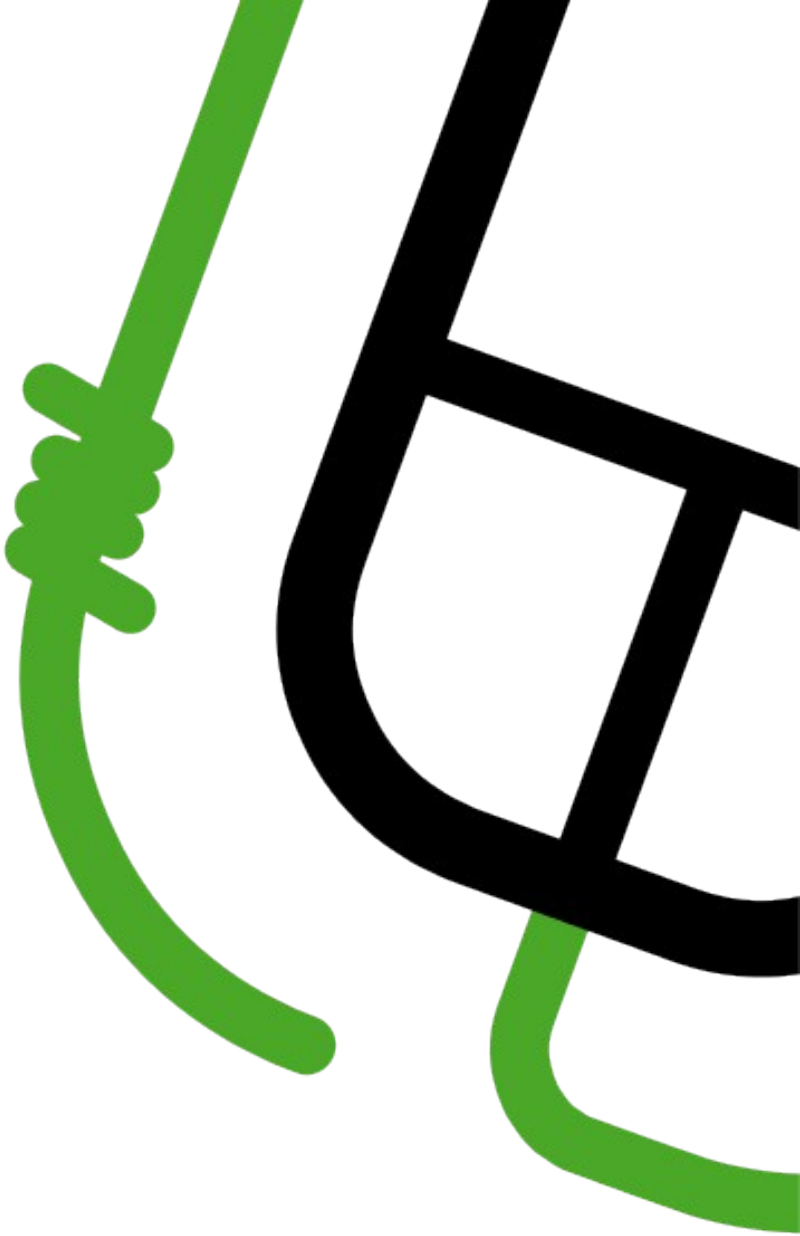
ONDER DE MOTORKAP VAN HET INTERNET



Van IP-adressen tot DNS-servers, van encryptie tot de cloud

Versie 16 mei 2013
zie voor de laatste versie bof.nl

BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Iedereen gebruikt het internet. Maar hoe werkt het internet eigenlijk? Een goed begrip van de techniek van het internet is belangrijk om de gevolgen van beleid goed in te schatten. Want sommige maatregelen werken niet, maar kosten wel geld. En sommige maatregelen werken wel, maar maken inbreuk op grondrechten. In deze gids leggen wij een aantal basisconcepten van het internet uit: van IP-adressen tot encryptie, van DNS-servers tot de cloud. Het is geen volledig overzicht – het is een eerste introductie van de techniek achter het internet. Tips of suggesties? Stuur ze naar info@bof.nl.

