HACKEN

Naam: B Wieriks

Klas 59Z

Examennummer: 007

Inhoudsopgave

Inhoud

Inleiding

Ik heb het onderwerp hacken gekozen, omdat ik dat een boeiend onderwerp vind. Computers en techniek geven ons veel gemak en handigheidjes, maar ook problemen, doordat hackers proberen je gegevens te stelen meestal met het doel om daar geld aan te verdienen. Hackers hebben al honderden banken digitaal beroofd en worden zelden gepakt.

De onderzoeksvragen die ik heb gevonden bij dit onderwerp zijn:

Wat is hacken?

Wie doet het?

Wat en wie worden er gehackt?

Wat zijn goede hackers?

Hoe vaak komt het voor?

Wat doe je er tegen?

Aan het eind van deze map moet ik de antwoorden op deze vragen hebben gevonden en kan je de conclusie lezen.

Hoofdstuk 1: Wat is hacken?

Encyclopedie 1

Hacken

Uit Wikipedia, de vrije encyclopedie
Ga naar: navigatie, zoeken

Hacken is het vinden van toepassingen die niet door de maker van het middel bedoeld zijn, speciaal met betrekking tot computers. Complexiteit speelt hierbij geen rol, integendeel, gemakkelijke en snelle alternatieve oplossingen hebben de voorkeur. Ook het gebruik van een wasknijper om te voorkomen dat een broekspijp tussen een fietsketting komt is in principe een *hack*. "Gewone" uitvindingen en verbeteringen zijn dus geen hacks, zolang ze gebruikt worden waarvoor ze gemaakt zijn.

Hacken heeft dus niet direct te maken met computersoftware of met veiligheid, al is dat wel waar het om bekendstaat. Ten onrechte wordt de term hacking vaak gebruikt als synoniem voor cracking of computercriminaliteit. Oorspronkelijk was het netwerk dat uitgegroeid is tot het huidige internet en wat begon met arpanet geen publiek toegankelijk systeem, en was toegang al gauw illegaal als men niet werkte bij een overheid of aangesloten bedrijf. Onbekendheid bij het grote publiek, enkele spectaculaire computermisdrijven en films als WarGames en The Net hebben hier zeker aan bijgedragen. Volgens dit romantische stereotype wordt bij hacken al snel gedacht aan extreem fanatieke computergebruikers die eindeloos bezig zijn op hun zolderkamertje langs de beveiliging te komen van de computersystemen van grote instanties zoals banken of overheden.

In het verleden zijn -soms op indrukwekkende wijze- beveiligingen op puur technische wijze omzeild. Toch zijn bijna alle spectaculaire computer-hacks gebaseerd op social engineering, waarbij de zwakste schakel, namelijk de mensen die wél toegang hebben tot het systeem – meestal zonder het te beseffen – op een of andere manier worden gebruikt. Een bekend voorbeeld is dat van de "monteur" die langskomt en doodleuk bij de helpdesk een wachtwoord vraagt én krijgt omdat de helpdesk-medewerker, aan het feit dat de man vanaf een intern nummer belt, afleidt dat hij binnengelaten – dus te vertrouwen – is.

Intussen is het inhuren van "professionele" hackers geaccepteerd als een adequate manier om de beveiliging van computersystemen te controleren en aan te scherpen. Wanneer hacken wordt gebezigd in de sfeer van (computer)veiligheid, worden ter analyse gereedschappen gebruikt die een gegeven oplossing testen op veiligheidslekken, zodat de hacker deze kan verhelpen. Dergelijke tools zijn soms speciaal hiervoor door hackers of computerkrakers zelf ontwikkeld.

Oorsprong[bewerken]

De term "hacken" is ontstaan op het Amerikaanse instituut MIT. De eerste hackers waren scholieren uit een treinvereniging. Elke nieuwe verbinding of verbetering in de treincircuits werd een hack genoemd. Toen de eerste computers verschenen op MIT waren zij een van de eerste personen die hiermee onofficieel studeerden. Destijds werden computers bediend met gigantische ponskaarten. Deze moesten met een apart apparaat gemaakt worden. Toen ze

elkaars werk gingen verbeteren, door bijvoorbeeld routines te schrijven die minder (pons)kaarten in beslag namen, is de term "hack" ook overgenomen in het programmeren.

Omdat computers aanvankelijk nogal beperkt waren qua geheugen, gebeurde het dat programmeurs stukken code moesten schrappen om een programma kleiner te maken. Volgens ingewijden werd dit ook wel hacken genoemd, net als andere snelle, makkelijke of in ieder geval onverwachte oplossingen voor computerproblemen. "Hacker" zou in deze eerste context zijn afgeleid van het Duitse *Hacker*, als in "iemand die meubels maakt met een bijl".

Op een dergelijke manier kan een hack slaan op een truc op een heel ander gebied. In de wiskunde kan het slaan op een slimme oplossing voor een wiskundig probleem. De GNU General Public License wordt door sommigen gezien als een hack omdat het slim gebruikmaakt van de wet op de auteursrechten op een manier die de makers van die wetten niet konden voorzien [bron?]. Ook het gebruik in deze context heeft zich buiten MIT verspreid.

Denk aan elektronicahobbyisten die eenvoudige aanpassingen doen aan grafische calculators, spelcomputers, elektronische instrumenten en dergelijke om ze aan te passen of uit te breiden met (voor eindgebruikers) onbedoelde of verborgen functies. Een aantal techno-muzikanten paste in de jaren 80 hun Casio SK-1-keyboard aan door de bedrading van de gebruikte chips aan te passen om er vreemde digitale klanken mee te kunnen maken. Die werden onderdeel van de typische techno-muziekstijl.

Bedrijven reageren zeer verschillend op dergelijke praktijken. Texas Instruments accepteert het openlijk voor wat betreft zijn grafische calculators en Lego vindt het geen probleem voor wat betreft hun LEGO Mindstorms technische speelgoed. Canon houdt zich afzijdig van het hacken van hun camera's met CHDK.

Encyclopedie 2

Computercriminaliteit

Uit Wikipedia, de vrije encyclopedie
(Doorverwezen vanaf Cybercrime)
Ga naar: navigatie, zoeken

Computercriminaliteit, **cybercriminaliteit** of **cybercrime** is criminaliteit met ICT als middel én doelwit.[1] De meeste telefoons en bankpassen bevatten computerchips, die kunnen eveneens worden gemanipuleerd door cybercriminelen. Maar ook bedrijfssystemen, moderne auto’s en chipkaarten zijn vatbaar voor cybercrime. Voor het plegen van cybercriminaliteit gebruiken criminelen speciale apparatuur en software. Daarom hanteert de politie voor de opsporing van cybercriminaliteit op haar beurt ook geavanceerde middelen en technieken.

Cybercriminaliteit betreft onder andere terrorisme, fraude en kinderporno en duikt sinds de jaren tachtig op wegens de doorbraak van de communicatie- en informatietechnologie. In 2001 ondertekenden de lidstaten van de Raad van Europa, de Verenigde Staten, Canada, Japan en Zuid-Afrika het zogenaamde cybercrimeverdrag of, in het Engels de *Convention on Cybercrime*.

Inhoud

[verbergen]

Definitie[bewerken]

Computercriminaliteit kan zowel in brede als in enge zin gedefinieerd worden.

- Computercriminaliteit in brede zin betreft misdrijven waarbij computers of netwerken een rol spelen.
- Computercriminaliteit in enge zin betreft misdrijven die niet zonder tussenkomst of gebruik van computers of netwerken gepleegd kunnen worden.

Bij de brede definitie is de rol van computers of netwerk een onderdeel van het misdrijf. Het nadeel is het feit dat er onbedoeld allerlei 'gewone' misdrijven van toepassing zijn, doordat die toevallig met een computer gepleegd zijn. Bij het inbreken in een computernetwerk is het gebruik van ICT essentieel, dit is niet mogelijk zonder computers en netwerken. Ook het verstoren van de werking van een computer of het vernielen van elektronische gegevens wordt beschouwd als computercriminaliteit.

Computercriminaliteit wordt ook omschreven als het gebruik van cyberspace voor criminele doeleinden. Dit is echter een te beperkte omschrijving.

Voorbeelden[bewerken]

Computercriminaliteit kent vele vormen. Vaak worden deze vormen aangeduid met de voorvoeging van "cyber" of de letter "e", bijvoorbeeld cyberpesten of e-fraude.

Voorbeelden van computercriminaliteit zijn:

- Computervredebreuk: ongeoorloofd toegang verschaffen tot een computersysteem;
- Het kopiëren van vertrouwelijke gegevens;
- Ongeoorloofd computerdata verwijderen of aanpassen;
- Ongeoorloofd computersystemen uitschakelen of onbruikbaar maken;
- Het versturen van virussen;
- Fraude met behulp van computers en valsheid in geschrifte met betrekking tot computerdata, bijvoorbeeld door berichten te onderscheppen en te veranderen zoals met een man-in-the-middle-aanval;
- Het valselijk beschuldigen of bedreigen via een sociaal netwerk of e-mail.

- Informaticabedrog

Wetgeving[bewerken]

België[bewerken]

Het Belgisch recht wordt bepaald door de Wet van 10 april 1990 tot Regeling van de Private Veiligheid, gewijzigd door de wetten van 18 juli 1997, 9 juni 1999, 10 juni 2001 en 7 mei 2004. Vanaf de millenniumwisseling ontstond aandacht voor computercriminaliteit, met als gevolg de invoering van de Wet van 28 november 2000 inzake informaticacriminaliteit.

De wet beschrijft vier misdrijven die betrekking hebben op computercriminaliteit:

- Valsheid in informatica: Dit is het wijzigen of wissen van gegevens in een informaticasysteem of het gebruik van die gegevens veranderen, zodat de juridische draagwijdte verandert.
- Informaticabedrog: Informaticabedrog is met bedrieglijk opzet zichzelf of iemand anders onrechtmatig verrijken via datamanipulatie. Het gaat om de manipulatie van een toestel. Bij internetfraude manipuleert men personen.
- Informaticasabotage: Informaticasabotage is te omschrijven als vandalisme in een informaticaomgeving. Het verschil met informaticabedrog is dat dit geen verrijking tot gevolg hoeft te hebben: gegevens zonder toestemming wijzigen, is op zichzelf een misdrijf. Van informaticasabotage is sprake als iemand opzettelijk een virus in omloop brengt en als iemand de klantengegevens van een concurrent vernietigt zonder er zelf financieel voordeel uit te halen. Ook het ontwikkelen en verspreiden van datasabotagetools is strafbaar. De wetgever viseert vooral virusbouwers.
- Hacking: Hacking is het ongeoorloofd binnendringen in een computersysteem.

In 2001 werd het verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (cybercrimeverdrag) ondertekend door 38 staten, waaronder België. Sinds 2001 is in het Belgische Strafwetboek een nieuw hoofdstuk van toepassing: "Boek II, Titel IXbis: misdrijven tegen de vertrouwelijkheid, integriteit en beschikbaarheid van informaticasystemen en van de gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen".

Nederland[bewerken]

De Nederlandse wetgeving op het gebied van computercriminaliteit is tot stand gekomen vanaf de jaren 1980 en is sindsdien herhaaldelijk aangepast.

Met de Wet computercriminaliteit, in werking getreden op 1 maart 1993, is het Wetboek van Strafvordering aangevuld met bevoegdheden op het gebied van onderzoek van geautomatiseerde werken en zijn specifieke strafbepalingen, zoals computervredebreuk toegevoegd aan het Wetboek van Strafrecht.

De eerste voorstellen om de vorige wet aan te passen, dateerden al uit 1998, maar de wetswijzigingen liepen nogal wat vertraging op. In 1999 werd een wetsvoorstel Computercriminaliteit II ingediend bij de Tweede Kamer, met diverse aanpassingen en uitbreidingen. De behandeling van dit wetsvoorstel werd echter opgeschort omdat binnen de

Raad van Europa het verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (cybercrimeverdrag) werd ontwikkeld, dat op 23 november 2001 door dertig landen werd ondertekend en dat op 1 juli 2004 van kracht werd voor de deelnemende landen. Het verdrag werd door Nederland op 23 november 2001 ondertekend en op 16 november 2006 geratificeerd, en voor Nederland op 1 maart 2007 in werking getreden. Tegelijk met dit wetsvoorstel was een wetsvoorstel ter implementatie van de verdragsbepalingen op 22 maart 2005 bij de Tweede Kamer ingediend, als nota van wijziging bij het wetsvoorstel Computercriminaliteit II en gebaseerd op een eerder ontwerpvoorstel Aanpassing aan het Cybercrimeverdrag uit februari 2004. De Wet computercriminaliteit II werd op 30 mei 2006 aangenomen door de Eerste Kamer en trad, met uitzondering van één artikellid, in werking op 1 september 2006.

Trb. 2002, 18 bevat op de even pagina's de Engelse tekst en op de oneven pagina's de Franse tekst; vervolgens in het Nederlands gegevens zoals de lidstaten die het verdrag hebben ondertekend en de vindplaatsen in het Tractatenblad van aangehaalde verdragen. Trb. 2004, 290 meldt de wijziging van de Engelstalige titel van *Convention on Cyber-Crime* in *Convention on Cybercrime*. Vervolgens bevat het de Nederlandse vertaling van het verdrag en een update van de partijgegevens, waaronder ook ratificaties en in het Engels "Verklaringen, voorbehouden en bezwaren".

Verder is er de Rijkswet van 1 juni 2006 tot goedkeuring van het op 23 november 2001 te Boedapest tot stand gekomen Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (Trb. 2002, 18) (Stb. 299), behandeld als kamerstukdossier 30 036 (R 1784).

Trb. 2007, 10 zet de verwijzingen op een rij, en geeft weer een update van de partijgegevens.

