsmål om implementering af Security Headers	17
8.3.1 Virksomhed 1 (karakter: D)	17
8.3.2 Virksomhed 2 (karakter: D)	17
8.3.3 Virksomhed 3 (karakter: D).....	18
8.3.4 Virksomhed 4 (karakter: D)	18

IT-sikkerhed: Security headers

1. Problemstilling

Internettet vokser ekstremt hurtigt. Antallet af brugere er steget hvert år siden 1995, ligesom trafikken, mængden af udvekslet data, også er det. I dag er antallet af brugere over 4,5 milliarder¹, og trafikken krydsede allerede i 2017 de 100.000 PB (petabyte)².

I takt med det stigende antal brugere øges mængden af potentielle ondsindede hackere, det vil sige mennesker, der finder anerkendelse, ernærer eller morer sig ved at bryde ind i andre menneskers eller virksomheders computere og eksempelvis stjæle deres personlige oplysninger eller data i det hele taget og dernæst eventuelt afpresse dem økonomisk. Mængden af mennesker og virksomheder, der kan angribes, vokser selvfølgelig også, og ikke mindst vokser selve angrebsfladen, mængden af data, forbindelser og så videre, som en hacker kunne have interesse i at forstyrre, ødelægge eller opsnappe. Da computeren og mobiltelefonen i dag er hvermandseje, er både den enkelte bruger, virksomhederne og samfundet som samlet størrelse konstant i fare for at blive udsat for cyberangreb. Behovet for IT-sikkerhed, behovet for et stærkt forsvar, vokser dermed i samme grad, og her tænkes altså ikke blot på samfundet og virksomhederne og deres digitale infrastruktur og data, men bestemt også på den enkelte bruger og dennes data.

Ét af de mange steder, en virksomhed kan gøre en indsats for brugerens sikkerhed, er på virksomhedens hjemmeside. Her kan virksomheden forholdsvis overkommeligt iværksætte en række brugerbeskyttende forsvarsmekanismer, nemlig de såkaldte 'Security headers' (SH). På trods af overkommeligheden ved at implementere de fleste SH, så kan man ved et par stikprøver online hurtigt konstatere, at langt fra alle virksomheder har gjort det. Dette giver anledning til følgende spørgsmål: Hvordan forholder graden af SH-implementeringen sig? Hvorfor tager én virksomhed ansvaret på sig, mens en anden ikke gør? Har det noget med prioriteringer, holdninger, kunnen eller virksomhedens størrelse at gøre?

2. Problemformulering

De i problemstillingen gennemgåede overvejelser resulterer i følgende problemformulering:

- Der ønskes en undersøgelse af, hvad Security headers er samt undersøgelser af, hvorledes og i hvilket omfang Security headers er implementeret på nogle af de mest besøgte danske

¹ <https://www.internetworldstats.com/emarketing.htm>

² https://en.wikipedia.org/wiki/Internet_traffic

hjemmesider henholdsvis på de mest besøgte hjemmesider globalt set. Med udgangspunkt i undersøgelserne ønskes dernæst bud på, hvorfor arten og graden af implementeringerne er, som de er, og hvilken betydning dette har for online-sikkerhed generelt set.

Med 'arten' menes 'hvilke Security headers', og med 'graden' menes 'i hvilket omfang'.

3. Metodeovervejelser og metodevalg

Omfanget af et kort individuelt projekt kan ikke forventes at danne grundlag for nye, videnskabelige resultater med stor rækkevidde. De mange valg, der ligger til grund for problemformuleringen, herunder især valget af begreberne 'undersøgelse' og 'bud', afspejler dette.

Udformingen af problemformuleringen, besvarelsen af den, herunder udvalget af virksohmeder og forespørgslernes indhold (se afsnit 5.2), er tilpasset projektets omfang, og den valgte metode kan tilnærmelsesvist betegnes 'kvantitativ' i forhold til den danske del af implementeringsspørgsmålet (se afsnit 5.1.1) og 'kvalitativ' i forhold til virksohmhedsforespørgslerne (se afsnit 5.2).

4. Definitioner

4.1 Definition af Security headers

Når man indtaster en URL i sin computers browser og trykker enter, så sendes en forespørgsel (en request) af sted. URL'en hjælper requesten med at finde frem til den rigtige server, og serveren sender et svar (en response) tilbage. Svaret består af en HTTP Statuskode, en mængde server/response headers, en tom linje og en message body bestående af den ønskede data. Drejer det sig om en almindelig hjemmeside, vil den ønskede data bestå i en mængde HTML-, CSS- og JavaScript-kode, som browseren så bruger til at opbygge den pågældende hjemmeside med.

De fra serveren tilsendte headers står for at definere, hvordan transaktionen skal foregå, andre for at øge performance, og så er der de såkaldte Security headers, som nu defineres:

- Security headers er den delmængde af server/response headers, der giver klientsoftwaren, det vil sige eksempelvis en browser, og dermed brugeren et ekstra lag beskyttelse på særligt sårbare områder.