INHOUD

BITS OF FREEDOM
VERDEDIGT DIGITALE BURGERRECHTEN

Bits of Freedom komt op voor jouw vrijheid en privacy op internet. Deze grondrechten zijn onmisbaar voor je ontwikkeling, voor technologische innovatie en voor de rechtsstaat. Maar die vrijheid is niet vanzelfsprekend. Je gegevens worden opgeslagen en geanalyseerd. Je internetverkeer wordt afgeknepen en geblokkeerd. Bits of Freedom zorgt ervoor dat jouw internet jouw zaak blijft.

Stichting Bits of Freedom
Postbus 10746
1001 ES Amsterdam
+31 6 4499 5711

info@bof.nl

01. WAT IS HET INTERNET?

Vóór de komst van het internet bestonden er al netwerken waarmee één of meerdere computers met elkaar konden communiceren. Deze netwerken stonden veelal binnen bedrijven, overheden en universiteiten en spraken allemaal hun eigen taal. Die netwerken waren alleen niet met elkaar verbonden. Men is van "het internet" gaan spreken toen men die netwerken met elkaar wist te laten praten. Het internet is dus een netwerk van netwerken. Het internet werkt omdat het gebruik maakte van een nieuwe taal die ieder aan het internet verbonden apparaat spreekt: het Internet Protocol (IP – dat is dus waar de term IP adres vandaan komt).

Door de ontwikkeling van het Internet Protocol konden allerlei netwerken en apparaten met elkaar communiceren die dat voorheen niet konden. Je Windows PC, je Macbook, je Blackberry, je iPad of je internet TV: al deze machines wisselen informatie uit via datzelfde Internet Protocol.

Bij communicatie via het Internet Protocol wordt de informatie verdeeld in kleine pakketjes die voorzien zijn van een afzender en ontvanger. Op die manier weten de computers binnen het netwerk waar een

verzoek vandaan komt en waar het antwoord naartoe moet worden verstuurd.

De kracht van het Internet Protocol is dat mensen over dat protocol hun eigen protocollen kunnen

Alle computers op het internet spreken met elkaar via het Internet Protocol.

ontwikkelen. Zo bestaat er voor e-mail bijvoorbeeld het Simple Mail Transfer Protocol (SMTP) dat voorschrijft hoe e-mail aangeleverd moet worden voor verzending. Het HyperText Transfer Protocol schrijft voor hoe de informatie van websites opgevraagd en verzonden moet worden (afgekort met HTTP – dat is dus waar de http:// vandaan komt die je in sommige browsers ziet staan). Voor het Internet Protocol maakt het niet uit of e-mail, een website of een WhatsApp bericht wordt verstuurd, zolang er maar de juiste adressen op de pakketjes staan.

Dit universele gebruik van het Internet Protocol levert talloze voordelen op. Doordat je geen toestemming nodig hebt van een bedrijf om het protocol te implementeren kan iedereen een applicatie ontwikkelen die hiervan gebruik maakt en direct met alle computers op het internet communiceren. Omdat het niet uitmaakt welke informatie verstuurd wordt is er voor de onderdelen van de netwerken die de pakketjes transporteren ook geen noodzaak om de inhoud van de boodschap te weten.

02. WAT IS EEN IP ADRES?

Het hierboven besproken Internet Protocol maakt dus uitwisseling van informatie mogelijk. Dat gebeurt met behulp van zogenoemde IP adressen. Op het internet bestaan IP adressen niet uit straatnamen en postcodes, maar uit een serie getallen, zoals bijvoorbeeld 8.8.8.8. Een pakketje is altijd afkomstig ván een bepaald IP adres en wordt verstuurd náár een bepaald IP adres.

Een IP adres is altijd uniek maar het kan zijn dat er meerdere mensen van één adres gebruik maken. Zo heb je thuis hoogstwaarschijnlijk slechts één internetverbinding met slechts één internet adres terwijl daar toch verschillende computers en tablets aan zijn gekoppeld. Dit komt doordat het interne netwerk thuis gebruik maakt van privé adressen die niet gebruikt worden op het internet. De modem, het kastje met de daadwerkelijke internetverbinding, heeft als enige een publiek IP adres (zoals 8.8.8.8). De modem weet welk apparaat welk verzoek heeft gedaan en voorziet het juiste apparaat van het juiste antwoord. Alleen andere apparaten op het internet communiceren direct met de modem.

