Internetveiligheid, is dat belangrijk?

Laatst is Facebook gehackt en allerlei persoonlijke gegevens kwamen naar buiten. Zo zijn er afgelopen jaren veel grote internetwebsites en -webshops gehackt. Een van de andere bekende hackdoelen zijn verkiezingen. Zo is het een bijeenkomst van hackers gelukt om onder twee uur de stemapparaten van de Amerikaanse verkiezingen te hacken. Waar ligt dit aan? Ligt het aan de beveiliging of waren de bedrijven gewoon dom bezig? Maar een belangrijkere vraag is: zouden grote bedrijven op het internet goed beveiligd moeten zijn?

**DDoS**

DDoS, je hoorde het een tijd in het nieuws. Deze bekende aanval was gedaan met het zogeheten “Mirai” programma. Dit programma infecteert allerlei apparaten die met internet verbonden zijn. Die apparaten zijn vaak niet alleen computers, maar printers en dergelijke. Ze kunnen dan gebruikt worden voor een DDoS aanval. Een DDoS aanval legt je hele website plat en kan je dus veel schade berokkenen. Als groot bedrijf kan je dit voorkomen door een goed beveiligingsprogramma op je servers te zetten, zodat DDoS geen optie is.

**Leven**

Wanneer één of andere boze hacker kwaad aan wil richten dan zoekt hij zo snel mogelijk een ziekenhuis op. Denk bijvoorbeeld aan tante Hanne die nu in de Gelderse Vallei wordt geopereerd. Als die machines gehackt worden, zal waarschijnlijk de hele spoedeisende hulp de pijp uit gaan. Dan hebben we het nog niet eens over de andere afdelingen. Denk ook maar eens aan de brandweer of politie. Als die gehackt worden dan is niemand meer veilig, want iedereen krijgt vals alarm, maar de echte branden worden nooit gepakt en hetzelfde geldt voor criminelen. Het is dus voor levensreddende instituties zeer belangrijk om een goede beveiliging. De gevolgen zijn catastrofaal als zij hun beveiliging niet goed hebben gedaan.

**Data/Gegevens**

“Data Breaches”, “Data Leaks” en “Data Exposure”, het openbaar maken van persoonlijke gegevens. Hieronder vallen wachtwoorden, gezondheid, bankrekeningen, pincodes, identiteitsbewijzen en dergelijke. Als een bedrijf zijn gegevens niet goed beveiligd, kan iedereen erbij. Des te meer reden voor bedrijven om goede beveiliging aan te schaffen.

**Duur?**

Natuurlijk is een goede beveiliging handig, maar het is ook erg duur. ZZP’ers kunnen dat niet altijd betalen. Het kost namelijk vaak meer dan zestig euro per vijf apparaten voor een simpel antivirusprogramma en als je een echt goede beveiliging wilt loopt dat al snel op naar de honderden euro’s. Dat is voor ZZP’ers al duur. Denk je eens in hoe duur het wel niet is voor de overheid, die tienduizenden computers heeft. De beveiliging wordt snel duur en dat alleen voor een simpel antivirusprogramma. Dan hebben we het nog niet eens over de geavanceerde cybersecurityprogramma’s van de AIVD of andere belangrijke instellingen, maar gewoon over de normale computers van de gemeente. De kosten lopen dus hoog op en dat is dus een enorme kostenpost voor bedrijven en de overheid.

**Back-ups?**

Verder is een duur cybersecurityprogramma kopen niet nodig als je gewoon back-ups kan maken van je data. Zodat je nog steeds je data hebt als je servers worden gehackt. Back-ups zijn ook handig bij ‘ransomware-aanvallen’, want als je geen antivirusprogramma hebt kan je snel last krijgen van ‘ransomware’, dit zijn programma’s die je bestanden ‘gijzelen’ en je losgeld vragen, maar met back-ups hoeft dit losgeld niet betaald te worden. Je hebt namelijk een kopie van al je bestanden, die gegijzeld zijn, en daarom heeft het geen effect. Je hebt dus altijd al je bestanden nog, zonder een antivirusprogramma nodig te hebben.

