Computercriminaliteit

Auteur Its Academy

Laatst gewijzigd 17 september 2013

Webadres https://maken.wikiwijs.nl/45980

Inhoudsopgave

Home

Welkom bij de module "Computercriminaliteit".

Welkom bij de E-klas Computercriminaliteit. Deze E-klas gaat over criminaliteit die met de computer uitgevoerd kan worden. De meest voorkomende criminaliteit vindt plaats via internet en via e-mail. In deze module kom je meer te weten over de gevaren die je tegenkomt op het moment dat je een computer op internet aansluit. Denk bij gevaren bijvoorbeeld aan virussen en hackers, maar bijvoorbeeld ook aan spam en phising e-mail. Al deze onderwerpen worden behandeld in deze module. Wat zijn de gevaren, hoe werken ze en hoe kun je jezelf ertegen beschermen?

Deze E-klas zal ook beschrijven hoe de wet computercriminaliteit ziet. Er staat natuurlijk in de wet dat het niet mag, maar wat mag er dan precies niet?

Het lesmateriaal bestaat uit hoofdstukken en ieder hoofdstuk bestaat uit een aantal paragrafen. I eder hoofdstuk zal worden afgesloten met een toets. De studiewijzer beschrijft wanneer elke paragrafen en toets af moet zijn.

Deze E-klas zal worden afgesloten met een eindopdracht. In deze eindopdracht leer je computercriminaliteit nog beter kennen door in de huid te kruipen van een hacker of van zijn vervolger.

Studiewijzer

Deze studiewijzer beschrijft wanneer elke paragrafen en toets ongeveer af moet zijn. Het lesmateriaal bestaat uit hoofdstukken en ieder hoofdstuk bestaat uit een aantal paragrafen. Ieder hoofdstuk zal worden afgesloten met een toets.

Deze E-klas zal worden afgesloten met een eindopdracht. In deze eindopdracht leer je computercriminaliteit nog beter kennen door in de huid te kruipen van een hacker of van zijn vervolger.

Week	Wat te doen	Opdrachten en Toetsen
1	Inleiding Virussen	Concept Map Virussen
2	Virusbestrijding	Virussen en Virusbestrijding
3	Ongewenste e-mail	Ongewenste e-mail
4	Cryptografie	Cryptografie
5	RFID en De wet	RFID De Wet
6	Hacken	Hacken
7	Eindopdracht:	Practicum: What the Hack Opdracht: computercriminaliteit en de wet.

Index

Computercriminaliteit Index

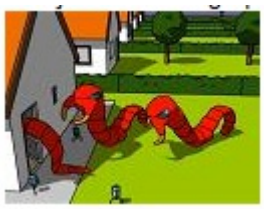
Lesmateriaal

Inleiding

Computercriminaliteit Inleiding

Bekijk als inleiding op het onderwerp computercriminaliteit het animatiefilmpje.

https://youtu.be/AWEtr8GMhKM



Deze module gaat over computercriminaliteit. Criminaliteit op internet en e-mail, maar ook op zogeheten RFID-chips. In deze module kom je dus meer te weten over de gevaren die je tegenkomt op het moment dat je je computer op internet aansluit. Via het internet kun je bijvoorbeeld heel handig dingen snel opzoeken en spelletjes spelen en via e-mail en MSN kun je makkelijk contact houden met vrienden. Maar het internet is niet geheel ongevaarlijk.

Denk bij gevaren bijvoorbeeld aan virussen en hackers, maar bijvoorbeeld ook aan spam en phishing e-mails. Al deze onderwerpen zullen behandeld worden in deze module. Wat zijn de gevaren precies? Hoe werken ze? En ook hoe je je ertegen kunt wapenen, door spamfilters en virusscanners te installeren.

Gelukkig is er ook nog de wet. In de wet staan een aantal artikelen over computercriminaliteit. Er staat natuurlijk in dat het niet mag, maar wat mag er dan precies niet? In deze module kom je het te weten.

Uiteindelijk leer je in het practicum om zelf te hacken.

Computercriminaliteit is geen nieuw fenomeen, maar met het toenemen van het aantal computers lijkt deze vorm van criminaliteit grotere vormen aan te nemen. De criminaliteit wordt niet alleen steeds heviger en schadelijker, ook worden steeds opnieuw nieuwe vormen van computercriminaliteit uitgedacht en toegepast.

Twee recente voorbeelden:

- In 2007 was het gemiddelde spampercentage maar liefst 91,9%: een absoluut record. In de traditioneel drukke spam-maand december kwam het maandgemiddelde zelfs uit op 96%;
- Door politieke motieven gedreven hackers hebben in januari 2007 ingebroken in de computers van het Belgische leger. Vervolgens hebben ze de website voorzien van andere informatie. Bezoekers die vervolgens de website bezochten kwamen terecht op een andere website.

Als je naar deze twee voorbeelden kijkt is de situatie niet erg hoopgevend. Zowel de provider als het Belgische leger zijn professionele organisaties en toch blijken ze niet in staat om de criminelen buiten de deur te houden. Je vraagt je zelfs af of het nog wel verstandig is om je eigen PC aan te zetten.