Dit heeft als gevolg dat, vanaf het internet bezien, alle communicatie van het publieke IP adres (8.8.8.8) afkomstig is, zelfs als daar verschillende computers

Er kunnen meerdere mensen gebruik maken van één IP adres. Identificatie is daarom lastig.

achter zitten. Hierdoor is het moeilijker om mensen uniek te identificeren aan de hand van een IP adres. Bij grote organisaties waar soms wel honderden of

duizenden computers gebruik maken van hetzelfde publieke adres is dit nog veel lastiger.

Vergelijk het met een poststuk dat geretourneerd moet worden en als afzender uitsluitend *Schedeldoekshaven 100, Den Haag* heeft staan. De postbode kan het stuk wel op dat adres afleveren, maar welk van de honderden medewerkers van het Ministerie van Justitie dit poststuk verzonden heeft weet hij niet.

03. WAT IS DEEP PACKET INSPECTION (DPI)?

Zoals we eerder gezien hebben wordt alle data via het internet verzonden in pakketjes. Het Internet Protocol knipt grote bestanden op in kleine pakketjes en verstuurt die via de meest optimale route naar de eindbestemming zonder te kijken naar de inhoud.

Ook software die werd ingezet om netwerken te beschermen, firewalls, keek vroeger niet naar de inhoud van het pakket: op basis van de afzender, de ontvanger en de dienst die werd opgevraagd werd beoordeeld of verkeer wel of niet mocht worden doorgelaten. Als een pakketje bijvoorbeeld afkomstig was van een adres dat op de zwarte lijst van de firewall stond, dan werd dat pakketje geblokkeerd.

Met de groei van het internet nam ook misbruik toe. Zo ontdekte men dat je computer op het internet kon bombarderen met zoveel pakketjes uit verschillende delen van het internet dat die computer onbereikbaar werd: een zogenaamde Distributed Denial of Service (DDoS) aanval.

Netwerkbeheerders probeerden dit soort aanvallen af te weren door de ontvangen pakketjes verder te bestuderen. De apparatuur keek vroeger altijd alleen naar de adresgegevens van het pakketje, maar door iets verder te lezen kon ook de inhoud van het pakketje worden bekeken.

Op die manier konden aanvallen met pakketjes die allemaal dezelfde soort inhoud hebben zo onderscheiden worden van legitieme bezoekers. De pakketjes van een DDoS aanval konden klakkeloos genegeerd worden terwijl ze voorheen het hele netwerk tot stilstand konden brengen. Deze nieuwe firewalls staan bekend als Intrusion Prevention Systems (IPS).

Overheden, bedrijven en belangenorganistaties realiseerden zich dat deze techniek ook voor andere

doeleinden kon worden ingezet. Zo wilden telecombedrijven deze techniek gebruiken om Skype en WhatsApp te blokkeren. Overheden gebruiken dezelfde techniek voor surveillance en aftappen en belangenorganisaties zoals Stichting Brein willen deze techniek inzetten voor het bestrijden van inbreuk op auteursrecht door te kijken of mensen muziek en films downloaden.

Je kunt je afvragen in welke gevallen de toepassing van DPI een schending van het communicatiegeheim oplevert.

04. WAT IS HET DOMAIN NAME SYSTEM (DNS)?

Tot nu toe hebben we het gehad over het Internet Protocol en bijbehorende IP adressen. Toch heb je waarschijnlijk zelden, misschien zelfs wel nooit, een IP adres ingetypt. Als je de website van Bits of Freedom wilt bezoeken typ je immers bof.nl in, en niet 82.94.216.82.

Het systeem dat het mogelijk maakt om domeinnamen in plaats van IP adressen te gebruiken heet het Domain Name System, kortweg DNS. Je kunt DNS vergelijken met een telefoonboek dat het nummer bij de naam zoekt. Het gebruik van domeinnamen is veel gebruikersvriendelijker dan het gebruik van adressen. Op die manier kan je immers makkelijker te onthouden namen (zoals bof.nl) gebruiken, in plaats van ingewikkelde IP adressen.