4.2 Definitioner af seks specifikke Security headers

IT-sikkerhedskonsulenten Scott Helme har lavet et værktøj til at tjekke implementeringen af Security headers (SH) på en hvilken som helst hjemmeside³. Værktøjet tjekker implementeringen af seks SH, som han har udvalgt på grund af det høje beskyttelsesniveau, de ifølge ham giver. Af hensyn til empirimængden har jeg valgt at benytte værktøjet i de videre undersøgelser, hvorfor de seks SH's funktioner nu gennemgås:

- Strict-Transport-Security (betegnes også HSTS, som står for HTTP Strict-Transport-Security): Sørger for, at browseren altid forbinder via HTTPS og aldrig HTTP. Den ukrypterede HTTP-forbindelse ønskes ikke, da al request- og responsdata ellers i teorien vil kunne ses af alle.
- Content-Security-Policy: Laver en slags firewall i browseren ved at fastsætte, hvilke domains HTML-dokumentet må indlæse scripts fra. Skulle det lykkes en hacker at requeste et script, der falder udenfor de tilladte, så vil browseren afvise at indlæse det.
- X-Frame-Options: Angiver om browseren har tilladelse til at gengive en side i et frame- eller iframe-tag. Dermed kan clickjacking-angreb udført via frame-teknik forhindres.
- X-Content-Type-Options: Forhindrer browseren i at tillade indhold, der er noget andet, end det giver sig ud for at være. Med andre ord forhindres browseren i selv at forsøge at regne ud, hvordan den skal behandle forskellige filtyper. Dermed forhindres sniffing-angreb, hvor en hacker eksempelvis uploader en ondsindet Java-Script-fil, der giver sig ud for at være et billede, som browseren så kører som det script, det rent faktisk er.
- Referrer-Policy: Begrænser mængden af data, der deles via URL'er, ved at fastsætte, hvor meget af URL'en, der skal medsendes, når brugeren klikker på forskellige links.
- Feature-Policy: Bruges til at justere browserens forskellige indbyggede egenskaber. Eksempelvis kan man slukke for alle de funktionaliteter, man alligevel ikke har tænkt sig at bruge på siden og dermed undgå de mulige sårbarheder, de indbefatter.

5. Analyse

5.1 Implementeringsart og -omfang

5.1.1 Mest besøgte danske hjemmesider

På hjemmesiden SimilarWeb⁴ kan man se en oversigt over de 50 hjemmesider, der får flest besøg af brugere globalt set eller fra et udvalgt land. Vælges Danmark, fremkommer listen, der fremgår af

³ <http://www.securityheaders.com>

⁴ <https://www.similarweb.com/top-websites> - opdateret pr. 1. februar 2020

bilag 1. 26 af hjemmesiderne er egentligt danske, det vil sige henvendt specifikt til danskere, hvorfor netop deres brug af Security headers (SH) undersøges. Derudover undersøges yderligere 35 danske hjemmesider i mere tilfældige stikprøve-repræsenterende nedslag, så eksempelvis også hospitaler, uddannelsesinstitutioner og lægehuses brug af SH bliver belyst. Resultatet af denne undersøgelse fremgår af tabellen i bilag 2, der både figurerer i det egentlige bilag længere fremme og som vedhæftet excel-fil. I bilaget er de 26 hjemmesider fra listen over de 50 mest besøgte hjemmesider i Danmark markeret med *, og med de derudover 35 danske hjemmesider er der i alt 61 hjemmesider i tabellen. På følgende side vises en tilskåret del af bilaget.

Gruppe	Ejer/navn	Strict-Transport-Security	Content-Security-Policy	X-Frame-Options	X-Content-Type-Options	Referrer-Policy	Feature-Policy	Antal headers	Grade
Store virksomheder	Arla	1		1	1	1		4	B
	LEGO	1			1			2	D
	Danfoss			1	1			2	D
	Ørsted			1				1	D
	Mærsk		1	1				2	D
	Bestseller							0	F
	Grundfos							0	F
	Coop							0	F
Banker	Danske Bank*	1	1	1	1	1	1	6	A
	Sydbank	1	1		1	1		4	A
	Jyske bank	1	1		1	1		4	A
	Sparekassen Sjælland	1	1		1	1		4	A
	Nordea*	1		1	1			3	C
	Vestjysk Bank	1		1	1			3	C
	Saxo Bank	1		1				2	D
	Sparekassen Vestsjælland	1			1			2	D
	Lån og Spar	1			1			2	D
	Jutlander Bank	1						1	D
	Coop Bank							0	F
Nyheds-medier	DR*	1		1				2	D
	Ekstra Bladet*	1						1	D
	BT*	1						1	D
	Berlingske*	1						1	D
	Jyllands-Posten*	1			1			2	D
	Se og Hør*				1			1	D
	bold.dk*			1				1	D
	Politiken*							0	F
	TV2*							0	F
	Børsen							0	F
Rejse-selskaber	Albatros Travel	1		1	1			3	C
	Sun Tours	1						1	D
	Adventure Holidays							0	F
	Aarhus Charter							0	F
	Africa Tours							0	F
Kommuner	Københavns Kommune		1	1	1	1	1	5	A
	Aarhus Kommune			1	1	1		3	C
	Tjander Kommune	1		1	1			3	C
	Odense Kommune							0	F
	Haderslev Kommune							0	F
	Aalborg Kommune							0	F
	Kolding Kommune							0	F
Diverse	borger.dk*	1	1	1	1			4	A
	Viaplay*	1	1	1	1			4	A
	Dokk1	1		1	1			3	C
	DBA*	1		1	1			3	C
	Bilbasen*	1		1	1			3	C
	Elgiganten*	1						1	D
	Jobnet*		1	1				2	D
	Boligsiden*			1				1	D
	Danske Spil*	1		1				2	D
	Yousee*	1						1	D
	e-boks*			1				1	D
	Aarhus Universitet				1			1	D
	Aarhus Universitetshospital				1	1		2	D
	Besøg lægen			1				1	D
	Nemlog-in*							0	F
	Gyldendal*							0	F
	Pricerunner*							0	F
	Krak*							0	F
	Lectio*							0	F
	Trøjborg Lægehus							0	F
I alt		28	9	24	24	8	2	95	
Gennemsnit (header/hjemmeside)		46%	15%	39%	39%	13%	3%	26%	D