Opdracht

Maak nu de opdracht "Concept Map Computercriminaliteit " uit het menu-onderdeel "Opdrachten en Toetsen".

1. Virussen

1 Virussen

Een virus is een computerprogramma dat zich op je computer kan bevinden, vaak zonder dat jij daar weet van hebt. Alhoewel dit soms weinig kwaad kan, worden computervirussen in het algemeen als schadelijk beschouwd. In ieder geval nemen ze schijfruimte en computertijd in beslag. In ernstige gevallen kunnen ze in de computer meer schade aanrichten: bijvoorbeeld het verwijderen van belangrijke bestanden of het verspreiden van gevoelige informatie.

Virussen zijn gemaakt om zichzelf te dupliceren en te verspreiden. Op die manier besmetten ze zoveel mogelijk computers. Net als organische virussen (het griepvirus bijvoorbeeld) kunnen sommige computervirussen niet apart bestaan. Dan zijn het stukjes code die aan een ander programma vastgeplakt zitten.

Virussen verspreiden zich door van het ene (besturings)systeem naar het andere over te gaan, door van het ene bestand naar het andere overgebracht te worden en van een digitaal transportmedium naar het andere vervoerd te worden. Veel virussen hebben een “gastheer” nodig: een bestand waar het gebruik van kan maken, of waar het zich aan kan hechten. Zo’n bestand is meestal een *executable*, een programma dat je in werking kunt stellen, bijvoorbeeld een spelletje dat je wilt spelen.

De schade die een virus kan aanbrengen, varieert van geen tot heel veel. Geen schade brengt het aan als het bijvoorbeeld alleen bijvoorbeeld een pop-up laat zien met een boodschap die je een beetje in verwarring kan brengen. Een onverwacht bericht “*Uw printer kan nu niet meer gebruikt worden*” terwijl het apparaat uitstekend functioneert, kan storend werken maar het richt geen schade aan. In het begin werden vooral virussen met een wat pesterig karakter verspreid. Sommige virussen zorgden voor de aantasting van het normale computerbeeld door op willekeurige plekken pixelkleuren te veranderen of die zwart te maken, waardoor het leek alsof ze uitgevallen waren. Serieuzer wordt het als het virus allerlei onzinpagina’s op je printer laat afdrukken, want dat kost je papier en inkt of toner. En erg kwalijk is het als een virus bestanden gaat verwijderen, zodat je na herstart van je pc niet meer (goed) kunt werken.

Er bestaan verschillende soorten virussen. De belangrijkste typen zijn:

- **Bestandsvirus** : Een bestandsvirus hecht zichzelf aan een programmabestand. Programmabestanden zijn de bestanden die je uit kunt voeren; je kunt ze herkennen aan de extensies .EXE of .COM (onder extensie verstaan we de letters achter de punt in een bestandsnaam). Zodra een besmet programmabestand geopend wordt, wordt het virus actief.
- **Macrovirus** : Macrovirussen komen voor in Word- of Excel-documenten. Ze worden actief als het document gestart wordt. Macrovirussen komen bijna niet meer voor, de laatste grote uitbraak was in 1999.
- **Bootsectorvirus** : Bootsectorvirussen richten schade aan in de bestanden die nodig zijn om een computer op te starten. Een bootsectorvirus kan er voor zorgen dat een computer niet meer kan worden opgestart.
- **Polymorf virus** : Een polymorf virus verandert steeds van verschijningsvorm als het zich verspreidt.
- **Tijdbom virussen** : Tijdbom virussen zijn geprogrammeerd om op een bepaalde datum of tijd in actie te komen. Voor die tijd doen ze niets.
- **Mobielvirus** : Een mobielvirus richt zich niet op computers, maar op mobiele telefoons of PDA’s. Het virus kan zich verplaatsen van de ene mobiele telefoon naar de andere.

1.1 Wormen

Wormen zijn stukjes programmacode die zich in een computer nestelen.

Belangrijke eigenschappen van een worm zijn:

- de worm verspreidt zich via netwerkpoorten, waarbij hij zelfstandig op zoek gaat naar computers op het netwerk (Internet of een ander netwerk)
- de worm werkt op zichzelf en niet via een ander programma;
- hij gaat van systeem naar systeem en infecteert geen bestanden, maar systemen.

Een wormvirus zoekt bijvoorbeeld slecht beveiligde computers op waar hij op kan binnendringen. Van daaruit verspreidt hij zich weer verder. Zoals gezegd verspreiden wormen zich zelfstandig, ze hoeven niet mee te liften met een e-mail of een of ander programma.