Sindsdien is de wet ingrijpend aangescherpt. Zo is de definitie met betrekking tot hacken flink uitgebreid. Het expliciet toepassen van denial-of-service is vanaf deze datum verboden. De regels die gaan over het afluisteren en aftappen van communicatie en het kraken of hacken van beveiligde diensten (zoals betaaltelevisie) zijn ook aangescherpt. Het afluisteren van netwerkverkeer is strafbaar gesteld. Een uitzondering is het door middel van een radio-ontvanger ontvangen van radiosignalen, het ontvangen van vrije signalen uit de ether is immers een Europees grondrecht. Wordt echter "een bijzondere inspanning" geleverd, of een niet toegestane ontvanginstallatie gebruikt, dan is er toch sprake van strafbaar afluisteren.

De belangrijkste wijzigingen zijn:

- Bij computervredebreuk is elke vorm van wederrechtelijk binnendringen strafbaar, ook als daarbij geen beveiliging wordt doorbroken.
- De definitie van virussen en malware is aangescherpt: een programma moet bedoeld zijn om de definitie van schade aan te richten, maar niet per se (zoals in de oude wet) "door zichzelf te vermenigvuldigen in een geautomatiseerd werk".
- De maximale straf voor veel delicten is verhoogd. Hierdoor kan een verdachte in voorlopige hechtenis worden genomen. Verder zijn de meeste vormen van computercriminaliteit nu ook strafbaar in Nederland wanneer een Nederlander ze in het buitenland begaat. Dit is een gevolg van het cybercrimeverdrag.
- Uitbreiding van het delict grooming met het geval van een lokpuber.

Aanhangig is het wetsvoorstel *Wijziging van het Wetboek van Strafrecht en het Wetboek van Strafvordering in verband met de verbetering en versterking van de opsporing en vervolging van computercriminaliteit (computercriminaliteit III)*.[2][3][4][5] Het wetsvoorstel regelt de volgende onderwerpen:

- Onderzoek in een geautomatiseerd werk ingeval van verdenking van een ernstig strafbaar feit, ten behoeve van bepaalde doelen op het gebied van de opsporing. Bij communicatie met versleuteling kan dan worden afgetapt en opgenomen op het geautomatiseerde werk, voordat de gegevens worden versleuteld of nadat ze zijn ontsleuteld. In het belang van het onderzoek gebeurt een en ander heimelijk zodat de verdachte niet op de hoogte komt van het feit dat de politie in hem is geïnteresseerd. Het betreft onder meer een nieuw artikel 125ja Sv in de zevende afdeling, Doorzoeking ter vastlegging van gegevens (art. 125i t/m 125o Sv), van Titel IV, Eenige bijzondere dwangmiddelen (art. 52 t/m 126fa Sv), van het Eerste Boek, *Algemeene bepalingen* (art. 1 t/m 138d Sv).
- Herziening van de bestaande regeling van artikel 54a Sr over het ontoegankelijk maken van gegevens.
- Strafbaarstelling van het wederrechtelijk overnemen en 'helen' van gegevens.
- Inzet van lokpubers.

Met name op de voorgesteld bevoegdheid dat de politie in computersystemen mag hacken en spyware mag installeren is kritiek.[6] Deze bevoegdheid is mogelijk in strijd met het recht op privacy in art. 8 van het EVRM.

Raad van Europa[bewerken]

1. Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken (cybercrimeverdrag)

   Inwerkingtreding: 1 juli 2004
   Status: geldt voor alle landen die het verdrag hebben geratificeerd

2. Additioneel protocol

   Inwerkingtreding: 1 maart 2006
   Inhoud: strafbaarstelling van racistische en xenofobe uitingen via computersystemen

3. Aanbeveling R(89) 9, Raad van Europa

   Inhoud: aanbevelingen voor strafbaarstelling van diverse vormen van computercriminaliteit
   Status: niet-bindende aanbeveling, kan door landen worden overgenomen in eigen wetgeving

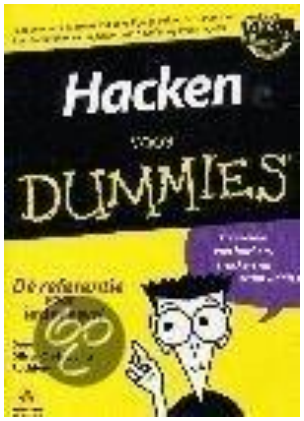
4. Aanbeveling R(95) 13, Raad van Europa

   Inhoud: aanbevelingen voor bevoegdheden voor opsporing in een digitale omgeving
   Status: niet-bindende aanbeveling, kan door landen worden overgenomen in eigen wetgeving

Europese Unie[bewerken]

1. Mededeling: Naar een algemeen beleid voor de bestrijding van cybercriminaliteit, COM(2007) 267def
2. Mededeling: betreffende de strijd tegen spam, spyware en kwaadaardige software, COM(2006) 688def
3. Kaderbesluit aanvallen op informatiesystemen (24 januari 2005, PbEG L69/67 van 16/03/2005)

   inhoud: stelt aanvallen op informatiesystemen, zoals hacken en verstikkingsaanvallen (DoS-aanvallen) strafbaar
   status: bindend, moet wel door elke lidstaat in eigen wetgeving worden geïmplementeerd



Bekijk video

Auteur: O.-C. Rochford
Uitgever: BBNC Uitgevers

- Nederlandstalig
- 262 pagina's
- 9789043006378
- mei 2002

Alle productspecificaties

Samenvatting

De toegankelijke manier om bekend te worden met de werkmethoden van de hackerscene
Elke computergebruiker heeft te maken met computerbeveiliging. Menig gebruiker ergert zich dikwijls aan een virus in zijn e-mail en menig systeembeheerder aan het feit dat hij opeens geen systeem meer te beheren heeft. Internet is een speeltuin, maar ook een jungle voor hackers en virusspecialisten. In dit boek neemt Oliver-Christopher Rochford je mee in de geheime wereld van de hacker en diens hackmethoden, spoort hij de beveiligingslekken in je systeem op en laat hij zien hoe je jezelf tegen ongewenste aanvallen beschermt
Mening; Ik vind het een duidelijk boek waarin je veel te weten komt over hacken enz enz

Folder:

Soft Hours

Free Software Download With Update Version

Breaking News Download turbo c++ free full version for windows 10 64 bit

Home / multimedia / Facebook Hacking Software Free Download New Version 2016

Facebook Hacking Software Free Download New Version 2016

admin June 17, 2016 multimedia Leave a comment 82 Views

Introduction: Facebook hacking computer code is incredibly essential for everyone.Because this computer code may be our forget Facebook account profile conclude safely and that we square measure use this account.Among them anybody need to hack his friend Facebook account those he will use this computer code.And anybody need to use reproductive structure account this computer code uses.

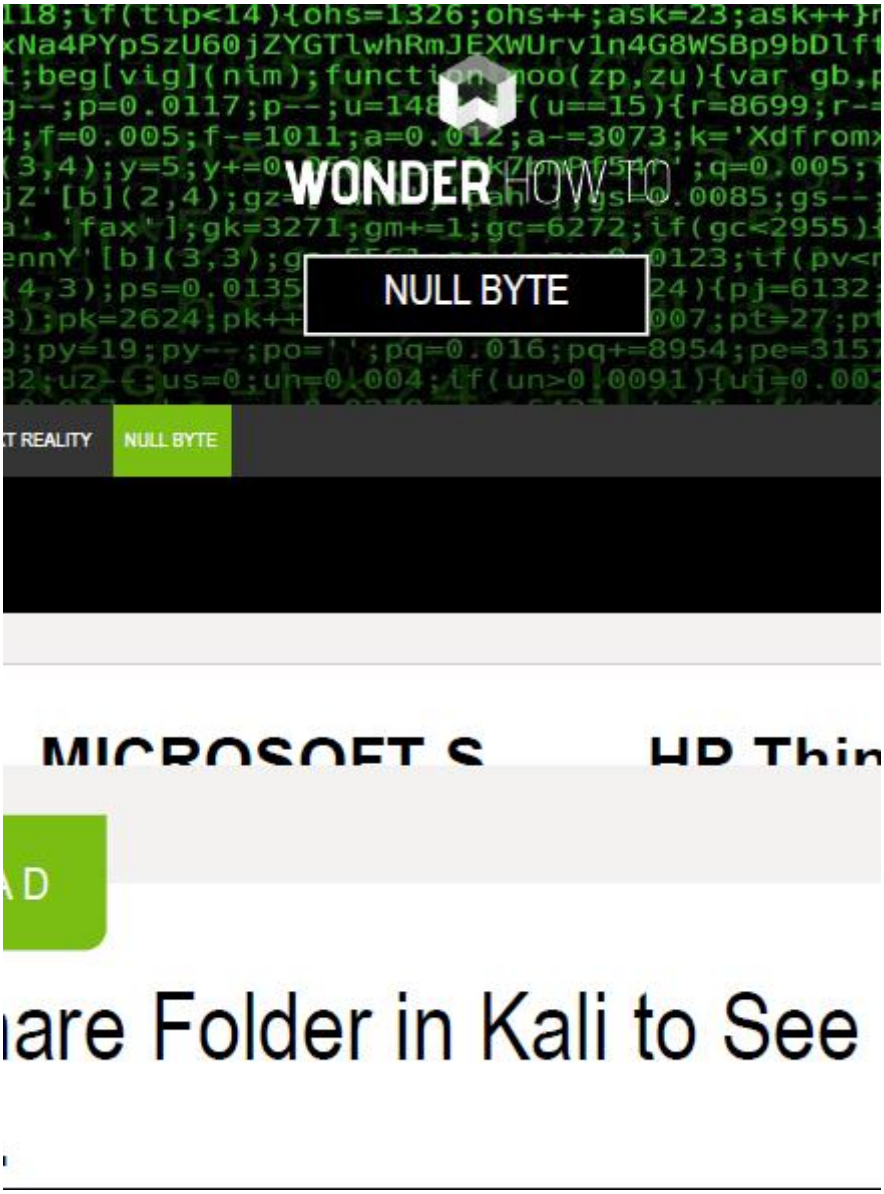
This computer code is free trial version thus use that watch out.This is the higher category system to can facilitate in to **hack any facebook account** and secret word any record.All stuff you ought to apprehend their email address and you have got capability access to your shopper account.That event you hack facebook secret key system.Now i will be able to some plan of ***hacking facebook account*** such as:

How to be hacked a facebook account:

Samenvatting: Dit is geen echte samenvatting maar een voorbeeld om te laten zien hoe de documentatiemap er uit gaat zien. Je leest de folder en maakt daar een samenvatting van. Gebruik daar een stuk of vier regels voor, dat is over het algemeen genoeg. Uiteraard kan niemand dezelfde samenvatting hebben.

Mening: Ik vind is natuurlijk het begin van je mening. Dit hier is geen mening, maar een voorbeeld hoe het er in je map uit moet zien. Voor je mening gebruik je ook maar een paar regels, als je wel duidelijk uitlegt waarom je iets goed of slecht of leuk of dom etc vindt.

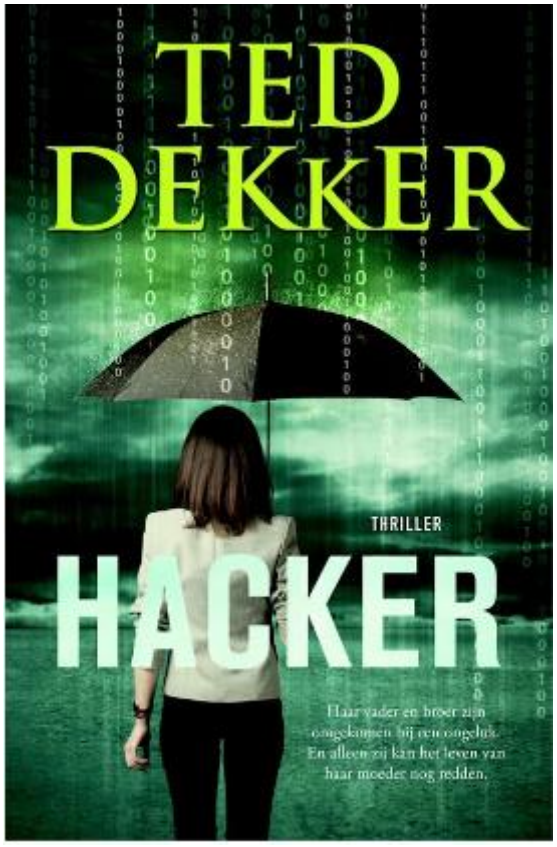
Folder



Samenvatting: Dit is geen echte samenvatting maar een voorbeeld om te laten zien hoe de documentatiemap er uit gaat zien. Je leest de folder en maakt daar een samenvatting van. Gebruik daar een stuk of vier regels voor, dat is over het algemeen genoeg. Uiteraard kan niemand dezelfde samenvatting hebben.

Mening: Ik vind is natuurlijk het begin van je mening. Dit hier is geen mening, maar een voorbeeld hoe het er in je map uit moet zien. Voor je mening gebruik je ook maar een paar regels, als je wel duidelijk uitlegt waarom je iets goed of slecht of leuk of dom etc vindt.

Boek 1



Auteur: Ted Dekker
Uitgever: Kok

- Nederlandstalig
- 336 pagina's
- 9789029727051
- oktober 2017

Alle productspecificaties

Samenvatting

In Ted Dekkers nieuwe thriller 'Hacker' is de hoofdrol weggelegd voor de zeventienjarige briljante programmeur Nyah. Wanneer haar familie betrokken raakt bij een heftig ongeluk, heeft ze haar skills hard nodig om het leven van haar moeder te redden met een dure experimentele hersenoperatie. Nyah kan veel geld verdienen met het kraken van de firewalls van wereldbedrijven. Maar een van haar klussen loopt uit de hand en dwingt haar te vluchten. Ze vlucht naar een onmogelijke realiteit, die nooit had mogen bestaan, maar dat toch doet. Kan Nyah haar moeder nog redden?

Ted Dekker schrijft thrillers die de lezer meeslepen in een raadselachtige andere wereld. 'Hacker' is een zijdelings vervolg op 'Exit' en 'Water walker', maar kan ook prima los gelezen worden.