Wanneer je bof.nl bezoekt op je computer dan zal je computer via het DNS systeem vragen welk IP adres hierbij hoort. Mocht een website veranderen van IP adres dan heb je hier dankzij DNS geen last van: de domeinnaam blijft immers hetzelfde en alleen het achterliggende IP adres wijzigt.

05. WAT IS HET WORLD WIDE WEB (WWW)?

Het wereldwijde web (World Wide Web) is een aanduiding voor een verzameling met elkaar verbonden pagina's. Vrijwel alles wat je bekijkt in je browser, zoals Internet Explorer of Firefox, is onderdeel van het wereldwijde web. Deze pagina's tonen vaak tekst, afbeeldingen, video's en andere multimedia en zijn aan elkaar gekoppeld door middel van hyperlinks. Door op zo'n hyperlink te klikken vraag je de volgende pagina op.

De pagina's op het wereldwijde web zijn in een bepaald formaat opgemaakt: HyperText Markup Language (HTML). Er wordt voortdurend verder ontwikkeld aan HTML. We zitten nu al op versie 5. Doordat je geen licentie nodig hebt voor het gebruik van HTML staat het iedereen vrij om HTML pagina's of browsers te ontwikkelen. Ook kan iedereen bijdragen aan het ontwikkelen van de standaard. Doordat iedereen dezelfde standaard aanhoudt biedt het dezelfde voordelen als bij het Internet Protocol:

Via het Domain Name System (DNS) worden domeinnamen aan IP adressen gekoppeld.

allerhande apparaten en software kunnen dit soort pagina's tonen of bewerken.

HTML pagina's worden verstuurd via het zogenaamde HyperText Transfer Protocol (HTTP). Deze afkorting zie je daarom ook vaak terug voor een web adres in je browser: http://www.bof.nl/

Je browser vraagt via HTTP een pagina op bij een computer die aan het internet is verbonden (een zogenoemde webserver). De daadwerklijke data wordt vervolgens verzonden via het eerder besproken IP

Wanneer een IP adres wordt geblokkeerd, zijn alle websites achter dat IP adres ontoegankelijk.

protocol. HTTP gebruikt dus het Internet Protocol voor het verzenden en ontvangen van de data.

Eerder hebben we beschreven hoe meerdere mensen gebruik kunnen maken van één IP adres. Dit geldt ook voor websites. Zo kunnen er op het IP adres 10.11.12.13 wel honderden websites aangeboden worden, ieder met hun eigen domeinnaam. Doordat de domeinnaam ook in de browser wordt ingetypt en dus wordt doorgegeven aan de webserver, weet de webserver welke website moet antwoorden.

Wanneer een website wordt geblokkeerd aan de hand van een IP adres zijn alle andere websites die hetzelfde IP adres gebruiken dus ook geblokkeerd.

HTTP verkeer is niet versleuteld en alle onderdelen in het netwerk die een HTTP-pakketje vervoeren kunnen dus naast het adres op het pakketje ook de boodschap lezen. In de loop van de jaren is er daarom ook een beveiligde versie ontwikkeld: HTTPS, wat staat voor HyperText Transfer Protocol Secure. Je maakt gebruikt van een beveiligde verbinding als je bijvoorbeeld contact maakt met een bank.

Bij een beveiligde verbinding maakt de website gebruik van een certificaat. Dit certificaat wordt afgegeven door een Certificate Authority die de identiteit van de website vaststelt. Op die manier wordt gecontroleerd dat alleen de Rabobank een certificaat voor de Rabobank kan aanvragen en u als bezoeker weet dus zeker dat u met de Rabobank communiceert.

Bij dit certificaat hoort een cryptografische sleutel die vervolgens wordt gebruikt voor het versleutelen van de informatieuitwisseling, waardoor alleen nog de eindgebruiker en de website de communicatie kunnen ontcijferen. De onbeveiligde HTTP verbinding wordt bij HTTPS dus in een soort verzegelde enveloppe gestopt waardoor de postbode niet langer naar de boodschap zelf kan kijken.