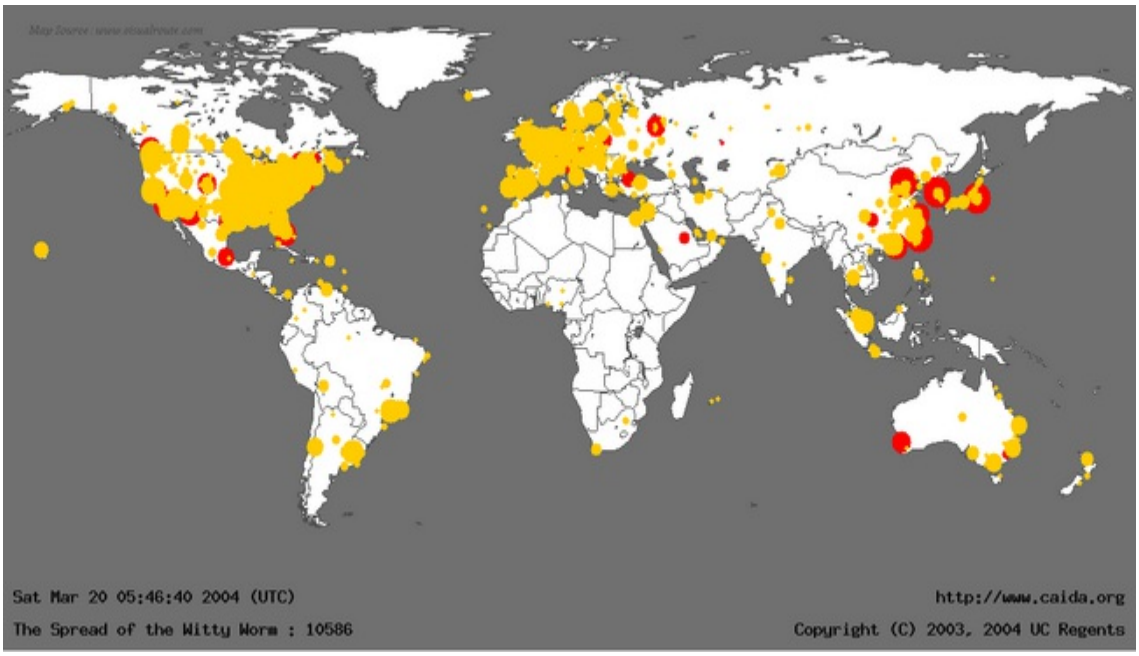
Wormen kunnen allerlei nare effecten hebben. In het eenvoudigste geval benadelen ze het netwerkgebruik door zelf bandbreedte te gebruiken, waardoor je computer heel traag wordt. Ze kunnen echter ook de geïnfecteerde computer schade toebrengen door bestanden te vernielen. Sommige wormen versturen *spam* vanaf de computers die ze infecteren, of ze laten aanvallen uitvoeren op andere computers op Internet.

Belangrijk is te weten dat een worm een pc kan omvormen tot een zogenaamde *zombie* of *bot* (afgeleid van het woord robot).

De eerste worm op het internet werd gemaakt door Robert Tappan Morris jr in 1988. De worm heette daardoor ook de Morris Worm.

In 2004 verspreidde zich de W32/Amus-A worm via e-mail. Als een gebruiker het meegestuurde bestand opende, dan werd er een boodschap voorgelezen. Deze pratende worm maakte gebruik van de Microsoft speech engine in Windows.

Omdat wormen zich zelfstandig verspreiden gaat dit veel sneller dan bij virussen. In de animatie hieronder is te zien hoe de worm Witty zich in 2004 binnen 2 uur over de hele wereld kon verspreiden



Opdracht

Maak nu de opdracht "Wormen" uit het menu-onderdeel "Opdrachten en Toetsen".

1.2 Logic Bomb

Een *logic bomb* is een soort digitale tijdbom die onder bepaalde voorwaarden afgaat. Je pc zal er niet door ontploffen, maar een logic bomb kan alles uithalen wat ook door malware (schadelijke software) kan gebeuren. Iemand die weet hoe hij zo'n logic bomb kan programmeren, kan er voor zorgen dat het ding afgaat als bijvoorbeeld niet aan zijn wensen wordt voldaan. Denk aan een ict-beheerder die ontslagen dreigt te worden en dan met behulp van zijn logische bom het netwerk zodanig kan ontregelen dat hij de enige is die het systeem kan herstellen. Je vraagt je dan natuurlijk wel af of zo iemand weer in dienst genomen wordt …
De meeste logic bombs worden gemaakt met kwaadaardige doeleinden. Ook gewone virussen kunnen logic bombs zijn, als ze op een bepaalde dag of een bepaalde tijd hun kwalijke werk gaan verrichten. Vrijdag de 13e is zo'n beruchte dag.