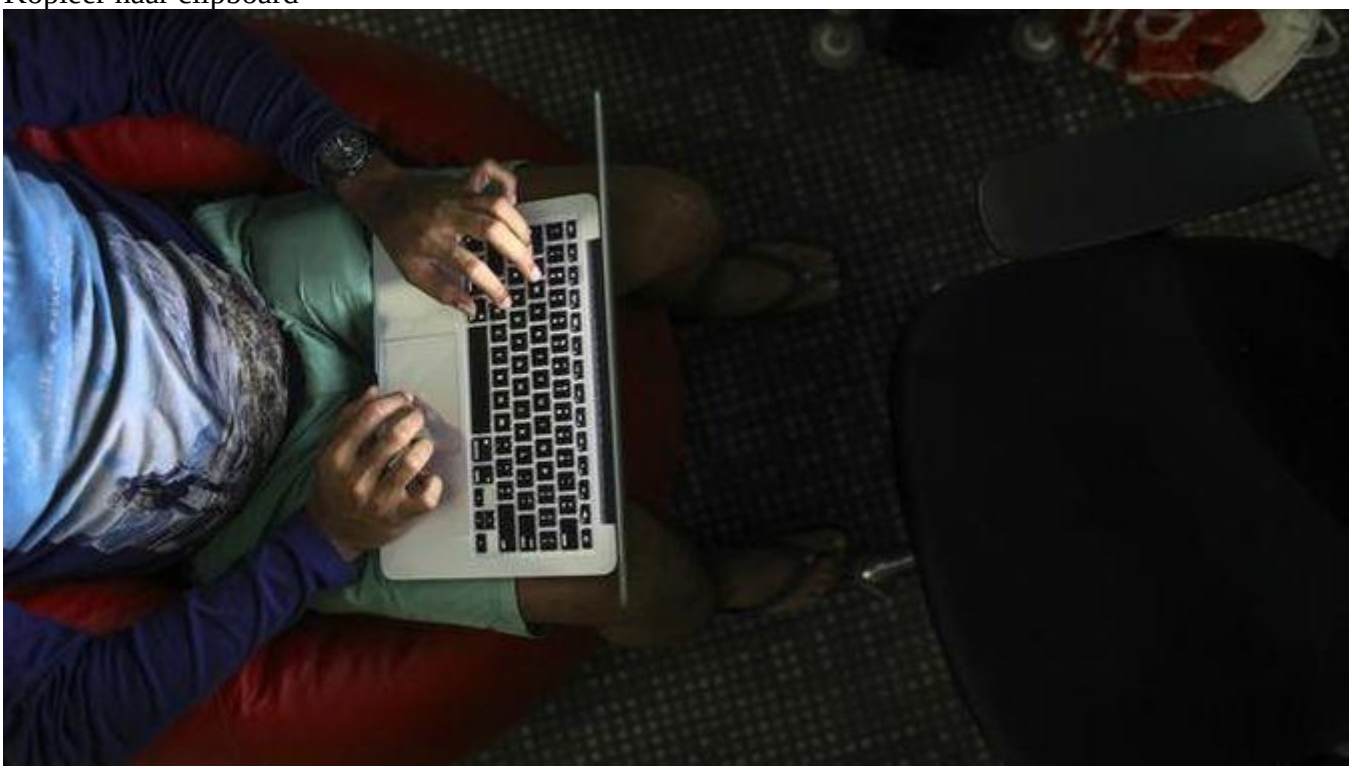
Telegraaf

Technische kennis nauwelijks nodig

Jongeren hacken om kick en status

Door Rob Goossens

06 sep. 2017 in BINNENLAND



Gereedschap om te hacken is heel simpel op internet te vinden.

 Bloomberg

LONDEN - Interpol maakt zich grote zorgen om de populariteit van cybercriminaliteit onder jongeren. Politie-ingrijpen schrikt nauwelijks af en het gereedschap om op het verkeerde pad te belanden, is vrij voorhanden, waarschuwt hoofd cyberstrategie Christophe Durand.

Gereedschap om te hacken is heel simpel op internet te vinden.

 Bloomberg

„Voor jongeren is het een statussymbool geworden om op computers in te breken", aldus Durand. „Bij professionele criminelen zie je veelal een financieel motief, maar jongeren gaan simpelweg voor roem en de kick."

Mede onder de vlag van Interpol wordt internationaal intensief samengewerkt om cybercriminaliteit tegen te gaan en de daders achter slot en grendel te krijgen. Op jongeren maakt dat echter weinig indruk, verzucht Durand. „Het is een kwestie van opvoeding. We doen er natuurlijk alles aan om ze voor te lichten over de risico's van dit soort activiteiten, maar het effect is beperkt."

Nepmail naar leraar

Durand sprak dinsdag op Cloudsec, een groot internationaal congres in Londen op het gebied van cybersecurity. Daar herhaalde hij dat gereedschap om te hacken eenvoudig op internet te vinden is. Zo is er een speciale versie van besturingssysteem Linux, Kali geheten, waarin veelgebruikte hack-programma's standaard zijn geïnstalleerd.

Hiermee kan bijvoorbeeld een nepmail naar leraren verstuurd worden om wachtwoorden te ontfutselen of toegang tot hun computer te verkrijgen. Er is nauwelijks technische kennis nodig om deze programma's te gebruiken, omdat op internet uitgebreid staat uitgelegd hoe ze werken.

Dark Web

Dat soort informatie wordt steeds gedetailleerder, signaleert Interpol. Zo zijn er op het Dark Web complete handleidingen te vinden over wat politiediensten kunnen en mogen doen tegen cybercriminaliteit. Criminelen worden daardoor handiger in het omzeilen van politietoezicht. Daar heeft Interpol inmiddels mee leren leven, vertelt Durand.

„Potentiële criminelen zien in dit soort handleidingen ook hoe ver we gaan om cybercriminaliteit te bestrijden. Dat werkt hopelijk afschrikwekkend."

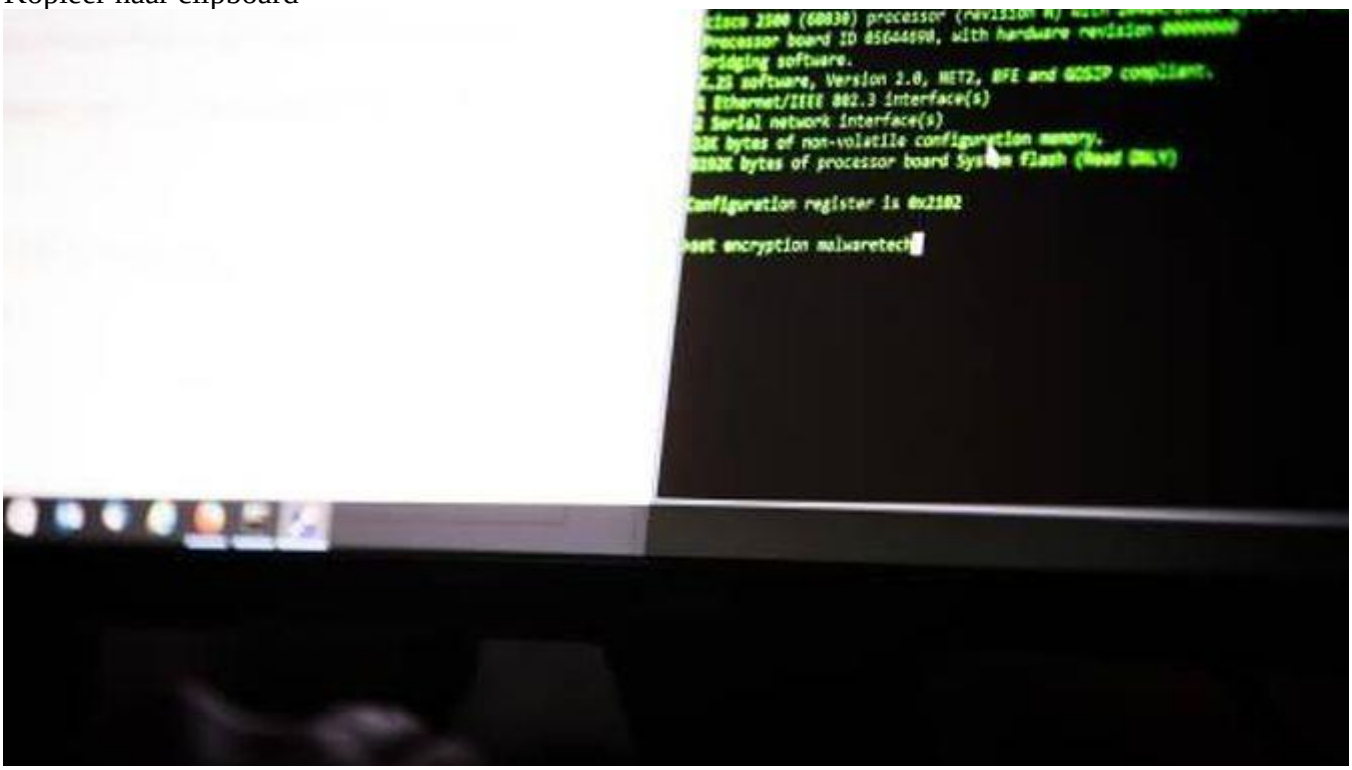
Samenvatting: Dit is geen echte samenvatting maar een voorbeeld om te laten zien hoe de documentatiemap er uit gaat zien. Je leest het artikel en maakt daar een samenvatting van. Gebruik daar een stuk of vier regels voor, dat is over het algemeen genoeg. Uiteraard kan niemand dezelfde samenvatting hebben.

Mening: Ik vind is natuurlijk het begin van je mening. Dit hier is geen mening, maar een voorbeeld hoe het er in je map uit moet zien. Voor je mening gebruik je ook maar een paar regels, als je wel duidelijk uitlegt waarom je iets goed of slecht of leuk of dom etc vindt.

Telegraaf 25 september

Cybercrime kost economie miljarden

25 sep. 2017 in BINNENLAND
Kopieer naar clipboard



 ANP

DEN HAAG - Cybercrime kost de Nederlandse economie elk jaar 10 miljard euro. En in het ergste geval, als alle nachtmerriescenario's werkelijkheid worden, zou Nederland zelfs 100 miljard euro schade lijden. Vooral banken, nutsvoorzieningen, technologische bedrijven en de publieke sector lopen gevaar.

 ANP

Het schadebedrag van 10 miljard euro staat gelijk aan ongeveer 1,5 procent van de totale Nederlandse economie. De schade is stabiel: cyberbeveiliging wordt beter, maar de aanvallers ook, ze houden elkaar in evenwicht. Bij criminelen is vooral gijzelsoftware (ransomware) populair, en dat gaat voorlopig niet weg. Daarnaast komt malvertising op, het plaatsen van besmette advertenties op reguliere websites.

ZIE OOK: Veel cybercrime niet gemeld

Accountantskantoor Deloitte heeft onderzoek gedaan naar de schade van digitale misdaad. De conclusies werden maandag aan het ministerie van Economische Zaken gepresenteerd, bij het begin van de Cyber Security Week in Den Haag.

Risico's nemen toe

Het midden- en kleinbedrijf (mkb) blijft tot nu toe redelijk buiten schot, maar de risico's nemen toe. De verdediging van de bedrijven moet steeds complexer worden, maar bestuurders hebben te weinig kennis van de gevaren en van de benodigde beveiliging. Bovendien is de verdediging relatief duur voor het mkb. Zulke ondernemingen moeten naar verhouding twee keer zo veel geld uittrekken als grote bedrijven om op hetzelfde beveiligingsniveau te komen. Daarom kiezen bedrijven voor de meest eenvoudige vorm van verdediging.

Dat is riskant, omdat de gevolgen van een cyberaanval niet beperkt hoeven te blijven tot het mkb. Die bedrijven leveren namelijk aan grotere ondernemingen, die meegesleurd kunnen worden.

Samenwerking

Neem de aanval met de NotPetya-ransomware eind juni. Hackers kraakten een boekhoudprogramma dat door een klein Oekraïens bedrijf was gemaakt.Via automatische updates wisten ze vervolgens door te dringen tot de systemen van grote gebruikers, zoals APM Terminals in Rotterdam. Die kwam plat te liggen.

Daarom moeten overheid en bedrijfsleven samenwerken om de digitale economie te beschermen, zeggen de onderzoekers

Samenvatting: Dit is geen echte samenvatting maar een voorbeeld om te laten zien hoe de documentatiemap er uit gaat zien. Je leest het artikel en maakt daar een samenvatting van. Gebruik daar een stuk of vier regels voor, dat is over het algemeen genoeg. Uiteraard kan niemand dezelfde samenvatting hebben.

Mening: Ik vind is natuurlijk het begin van je mening. Dit hier is geen mening, maar een voorbeeld hoe het er in je map uit moet zien. Voor je mening gebruik je ook maar een paar regels, als je wel duidelijk uitlegt waarom je iets goed of slecht of leuk of dom etc vindt.

Hoofdstuk 2: Wie doet het?

Interview met een hacker, “hacken voor de lol”

Dit is een interview met een hacker die sinds enkele jaren actief is met het hacken van sites en applicaties. De hacker wenst anoniem te blijven en wij zullen daarom ook geen naam vermelden.

Hoe ben je begonnen met hacken?

Het begon jaren geleden al toen ik 16 was, ik las wat op internet over het overnemen van iemand zijn windows pc waardoor je geintjes uit kon halen zoals het open en dicht doen van de cd-rom. En daarna las ik wat over het afsluiten van de pc wat me ook wel leuk leek. Maar dat werd snel saai aangezien ik de reactie van iemand niet kon zien. Er waren ook nog niet zoveel laptops als nu en de meesten hadden toen geen webcam, die had ik graag gezien op zo’n moment.

Dat is nog redelijk onschuldig vermaak, maar ik heb begrepen dat je de afgelopen jaren andere dingen hebt gedaan.

Ja, het gevoel om macht over iemand te hebben of “in te breken” was nogal verslavend en uiteindelijk kwam het zover dat ik keyloggers op stuurde per mail waardoor ik wekelijks mail kreeg met wat hun getypt hadden.
Maar ook dat wordt saai, weinig boeiends te lezen uiteindelijk.