06. HOE WERKT E-MAIL?

Met elektronische post, kortweg e-mail, bedoelen we berichten die via het internet worden verstuurd met het Simple Mail Transfer Protocol (SMTP). Net als bijvoorbeeld het eerder besproken HyperText Transfer Protocol voor websites is SMTP een serie afspraken over hoe e-mail verzonden wordt op het internet.

Na het opstellen van een nieuw bericht in je mailprogramma, of bijvoorbeeld een webmail programma zoals Hotmail of Gmail, wordt het bericht via SMTP verzonden naar zijn uiteindelijke bestemming. Het bericht gaat daarbij van de verzendende e-mail server naar de ontvangende e- mail server. De ontvangende mailserver bewaart het bericht zodat het kan worden bekeken door de ontvanger.

E-mailservers gebruiken ook het eerder besproken Domain Name System om te achterhalen naar welk IP adres een e-mail verzonden moet worden. Zij vertalen hiervoor de domeinnaam achter het @-teken (bijvoorbeeld info@bof.nl) naar cijfers om het adres te

achterhalen en sturen de e-mail vervolgens naar dat IP adres.

07. WAT IS ADVERTEREN OP BASIS VAN GEDRAG?

"Behavioural advertising" of "targeted advertising" is adverteren op basis van online gedrag van de gebruiker. Als de beheerder van een website wil uitvinden of mensen zijn website vaker bezoeken is het niet handig om te kijken of een bepaald IP adres de website bezoekt, omdat meerdere gebruikers één IP adres kunnen gebruiken. Daarom plaatsen websites een uniek getal op de computer van een gebruiker en iedere keer als de gebruiker terugkomt, kunnen zij de gebruiker daaraan herkennen. Aan de hand hiervan kunnen zij bijvoorbeeld hun website aanpassen op de gebruiker.

Een simpel voorbeeld hiervan is een online boekenwinkel die weet welke boeken je gekocht hebt. Op basis van de boeken die je eerder gekocht hebt weet de boekenwinkel bijvoorbeeld of je van thrillers houdt of van romans. Op basis van deze informatie kan de online boekenwinkel je tips geven voor nieuwe boeken die je nog niet gelezen hebt.

Het is echter ook mogelijk om het bezoekpatroon van *verschillende* websites bij te houden, als achter de schermen deze informatie aan elkaar gekoppeld wordt. Dan kan dus worden vastgesteld dat de gebruiker met cookie 123456 eerst google.com bezocht, en vervolgens naar nu.nl ging. Advertentienetwerken bieden advertentieruimte op heel veel verschillende websites – en zij kunnen een gebruiker dus op al die websites volgen.

Bij bezoeken aan andere websites waar dezelfde adverteerder actief op is, wordt gecontroleerd of de bezoeker zo'n cookie heeft. Wanneer dit het geval is wordt het unieke nummer uit de cookie opgeslagen samen met de informatie over welke website hij bezocht heeft. Door gebruikers zo te volgen tijdens hun online reis wordt het dus mogelijk om te zien dat iemand bijvoorbeeld een reis geboekt heeft, een auto probeert te huren en op zoek is naar een hotel. Op basis van die informatie is het mogelijk om een gedetailleerd profiel van de gebruiker te maken. Ook kun je gerichte advertenties aan de hand van dit profiel tonen.

Overigens kunnen gebruikers ook op een andere manier dan met cookies worden gevolgd. Er zijn namelijk verschillende technieken om unieke informatie op een computer te plaatsen en die vervolgens weer op te vragen.

08. WAT IS CLOUD COMPUTING?

Cloud computing is een nogal hippe term, maar het concept is niet nieuw. Met cloud computing wordt gedoeld op diensten die worden aangeboden op computers in het externe netwerk in plaats van op de computer van de eindgebruiker. Je kan er bijvoorbeeld voor kiezen om gegevens op te slaan bij de servers van Amazon in de Verenigde Staten in plaats van op je eigen computer. Dan sla je die gegevens "in de cloud" op.

Bij cloud computing verplaatst rekencapaciteit en opslag van je computer naar het netwerk.