Celstraf voor systeembeheerder wegens digitale tijdbom

Een voormalig systeembeheerder van Medco Health Solutions heeft een gevangenisstraf van dertig maanden en een boete van tachtigduizend dollar gekregen wegens sabotage van computersystemen. De straf die de ex-systeembeheerder Yung-Hsun Lin in het vonnis kreeg opgelegd was uitzonderlijk hoog, aangezien de gegevens die de man probeerde te wissen, zeer gevoelig waren. De voormalige werkgever Lin verwerkte farmaceutische gegevens van particulieren. Aangezien artsen de Medco-database raadplegen bij het voorschrijven van medicatie, werd voor de hoge straf gekozen.
Yung-Hsun Lin probeerde in oktober 2003 een zogenaamde logic bomb te plaatsen bij zijn toenmalige werkgever. Doel was om de gegevens op ruim zeventig HP-Unix servers te wissen, omdat hij verwachtte dat hij op korte termijn ontslagen zou worden. De 'bom' zou op zijn verjaardag, 23 april 2004 moeten afgaan, maar weigerde door een programmeerfout tot actie over te gaan. Hoewel hij zijn baan op dat moment nog niet kwijt was, herprogrammeerde Lin zijn software zodat die een jaar later af zou gaan. Een paar maanden voor die datum ontdekte een collega-systeembeheerder de software echter waarna de bom ontmanteld werd.

Naar: Willem de Moor, Tweakers.net, 9 januari 2008

1.3 Trojaanse paarden

Een Trojaans paard is een programma dat nuttig lijkt maar heel vervelende eigenschappen heeft. Je downloadt het programma omdat je denkt dat het nuttig is, maar nadat je het programma hebt gestart blijkt vaak dat het programma de beveiliging op je PC heeft lekgeprikt.

Een Trojaans paard vermenigvuldigt zichzelf niet zoals wormen en sommige andere virussen dit doen, maar zorgt ervoor dat gebruikers zelf de code binnenhalen. Het programma komt meestal in de vorm van een handig hulpprogramma, een leuke screensaver of als zogenaamde upgrade. Of misschien als gratis fotobewerkingsprogramma, omdat de legale varianten daarvan best wel wat kosten. Wil je zo'n hebbedingetje dan op je pc hebben staan, dan download je het bestand en besmet je zo je eigen computer. Vooral in peer-to-peer netwerken zijn veel trojans actief. Peer-to-peer netwerken zijn min of meer directe verbindingen tussen diverse computers op Internet, die rechtstreeks van elkaar bestanden kunnen downloaden of uploaden.

Zo'n "aantrekkelijk" programmaatje heeft bijvoorbeeld de bestandsnaam *Christina_Aguilera_bloot_in_bad.exe*. Mensen die Christina Aguilera leuk vinden, downloaden het bestand en klikken erop. Het lijkt of er niks gebeurt, maar in feite wordt de computer dan onzichtbaar besmet en verandert het systeem in een *zombie* (een computer die op afstand

bestuurbaar is door degenen die de trojan hebben gemaakt). Trojans hoeven niet meteen aan de slag te gaan, dus je merkt er soms de eerste tijd niks van dat je het Trojaanse paard in huis gehaald hebt. Maar na een tijdje begint de trojan zijn kwalijke activiteiten en kan hij bijvoorbeeld wachtwoorden stelen, bestanden verwijderen, of poorten op je pc openzetten.

Een voorbeeld hiervan is een Trojaans paard dat zich voordeed als een gratis programma tegen de Blasterworm. Maar wie het programmaatje installeerde zette zijn computer open voor hackers.

De naam Trojaans paard heeft te maken met een verhaal over de Trojaanse Oorlog.

De Trojaanse oorlog (rond 1180 voor Christus):
Al tien jaar vochten de Grieken tegen de Trojanen. Het lukte de Grieken maar niet om de stad Troje in te nemen. Daarom bedacht de Griek Odysseus een list.
De Grieken bouwden een reusachtig houten paard. Soldaten verstopten zich in de buik van het paard. Dit paard werd 's avonds voor de poort van Troje achtergelaten. De Grieken verzonnen een list zodat de Trojanen dachten dat het paard van Pallas Athena kwam en de stad zou beschermen. De Trojanen trapten in de list en haalden het paard met veel moeite de stad binnen. Ze dachten dat ze gewonnen hadden en vierden de hele avond feest om de overwinning te vieren. Toen 's nachts alle Trojanen sliepen, verlieten de Grieken het paard en openden de poorten zodat de Grieken die nog buiten waren, naar binnen konden. De Trojanen waren te moe en te dronken om de stad nu nog te verdedigen. De Grieken staken alles in brand en binnen korte tijd was er niets meer van Troje over.

1.4 Botnets

Een bot is een programma dat zelfstandig geautomatiseerde taken kan uitvoeren. Zo worden bots vaak gebruikt om zaken te doen die bijna onmogelijk zijn voor mensen.

Het woord bot komt van robot. Als een hacker op duizenden pc's tegelijk een virus loslaat, die de duizenden pc's tot botnet omtovert, dan kan de hacker dit botnet op afstand beheersen. Al de machines in een botnet zijn in de macht van de hacker die ze kan gebruiken om spam te versturen, wachtwoorden en creditcardgegevens te verzamelen en nog veel meer. Een botnet van enkele duizenden computers wordt overigens beschouwd als een kleine jongen. De echt zware jongens tellen honderdduizenden tot miljoenen computers. Een bot van een botnet draait meestal op de achtergrond zodat hij niet opvalt op de computer. Vaak heeft de (kwaadwillende) beheerder van een botnet de beschikking over een aantal hulpmiddelen om firewalls en buffers op andere computers te omzeilen. Heel slimme bots kunnen vaak zelf zwakke punten in een computer opzoeken. Met de worm en bot zijn we al een heel eind verwijderd van de oorspronkelijke virus.