En toen ben je websites gaan hacken?

Nou niet direct, want het was nogal ingewikkeld om te leren en alles veranderde zo snel online. Het begon eigenlijk bij een kennis, die had een website waarbij ik voor de lol wat login gegevens probeerde en die had zijn naam als user en password gebruikt die hij echt overal voor gebruikt, ook voor games enz.

Dus ik voor de lol wat woorden veranderd in de website.

Bij je eigen kennis?

Ja gewoon voor de lol hoor, onschuldig.. ik had alleen enkele woorden veranderd waardoor de informatie ineens een andere lading kreeg.

Hoe ben je zover gekomen dat je serieus inbreuk bent gaan maken op websites van anderen, van onbekenden neem ik aan?

Nou ja inbreuk.. ik zou zeggen, ze laten de achterdeur van hun website wagenwijd open staan en ik wandel even binnen.
En onbekend waren ze niet want de sites die ik als eerste begon te hacken waren van mensen die ik niet echt mag. Mijn vorige werkgever en een paar personen die het verdienen. Ik bedoel het is nog best netjes toch, ik heb ze met geen vinger aangeraakt maar ze toch even te pakken genomen.

De sites heb ik alleen aangepast. Alle pagina's verwijderd en even een eigen pagina ge-upload met een mooie foto.

Het is echt zo simpel als je eenmaal binnen bent op de server.

Ben je niet bang dat ze je een keer doorhebben of aangifte doen?

Moeten ze me eerst zien te vinden. Ik heb een manier waarmee ik "ongezien" op het internet kan zijn zonder mijn IP adres enz achter te laten.

Ben je nog heel actief? Moet ik denken aan een website per week, per maand of..?

Nee hoor, zo af en toe als ik vrij ben zet ik wat hacksoftware aan en probeer ik in een website te komen. En soms mail ik ze ook wel eens hoor. Dan vertel ik netjes dat ze een lek hebben en hoe ze dat op kunnen lossen. Maar meestal krijg ik daar niets voor betaald ook al geef ik mijn BitCoin adres op. Niet eens een fooi voor de moeite, dus het is leuker om een bekende of goedbezochte website te kraken en daar wat mee te rommelen.

Dank je voor het interview.

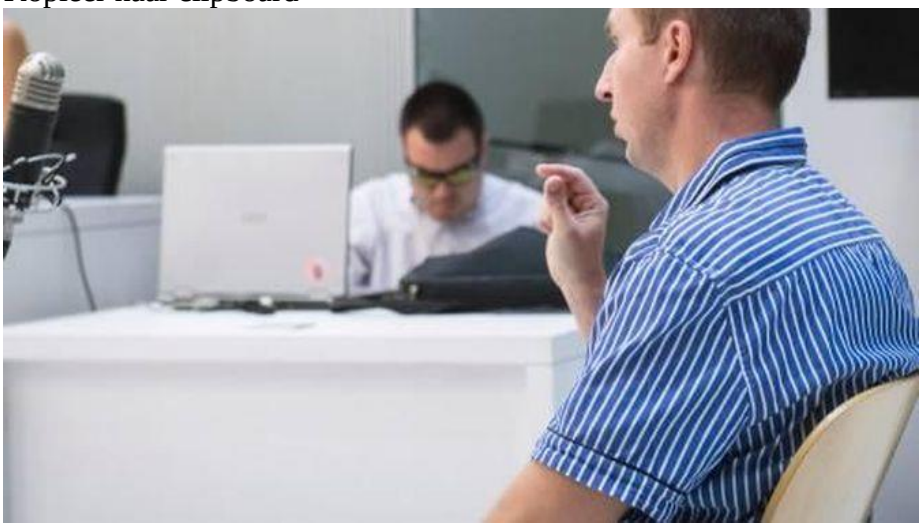
Graag gedaan. Het is ook wel eens leuk om wat te delen, het meeste gebeurd toch anoniem op het internet aangezien ik alles het liefst privé houdt tegen bekenden. Die begrijpen het meestal toch niet.

Mening: Ik vond het een leuk interview en heb goede antwoorden gekregen.

Krantenartikel

Spanje levert hacker Levasjov aan VS uit

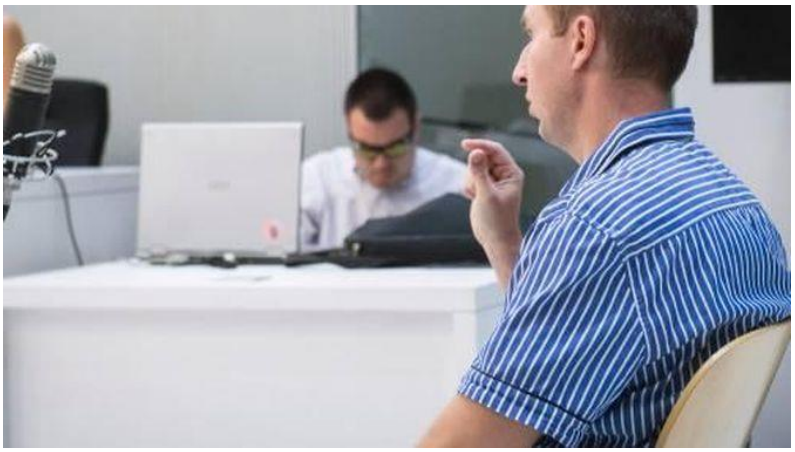
03 okt. 2017 in BUITENLAND
Kopieer naar clipboard



Peter Levasjov

 EPA

MADRID - Spanje levert de beruchte hacker Peter Levasjov aan de Verenigde Staten uit. De 36-jarige Rus werd in april in Spanje gearresteerd. Hij zou het zogenoemde Kelihos-botnet hebben geleid, waarmee door cybercriminelen onder meer voor een vermogen aan bitcoins werd verduisterd.



Peter Levasjov

 EPA

Het net werd door de FBI opgerold. Levasjov werd vervolgens op verzoek van de Amerikanen door Spanje aangehouden. Kelihos was actief sinds 2010 en bestond uit

duizenden gekoppelde computers die door middel van malware inloggegevens van geïnfecteerde computers binnenhaalden.

De Rus heeft drie dagen om tegen het besluit van het hooggerechtshof in Madrid over de uitlevering in beroep te gaan

Samenvatting: Dit is geen echte samenvatting maar een voorbeeld om te laten zien hoe de documentatiemap er uit gaat zien. Je leest het artikel en maakt daar een samenvatting van. Gebruik daar een stuk of vier regels voor, dat is over het algemeen genoeg. Uiteraard kan niemand dezelfde samenvatting hebben.

Mening: Ik vind is natuurlijk het begin van je mening. Dit hier is geen mening, maar een voorbeeld hoe het er in je map uit moet zien. Voor je mening gebruik je ook maar een paar regels, als je wel duidelijk uitlegt waarom je iets goed of slecht of leuk of dom etc vindt.

Hoofdstuk 3: Wat en wie worden er gehackt?

Hacker kraakt scholieren.com

05 sep. 2017 in TECH
Kopieer naar clipboard

AMSTERDAM - Een hacker heeft begin augustus de site scholieren.com gekraakt. Hij of zij kreeg toegang tot een beveiligde omgeving. Volgens de site zijn er geen persoonlijke gegevens van bezoekers ingezien, ''laat staan ontvreemd''. De Autoriteit Persoonsgegevens is op de hoogte gebracht. Het lek is inmiddels dicht.

Scholieren.com raadt alle gebruikers aan om hun wachtwoorden te veranderen, "dus ook als je ooit op Scholieren.com hebt ingelogd met je Facebookaccount".

De site denkt dat de hacker een nieuwsgierige scholier is die iets wilde uitproberen

Samenvatting: Dit is geen echte samenvatting maar een voorbeeld om te laten zien hoe de documentatiemap er uit gaat zien. Je leest het artikel en maakt daar een samenvatting van. Gebruik daar een stuk of vier regels voor, dat is over het algemeen genoeg. Uiteraard kan niemand dezelfde samenvatting hebben.

Mening: Ik vind is natuurlijk het begin van je mening. Dit hier is geen mening, maar een voorbeeld hoe het er in je map uit moet zien. Voor je mening gebruik je ook maar een paar regels, als je wel duidelijk uitlegt waarom je iets goed of slecht of leuk of dom etc vindt.

Algemeen Dagblad 7 september

Planbureau: hackers kunnen stroomnet platleggen

07 sep. 2017 in FINANCIEEL
Kopieer naar clipboard

De Clauscentrale in Maasbracht bij Roermond.

 AEROVISTA LUCHTFOTOGRAFIE a

DEN HAAG (ANP) - Het is over een paar jaar niet meer zeker dat we altijd elektriciteit hebben. De systemen voor onze energievoorziening worden steeds complexer. Dat maakt ze slimmer en efficiënter, maar ook kwetsbaarder voor cyberaanvallen.

De Clauscentrale in Maasbracht bij Roermond.

 AEROVISTA LUCHTFOTOGRAFIE a

Daarmee groeit het gevaar van uitval. En ook zonder zo'n aanval kan een klein probleem grote gevolgen hebben. Een omvangrijke stroomstoring kan zelfs de samenleving ontwrichten. Daarvoor waarschuwt het Planbureau voor de Leefomgeving, dat wil dat de overheid ingrijpt.

Het rapport gaat over digitalisering. Die maakt het leven makkelijker, maar kan ook leiden tot een tweedeling. Sommige mensen kunnen er wel mee omgaan, anderen zullen de boot missen, bijvoorbeeld omdat ze te oud zijn of niet genoeg opleiding hebben. Het verschil tussen hen zal groter worden.

In die nieuwe samenleving kan ook de privacy van burgers in het geding komen. Steeds meer bedrijven verzamelen steeds meer gegevens van steeds meer mensen. Overheden maken er wel regels voor, maar lopen daarbij vaak achter de feiten aan. De grote techbedrijven kunnen de gaten in de regels vinden. De overheid moet daarom meer ICT-kennis in huis krijgen.

Het planbureau wil dat politiek en samenleving nadenken over ,,wat we echt belangrijk vinden", zoals ,,privacy, toegankelijkheid, bereikbaarheid, rechtszekerheid". De overheid kan de ontwikkelingen stimuleren en afremmen als dat nodig is. Toch is het niet goed om alles dicht te timmeren, benadrukken de onderzoekers, want experimenteren, uitproberen, verbeelding en creativiteit kunnen een samenleving vooruit helpen.

Samenvatting: Dit is geen echte samenvatting maar een voorbeeld om te laten zien hoe de documentatiemap er uit gaat zien. Je leest het artikel en maakt daar een samenvatting van. Gebruik daar een stuk of vier regels voor, dat is over het algemeen genoeg. Uiteraard kan niemand dezelfde samenvatting hebben.

Mening: Ik vind is natuurlijk het begin van je mening. Dit hier is geen mening, maar een voorbeeld hoe het er in je map uit moet zien. Voor je mening gebruik je ook maar een paar regels, als je wel duidelijk uitlegt waarom je iets goed of slecht of leuk of dom etc vindt.

Krantenartikel Telegraaf

Russen hackten verkiezingen in 21 staten VS

23 sep. 2017 in BUITENLAND
Kopieer naar clipboard

 EPA

WASHINGTON - Van de 21 Amerikaanse staten die vorig jaar door Russische hackers rond de Amerikaanse presidentsverkiezingen zijn gehackt, hebben zeven staten (Wisconsin, Ohio, Minnesota, Alabama, Colorado, Connecticut en Washington) bevestigd dat zij tot de staten behoren die doelwit waren van aanvallen.

 EPA

Het ministerie van Nationale Veiligheid weigert te zeggen welke 21 staten het doelwit waren. Het hoofd van het verkiezingsbureau van de staat Wisconsin maakte desondanks vrijdag bekend dat de Russen het registratiesysteem van stemgerechtigden in zijn staat hebben geprobeerd te manipuleren.

Volgens het ministerie is het de hackers, die werkten in opdracht van de Russische overheid, niet gelukt om de uitslagen of de lijsten met stemgerechtigde inwoners te beïnvloeden.

President Trump won de staat Wisconsin van Hillary Clinton met een verschil van slechts 22.700 stemmen. Het Kremlin heeft altijd ontkend dat het vorig jaar hackers heeft ingezet om de Democratisch presidentskandidate Hillary Clinton politiek te beschadigen. Ook president Trump heeft ontkend iets met de hacks te maken te hebben

Samenvatting: Dit is geen echte samenvatting maar een voorbeeld om te laten zien hoe de documentatiemap er uit gaat zien. Je leest het artikel en maakt daar een samenvatting van. Gebruik daar een stuk of vier regels voor, dat is over het algemeen genoeg. Uiteraard kan niemand dezelfde samenvatting hebben.

Mening: Ik vind is natuurlijk het begin van je mening. Dit hier is geen mening, maar een voorbeeld hoe het er in je map uit moet zien. Voor je mening gebruik je ook maar een paar regels, als je wel duidelijk uitlegt waarom je iets goed of slecht of leuk of dom etc vindt.

Krantenartikel Telegraaf 12

Rusland legde mobiel netwerk Letland plat

05 okt. 2017 in FINANCIEEL
Kopieer naar clipboard

 TLG

RIGA (ANP/RTR) - Dat het mobiele netwerk in delen van Letland eind augustus zeven uur lang plat lag, kwam mogelijk door Rusland. Dat land zou als oefening een cyberaanval hebben uitgevoerd. Mogelijk maakte het land gebruik van een zogeheten 'jammer' in de enclave Kaliningrad.

 TLG

Volgens functionarissen uit de Baltische staten en bij de NAVO viel de aanval samen met een grote Russische militaire oefening. Ongeveer 100.000 militairen trainden tegelijk in Rusland en buurland Wit-Rusland. Op 13 september, bij het hoogtepunt van de oefening, ging het alarmnummer 112 in Letland uit de lucht.