Resultaterne er fremkommet ved brug af værktøjet på www.securityheaders.com.

*Blandt de 50 mest besøgte danske hjemmesider. Blandt de 50 mest besøgte danske hjemmesider er derudover zalando.dk og unilogin.dk.

Værktøjet på www.securityheaders.com timede ud i forsøget på at kontakte de to sider.

Figur 1: Udsnit af bilag 2: "Oversigt over implementeringen af Security headers på de af danske brugere mest besøgte danske hjemmesider og et udpluk af øvrige danske hjemmesider pr. 26. marts 2020".

Oversigten viser mange bemærkelsesværdige forhold:

- 95 SH er i alt implementeret på de 61 hjemmesider, hvilket resulterer i en gennemsnitlig implementeringsgrad på: 1,6 SH/side (95 SH/61 sider)
- De 6 SH er hver især implementeret i følgende andele på de 61 hjemmesider:

Strict-Transport-Security:	46%	(28/61 sider)
X-Frame-Options:	39%	(24/61 sider)
X-Content-Type-Options:	39%	(24/61 sider)
Content-Security-Policy:	15%	(9/61 sider)
Referrer-Policy:	13%	(8/61 sider)
Feature-Policy:	3%	(2/61 sider)
- Fordelingen blandt de 61 hjemmesiders karakterer ser således ud:

A-hjemmesider (4-6 SH):	11%	(7/61 sider)
B/C-hjemmesider (3-4 SH):	15%	(9/61 sider)
D/E-hjemmesider (1-2 SH):	41%	(25/61 sider)
F-hjemmesider (0 SH):	33%	(20/61 sider)
- Fordelingen blandt de 26 mest besøgte danske hjemmesiders karakterer ser således ud:

A-hjemmesider (4-6 SH):	12%	(3/26 sider)
B/C-hjemmesider (3-4 SH):	12%	(3/26 sider)
D/E-hjemmesider (1-2 SH):	50%	(13/26 sider)
F-hjemmesider (0 SH):	27%	(7/26 sider)
- Bedste karakter til et nyhedsmedie er D (2 SH).
- Størstedelen af bankerne har 3 SH eller færre. Bundskraberen er Coop Bank med 0 SH.
- Bestseller, Grundfos, Coop, Coop Bank, Politiken, TV2, Børsen, Gyldendal, Pricerunner, Krak, Lectio, over halvdelen af kommunerne og over halvdelen af rejseselskaberne har 0 SH.

5.1.2 Mest besøgte hjemmesider globalt set

Hvor der på det specifikt danske område ikke foreligger undersøgelser af brugen af SH, så er det modsatte tilfældet på det globale område. Buchanan, Helme og Woodward udgav i 2017 artiklen "Analysis of the adoption of security headers in HTTP"⁵, og Lavrenovs og Melón udgav i 2018 artiklen "HTTP Security Headers - Analysis of Top One Million Websites"⁶. I begge artikler præsenteres analyser af SH-implementeringen på de 1.000.000 mest besøgte hjemmesider. Derudover medtages som empiri webudvikleren Andrew Betts' forelæsning under begivenheden Øredev 2018⁷, hvor han går i dybden med SH og fremviser tal fra sine egne undersøgelser, ligeledes af de 1.000.000 mest besøgte hjemmesider. Artiklerne betegnes efterfølgende 'BHW' og 'LM', mens forelæsningen betegnes 'B'.

I første omgang har jeg samlet tallene fra de tre kilders undersøgelser (kilderne er angivet i parenteser):

Security header / År	2015 (BHW)	2017 (BHW)	2018 (LM)	2018 (B)
Strict-Transport-Security	1,2%	5,4%	17,5%	11,0%
Content-Security-Policy	0,2%	1,6%	1,6%	2,9%
X-Frame-Options	5,9%	11,1%	-	22,7%
X-Content-Type-Options	4,8%	10,6%	-	-
Referrer-Policy	-	-	-	2,4%
Feature-Policy	-	-	-	0,001%

Figur 2: Tabel over udviklingen i Security header-implementering på de 1.000.000 mest besøgte hjemmesider

Udover at LM-kildens resultater ikke virker ligeså troværdige som de øvrige, så bemærkes følgende: Implementeringen af alle seks SH er stiger langsomt, der var i 2018 stadig meget langt op til tilfredsstillende andele, og Content-Security-Policy, Referrer-Policy og Feature-Policy har exceptionelt lave implementeringsgrader.