Een van de eerste voorbeelden van cloud computing is

e-mailen via je browser ("webmail"). Gebruikers van webmail kunnen vanaf ieder apparaat met een internetverbinding bij hun e-mail in plaats van alleen via hun eigen computer. Voorbeelden van webmaildiensten zijn Yahoo! Mail, Hotmail en Gmail.

Met encryptie kan je vertrouwelijke gegevens bij diefstal beschermen.

Doordat internet steeds sneller werd en browsers steeds beter werden is de diversiteit van webdiensten enorm toegenomen in recente jaren. Zo is het vandaag de dag bijvoorbeeld mogelijk om grote hoeveelheden data op te slaan in de "cloud" door gebruik te maken van virtuele schijven zoals bijvoorbeeld aangeboden door Microsoft Live. Ook worden online tekstverwerkings- en database technologiën steeds vaker op deze wijze aangeboden: je kan bijvoorbeeld een stuk schrijven in Google Docs (dus op servers van Google) in plaats van op je eigen computer.

Google's besturingssysteem Chrome gaat nog een stap verder. Als je een laptop met Google Chrome gebruikt, draait vrijwel niets op je eigen computer – alleen maar een browser. Via die browser kan je vervolgens allerlei software in de cloud draaien. Dit staat haaks op de traditionele aanpak waarbij vrijwel alle software op de computer van de gebruiker geïnstalleerd moet worden, zonder verdere afhankelijkheid van de cloud.

09. WAT IS ENCRYPTIE?

Encryptie is een ander woord voor het versleutelen van gegevens, zodat alleen bepaalde personen toegang hebben tot die gegevens. Dat gebeurt al duizenden jaren, maar met de komst van de computer heeft cryptografie, de wetenschap van het versleutelen, een grote vlucht genomen. Versleutelingsmethodes die tot de komst van de computer redelijk veilig leken, konden ineens in een mum van tijd worden gekraakt en nieuwe, betere versleutelingstechnieken konden door de komst van snelle computers ineens eenvoudig worden ingezet.

Zoals we eerder hebben gelezen zijn veel van de op het internet gebruikte protocollen niet standaard versleuteld. E-mail wordt van oudsher onversleuteld verzonden, maar ook de meeste websites die je bezoekt maken geen gebruik van encryptie. Dit zorgt er voor dat kwaadwillenden die mee luisteren je berichtenverkeer eenvoudig kunnen onderscheppen.

Daarom wordt voor de communicatie van gevoelige gegevens, zoals bankgegevens, vaak wel versleuteling gebruikt. Toch gebeurt dit nog te weinig. Het internet is een netwerk van netwerken en pakketjes worden via verschillende onderdelen van het netwerk getransporteerd. Alle onderdelen van het netwerk kunnen die communicatie onderscheppen. Daarom is het belangrijk om internetverkeer goed te versleutelen.

Ook e-mail berichten wordt onversleuteld verzonden. Dit heeft als nadeel dat e-mails door alle onderdelen van het netwerk waarlangs het bericht wordt verstuurd onderschept en gelezen kunnen worden, bijvoorbeeld door de e-mail server van je provider waarmee je het bericht verstuurt of door de mailserver van de ontvangende partij.

Om dit te voorkomen kun je je e-mail versleutelen, bijvoorbeeld met een programma zoals Pretty Good

Privacy. Hiermee versleutel je het bericht met een sleutel die alleen jij en de beoogde ontvanger kennen. Voor iedereen die onderweg het bericht onderschept is het hierna zeer complex, zo niet onmogelijk, om het bericht te ontcijferen.

Encryptie wordt ook gebruikt om gegevens op de harde schijf te beveiligen. De meeste moderne besturingssystemen versleutelen standaard de gegevens van de gebruiker. Als een laptop bijvoorbeeld gestolen wordt, dan heeft de dief zo geen toegang tot de gegevens als hij het wachtwoord niet kent.

Encryptie heeft nog een andere functie: ook de “integriteit” van de gegevens kan hiermee worden gecontroleerd. Met integriteit wordt gedoeld op de vraag of informatie is aangepast. Met behulp van encryptie kan je dus ook controleren of een bericht niet is onderweg gewijzigd.


BY
ND