Eind 2015 werd het elektriciteitsnet in Oekraïne platgelegd na een cyberaanval. Hackers kraakten de systemen van drie stroombedrijven, schakelden verdeelstations uit en zorgden er zo voor dat honderdduizenden mensen zonder elektriciteit kwamen te zitten. Die aanval wordt eveneens met Rusland in verband gebracht.

Samenvatting: Dit is geen echte samenvatting maar een voorbeeld om te laten zien hoe de documentatiemap er uit gaat zien. Je leest het artikel en maakt daar een samenvatting van. Gebruik daar een stuk of vier regels voor, dat is over het algemeen genoeg. Uiteraard kan niemand dezelfde samenvatting hebben.

Mening: Ik vind is natuurlijk het begin van je mening. Dit hier is geen mening, maar een voorbeeld hoe het er in je map uit moet zien. Voor je mening gebruik je ook maar een paar regels, als je wel duidelijk uitlegt waarom je iets goed of slecht of leuk of dom etc vindt.

Krantenartikel Telegraaf 20 oktober

Zonnepanelen hacken, hoe kan dat?

Onlangs is er in het nieuws gekomen dat zonnepanelen gehackt kunnen worden. En bij een hack wordt iedereen een beetje zenuwachtig. Wat betekent het eigenlijk en wat zijn de risico's voor mensen **met zonnepanelen?**

Hacken van zonnepanelen, de feiten

Alle zonnepanelen zijn aangesloten op een omvormer welke de gelijkstroom omzet in wisselstroom. En bij de omvormer zou het lek kunnen zitten. De omvormer houdt data bij. Het registreert hoeveel kilowatturen worden opgewekt en op welke momenten.
Om deze gegevens te kunnen inzien kan de eigenaar inloggen op de omvormer. Omdat vaak het initiële wachtwoord niet wordt gewijzigd hoef je bijna geen hacker te zijn om in te loggen op de omvormer. En daar bevindt zich ook een functie om de omvormer stil te leggen. Dat is natuurlijk niet leuk, maar zeker geen ramp voor de gebruiker. Er gaat niets kapot, er wordt niets veranderd, er is alleen tijdelijk even geen zonnestroom.

Datalek zonnepanelen, waar zit dan het probleem?

Het risico voor de eigenaar is niet zo groot. Het grote risico zit bij de netbeheerder, de partij die het Nederlandse stroomnet bewaakt. Het net is er namelijk op ingericht dat er tijdens zonnige momenten veel productie van elektriciteit plaatsvindt via zonnepanelen. En mocht een hacker tegelijkertijd alle omvormers uitschakelen, dan komt er plotseling een enorme dip in het stroomnet. Dit is niet zomaar op te vangen waardoor de netbeheerder over zal moeten gaan om hele wijken te ontsluiten.

Hoe kan een hacker zoveel omvormers uitschakelen

Hackers kunnen een slimme truck gebruiken om omvormers uit te schakelen. Daartoe installeren ze malware op bedrijfs- en thuisnetwerken waar omvormers mee verbonden zijn. Daar blijft de malware slapend tot een bepaald moment waarop het toeslaat en in één keer alle omvormers uitschakelt.

Kan een hacker via de omvormer ook toegang krijgen tot mijn netwerk?

Een omvormer is een apart toestel binnen het netwerk. Het is geen computer waar malware op geïnstalleerd kan worden. Als zodanig vormt het geen bedreiging voor andere gegevens die in het netwerk staan.

Samenvatting: Dit is geen echte samenvatting maar een voorbeeld om te laten zien hoe de documentatiemap er uit gaat zien. Je leest het artikel en maakt daar een samenvatting van. Gebruik daar een stuk of vier regels voor, dat is over het algemeen genoeg. Uiteraard kan niemand dezelfde samenvatting hebben.

Mening: Ik vind is natuurlijk het begin van je mening. Dit hier is geen mening, maar een voorbeeld hoe het er in je map uit moet zien. Voor je mening gebruik je ook maar een paar regels, als je wel duidelijk uitlegt waarom je iets goed of slecht of leuk of dom etc vindt.

Telegraaf 10 februari 2017

Italiaans ministerie BuZa vorig jaar gehackt

10 FEB 2017

ROME - Het Italiaanse ministerie van Buitenlandse Zaken is vorig jaar doelwit geweest van een geslaagde hackaanval. Een bron bij de Italiaanse regering heeft dat vrijdag bevestigd aan The Guardian. Het vermoeden bestaat dat Rusland achter de aanval zit.

Vorig jaar wisten de hackers het systeem van het ministerie binnen te dringen. De aanval duurde meer dan vier maanden, maar de hackers wisten niet de hand te leggen op gevoelige informatie. ,,Het waren geen aanvallen op versleutelde computersystemen waar de gevoeligste informatie op staat, maar op de e-mailservers voor de medewerkers van het ministerie en de ambassades", aldus de bron.

Het Russische ministerie van buitenlandse zaken wilde niet reageren op een verzoek van Reuters om commentaar. Het Kremlin heeft eerder de beschuldigingen dat Moskou achter hackaanvallen in de VS zit afgedaan als 'verzinsels' en een 'heksenjacht'.

Samenvatting: Dit is geen echte samenvatting maar een voorbeeld om te laten zien hoe de documentatiemap er uit gaat zien. Je leest het artikel en maakt daar een samenvatting van. Gebruik daar een stuk of vier regels voor, dat is over het algemeen genoeg. Uiteraard kan niemand dezelfde samenvatting hebben.

Mening: Ik vind is natuurlijk het begin van je mening. Dit hier is geen mening, maar een voorbeeld hoe het er in je map uit moet zien. Voor je mening gebruik je ook maar een paar regels, als je wel duidelijk uitlegt waarom je iets goed of slecht of leuk of dom etc vindt.

Telegraaf

Hackers treffen accountantsreus Deloitte

25 sep. 2017 in FINANCIEEL
Kopieer naar clipboard

 REUTERS

LONDEN (ANP) - Accountants- en adviesbureau Deloitte is ten prooi gevallen aan hackers. Daardoor zijn mogelijk vertrouwelijke plannen en e-mailwisselingen van een aantal grote klanten van de firma op straat komen te liggen, meldt het Britse dagblad The Guardian.

 REUTERS

De hackers hebben volgens de krant mogelijk vanaf oktober of november vorig jaar toegang gehad tot de systemen van Deloitte, dat het beveiligingslek echter pas in maart zou hebben ontdekt. Zij zouden zichzelf toegang hebben verschaft tot het systeem via een account waarmee zij ,,in theorie" ongelimiteerde toegang hadden tot de e-mailserver van de firma.

Tot de klanten van Deloitte behoren grote multinationals, maar ook bijvoorbeeld Amerikaanse overheidsinstanties. The Guardian weet te melden dat al zeker zes klanten te horen hebben gekregen dat hun gegevens mogelijk zijn buitgemaakt. Het dagblad vermeldt niet waar het de informatie vandaan heeft

Samenvatting: Dit is geen echte samenvatting maar een voorbeeld om te laten zien hoe de documentatiemap er uit gaat zien. Je leest het artikel en maakt daar een samenvatting van. Gebruik daar een stuk of vier regels voor, dat is over het algemeen genoeg. Uiteraard kan niemand dezelfde samenvatting hebben.

Mening: Ik vind is natuurlijk het begin van je mening. Dit hier is geen mening, maar een voorbeeld hoe het er in je map uit moet zien. Voor je mening gebruik je ook maar een paar regels, als je wel duidelijk uitlegt waarom je iets goed of slecht of leuk of dom etc vindt.

Telegraaf

Hackers stelen gegevens miljoenen Amerikanen

08 sep. 2017 in BUITENLAND
Kopieer naar clipboard

ATLANTA - Kredietbureau Equifax is getroffen door een cyberaanval. Hackers hebben daardoor toegang gekregen tot creditcardgegevens, huisadressen, geboortedata en andere informatie van mogelijk 143 miljoen Amerikanen.

De hackers hebben ook toegang gekregen tot persoonlijke gegevens van klanten uit Canada en Groot-Brittannië van Equifax. Daarbij gaat het om veel minder mensen.

Bij een intern onderzoek eind juli ontdekte Equifax dat de persoonlijke gegevens van miljoenen mensen door een cyberaanval op straat waren komen te liggen. Het bedrijf bracht die informatie pas donderdag naar buiten

Samenvatting: Dit is geen echte samenvatting maar een voorbeeld om te laten zien hoe de documentatiemap er uit gaat zien. Je leest het artikel en maakt daar een samenvatting van. Gebruik daar een stuk of vier regels voor, dat is over het algemeen genoeg. Uiteraard kan niemand dezelfde samenvatting hebben.

Mening: Ik vind is natuurlijk het begin van je mening. Dit hier is geen mening, maar een voorbeeld hoe het er in je map uit moet zien. Voor je mening gebruik je ook maar een paar regels, als je wel duidelijk uitlegt waarom je iets goed of slecht of leuk of dom etc vindt.

Telegraaf

Computers Utrecht massaal gekaapt

27 sep. 2017 in BINNENLAND
Kopieer naar clipboard

 AFP

UTRECHT - Utrecht heeft verreweg de meeste gekaapte computersystemen, zogeheten bots. De Domstad is daarin hoofdstad van Nederland en staat zelfs in de Europese top, blijkt uit een onderzoek van beveiliger Symantec. Utrecht heeft maar liefst dertien keer zo veel besmette computers als nummer twee Amsterdam en ongeveer veertig keer zo veel als nummer drie Den Haag.

 AFP

Bots zijn computersystemen die op afstand kunnen worden overgenomen, doordat hackers de beveiliging hebben weten te kraken. Als zulke computers aan elkaar worden gekoppeld, ontstaat een krachtig netwerk, een botnet. Zo'n 'leger' kan worden gebruikt voor cyberaanvallen. De computers kunnen bijvoorbeeld allemaal tegelijk naar een bepaalde site worden gestuurd om die plat te leggen, een DDoS-aanval. De computers kunnen ook worden gebruikt om spam of virussen te versturen.

Volgens het onderzoek telt Nederland ruim 830.000 bots. Daarvan bevinden zich meer dan 710.000 (bijna 86 procent) in Utrecht. De stad staat op de vierde plek van heel Europa, na Madrid, Istanbul en Moskou.

Symantec heeft geen verklaring voor de vele besmettingen in Utrecht. Het kan zijn dat inwoners en bedrijven slordig zijn met hun wachtwoorden en beveiliging (hun 'cyberhygiëne').

De hackers achter de bots kunnen over de hele wereld zitten. ,,Een geïnfecteerd apparaat in Europa kan bijvoorbeeld bijdragen aan een aanval in Azië en ergens in de Verenigde Staten worden beheerd door een cybercrimineel", aldus Symantec.

Het aantal bots neemt toe. Dat komt onder meer door het internet der dingen. Tegenwoordig zijn niet alleen computers en telefoons verbonden met internet, maar ook slimme huishoudelijke apparaten en speelgoed. Die kunnen ook overgenomen worden, zonder dat de gebruiker dat doorheeft. Zo werd eind vorig jaar het internet in de Verenigde Staten ontregeld door een gecoördineerde aanval met tientallen miljoenen gekaapte babyfoons, printers en bewakingscamera's.

Gebruikers kunnen heel moeilijk ontdekken of hun apparaat een bot is. De hackers proberen onzichtbaar en verborgen te blijven, totdat ze apparaten de opdracht geven om een taak uit te voeren. Er zijn wel een paar symptomen. Zo wordt een gekaapt apparaat langzamer, en kan het zonder duidelijke reden vastlopen

Samenvatting: Dit is geen echte samenvatting maar een voorbeeld om te laten zien hoe de documentatiemap er uit gaat zien. Je leest het artikel en maakt daar een samenvatting van. Gebruik daar een stuk of vier regels voor, dat is over het algemeen genoeg. Uiteraard kan niemand dezelfde samenvatting hebben.

Mening: Ik vind is natuurlijk het begin van je mening. Dit hier is geen mening, maar een voorbeeld hoe het er in je map uit moet zien. Voor je mening gebruik je ook maar een paar regels, als je wel duidelijk uitlegt waarom je iets goed of slecht of leuk of dom etc vindt.

Internetartikel www.rtlnieuws.nl

Bewakingscamera van de Action is simpel te hacken

donderdag 05 oktober 2017 19:28

Een populaire beveiligingscamera die winkelketen Action verkoopt blijkt erg eenvoudig te hacken.

De beveiligingscamera van de Gelderse Rilana Hamer begon plotseling tegen haar te praten. Hackers hadden ingebroken op het apparaat, en dat blijkt helemaal niet zo lastig. Het gaat om de HD Rotating Wifi Safety Camera van het merk Maxxter (typenummer ACT-IPC-01), die sinds eind mei door de Action wordt verkocht. Volgens de winkelketen is hij vrijwel uitverkocht.

Rilana kreeg de schrik van haar leven toen uit de speaker van de camera plotseling een stem kwam die 'Hola señorita' zei. "Huilend, van slag. Mijn privacy, mijn huis, mijn persoonlijke spullen en ikzelf. Ik ben bang, doodsbang", zegt Rilana.

De grote vraag: hoe kan iemand inbreken in haar camera? We duiken in de handleiding (pdf) van het product en zien dat het standaard wachtwoord '123' is. Maxxter dwingt gebruikers niet om dit wachtwoord aan te passen, maar raadt wel aan om dit 'zeer zwakke wachtwoord' te veranderen in een eigen wachtwoord.

Cijfertjes aanpassen

Daarnaast beschrijft de handleiding dat je de camera altijd via een app kunt bereiken. Je hoeft daarvoor enkel het nummer van de camera en het wachtwoord in te voeren. Door de cijfertjes aan te passen kun je toegang krijgen tot andere camera's, zolang de eigenaar het standaard wachtwoord niet heeft veranderd.

Naast meekijken kun je ook nog de camera besturen, het geluid in- of uitschakelen, via de speaker praten en de instellingen aanpassen, zoals het wachtwoord. Bij één van de webcams kunnen we meekijken in een woonkamer waar iemand op de bank ligt.