De øvrige interessante betragtninger i de to artikler gennemgås nu. I BHW fremhæves forsigtigt, at udviklingen i implementeringen af de tre øverste SH i tabellen virker lovende⁸, men at de stadig ikke er implementeret på mange topsider⁹. Bekymrende er det dog, at "The vast majority of sites scored an F grade on the securityheaders.io scan."¹⁰

I LM fremføres, at HTTPS-hjemmesider generelt har flere SH end HTTP-hjemmesider¹¹.

⁵ Buchanan, Helme, Woodward (2017)

⁶ Lavrenovs, Melón (2018)

⁷ https://www.youtube.com/watch?v=x_FxJxKIXI8

⁸ Buchanan, Helme, Woodward (2017): s. 6

⁹ ibid.: s. 1

¹⁰ ibid.: s. 5

¹¹ Lavrenovs, Melón (2018): s. 367

Eksempelvis er Content-Security-Policy implementeret på 1,6% af alle siderne, mens tallet isoleret set er 3,4% for HTTPS-hjemmesider og 0,4% for HTTP-hjemmesider¹². Derudover har man fundet, at meget populære hjemmesider generelt har flere SH end mindre populære hjemmesider¹³. I LM konkluderes, at implementeringen af SH stadig er lav og på et utilfredsstillende niveau, men at den er steget siden 2017¹⁴.

5.2 Grunde til implementeringsart og -omfang

For at fremkomme med bud på grunde til implementeringsart og -omfang af SH, har jeg konstrueret følgende tre spørgsmål:

1. Er I opmærksomme på security headers?
2. Hvor vigtige er security headers ifølge jer?
3. Hvorfor er security headers implementeret i det omfang, de er hos jer?

Spørgsmålene er blevet sendt til 20 danske virksomheder af meget forskellige størrelser.

Virksomhederne holdes anonyme. Fire virksomheder har svaret, og alle svarene samt efterfølgende korrespondancer fremgår af bilag 3. Opsummerende svarer de fire virksomheder således:

- Virksomhed 1 (karakter: D): Størstedelen af SH virker irrelevante for os. Vi har blot implementeret dem, der har relevans for os. Egentlig er det dog kun HSTS, der er vigtig, som vi bruger til at skabe hurtigere forbindelse for brugeren, når vi kræver HTTPS.
- Virksomhed 2 (karakter: D): Vi er meget opmærksomme på sikkerhed, da vi har ansvaret for vores kunders data. Vi scorer lavt på securityheaders.com, da vores hjemmeside er bygget i vores egen CMS (Content Management System), hvormed en sådan test ikke siger noget om vores sikkerhed. Ingen hacker er nogensinde kommet ind i hverken backend eller frontend af vores produkter.
- Virksomhed 3 (karakter: D): Vi er opmærksomme på SH og implementerer dem i stigende grad, men vi har mange andre ting, der prioriteres højere.
- Virksomhed 4 (karakter: D): Vi er opmærksomme på SH, men et eksternt bureau har ansvaret for det.

Flere mulige grunde kan konstrueres på baggrund af svarene, men ikke uden en vis fortolkningsfrihed, og derudover er der mange mulige fejlkilder: Var det personen med ansvaret for

¹² ibid.: s. 368

¹³ ibid.: s. 367

¹⁴ ibid.

lige præcis det område, der svarede? Hvad implicerer det, når en person siger, at "noget virker irrelevant for os"? - Kan man deraf udlede, at virksomheden ikke bekymrer sig om kunden (brugeren), eller at visse SH i praksis ingen forskel gør for hverken virksomheden eller kunden? Følgende fortolkninger skal altså tages med et vist forbehold.

Hos virksomhed 1 er der tilsyneladende tale om mangel på viden og ekspertise ("virker irrelevante"), og måske også en ligegyldighed overfor kundens (brugers) sikkerhed. Virksomhed 2 går mere op i sikkerhed, men virksomhed 2's udsagn rejser først og fremmest tvivl om vigtigheden af SH: En bestemt header giver selvfølgelig en bestemt beskyttelse, men måske kan samme beskyttelse være iværksat på andre måder? Virksomhed 3 har ligeledes stort fokus på sikkerhed og arbejder aktivt med SH men finder mange andre sikkerhedsaspekter vigtigere. Virksomhed 4 tager ikke selv ansvar for sikkerheden på deres hjemmeside.

Inden buddene summeres op, skal tidligere omtalte Betts, Lavrenovs og Melón atter bringes på banen. De to sidstnævnte anfører, at der kan være en sammenhæng mellem en virksomheds størrelse og implementeringsgraden¹⁵. Betts giver i løbet af sin Øredev 2018-forelæsning (omtalt i afsnit 5.1.2) mange eksempler på manglende ekspertise (eller lemfældighed) fra hjemmesideindehavernes side i forhold til response headers i det hele taget: Headeren P3P er implementeret på mange hjemmesider men er aldrig blevet valideret og har dermed ingen funktion¹⁶. 64% af de undersøgte hjemmesider har både Expires og Cache Control, men Expires ignoreres, hvis man også bruger Cache Control¹⁷. Pragma benyttes som response header, selvom den kun har en funktion som request header¹⁸. X-Cache benyttes på 13% af hjemmesiderne, skønt en header med det navn ikke findes¹⁹. Der findes yderligere tusindvis af brugte headere, som ingen betydning eller funktion har²⁰. Derudover nævner Betts, at Content-Security-Policy godt nok er konceptuelt enkel, men at den kan kræve store ressourcer at implementere, hvilket dermed kan være en del af forklaringen på denne headers lave implementeringsgrad²¹.