Een bot kan heel onschuldig en zelfs handig zijn, maar ook heel vervelend. Een computer die besmet is met een bot wordt ook wel een zombie genoemd. Een botnet is een netwerk van een groot aantal willoze zombies die allemaal besmet zijn met dezelfde bot. Vanuit één centraal punt kan een kwaadwillend persoon alle zombies in het netwerk opdracht geven dezelfde taak uit te voeren.

Opdracht

Maak nu de opdracht "Bots" uit het menu-onderdeel "Opdrachten en Toetsen".

1.5 Meelifters

1.5a Spyware

Spyware is de naam voor computerprogramma's (of delen daarvan) die informatie vergaren over een computergebruiker en deze doorsturen naar een derde partij. Het doel van spyware is meestal geld verdienen. De term is een samentrekking van het Engelse woord *spy* van spion en *ware*, dat aangeeft dat het om software gaat.
De opkomst van spyware is onder andere het gevolg van het illegaal kopiëren van software. De programmamakers zoeken, nu ze minder inkomsten uit verkopen halen, naar andere manieren om geld te verdienen. Het toevoegen van spyware aan een programma is een manier om dat te bereiken. Zo zijn er twee versies van het peer-to-peerprogramma Kazaa: de ene kost geld, de andere bevat spyware.
Naast deze commerciële vorm van spyware bestaat er ook een vorm met meer criminele doeleinden.

Meestal hebben gebruikers geen weet van de spywarefunctie van een programma. Er zijn echter varianten waarbij gebruikers wel over de spywarefunctionaliteiten ingelicht worden. Vaak vindt dit dan op een listige wijze in de algemene voorwaarden plaats.

Voorbeelden van het aftappen van gegevens zijn bezochte internetpagina's inclusief de tijdsduur van het bezoek, e-mailadressen, gebruikte en geïnstalleerde programma's. Deze informatie wordt voornamelijk gebruikt voor reclamedoeleinden, het belangrijkste doel is dan ook geld verdienen.

Spyware is de verzamelnaam voor de volgende types software:

- **Trackingcookies** : Een cookie is een klein bestandje met informatie dat op je computer terecht komt na het bezoeken van een website. Vaak zijn cookies nuttig: ze onthouden bijvoorbeeld je instellingen of loginnaam voor een bepaalde site. Trackingcookies zijn minder onschuldig, ze volgen je surfgedrag (dus welke websites je bezoekt) en sturen dat door naar de site dat het trackingcookie heeft geplaatst. Zo is het voor bedrijven mogelijk om met trackingcookies je surfgedrag te volgen.

- **Reclame banners** : Een reclame banner is een pop-up venster met reclame. Naast de pop-up schermpjes bestaan er ook pop-under vensters. De verbergen zich onder de openstaande vensters. Je ziet het pop-under scherm dus pas later als je de openstaande vensters wegklikt. Reclame banners zijn niet gevaarlijk, maar kunnen wel irritant zijn.
- **Browser hijackers** : Browser hijackers zorgen ervoor dat bepaalde aspecten van de browser aangepast worden. Hierbij is te denken aan het aanpassen van startpagina's, zoekpagina's of favorieten zonder dat je dat zelf wilt.
- **Keyloggers** : Keyloggers zijn programma's die elke toets die jij op je toetsenbord intikt registreren. De zo verkregen gegevens kunnen verstuurd worden naar een centrale computer, waardoor wachtwoorden te achterhalen zijn. Er bestaan ook hardware keyloggers (zie het plaatje hiernaast). Key logging wordt dan gerealiseerd door een apparaatje te gebruiken waarin de toetsenbordkabel ingeplugd wordt. Vervolgens wordt dit apparaat aan de pc gekoppeld en onthoudt het in zijn flashgeheugen welke toetsen zijn ingedrukt. De hardware keylogger kan niet gevonden worden door een virusscanner, de softwareversie vaak wel.

- **Adware**: Adware staat voor *advertising supported software.* Het staat voor elk soort software

die automatisch advertenties toont of downloadt op de pc waar de adware op is geïnstalleerd of dat zelfs doet tijdens het gebruik van de adware. Sommige vormen van adware kunnen *spyware* zijn en mogen dus gezien worden als privacy aantastende software. In de volgende paragraaf lees je hier meer over.

1.5b Adware

Adware staat voor *advertising supported software.* Het staat voor elk soort software die automatisch advertenties toont of downloadt op de pc waar de adware op is geïnstalleerd of dat zelfs doet tijdens het gebruik van de adware. Sommige vormen van adware kunnen spyware zijn en mogen dus gezien worden als privacy aantastende software.