**Goede hackers**

Goede hackers zijn zeldzaam, maar wel de enigen die echte schade kunnen aanbrengen. Je hebt daarnaast natuurlijk wel middelmatige hackers, maar het beste wat die kunnen doen is je site platleggen met DDoS-aanvallen. Er zijn ongeveer 100 bekende hackers/hackergroepen en die komen meestal toch wel binnen virusprogramma of niet. Als je goede hackergroepen boos maakt dan kan niks je nog redden, maar er zijn er dus niet zo veel. Je hebt dan dus ook niet vaak een cybersecurityprogramma nodig.

**Conclusie**

Op de vraag: “Internet veiligheid is dat belangrijk?”, kunnen meningen verschillen. Aan de ene kant hebben is goede beveiliging erg duur en je kan ook gewoon een back-up maken zonder al te veel kosten. Er zijn ook maar een beperkt aantal goede hackers die echt grote schade aan kunnen richten. Aan de andere kant zorgt het wel voor een vermindering van data leaks en DDOS-aanvallen. Ook zorgt het ervoor dat er veel levens gered kunnen blijven worden.

Literatuurlijst:

Lijst hackers

1. Gabriel, Trip (14 January 1995). ["Reprogramming a Convicted Hacker; To His On-Line Friends, Phiber Optik Is a Virtual Hero"](https://www.nytimes.com/1995/01/14/nyregion/reprogramming-convicted-hacker-his-line-friends-phiber-optik-virtual-hero.html). [The New York Times](https://en.wikipedia.org/wiki/The_New_York_Times). (17-10-2018)
2. ^ [Jump up to:**a**](https://en.wikipedia.org/wiki/List_of_hackers) [**b**](https://en.wikipedia.org/wiki/List_of_hackers)[**c**](https://en.wikipedia.org/wiki/List_of_hackers)[**d**](https://en.wikipedia.org/wiki/List_of_hackers)Bright, Peter (16 May 2013). [""The cutting edge of cybercrime"—Lulzsec hackers get up to 32 months in jail"](https://arstechnica.com/tech-policy/2013/05/the-cutting-edge-of-cybercrime-lulzsec-hackers-get-up-to-32-months-in-jail/). [Ars Technica](https://en.wikipedia.org/wiki/Ars_Technica). (17-10-2018)
3. Tweney, Dylan (29 March 2009). ["DIY Freaks Flock to 'Hacker Spaces' Worldwide"](https://www.wired.com/2009/03/hackerspaces/). wired.com. Wired. (17-10-2018)
4. [Emmanuel Goldstein](https://en.wikipedia.org/wiki/Eric_Corley); Mitch Altman; Bre Pettis; "[dot]Ret"; Bernie S.; Jim Vichench; Rob Vincent; Mike Castleman (13 January 2010). ["Off The Hook 13 January"](http://www.2600.com/offthehook/2010/0110.html) ([MP3](https://en.wikipedia.org/wiki/MP3)). [Off The Hook](https://en.wikipedia.org/wiki/Off_the_Hook_(radio_program)), [2600: The Hacker Quarterly](https://en.wikipedia.org/wiki/2600:_The_Hacker_Quarterly), [WBAI](https://en.wikipedia.org/wiki/WBAI). (17-10-2018)
5. **J** [Rich, Nathaniel](https://en.wikipedia.org/wiki/Nathaniel_Rich_(novelist)) (1 December 2010). ["The American Wikileaks Hacker"](https://www.rollingstone.com/culture/news/meet-the-american-hacker-behind-wikileaks-20101201). [Rolling Stone](https://en.wikipedia.org/wiki/Rolling_Stone). (17-10-2018)
6. **J** Assange, Julian (22 September 2011). ["Julian Assange: 'I am – like all hackers – a little bit autistic'"](https://www.independent.co.uk/news/uk/home-news/julian-assange-i-am-ndash-like-all-hackers-ndash-a-little-bit-autistic-2358654.html). [The Guardian](https://en.wikipedia.org/wiki/The_Guardian). (17-10-2018)