Bud på, hvad der kan have trukket implementeringsarten og -graden i opadgående retning:

- Fokus på sikkerhed
- Følelse af ansvar for brugere/kunder og deres data
- Virksomhedens store størrelse

¹⁵ ibid.

¹⁶ https://www.youtube.com/watch?v=x_FxJxKIXl8: 6 min.

¹⁷ ibid.: 10 min.

¹⁸ ibid.

¹⁹ ibid.: 11 min.

²⁰ ibid.: 12 min.

²¹ ibid.: 16 min.

- Hjemmesidens popularitet

Den logiske følge er muligvis omvendt: Måske er det fokuseringen på sikkerhed, herunder implementeringen af SH, der har været med til at gøre hjemmesiden populær og virksomheden stor.

Bud på, hvad der kan have holdt implemteringsarten og -graden nede:

- Mangel på viden og ekspertise
- Mangel på følelse af ansvar for brugere/kunder og deres data
- Systemer, der er indrettet på en måde, der gør visse SH overflødige
- Andre sikkerhedsaspekter prioriteres højere
- Virksomhedens lille størrelse
- Visse SH, som fx Content-Security-Policy, er meget ressourcekrævende at implementere
- Ingen umiddelbar økonomisk gevinst (ikke retfærdiggjort i gennemgangen)

6. Konklusion

Analysens afsnit 5.1.1 viser, at Strict-Transport-Security, X-Frame-Options og X-Content-Type-Options aktuelt er implementeret på omkring 40%-50% af de allermest populære danske hjemmesider, og afsnit 5.1.2 viser, at de samme tre Security headers (SH) også ligger højest, når det kommer til den globale scene. Anderledes står det til med Content-Security-Policy, Referrer-Policy og Feature-Policy: De to førstnævnte er både i dansk og global sammenhæng implementeret på under hver femte af de mest populære hjemmesider, mens den sidstnævnte estimeres til at findes på færre end hver 20. hjemmeside.

Analysens sidste del, afsnit 5.2, giver følgende bud på, hvad der kan have trukket implemteringsarten og -graden i opadgående retning:

- Fokus på sikkerhed
- Følelse af ansvar for brugere/kunder og deres data
- Virksomhedens store størrelse
- Hjemmesidens popularitet

og følgende bud på, hvad der kan have holdt implemteringsarten og -graden nede:

- Mangel på viden og ekspertise
- Mangel på følelse af ansvar for brugere/kunder og deres data
- Systemer, der er indrettet på en måde, der gør visse SH overflødige

- Andre sikkerhedsaspekter prioriteres højere
- Virksomhedens lille størrelse
- Visse SH, som fx Content-Security-Policy, er meget ressourcekrævende at implementere
- Ingen umiddelbar økonomisk gevinst (ikke retfærdiggjort i gennemgangen)

Samlet set viser resultaterne af undersøgelserne, at arten og graden af den generelle SH-implementering er særdeles mangelfuld. Den generelle hjemmesidebruger kan på ingen måde regne med at være beskyttet af SH på selv de mest populære hjemmesider, hvad end det drejer sig om banker, nyhedsmedier eller de allerstørste virksomheder. Behovet for IT-sikkerhed, det vil sige brugerbeskyttelse i forbindelse med hjemmesidebesøg i denne sammenhæng, er vokset i takt med internettet, datastrømmen og antallet af forbindelser, men behovet er altså langt fra dækket i øjeblikket, og den generelle online-sikkerhed lider voldsomt derunder. Den generelle bruger er sig slet ikke Security headers, deres funktioner og farerne ved deres fravær bevidst, så det er et stort problem og udtryk for uansvarlighed, når langt størstedelen af hjemmesideindehavere ikke benytter sig af en generelt set så lettilgængelig brugerbeskyttende mekanisme, som Security headers udgør.

7. Litteraturliste

- Buchanan, Helme, Woodward (2017): *Analysis of the adoption of security headers in HTTP*. IET Information Security 12(2).
- Lavrenovs, Melón (2018): "HTTP Security Headers - Analysis of Top One Million Websites", *10th International Conference on Cyber Conflict - CYCON X, : Maximizing Effects*. Eds.: Minárik, Jakschis, Lindström. NATO CCD COE Publications, 345-370.
































7.1 URL'er

- <https://www.internetworldstats.com/emarketing.htm>
- https://en.wikipedia.org/wiki/Internet_traffic
- <http://www.securityheaders.com>
- <https://www.similarweb.com/top-websites>
- https://www.researchgate.net/publication/320247591_Analysis_of_the_Adoption_of_Security-Headers_in_HTTP
(Buchanan, Helme, Woodward (2017): *Analysis of the adoption of security headers in HTTP*. IET Information Security 12(2))
- https://ccdcoe.org/uploads/2018/10/CyCon_2018_Full_Book.pdf
(Lavrenovs, Melón (2018): "HTTP Security Headers - Analysis of Top One Million Websites", *10th International Conference on Cyber Conflict - CYCON X, : Maximizing Effects*. Eds.: Minárik, Jakschis, Lindström. NATO CCD COE Publications, 345-370)
- https://www.youtube.com/watch?v=x_FxJxKIXl8
(Andrew Betts forelæsning om Security headers ved Øredev 2018)
- <https://www.similarweb.com/top-websites/denmark>