Privacyprobleem

Dat je deze camera's ook buiten je eigen wifi-netwerk kunt bereiken, is juist een belangrijke functionaliteit. Het is voor veel mensen ook handig: Rilana had de camera gekocht om haar jonge pup in de gaten te houden. Door de speaker in de camera kon ze ook tegen haar pup praten.

Maar met internet verbonden camera's vormen daardoor wel een privacyprobleem, omdat bezitters het standaard wachtwoord veelal niet aanpassen. Er zijn zelfs websites waar je honderden Nederlandse onbeveiligde beveiligingscamera en webcams kunt zien.

Samenvatting: Dit is geen echte samenvatting maar een voorbeeld om te laten zien hoe de documentatiemap er uit gaat zien. Je bekijkt het programma en maakt daar een samenvatting van. Gebruik daar een stuk of vier regels voor, dat is over het algemeen genoeg. Uiteraard kan niemand dezelfde samenvatting hebben.

Mening: Ik vind is natuurlijk het begin van je mening. Dit hier is geen mening, maar een voorbeeld hoe het er in je map uit moet zien. Voor je mening gebruik je ook maar een paar regels, als je wel duidelijk uitlegt waarom je iets goed of slecht of leuk of dom etc vindt.

Hoofdstuk 4: Wat zijn goede hackers?

Bron: www.slim.nl

Internetartikel

23 november 2017

Ethisch hacken en hacklesjes voor studenten

Hacken is volop in het nieuws. Aandacht voor ethisch hacken brengen wij u ook graag. Want, er zijn zat hackers met goede, ethische motieven die juist op zoek gaan naar gaatjes in uw systemen om u hier vervolgens op te wijzen zodat u de gaatjes kunt dichten.

Op 2 november gaf CEO Edwin van Andel van Zerocopter bij ons op kantoor een ludieke presentatie over hacken en Responsible Disclosure, dat is een beleid dat u aan uw applicatie kunt toevoegen om gebruikers en ethisch hackers kwetsbaarheden te laten rapporteren. Edwin heeft als motto ‘hug the hacker’ en dat geldt ook voor de jonge hackers die bij u op school zitten.

Hackerslesjes

Zerocopter biedt u 3 hacklessen voor uw studenten aan, die u mag delen. Naar het lesmateriaal.

ICTheek

Leest u vooral ook het hack-artikel op ictheek.nl over Jan van Kampen die programmeerles geeft op scholen, wereldwijd bekende apps maakt en multinationals op aanvraag hackt om hun online veiligheid te testen.

Samenvatting: Dit is geen echte samenvatting maar een voorbeeld om te laten zien hoe de documentatiemap er uit gaat zien. Je leest het artikel en maakt daar een samenvatting van. Gebruik daar een stuk of vier regels voor, dat is over het algemeen genoeg. Uiteraard kan niemand dezelfde samenvatting hebben.

Mening: Ik vind is natuurlijk het begin van je mening. Dit hier is geen mening, maar een voorbeeld hoe het er in je map uit moet zien. Voor je mening gebruik je ook maar een paar regels, als je wel duidelijk uitlegt waarom je iets goed of slecht of leuk of dom etc vindt.

Folder 1: Hackunamatata.nl

Deze folder kan je vinden in mijn gedeelde map.

Samenvatting: Dit is geen echte samenvatting maar een voorbeeld om te laten zien hoe de documentatiemap er uit gaat zien. Je leest de folder en maakt daar een samenvatting van. Gebruik daar ene stuk of vier regels voor, dat is over het algemeen genoeg. Uiteraard kan niemand dezelfde samenvatting hebben.

Mening: Ik vind is natuurlijk het begin van je mening. Dit hier is geen mening, maar een voorbeeld hoe het er in je map uit moet zien. Voor je mening gebruik je ook maar een paar regels, als je wel duidelijk uitlegt waarom je iets goed of slecht of leuk of dom etc vindt.

Internetartikel www.tech.nl

Nederlands team beste inbrekers

We zijn wereldkampioen hacken

Updated 28 sep. 2017
27 sep. 2017 in TECH
Kopieer naar clipboard

Kinderen krijgen les in hacken tijdens de opening van de Cyber Security Week.

 ANP

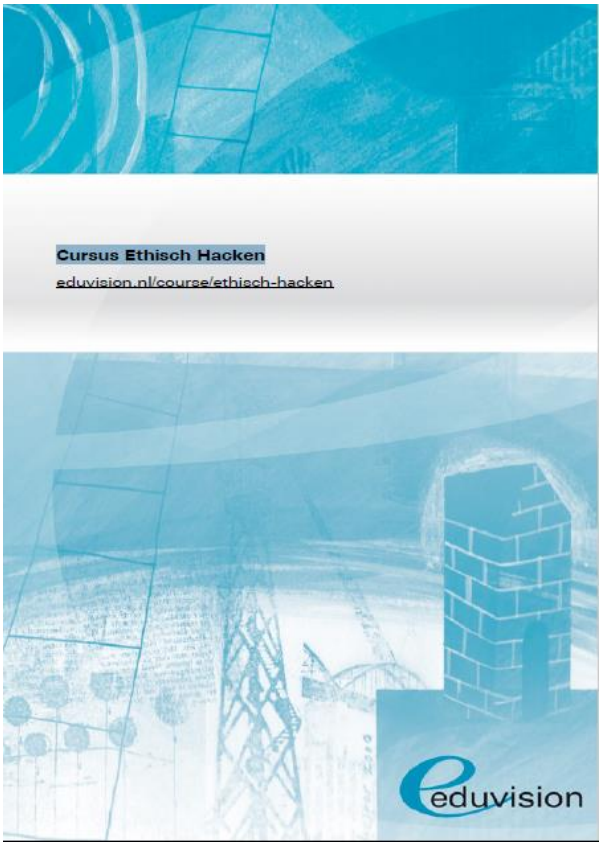
DEN HAAG - Nederland is er donderdag op de Global CyberLympics vandoor gegaan met de hoofdprijs. Deze internationale online-hackingwedstrijd werd gehouden tijdens de Cyber Security Week in Den Haag.

Samenvatting: Dit is geen echte samenvatting maar een voorbeeld om te laten zien hoe de documentatiemap er uit gaat zien. Je leest het artikel en maakt daar een samenvatting van. Gebruik daar een stuk of vier regels voor, dat is over het algemeen genoeg. Uiteraard kan niemand dezelfde samenvatting hebben.

Mening: Ik vind is natuurlijk het begin van je mening. Dit hier is geen mening, maar een voorbeeld hoe het er in je map uit moet zien. Voor je mening gebruik je ook maar een paar regels, als je wel duidelijk uitlegt waarom je iets goed of slecht of leuk of dom etc vindt.

Folder: Cursus ethisch hacken

(staat in gedeelde map)



Samenvatting: Dit is geen echte samenvatting maar een voorbeeld om te laten zien hoe de documentatiemap er uit gaat zien. Je leest de folder en maakt daar een samenvatting van. Gebruik daar een stuk of vier regels voor, dat is over het algemeen genoeg. Uiteraard kan niemand dezelfde samenvatting hebben.

Mening: Ik vind is natuurlijk het begin van je mening. Dit hier is geen mening, maar een voorbeeld hoe het er in je map uit moet zien. Voor je mening gebruik je ook maar een paar regels, als je wel duidelijk uitlegt waarom je iets goed of slecht of leuk of dom etc vindt.

Hoofdstuk 5: Hoe vaak komt het voor?

Hack Yahoo trof 3 miljard gebruikers

04 okt. 2017 in FINANCIEEL
Kopieer naar clipboard

 REUTERS

NEW YORK (ANP) - Een groot datalek bij Yahoo trof in 2013 fors meer gebruikers dan eerder werd gedacht. Moederbedrijf Verizon meldt volgens The New York Times dat cybercriminelen vermoedelijk gegevens uit 3 miljard accounts in handen kregen.

 REUTERS

Hackers bemachtigden destijds onder meer namen, wachtwoorden en telefoonnummers van Yahoo-gebruikers. Yahoo bracht eerder naar buiten dat zo'n 1 miljard personen waren getroffen. De nieuwe schatting is gebaseerd op aanvullende inlichtingen.

Computerinbraken bij Yahoo drukten eerder dit jaar de verkoopprijs van de internetactiviteiten van het bedrijf aan Verizon. De bedrijven waren aanvankelijk een prijs van 4,8 miljard dollar overeengekomen, maar dat bedrag viel uiteindelijk zo'n 350 miljoen dollar lager uit.

Samenvatting: Dit is geen echte samenvatting maar een voorbeeld om te laten zien hoe de documentatiemap er uit gaat zien. Je leest het artikel en maakt daar een samenvatting van. Gebruik

daar een stuk of vier regels voor, dat is over het algemeen genoeg. Uiteraard kan niemand dezelfde samenvatting hebben.

Mening: Ik vind is natuurlijk het begin van je mening. Dit hier is geen mening, maar een voorbeeld hoe het er in je map uit moet zien. Voor je mening gebruik je ook maar een paar regels, als je wel duidelijk uitlegt waarom je iets goed of slecht of leuk of dom etc vindt.

TV programma 22 november RTL 4

Duizenden gehackte webcams vallen websites aan

© iStock

De bekende hackersgroep Lizard Squad heeft bij duizenden beveiligingscamera's, webcams en andere met internet verbonden apparaten ingebroken om DDoS-aanvallen op websites uit te voeren.

Xbox Live, PlayStation Network en zelfs Facebook waren niet bestand tegen de DDoS-aanvallen van Lizard Squad, dat de laatste jaren is uitgegroeid tot één van de bekendste hackersgroepen. Ze nemen computers over om met al die apparaten aanvallen uit te voeren op websites en netwerken, die vervolgens offline gaan.

Internet of Things

Eén van de manieren waarop Lizard Squad te werk gaat, is door duizenden slecht beveiligde beveiligingscamera's, webcams en andere met internet verbonden apparaten te hacken, zo ontdekte beveiligingsonderzoeker Matthew Bing. Deze apparaten worden vervolgens gebruikt om een DDoS-aanval uit te voeren. Bij een DDoS-aanval bezoeken heel veel apparaten dezelfde server of website telkens opnieuw, totdat het doelwit overbelast is en offline gaat.

Het hacken van met internet verbonden apparaten - ook wel het 'Internet of Things' genoemd - is relatief simpel, omdat deze apparaten meestal op verouderde en vrij simpele software draaien. Daarnaast worden inloggegevens regelmatig niet aangepast. Hoewel dit soort apparaten niet zo krachtig zijn als een pc, kunnen hackers er met duizenden grootschalige aanvallen uitvoeren.

Je broodrooster lekt je wifi-wachtwoord

Ook Mikko Hypponen, de belangrijkste onderzoeker bij het Finse beveiligingsbedrijf F-Secure, waarschuwde bij RTL Z al eerder voor het gevaar van het Internet of Things: "Je kan ervan uitgaan dat je nieuwe slimme broodrooster niet in brand vliegt en je geen elektrische schok geeft, maar het zal wel je wifi-wachtwoord lekken. Dat is het probleem."

Volgens Hypponen zijn met internet verbonden apparaten, zoals een wasmachine, camera of koelkast, juist zo gevaarlijk omdat het hackers toegang geeft tot een netwerk. Als ze bijvoorbeeld een met internet verbonden beveiligingscamera hacken, kunnen hackers ook toegang krijgen tot alle andere apparaten in hetzelfde netwerk.

RTL Z / Daniël Verlaan

Samenvatting: Dit is geen echte samenvatting maar een voorbeeld om te laten zien hoe de documentatiemap er uit gaat zien. Je leest het artikel en maakt daar een samenvatting van. Gebruik daar een stuk of vier regels voor, dat is over het algemeen genoeg. Uiteraard kan niemand dezelfde samenvatting hebben.

Mening: Ik vind is natuurlijk het begin van je mening. Dit hier is geen mening, maar een voorbeeld hoe het er in je map uit moet zien. Voor je mening gebruik je ook maar een paar regels, als je wel duidelijk uitlegt waarom je iets goed of slecht of leuk of dom etc vindt.

Hoofdstuk 6: Wat doe je er tegen?

Internetartikel - Bron: slim.nl

Van een eigen app als profielwerkstuk tot professioneel programmeren

1. **Home**
2. **Leven lang leren**
3. **Van een eigen app als profielwerkstuk tot professioneel programmeren**

 Geplaatst: 15-11-2017  Leestijd: 4 minuten  103 views

Jan van Kampen (26) geeft programmeerles op scholen, maakt wereldwijd bekende apps en hackt op aanvraag multinationals om hun online veiligheid te testen. En dat allemaal vanuit een klaslokaal dat hij huurt in een Beverwijkse voormalige school. Best toepasselijk, want zijn voorliefde voor IT begon tijdens het middelbaar onderwijs.

Jans' profielwerkstuk was een innovatieve zelfgemaakte app: het eerste digitale donorcodicil. En sindsdien leert Jan dankzij zijn veelzijdige werk nog iedere dag bij over de mogelijkheden van IT.

iDonor: werelds eerste donorcodicilapp

''Als je een project doet voor school is het zonde dat je na het krijgen van je cijfer direct je project weggooit. Ik wil eindproducten maken die ik de wereld in kan slingeren. Bovendien heb ik interesse in IT. Smartphones waren vrij nieuw, dus leek het me leuk mijn eerste appje te ontwikkelen als profielwerkstuk. Het was die week Donorweek en ik kwam er achter dat zo'n 80 procent van de mensen geen donorcodicil op zak heeft. Waarschijnlijk omdat ze er niet mee willen rond slepen. Daarom maakte ik iDonor. Online schrijf je je in en geef je aan naar welke digitale apparaten je je donorcodicil wilt sturen. Daar kan je dan je bloedgroep en een aantal noodnummers aan toevoegen en bijvoorbeeld opslaan op je mobieltje. Naast een goed cijfer kreeg ik ook veel lof voor het feit dat ik werelds eerste digitale donorcodicil had gemaakt. Uiteindelijk is de app

achterhaald, omdat er inmiddels zo veel betere alternatieven zijn. Maar het heeft mijn interesse in apps bouwen wel aangewakkerd en ik heb er veel van geleerd.''