Adware wordt vaak gebruikt bij freeware-programma's (gratis software) waarbij je die advertenties voor lief moet nemen. Gebruik je zulke freeware programma's zonder betaling, hetgeen meestal toegestaan wordt, dan word je telkens lastig gevallen met de pop-ups die je aanzetten tot officiële betaling en registratie van het programma. De adware wijst je op de grote voordelen van het gebruik van een geregistreerde en vaak uitgebreidere versie van het programma. De betaalde versie bevat de adware dan niet meer.

Omdat adware je tot kopen wil aanzetten, zou je kunnen denken dat het niet de bedoeling is dat adware iets op je pc uitspookt dat je niet wenst. Dat is helaas niet altijd het geval. Adware kan je browse-gedrag, je uitgaven en je netwerk-activiteiten nagaan. En dat kan weer aanzetten tot andere reclame-uitingen die daar specifiek op zijn gericht.

1.5c Cookies

Een cookie is een link tussen je pc en de webserver die de cookie gestuurd heeft, zodat deze link na de eerste keer het contact met de webserver vergemakkelijkt. De cookie wordt op je pc opgeslagen in een aparte cookie-map die meestal te vinden is onder de Windows-map. Op deze wijze word je herkend als iemand die al eens eerder de site op de webserver bezocht heeft, zodat de communicatie gemakkelijker kan verlopen. Dit hoeft niet altijd verkeerd te zijn. Het kan zelfs heel gemakkelijk zijn.

voorbeeld

Een cookie kan er als volgt uitzien als je het in een tekstprogramma opent. In dit geval is er een Google cookie aangemaakt.

SNID
13=6pA57EAFsZQdg-dltNtE3x85msasws_RCDoPqC2G=eps3y4VB5Ltb6mv-C
google.com/verify
1536
3088610304
30096276
3333325200
29949425
*

Je ziet dat in codevorm gegevens vastgelegd worden.

Cookies kunnen gebruikt worden voor

- het onthouden van een login-naam of instellingen;
- het vergaren van surfinformatie (de zgn. *profiling*);
- het koppelen van een browser aan tijdelijke variabelen op de server (*session cookie*).

Dit lijkt allemaal heel onschuldig, maar we noemen de cookies niet voor niks in deze module. Het tweede aandachtspunt dat je hiervoor ziet (profiling) is namelijk een punt dat ook misbruikt kan worden door de cookie-aanvrager. In 1997 kwam er een voorstel dat browsermakers aanmoedigde om het gebruik van cookies inzichtelijker te maken voor de gebruiker. Het gevolg hiervan was dat de gebruiker vanaf toen kon instellen in welke mate cookies geaccepteerd mogen worden en of aan de gebruiker gevraagd moet worden of een cookie geaccepteerd mag worden. Dit was om het eerder genoemde profiling tegen te gaan want als gebruikers de cookies van een Internet-advertentiebureau niet accepteren, kan dit advertentiebureau geen profile samenstellen.

Cookies kwamen pas echt in opspraak toen DoubleClick, een Internet-advertentiebureau, een bedrijf overnam met een grote klantendatabase. DoubleClick wilde de naamsgegevens koppelen aan de profiles van surfers en was van plan deze gegevens te verkopen. Deze combinatie van een naamsgegevens en profile is heel aantrekkelijk voor marketingbedrijven, want zij kunnen hiermee advertenties gericht naar iemand sturen. De reclame wordt dan gerichter verspreid, waardoor er meer geld voor een advertentie gevraagd kan worden. Onder druk van verschillende privacy-organisaties heeft DoubleClick de gegevens niet verkocht.

In 2002 is de eerste *P3P-recommendation* gepubliceerd door de *W3C*. Browsers die zich aan deze specificatie houden, accepteren standaard veel minder cookies. De gebruiker kan desgewenst de instellingen van de browser aanpassen. Zo worden bijvoorbeeld cookies in een frame van een ander domein niet meer automatisch geaccepteerd door zo'n browser, tenzij de server een statement opstuurt dat de cookies niet gebruikt worden om privacygevoelige informatie op te slaan.

1.6 Mailvirus

Een mailvirus is een 'ouderwets' virus dat zichzelf als bijlage verspreidt via e-mail. Tijdens een besmetting kan er automatisch een mailserver geïnstalleerd worden, zodat er geen gebruik gemaakt hoeft te worden van een e-mailprogramma op de geïnfecteerde computer. Ook de mailserver van de internetprovider waarmee de besmette computer verbonden is, hoeft niet te worden gebruikt. Internetproviders controleren streng op dit soort virussen, waardoor de kans groot is dat de verdachte berichten er direct uitgefilterd zouden worden als ze via de provider verstuurd worden.