8. Bilag

8.1 Bilag 1: De 50 hjemmesider, der er mest besøgt af danske brugere






































































Fra <https://www.similarweb.com/top-websites/denmark> d. 27. marts 2020:

Rank ①	Website ①	Category ①	Change ①	Avg. Visit Duration ①	Pages / Visit ①	Bounce Rate ①
1	 google.com	Computers Electronics and Technology > Search Engines	=	🔒	🔒	🔒
2	 youtube.com	Arts and Entertainment > TV Movies and Streaming	=	Available with  SimilarWeb Get country specific data and a full analysis for any website or app today - See Pricing		
3	 facebook.com	Computers Electronics and Technology > Social Networks and Online Communities	=			
4	 ekstrabladet.dk	News and Media	=	🔒	🔒	🔒
5	 google.dk	Computers Electronics and Technology > Search Engines	+1	🔒	🔒	🔒
6	 bt.dk	News and Media	-1	🔒	🔒	🔒
7	 dr.dk	Arts and Entertainment > TV Movies and Streaming	=	🔒	🔒	🔒
8	 tv2.dk	Arts and Entertainment > TV Movies and Streaming	=	🔒	🔒	🔒
9	 instagram.com	Computers Electronics and Technology > Social Networks and Online Communities	=	🔒	🔒	🔒
10	 pornhub.com	Adult	+1	🔒	🔒	🔒
11	 wikipedia.org	Reference Materials > Dictionaries and Encyclopedias	-1	🔒	🔒	🔒
12	 twitter.com	Computers Electronics and Technology > Social Networks and Online Communities	=	🔒	🔒	🔒
13	 dba.dk	E commerce and Shopping > Classifieds	+3	🔒	🔒	🔒
14	 xnxx.com	Adult	-1	🔒	🔒	🔒
15	 live.com	Computers Electronics and Technology > Email	=	🔒	🔒	🔒
16	 netflix.com	Arts and Entertainment > TV Movies and Streaming	-2	🔒	🔒	🔒
17	 reddit.com	Computers Electronics and Technology > Social Networks and Online Communities	+1	🔒	🔒	🔒
18	 xvideos.com	Adult	-1	🔒	🔒	🔒
19	 xhamster.com	Adult	+2	🔒	🔒	🔒
20	 yousee.dk	Finance > Banking Credit and Lending	-1	🔒	🔒	🔒
21	 lectio.dk	Science and Education > Education	-1	🔒	🔒	🔒
22	 e-boks.dk	Finance > Banking Credit and Lending	=	🔒	🔒	🔒
23	 linkedin.com	Computers Electronics and Technology > Social Networks and Online Communities	+1	🔒	🔒	🔒
24	 berlingske.dk	News and Media	-1	🔒	🔒	🔒
25	 google.com.br	Computers Electronics and Technology > Search Engines	+7	🔒	🔒	🔒
26	 krak.dk	Reference Materials > Public Records and Directories	-1	🔒	🔒	🔒
27	 twitch.tv	Games > Video Games Consoles and Accessories	+6	🔒	🔒	🔒
28	 danskespil.dk	Sports > Sports	+2	🔒	🔒	🔒
29	 viaplay.dk	Arts and Entertainment > Arts and Entertainment	+2	🔒	🔒	🔒
30	 politiken.dk	News and Media	-2	🔒	🔒	🔒

Navn: Brian Borchert
 Titel: IT-sikkerhed: Security headers
 Antal tegn: 18.902

Fag: IT-sikkerhed
 Underviser: Morten Empeno

Institution: SmartLearning
 Afleveret: d. 3. april 2020
 Eksamen: d. 6./7./8. april 2020

31	 imdb.com	Arts and Entertainment > TV Movies and Streaming	-5			
32	 yahoo.com	News and Media	+7			
33	 seoghoer.dk	Arts and Entertainment > Arts and Entertainment	+3			
34	 bold.dk	Sports > Soccer	+7			
35	 nordea.dk	Finance > Banking Credit and Lending	=			
36	 nemlog-in.dk	Finance > Banking Credit and Lending	+4			
37	 jyllands-posten.dk	News and Media	+5			
38	 boligsiden.dk	Business and Consumer Services > Real Estate	+8			
39	 jobnet.dk	Jobs and Career > Jobs and Employment	-1			
40	 borger.dk	Finance > Banking Credit and Lending	+5			
41	 zalando.dk	Lifestyle > Fashion and Apparel	-14			
42	 job.jobnet.dk	Jobs and Career > Jobs and Employment	+2			
43	 elgiganten.dk	Games > Games	-9			
44	 office.com	Computers Electronics and Technology > Programming and Developer Software	+7			
45	 unilogin.dk		=			
46	 pricerunner.dk	E commerce and Shopping > Price Comparison	-9			
47	 danskebank.dk	Finance > Banking Credit and Lending	=			
48	 gyldendal.dk	Science and Education > Education	-5			
49	 ikea.com	Home and Garden > Home and Garden	=			
50	 bilbasen.dk	Vehicles > Vehicles	+2			

8.2 Bilag 2: Oversigt over implementeringen af Security headers på de af danske brugere mest besøgte danske hjemmesider og et udpluk af øvrige danske hjemmesider pr. d. 26. marts 2020