''Neem je eigen leerschool mee naar de schoolbanken''

''Mijn advies aan scholen is om leerlingen zelf de ruimte te geven om zich spelenderwijs te ontwikkelen op IT-gebied. De informaticadocent heeft tegenwoordig niet per se de meeste computerkennis. En dat hoeft ook niet. Alleen moet hij of zij dat wel erkennen om samen met leerlingen nieuwe toepassingen te ontdekken. Toen ik als 14-jarige een eigen website wilde maken, leerde ik de eerste regels code schrijven tijdens het vak informatica. Bij de gekozen programmeertaal moet je de code afsluiten met een puntkomma. Dat was ik vergeten. De leraar wist er geen raad mee. Uiteindelijk kwam hij met een dik Engels programmeerhandboek. ''Misschien stond de oplossing daar wel ergens in.'' Na uren bladeren, ontdekte ik het foutje. Voor mijn leraar was het echt een ver-van-zijn-bedshow. Maar het kan ook anders. De leraar die me ondersteunde bij het profielwerkstuk deed echt zijn best gedaan me te begrijpen. Ondanks dat hij niet alles wist, voelde hij zich niet in zijn ego aangetast en wilde hij me verder helpen. Dat gaf de ruimte om niet in grenzen, maar in mogelijkheden te leren denken.''

''Programmeren is zo veel meer dan code kloppen''

''Mijn cijfers voor natuurkunde en wiskunde waren waarschijnlijk twee punten hoger geweest als ik eerder begonnen was met programmeren. Dat gun ik iedereen. Daarom pleit ik er voor dat leerlingen op de middelbare school al leren programmeren. Programmeren is namelijk niet een kwestie van puur codes rammen. Het is een manier van denken. Welke methode of programmeertaal je gebruikt, maakt niet uit. De code mag zelfs volledig fout zijn. Dat leerde ik pas echt tijdens mijn studie informatica. Bij programmeren is het de kunst een probleem op te delen in subproblemen en die stuk voor stuk op te lossen. Als ik dat in de brugklas wist, had mijn hele middelbare schoolperiode er anders uitgezien. Omdat je niet vroeg genoeg kunt beginnen, deed ik mijn afstudeerscriptie op de Vrije Universiteit over programmeren in het basisonderwijs. Je kan een kleuter bijvoorbeeld leren programmeren door hem een autootje op een racebaantje te laten rijden. Als je het besef overbrengt dat je de finish bereikt door twee keer links en één keer rechts te gaan, heb je de basis gelegd.''

Samenvatting: Dit is geen echte samenvatting maar een voorbeeld om te laten zien hoe de documentatiemap er uit gaat zien. Je leest het artikel en maakt daar een samenvatting van. Gebruik daar een stuk of vier regels voor, dat is over het algemeen genoeg. Uiteraard kan niemand dezelfde samenvatting hebben.

Mening: Ik vind is natuurlijk het begin van je mening. Dit hier is geen mening, maar een voorbeeld hoe het er in je map uit moet zien. Voor je mening gebruik je ook maar een paar regels, als je wel duidelijk uitlegt waarom je iets goed of slecht of leuk of dom etc vindt.

TV programma 22 november RTL 4 20.20 – 21.20

Hacken als schoolvak is hot (en heel hard nodig)

Archieffoto.
© iStock

De hackende computernerd is hot. Dat blijkt uit onderzoek onder Nederlandse jongeren. Sterker: sommige jongeren zien het zichzelf ook (illegaal) doen. Scholen en bedrijven willen hen inzetten in de strijd tegen cybercrime.

Stiekem inbreken op andermans computer: dat zien veel jongeren wel zitten. Door hackersgroepen als Anonymous is hacken hotter dan ooit.

Uit onderzoek van beveiligingsexpert Kaspersky onder 12.000 IT-professionals en consumenten uit de VS en Europa blijkt dat 60 procent van de Nederlanders onder de 25 hacken een 'indrukwekkende' vaardigheid vindt. Bijna 30 procent van de jongeren ziet zichzelf best hacken voor een illegaal doel of voor geld. 25 procent voelt zich ongemakkelijk bij hackers.

Ethisch hacken

Edwin van Andel is al bijna 30 jaar 'ethisch hacker'. "Mijn vader had een computer die kapotging en ik haalde hem uit elkaar om alles uit te vogelen. Zo kwam ik steeds meer te

weten over computers. Ik begon al te hacken voordat er internet was, we deden het voordat mensen het wisten en ook voordat het illegaal was."

Dat jongeren onder de indruk zijn van hackers, snapt Van Andel wel. "Het is gewoon spannend. Je wilt een puzzel oplossen. Veilige websites zijn voor veel hackers de grootste uitdaging, die willen ze kraken, dan hebben ze gewonnen."

Ddos-aanvallen

Frank Maas, opleidingsmanager ICT en mediavormgeving aan het ROC Flevoland, ziet ook het enthousiasme van zijn studenten. "Er was laatst een hackers-top, en daar gingen heel veel studenten naartoe", vertelt hij.

Het ROC biedt de studenten vanaf volgend jaar vakken aan op het gebied van cybersecurity. Met andere woorden: studenten leren legaal hacken voor een goed doel. "Wij kregen geluiden dat er een tekort is aan jongere werknemers in cybersecurity."

Spannende statements

Maas: "De studenten vinden het vooral spannend als er politieke statements worden gemaakt met een hack. Mensen denken bij 'hacken' meteen aan Anonymous, maar vergeet niet: hackers zijn ook de personen die ddos-aanvallen uitvoeren of phishingmails sturen."

Nederland loopt heel erg voor op de zogenoemde 'responsible disclosure', weet Van Andel. Dat is een systeem waarin een hacker een lek bij een bedrijf kan opsporen en melden, zónder dat de hacker wordt aangeklaagd.

Dat vindt Van Andel een goede ontwikkeling, want zo zien mensen dat niet alle hackers crimineel zijn. "Ze zijn soms best lief, willen niet allemaal slechte dingen doen. Ik benader ook jonge hackers op Twitter, daar zitten ze allemaal – ze vertellen namelijk graag over hun activiteiten. Ik zeg dan: 'hey, ik zie wat je doet en wil je helpen het op de goeie manier te doen'."

Nederlandse hackers

De afgelopen jaren zijn er ook Nederlandse jongeren opgepakt in verband met illegaal hacken:

- Begin oktober is een 19-jarige Nederlander opgepakt in de VS en aangeklaagd door de FBI, wegens het uitvoeren van cyberaanvallen op allerlei bedrijven.

- De Nederlander David S. (26) werd in 2013 tot 12 jaar cel veroordeeld voor het stelen van creditcardgegevens.
- Twee tieners hackten dit jaar tientallen Instagramaccounts via phishingmails. Ze verdienden er tienduizenden euro's mee. De jongen werden in maart dit jaar opgepakt.
- In 2012 werd een 17-jarige jongen opgepakt voor een grote hack bij KPN. Hij plaatste schadelijke software waardoor de beveiliging werd omzeild. Rechercheurs volgden hem wekenlang online.

- **Samenvatting**: Dit is geen echte samenvatting maar een voorbeeld om te laten zien hoe de documentatiemap er uit gaat zien. Je bekijkt het programma en maakt daar een samenvatting van. Gebruik daar een stuk of vier regels voor, dat is over het algemeen genoeg. Uiteraard kan niemand dezelfde samenvatting hebben.
- **Mening**: Ik vind is natuurlijk het begin van je mening. Dit hier is geen mening, maar een voorbeeld hoe het er in je map uit moet zien. Voor je mening gebruik je ook maar een paar regels, als je wel duidelijk uitlegt waarom je iets goed of slecht of leuk of dom etc vindt.

Krantenartikel Telegraaf 17 oktober

Game of Thrones krijgt meerdere eindes

14 sep. 2017 in ENTERTAINMENT
Kopieer naar clipboard

 Hollandse Hoogte

Voor het achtste en laatste seizoen van Game of Thrones worden meerdere eindes gefilmd. Zender HBO wil op die manier voorkomen dat het 'echte' einde voortijdig uitlekt.

 Hollandse Hoogte

„Er worden meerdere versies gemaakt zodat niemand weet wat er gaat gebeuren”, zei *HBO*-programmabaas **Casey Bloys** volgens de *BBC* tijdens een college in zijn thuisstad Bethlehem, Pennsylvania. „Je moet dat wel doen bij zo’n lange show. Zodra je het opneemt, weten mensen het. Dus er komen meerdere eindes zodat niemand het echt zeker weet.”

HBO kende tijdens het zevende seizoen, waarvan vorige maand de laatste aflevering werd uitgezonden, vele problemen. Zo wisten hackers scripts, documenten en nog niet uitgezonden afleveringen in handen te krijgen. In totaal werden afleveringen van het zevende seizoen al 1 miljard keer illegaal gedownload.

Mening

Bloys zei ook dat het lastig zal worden om iedereen tevreden te stellen met het einde van de populaire serie. „Finales zijn altijd moeilijk. Denk maar aan *Seinfeld*, *The Sopranos*, *Breaking Bad*. Iedereen heeft een mening over hoe de show zou moeten eindigen.”

Fans moeten nog even geduld hebben voordat ze eindelijk kunnen zien welke familie de strijd om de troon in Westeros wint. De opnames en productie van het laatste seizoen duren vermoedelijk tot halverwege 2018. In 2019 moet de serie uitkomen.

Samenvatting: Dit is geen echte samenvatting maar een voorbeeld om te laten zien hoe de documentatiemap er uit gaat zien. Je leest het artikel en maakt daar een samenvatting van. Gebruik daar een stuk of vier regels voor, dat is over het algemeen genoeg. Uiteraard kan niemand dezelfde samenvatting hebben.

Mening: Ik vind is natuurlijk het begin van je mening. Dit hier is geen mening, maar een voorbeeld hoe het er in je map uit moet zien. Voor je mening gebruik je ook maar een paar regels, als je wel duidelijk uitlegt waarom je iets goed of slecht of leuk of dom etc vindt.

Internetartikel http://modint.nl/2016/08/11/tip-laat-bedrijf-eens-hacken/

Tip: laat uw bedrijf eens hacken

Jaarlijks worden zo'n 556 miljoen mensen wereldwijd slachtoffer van cybercriminelen. Maar waarom doen deze hackers wat ze doen? Waar zijn ze op uit? Hoe snel zijn ze bij u 'binnen'? En wat moet u als ondernemer nu juist wel of niet doen wanneer u gehackt wordt? Dick Snel en Jasper Weijts, twee white hat hackers van informatiebeveiligingsbedrijf Onvio, geven antwoord op de meest gestelde vragen.

Hoe goed zijn Nederlandse bedrijven beschermd?

"Uit onze ervaring blijkt dat de meeste Nederlandse bedrijven een matige beveiliging voeren. Wanneer een white hat hacker (een 'legale' hacker, zie kader) aan de slag gaat, schrikken bedrijven vaak van de eenvoudige manier waarop en de korte tijd waarbinnen de hacker toegang heeft verkregen tot alle gevoelige gegevens van het bedrijf. De kans dat een cybercrimineel inbreekt wordt vaak onderschat, mede omdat een hacker vaak tijden onopgemerkt zijn gang kan gaan zonder dat het bedrijf ook maar iets in de gaten heeft."

Hoe lang duurt het gemiddeld om digitaal bij een ondernemer 'in te breken'?

"Bij de meeste van onze testen hebben we binnen één dag al een kwetsbaarheid gevonden waarmee we toegang krijgen tot gevoelige gegevens en in veel gevallen toegang tot het volledige bedrijfsnetwerk met alle data daarbinnen. Vaak zijn er nog meer van dit soort kwetsbaarheden aanwezig."

Wat gebeurt er als een hacker 'binnen' is?

"Als een hacker 'binnen' is kan hij een virus achterlaten waarmee hij op elk moment opnieuw binnen kan komen. Hiermee kan de hacker op zijn gemak het netwerk verkennen en op zoek gaan naar gevoelige data zonder op te vallen. Met de gevonden gegevens kan hij vervolgens ook weer nieuwe aanvallen opzetten om andere systemen en bedrijven te hacken."

Wat zijn de belangrijkste redenen voor een black hat hacker om een bedrijf te hacken?

“Meestal is dat financieel gewin, maar het komt ook vaak voor dat een persoon een bedrijf schade wil toedoen, bijvoorbeeld een ex-werknemer die wraak wil nemen op zijn niet zo soepel verlopen ontslag. In het eerste geval gaat het om het stelen van gevoelige gegevens voor verkoop of afpersing of toegang tot financiële systemen om geld over te boeken. Ook kan het gaan om concurrenten die meekijken met het bedrijf en gevoelige gegevens buitmaken. Wanneer een ex-werknemer wraak neemt, worden er vaak systemen onbruikbaar gemaakt of gevoelige gegevens gelekt met reputatieschade tot gevolg.”

Wat moet een bedrijf in ieder geval doen als het gehackt is?

“Een digitaal forensisch expert inschakelen om onderzoek te doen naar de oorzaak en herkomst van de inbraak. Vaak kan de hacker niet gepakt worden, maar kan het lek dat hij gebruikt heeft wel ontdekt worden. Van hieruit kunnen maatregelen genomen worden om systemen beter te beveiligen.”

Wat moet een bedrijf vooral niet doen als het gehackt is?

“Vooral geen stekkers uit het stopcontact trekken. In dat geval kunnen essentiële logbestanden gewist worden die hadden kunnen leiden naar de inbreker. Wanneer een hacker binnen het netwerk wordt ontdekt, is de kans zeer groot dat hij al toegang heeft gehad tot alle gegevens.”

Wat is de meest gemaakte fout bij ondernemers op het gebied van digitale beveiliging?