Mailvirussen vervalsen het afzenderadres, vaak door adressen te gebruiken uit het adressenboek op de computer. Zo'n adressenboek heb je bijvoorbeeld staan in je Outlook-programma. Daardoor kan het gebeuren dat je een e-mail krijgt van het adres van je vriendin Marja, terwijl het bericht eigenlijk verstuurd is vanaf de computer van Carolien. Het virus doet dat zodat je Marja gaat lastigvallen in plaats van Carolien. Dat vergroot de chaos. Veel mailvirussen hebben namelijk als enige doel troep te maken en chaos te veroorzaken. Daardoor kunnen ze mailservers verstoppen, mailprogramma's onbruikbaar maken en daardoor e-mailverkeer ernstig bemoeilijken.

Wat heel belangrijk is: installeer een goede virusscanner die altijd up-to-date blijft. De meeste internetproviders filteren de virusmails er gelukkig al uit. Bij sommige providers moet daarvoor wel extra betaald worden.


Opdracht

Maak nu de opdracht "Virussen " uit het menu-onderdeel "Opdrachten en Toetsen".

2 Virusbestrijding

2 Virusbestrijding

Heeft jouw fiets of brommer een slot?

Dit is eigenlijk een retorische vraag. Natuurlijk heeft jouw fiets of brommer een slot, net als je huis een slot op de deur heeft. Het is normaal om je huis te beveiligen tegen inbraak en je fiets op slot te zetten tegen diefstal.
Waarom zou jouw computer geen slot hebben? Daar bewaar je toch al je documenten, bestanden, films, foto's etc. waarvan je niet wilt dat deze gestolen of beschadigd worden?

Iedereen heeft tegenwoordig toegang tot internet, en via dit medium is het een koud kunstje in te breken in jouw computer als deze niet de juiste bescherming heeft. Wat het nog extra moeilijk maakt is dat inbraak in jouw computer via internet in veel gevallen ongemerkt gaat...

Daar gaat het om bij virusbestrijding: zorgen dat jouw computer niet kwetsbaar is voor aanvallen via het internet door hackers, criminelen en andere 'kwaadwillenden'.

2.1 Virusscanners

In het vorige deel heb je gezien wat voor kwaadaardige software er allemaal bestaat. Als je de teksten zo leest, kun je al snel het idee hebben dat het internet een erg gevaarlijke en ongure plek is. Maar gelukkig kun je je als internetgebruiker goed beschermen tegen al die gevaren.

Hoe kun je dan virussen bestrijden? De belangrijkste maatregel is het installeren van een virusscanner.

Een tweede maatregel om virussen te bestrijden is om voorzichtig te zijn met het openen van bestanden die je van anderen hebt gekregen. Open nooit bijlagen van e-mails van personen die je niet kent.

Een derde maatregel is het goed updaten van alle software. Virusmakers maken gebruik van fouten in software. Softwaremakers lossen deze fouten weer op door middel van **patches**: kleine stukjes software die updates uitvoeren of fouten oplossen. Het is belangrijk om als gebruiker van deze software op tijd deze patches te installeren.

Virusscanners

Om computervirussen te kunnen tegengaan, zijn er virusscanners beschikbaar. Virusscanners kunnen virussen opsporen en vaak kunnen ze de virussen dan ook verwijderen. Virusscanners maken gebruik van verschillende technieken om te controleren op virussen:

Techniek 1 : de scanners
Virusscanners maken gebruik van virusdefinities, waarin voor elk bekend virus de fingerprint (= vingerafdruk) wordt vastgelegd. De fingerprint van een virus is een stukje code van het virus dat altijd hetzelfde is. Aan de hand van de fingerprint kan een scanner een virus dan herkennen.
Het grootste nadeel van deze techniek is dat scanners alleen virussen kunnen ontdekken waarvan ze de fingerprint kennen. Voor ieder nieuw virus geldt dat er eerst ergens een slachtoffer moet vallen voordat de makers van de scanner een bruikbare fingerprint kunnen vaststellen. En die fingerprint moet dan aan de scanners worden doorgegeven. Daarom is het belangrijk om je virusscanner vaak te updaten, zodat je altijd de nieuwste fingerprints hebt.

Techniek 2 : de checksummers
Checksummers maken gebruik van de checksums van alle bestanden op de computer. Een checksum is een controlegetal dat uitgerekend wordt aan de hand van de inhoud van een bestand.

Wanneer een programma wordt besmet, verandert het bestand en daarmee ook het controlegetal. De virusscanner controleert dus steeds of de checksum van elk bestand nog hetzelfde is als de checksum die de lijst staat.

Techniek 3 : de heuristische scanners
Een heuristische scanner controleert bestanden op eigenschappen die typisch zijn voor virussen. Voorbeelden van zulke eigenschappen zijn bijvoorbeeld: code om een datum te controleren of code die het adresboek van je e-mailprogramma raadpleegt.

Een goede virusscanner maakt gebruik van alledrie de technieken.