7. Moss, Stephen (13 July 2010). ["Julian Assange: the whistleblower"](https://www.theguardian.com/media/2010/jul/14/julian-assange-whistleblower-wikileaks). The Guardian. (17-10-2018)
8. Zetter, Kim. ["Appeals Court Overturns Conviction of AT&T Hacker 'Weev'"](https://www.wired.com/2014/04/att-hacker-conviction-vacated/). wired.com. Wired. (17-10-2018)
9. [Sterling, Bruce](https://en.wikipedia.org/wiki/Bruce_Sterling) (1991). The Hacker Crackdown: Law and Disorder on the Electronic Frontier. Bantam Books. [ISBN](https://en.wikipedia.org/wiki/International_Standard_Book_Number) [0-553-56370-X](https://en.wikipedia.org/wiki/Special:BookSources/0-553-56370-X). (17-10-2018)
10. ^ Rosenbaum, Ron (October 1971). ["Secrets of the Little Blue Box"](http://www.slate.com/articles/technology/the_spectator/2011/10/the_article_that_inspired_steve_jobs_secrets_of_the_little_blue_.html). slate.com (7 October 2011). [Esquire Magazine](https://en.wikipedia.org/wiki/Esquire_(magazine)). (17-10-2018)
11. Penenberg, Adam L. (10 October 1997). ["Hacking the corporate ladder"](https://www.forbes.com/1997/10/10/feat.html). [Forbes](https://en.wikipedia.org/wiki/Forbes). (17-10-2018)
12. [Levy, Steven](https://en.wikipedia.org/wiki/Steven_Levy) (1984). "[Hackers: Heroes of the Computer Revolution](https://en.wikipedia.org/wiki/Hackers:_Heroes_of_the_Computer_Revolution)". [Doubleday Publishing](https://en.wikipedia.org/wiki/Doubleday_(publisher)). [ISBN](https://en.wikipedia.org/wiki/International_Standard_Book_Number) [0-385-19195-2](https://en.wikipedia.org/wiki/Special:BookSources/0-385-19195-2). (17-10-2018)
13. [Clifford Stoll](https://en.wikipedia.org/wiki/Clifford_Stoll) (1989). [The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage](https://en.wikipedia.org/wiki/The_Cuckoo%27s_Egg). [Doubleday](https://en.wikipedia.org/wiki/Doubleday_(publisher)). [ISBN](https://en.wikipedia.org/wiki/International_Standard_Book_Number) [0-385-24946-2](https://en.wikipedia.org/wiki/Special:BookSources/0-385-24946-2). (17-10-2018)
14. Phil Lapsley; Steve Wozniak (January 2013). Exploding the Phone: The Untold Story of the Teenagers and Outlaws who Hacked Ma Bell. [Grove Press](https://en.wikipedia.org/wiki/Grove_Press). [ISBN](https://en.wikipedia.org/wiki/International_Standard_Book_Number) [9780802120618](https://en.wikipedia.org/wiki/Special:BookSources/9780802120618). (17-10-2018)
15. Martin, Douglas (20 August 2007). ["Joybubbles, 58, Peter Pan of Phone Hackers, Dies"](https://www.nytimes.com/2007/08/20/us/20engressia.html?_r=0). [The New York Times](https://en.wikipedia.org/wiki/The_New_York_Times). (17-10-2018)
16. ["Wired 12.04: The Homeless Hacker v. The New York Times"](https://www.wired.com/wired/archive/12.04/hacker_pr.html). Wired.com. (17-10-2018).
17. Heiman, J.D. (March 1997). ["Banned from the Internet"](https://web.archive.org/web/19980215154642/http://www.paranoia.com/~mthreat/swing.html). Swing Magazine. pp. 70–75. Archived from [the original](http://www.paranoia.com/~mthreat/swing.html) on 15 February 1998.. (17-10-2018)