Dette bilag er regnearket med navnet "Bilag 2", der er vedhæftet nærværende rapport. Regnearket vises her i billedform:

Gruppe	Ejer/Navn	Strict-Transport-Security	Content-Security-Policy	X-Frame-Options	X-Content-Type-Options	Referrer-Policy	Feature-Policy	Antal headers	Grade	Warnings	Hjemmeside/url
Store virksomheder	Arla	1		1	1	1		4	B	X-Frame-Options: der er duplicate X-Frame-Options header	https://www.arla.dk/
	LEGO	1			1			2	D		https://www.lego.com/dk-da/
	Danfoss			1	1			2	D		https://www.danfoss.com/en/
	Sterred			1				1	D		https://www.sterred.dk/
	Mærsk		1	1				2	D	Content-Security-Policy: har 'unsafe-inline' og 'unsafe-eval'	https://www.maersk.com
	Bestseller							0	F		https://dk.bestseller.com/dk/da/home
Banker	Grundfos							0	F		https://dk.grundfos.com/
	Coop							0	F		https://coop.dk/
	Danske Bank*	1	1	1	1	1	1	6	A	Content-Security-Policy: har 'unsafe-inline' og 'unsafe-eval'	https://danskebank.dk/
	Sydbank	1	1		1	1		4	A	Content-Security-Policy: har 'unsafe-inline' og 'unsafe-eval'	https://www.sydbank.dk/
	Jyske bank	1	1		1	1		4	A	Content-Security-Policy: har 'unsafe-inline' og 'unsafe-eval'	https://www.jyskebank.dk/
	Sparekassen Sjælland	1	1		1	1		4	A	Content-Security-Policy: har 'unsafe-inline' og 'unsafe-eval'	https://www.spsk.dk/
	Nordea*	1		1	1			3	C		https://www.nordea.dk/
	Vestjysk Bank	1		1	1			3	C		https://www.vestjyskbank.dk/
	Saxo Bank	1		1				2	D		https://www.home.saxo.dk-da/
	Sparekassen Vestsjælland	1			1			2	D		https://www.sparv.dk/
Nyhedsmedier	Lis og Spar	1			1			2	D		https://www.lis.dk/
	Jutlander Bank	1						1	D		https://jutlander.dk/
	Coop Bank							0	F		https://coopbank.dk/
	DR*	1		1				2	D		https://www.dr.dk/
	Ekstra Bladet*	1						1	D		https://ekstrabladet.dk/
	BT*	1						1	D		https://www.bt.dk/
	Berlingske*	1						1	D		https://www.berlingske.dk/
	Jyllands-Posten*	1			1			2	D		https://jyllands-posten.dk/
	Se og Hør*							1	D		https://www.seoghoer.dk/
	Bold.dk*			1	1			1	D		https://www.bold.dk/
Rejse-elskere	Politiken*							0	F		https://politiken.dk/
	TV2*							0	F		https://tv2.dk/
	Børsen							0	F		https://borsen.dk/
	Albatros Travel	1		1	1			3	C		https://www.albatros-travel.dk/
	Sun Tours	1						1	D		https://www.suntours.dk/
	Adventure Holidays							0	F		https://www.adventureholidays.dk/
	Aarhus Charter							0	F		https://www.aarhuscharter.dk/
	Africa Tours							0	F		https://www.africatours.dk/
	Kommuner		1	1	1	1	1	5	A	Content-Security-Policy: har 'unsafe-inline' og 'unsafe-eval'	https://www.kk.dk/
	København Kommune			1	1	1		3	C		https://www.kobenhavn.dk/
Diverse	Tårnby Kommune		1	1	1			3	C		https://www.taarby.dk/
	Odense Kommune			1	1			0	F		https://www.odense.dk/
	Haderslev Kommune							0	F		https://www.haderslev.dk/for-side/
	Aalborg Kommune							0	F		https://www.aalborg.dk/
	Kolding Kommune							0	F		https://www.kolding.dk/
	Borger.dk*	1	1	1	1			4	A	Content-Security-Policy: har 'unsafe-inline'	https://www.borger.dk/
	ViaPlay*	1	1	1	1			4	A		https://www.viplay.dk/
	Dansk1	1		1	1			3	C		https://dansk1.dk/
	DBA*	1		1	1			3	C		https://www.dba.dk/
	Bilbasen*	1		1	1			3	C		https://www.bilbasen.dk/
E-boks	Eliganten*	1						1	D		https://www.eliganten.dk/
	Jobnet*		1	1				2	D		https://jobnet.dk/
	Boligsiden*			1				1	D		https://www.boligsiden.dk/
	Danske Spil*	1		1				2	D		https://danske-spil.dk/
	Youtoo*	1						1	D		https://youtoo.dk/
	e-boks*			1				1	D		https://www.e-boks.com/corporate/da
	Aarhus Universitet				1			1	D		https://www.au.dk/
	Aarhus Universitetshospital				1	1		2	D	Referrer-Policy: "origin-when-cross-origin"-værdien anbefales ikke	https://www.auh.dk/
	Besøg lægen			1				1	D		https://www.besoglaegen.dk/login.aspx?Clinicid=070874
	Nemlog-in*							0	F		https://nemlog-in.dk/login.aspx?hospid=107
E-boks	Gyldensti*							0	F		https://www.gyldensti.dk/
	Pricerunner*							0	F		https://www.pricerunner.dk/
	Krak*							0	F		https://www.krak.dk/
	Lectio*							0	F		https://www.lectio.dk/
	Tripborg Lægehus							0	F	Kun tilgængelig over HTTP	https://www.tripborglaegehus.dk/
I alt		28	9	24	24	8	2	95			
Gennemsnit (Header/hjemmeside)		46%	15%	79%	79%	13%	7%	26%	D		

Resultaterne er fremkommet ved brug af værktøjet på www.securityheaders.com.