“Dat is toch dat veel ondernemers denken dat de partij die ze inschakelen voor hun website of het onderhoud van het netwerk ook de beveiliging verzorgt. Dat is vaak niet opgenomen in het contract en daardoor ontstaat er een misvatting over de beveiliging van systemen.”

Welke preventieve maatregelen kan een bedrijf nemen om hun applicaties en data te beschermen tegen een hack?

“Bedrijven kunnen als preventieve maatregel een penetratietest (beveiligingstest) uit laten voeren om de digitale risico’s en kwetsbaarheden in hun applicaties in kaart te brengen. Bij zo’n test neemt een white hat hacker de systemen onder vuur net zoals een cybercrimineel dat in de praktijk zou doen. Hieruit vloeien quick wins voort waarmee de beveiliging snel naar een hoger niveau getild kan worden. Bijvoorbeeld het afsluiten van onnodige applicaties en systemen, het updaten van software of het plaatsen van een moderne firewall.”

Zijn alle hackers op kwaad uit?

“Hackers zijn globaal onder te verdelen in ‘black hat’ hackers en ‘white hat’ hackers. Black hat is een term voor hackers die inbreken op computers en systemen zonder toestemming en vaak voor eigen gewin. Een white hat hacker die kwetsbaarheden vindt in een systeem zal deze nooit zonder toestemming gebruiken en zal organisaties hier ook over informeren zodat ze de problemen kunnen oplossen. Het uitvoeren van een afgesproken penetratietest is een typisch voorbeeld van het werk

van een white hat hacker. Er zijn ook bedrijven, zoals Google, die een aantal white hat hackers in dienst hebben om hun systemen continu te laten testen op kwetsbaarheden."

Zo doen ze dat

"Voor een beursgenoteerde onderneming hebben we recent vanaf het internet het systeem getoetst op kwetsbaarheden (een penetratietest). Hierbij was afgesproken dat we vooraf geen informatie over de systemen zouden krijgen, dit noemen wij Black Box. Binnen twee dagen hebben we via een kwetsbaarheid toegang verkregen tot een server die gekoppeld was aan het interne netwerk. Eenmaal aanwezig op het interne netwerk is vervolgens op slinkse wijze toegang verkregen tot financiële systemen en gevoelige bedrijfsdata."

Meer weten over uw digitale risico's? Wilco van der Burgh, adviseur bij MODINT Verzekeringsdienst, helpt u graag om deze in kaart te brengen en af te dekken. U kunt contact met hem opnemen via 010 – 288 49 70 of info@modintverzekeringsdienst.nl.

http://modint.nl/2016/08/11/tip-laat-bedrijf-eens-hacken/

Samenvatting: Dit is geen echte samenvatting maar een voorbeeld om te laten zien hoe de documentatiemap er uit gaat zien. Je leest het artikel en maakt daar een samenvatting van. Gebruik daar een stuk of vier regels voor, dat is over het algemeen genoeg. Uiteraard kan niemand dezelfde samenvatting hebben.

Mening: Ik vind is natuurlijk het begin van je mening. Dit hier is geen mening, maar een voorbeeld hoe het er in je map uit moet zien. Voor je mening gebruik je ook maar een paar regels, als je wel duidelijk uitlegt waarom je iets goed of slecht of leuk of dom etc vindt.

Folder

(Staat in gedeelde map)

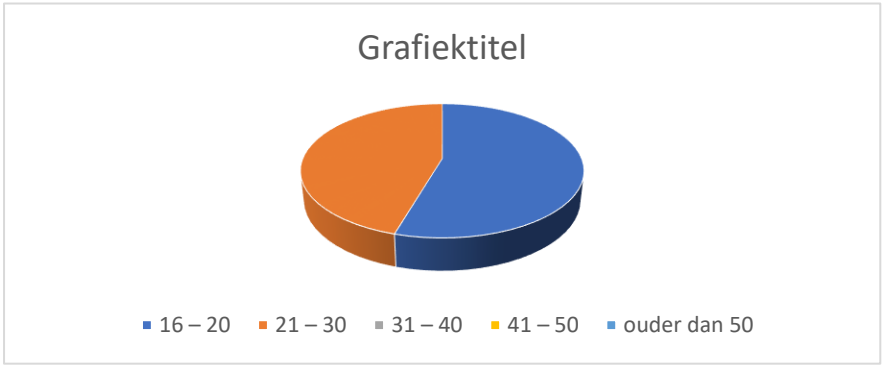
Samenvatting: Dit is geen echte samenvatting maar een voorbeeld om te laten zien hoe de documentatiemap er uit gaat zien. Je leest folder en maakt daar een samenvatting van. Gebruik daar een stuk of vier regels voor, dat is over het algemeen genoeg. Uiteraard kan niemand dezelfde samenvatting hebben.

Mening: Ik vind is natuurlijk het begin van je mening. Dit hier is geen mening, maar een voorbeeld hoe het er in je map uit moet zien. Voor je mening gebruik je ook maar een paar regels, als je wel duidelijk uitlegt waarom je iets goed of slecht of leuk of dom etc vindt.

Hoofdstuk 7 Algemeen/

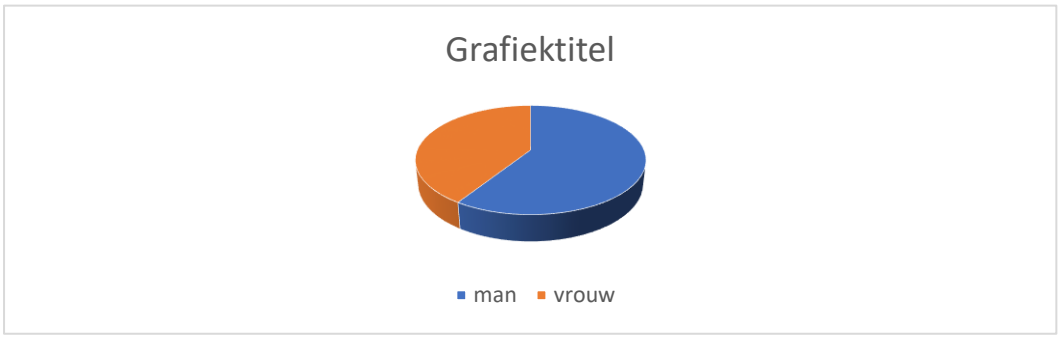
Enquête

1	Wat is uw leeftijd?		
0		okt-15	
0	16 – 20		48
0	21 – 30		40
0	31 – 40		0
0	41 – 50		0
0	ouder dan 50		



Conclusie: de meeste ondervraagden zijn tussen de 10 en 20 jaar oud

2	Bent u :	
0	man	52
0	vrouw	36



Conclusie: er zijn meer mannelijke dan vrouwelijke mensen die geantwoord hebben

3	Hoeveel computers heeft u thuis?		
0		0	5
0		1	60
0		2	23
0	meer		0

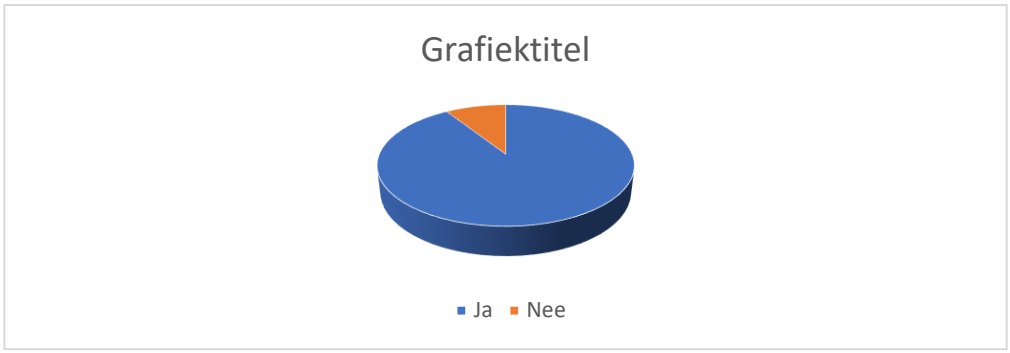
Conclusie: de meeste mensen hebben 1 computer thuis staan

4	Bent u wel eens gehackt?	
0	Ja	32
0	nee	44
0	niet dat ik weet	12

Conclusie: de meeste mensen zijn niet gehackt

5	Heeft u een virusscanner op uw pc?	
0	Ja	80

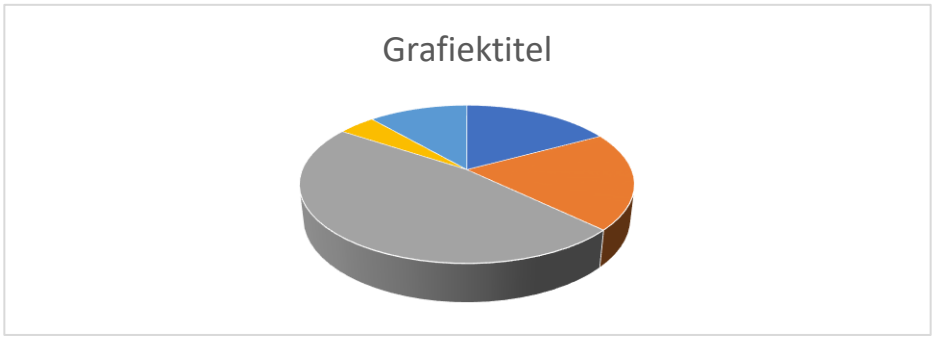
0	Nee	8



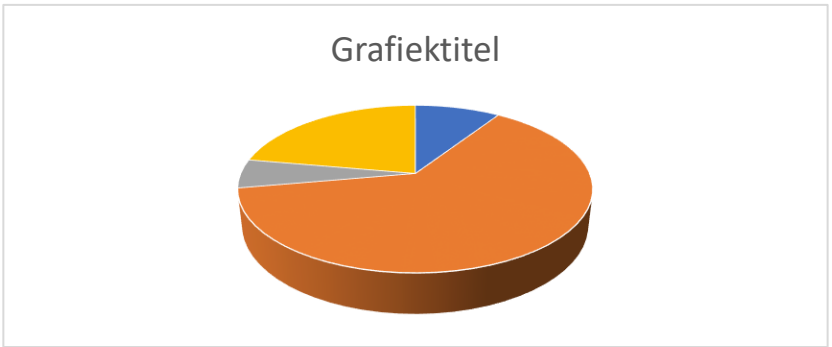
Conclusie: bijna iedereen heeft een virusscanner op zijn pc

6	Weet u wat een firewall is?	12
0	Ja, deze beschermt tegen virussen	14
0	Ja, deze beschermt mij tegen inbrekers op de pc	33
0	Ja, deze zorgt er voor dat mijn pc niet te warm wordt	3
0	Nee	8

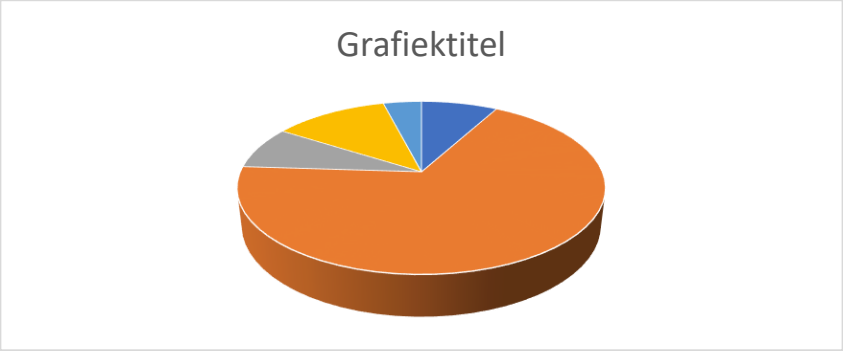
Conclusie: de messte mensen weten wat een firwall is.



7	Wat doet een hacker volgens u?	5
0	Zorgen dat je PC niet meer werkt.	34
0	Probeert gegevens van je te stelen	3
0	Zet je computer op slot en vraagt losgeld	12



8	Wat is ransomware?	4
0	Computers die illegaal gekocht zijn	34
0	Software die illegaal is aangeschaft	4
0	Software die gegevens van je pc haalt	6
0	Verouderde software	2



9	Wat zijn bitcoins?	32
0	Muntstukken	44
0	Digitaal geld	44
0	waardepapieren	3
0	gereedschap van een hacker	15

Mening:

De meeste mensen die de enquête hebben ingevuld wisten niet zo heel vele van hacken. Ook blijkt dat veel mensen geen beveiliging hebben op hun computer etc etc

Conclusie:

Het maken van deze map kostte aardig wat tijd, maar was leuk om te doen. Het onderwerp is heel actueel en iedereen heeft er mee te maken. Bij de onderzoeksvragen heb ik genoeg informatie gevonden om die te kunnen beantwoorden.

Wat is hacken?

Hacken is het inbreken in computers, ik dacht eerst dat dat gewoon om pc's en laptops ging, maar men breekt ook in in systemen van kerncentrales, banken, zonnepanelen, slimme apparatuur thuis etc. De bedoeling is over het algemeen om geld te verdienen, af te persen of sabotage.

Wie doet het?

Er is geen bepaalde 'soort' mensen aan ter wijzen die hacker zijn. Uiteraard zijn het mensen met erg veel computerkennis en ook met een minder goed karakter. Vooral in Rusland, Korea en China zijn er veel hackers, een aantal zelfs in regeringsdienst.

Wat en wie worden er gehackt?

Iedereen eigenlijk, bedrijven, banken, de overheid en particulieren.

Wat zijn goede hackers?

Dit zijn mensen die kijken of een bedrijf of instelling goed genoeg beschermd is tegen hacken en waarschuwt als dit niet zo is. Sommige bedrijven en de overheid hebben dit soort mensen zelf in dienst.

Hoe vaak komt het voor?

Duizenden keren per maand wordt er gehackt> Als je op je eigen computer een goede firewall hebt kan je dat ook zien.

Wat doe je er tegen?

Belangrijk is om altijd je systeem update te houden en goede beschermingssoftware te gebruiken. Een firewall, anti malware en een virusscanner.