18. Williams, Sam (1 March 2002). Free as in Freedom: Richard Stallman's Crusade for Free Software. [O'Reilly Media](https://en.wikipedia.org/wiki/O%27Reilly_Media). [ISBN](https://en.wikipedia.org/wiki/International_Standard_Book_Number) [0-596-00287-4](https://en.wikipedia.org/wiki/Special:BookSources/0-596-00287-4) – via [Free Software Foundation](https://en.wikipedia.org/wiki/Free_Software_Foundation) 2nd edition ("2.0") [online copy](https://static.fsf.org/nosvn/faif-2.0.pdf). ([PDF](https://en.wikipedia.org/wiki/PDF)). (17-10-2018)
19. Reed, Dan; Wilson, David L. (November 6, 1998). ["Whiz-kid hacker caught"](https://web.archive.org/web/20001007150311/http://www.mercurycenter.com/archives/reprints/hacker110698.htm). San Jose Mercury News. Archived from [the original](http://www.mercurycenter.com/archives/reprints/hacker110698.htm) on October 7, 2000. (17-10-2018)
20. Penenberg, Adam (7 Feb 2000). ["Space Rogue"](https://www.forbes.com/2000/02/07/penenberg_0207.html). [Forbes](https://en.wikipedia.org/wiki/Forbes). USA. Retrieved 25 May2018 (17-10-2018).
21. Michelle Slatalla; Joshua Quittner (December 1994). ["Gang War in Cyberspace"](http://archive.wired.com/wired/archive/2.12/hacker.html). archive.wired.com. [Wired Magazine](https://en.wikipedia.org/wiki/Wired_Magazine). p. 5. Retrieved 28 March 2015. (17-10-2018)
22. ["Suing Wikipedia: How a Dead Hacker Shut Down Wikipedia Germany"](http://www.spiegel.de/international/suing-wikipedia-how-a-dead-hacker-shut-down-wikipedia-germany-a-396307.html). [Spiegel Online](https://en.wikipedia.org/wiki/Spiegel_Online). 20 January 2006. Retrieved 28 March 2015. (17-10-2018)
23. [Fred Thompson](https://en.wikipedia.org/wiki/Fred_Thompson) (24 June 1998). ["Prepared Statement of Senator Fred Thompson, Chairman Committee on Governmental Affairs"](http://www.hsgac.senate.gov/download/?id=7ef5e7ad-2005-4006-801f-9b9c65839ded) ([PDF](https://en.wikipedia.org/wiki/PDF)). U.S. Federal Government. (17-10-2018)
24. Diane Frank; Paula Shaki Trimble (1999-12-22). ["Feds leave doors open for hackers"](http://archives.cnn.com/1999/TECH/computing/12/22/feds.easy.hack.idg/index.html). [CNN](https://en.wikipedia.org/wiki/CNN). (17-10-2018)
25. [Hacker Mudge Gets DARPA Job](http://news.cnet.com/8301-27080_3-10450552-245.html) (17-10-2018)

# Andere Bronnen

AVG. (2018, oktober 17). *the most dangerous hackers today*. Opgehaald van AVG.com: https://www.avg.com/en/signal/the-most-dangerous-hackers-today

NOS. (2018, oktober 16). *Zware DDoS-aanvallen: wie, wat, waar en waarom?* Opgehaald van NOS.nl: https://nos.nl/artikel/2214400-zware-ddos-aanvallen-wie-wat-waar-en-waarom.html

panda. (2018, 10 17). *pandasecurity*. Opgehaald van panda: https://www.pandasecurity.com/security-promotion/?reg=NL&lang=nl&track=100675&coupon=40OFFMULTIP&campaign=dome1802&option=mix&x-hideselection=true&telef=si&gclid=CjwKCAjwu5veBRBBEiwAFTqDwVls22Q40ls9kr5b3ztqFRlp8YNmN1PVW09WbFAr9JaLBrrUf0oVjhoCy4gQAvD\_BwE

seniorweb. (sd). *seniorweb*. Opgehaald van https://www.seniorweb.nl/artikel/back-up-maken-de-mogelijkheden