*Blandt de 50 mest besøgte danske hjemmesider. Blandt de 50 mest besøgte danske hjemmesider er derudover zalando.dk og unilogin.dk. Værktøjet på www.securityheaders.com timede ud i forsøget på at kontakte de to sider.

8.3 Bilag 3: Virksomheders svar på 3 spørgsmål om implementering af Security Headers

8.3.1 Virksomhed 1 (karakter: D)

2 anonyme personer indgår.

Svar 1 fra anonym person 1:

Har lige fået [anonym person 2's] svar på det, og han siger størstedelene virker irrelevante på ham og at vores valg er taget efter "relevans" for os. [Anonym person 2] skriver:

1. Ikke udover HSTS og CSP.
2. Kun HSTS er vigtig.
3. Vi bruger HSTS for at opnå hurtigere forbindelse til den besøgende når vi kræver HTTPS.

8.3.2 Virksomhed 2 (karakter: D)

2 anonyme personer indgår.

Svar 1 fra anonym person 1:

[...] Vi er meget opmærksomme på sikkerhed i alt hvad vi laver, dog er vi også godt opmærksomme på at vi ofte scorer ret lavt i den slags tests. Årsagen er at vores hjemmeside er bygget i vores eget CMS. Det var det vi levede af at lave de første [anonymt antal] år af firmaets historie. De her tests er typisk baseret på standarder såsom wordpress, sitecore, drupal osv - hvis man ikke bruger et standard CMS, så vil man ofte score lavt, selvom der faktisk er helt styr på sikkerheden. Vi har til dato aldrig oplevet nogen der har haft held til at knække nogen af vores kunders hjemmesider, så vores track record er efter [anonymt antal] år stadig 100%. Men det er ikke mig der er ansvarlig for sikkerheden hos os, og jeg har derfor videresendt din forespørgsel til vores sikkerhedsansvarlige. Jeg ser om ikke jeg kan få ham til at hjælpe med nogle uddybende svar :-)

Undertegnede's respons til svar 1:

Wow, [anonymiseret person], tusind tak!!!! Jeg håber, din kollega er ligeså disponibel som dig. (Tak uanset!) Spændende bliver det i hvert fald at høre nærmere, hvis det sker :-)
Security headers handler nemlig ikke kun om at beskytte ens egen hjemmeside, men også om at beskytte brugeren under brugen. Fx om at sørge for, at ingen kan liste et usynligt frame med knapper til ondsindede sider, pengeoverførsler og alt muligt andet ind foran siden, man besøger. Men ja, mon ikke det så er indbygget i jeres system på andre måder?
[...]

Svar 2 fra anonym person 1:

CMS'et blev bygget før min tid så jeg ved ikke så meget om teknikken... men jeg er ret sikker på at der er styr på det. Vi solgte en stor løsning til [anonymt firma] som bliver brugt til at drive ca 200 webshops via en stor central backend. I den forbindelse blev der sendt nogle white hat hackers efter os for at teste om de kunne finde nogle exploits. Efter et par uger fik vi en rapport tilbage om at de ikke havde fundet noget og ikke havde haft held til at komme ind hverken i backend eller frontend... vi kvitterede så ved at sende en rapport den anden vej hvor vi havde logget alle deres forsøg på at komme ind 😊 Så ja... vi plejer at have ret godt styr på tingene, men ingen er 100% - heller ikke os.

Men jeg har sendt din mail til min kollega, så vender han sikkert tilbage - det plejer han at gøre :-)

Undertegnede's respons til svar 2:

Ha ha, ja det lyder da til, at der er tænkt på det meste :-)

Svar 3 fra anonym person 1:

Det er vi lidt nødt til... da vi bare lavede hjemmesider var det ikke super kritisk... worst case røg siden ned eller lign... men nu er det jo kundernes data der er på spil - langt mere alvorligt :-)

8.3.3 Virksomhed 3 (karakter: D)

1 anonym person indgår.

Svar 1 fra anonym person 1:

Sårbarheder i applikationslaget er noget vi kigger på, også i stigende grad. Jeg ville dog være super glad hvis det var på min top 100 over opgaver. Det er også i stigende grad noget der bliver implementeret i processerne hos udviklerne. Hos bug bounty programmerne scorer sådanne fund vist heller ikke så godt. Jeg kan ikke lige i hovedet hvordan de scorer hos sårbarhedsscannere, men det er nok heller ikke så højt selvom fx HSTS er Nice.

8.3.4 Virksomhed 4 (karakter: D)

1 anonym person indgår.

Svar 1 fra anonym person 1:

Tak for din henvendelse
Vi er opmærksomme på det, men vi har et eksternt bureau til at sidde med det og varetager det for os.