 Reflectie

a) Noem een nadeel van de checksum-methode.

b) Noem een voordeel van de checksum-methode.

c) Een polymorf virus is een virus dat zichzelf kan veranderen als het zichzelf kopieert: hetzelfde virus komt dus voor als telkens net een ander bestandje met net wat andere inhoud/naam/bestandstype. Kan deze methode ook polymorfe virussen herkennen?

klik hier

 Reflectie

a) Noem een nadeel van de heuristische methode.

b) Noem een voordeel van de heuristische methode.

c) Kan deze methode ook polymorfe virussen herkennen?

Klik hier

 Reflectie

a) Noem een nadeel van de scanner methode.

b) Noem een voordeel van de scanner methode.

c) Kan deze methode ook polymorfe virussen herkennen?

Klik hier

2.2 Patches

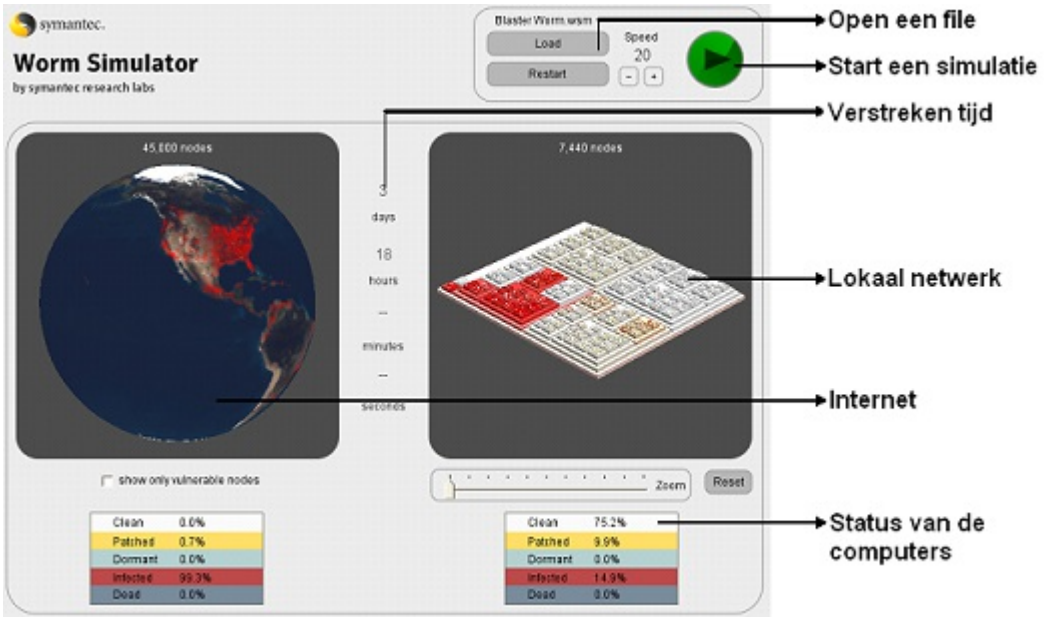
Niet alleen de virusscanner moet geüpdate worden. Ook makers van andere programma's brengen vaak patches uit (ze worden ook wel eens 'service packs' of 'software updates' genoemd). Een patch is een kleine wijziging in een programma om het programma te repareren of te verbeteren. Hierdoor worden ernstige beveiligingslekken in een programma gedicht. Het is aan te raden om patches altijd zo snel mogelijk te installeren.

Symantec, producent van antivirus-software, heeft het programma "Worm Simulator" ontwikkeld. Je hebt al met dit programma gewerkt. Met dit programma heb je kunnen zien hoe de bekendste wormen zich verspreiden en hoe snel patches geïnstalleerd worden door computergebruikers.

Open de Worm Simulator nog eens. Bekijk van de verschillende wormen hoe snel de eerste patches

beschikbaar zijn. Bij welke worm duurt het het langst voordat er een patch is?

Screenshot van het programma:



Een computer op het internet of in een lokaal netwerk kan 5 verschillende verschijningsvormen aannemen:

1. Clean : Dit betekent dat de computer nog geen worm heeft
2. Patched : Dit betekent dat de computer zijn virusdefinities heeft geüpdate of een patch heeft geïnstalleerd. Als een computer gepatched is zal hij dit altijd blijven.
3. Dormant : De worm bevindt zich op de computer maar is nog niet geactiveerd. De worm zit bijvoorbeeld in een nog ongeopende e-mail.
4. Infected : De computer heeft de worm
5. Dead : De computer heeft de worm niet overleefd en doet niets meer.

2.3 Voorzichtigheid en betrouwbaarheid

Het is normaal dat je je fiets op slot zet tegen diefstal. Ook is het normaal dat je jouw fiets niet midden op de weg op slot zet. Je zoekt een plekje in een fietsenstalling of tegen een muur.

Daar gaat het om bij voorzichtigheid, zorgen dat jouw computer niet kwetsbaar is voor aanvallen via bepaalde programma's die op jouw computer draaien. Denk b.v. aan macro's, Java en ActiceX bestanden

2.3a Macro

Een macro is een opeenvolging van handelingen die automatisch uitgevoerd worden. Macro's zijn terug te vinden in Microsoft Word, Excel, Access, PowerPoint, Frontpage, Outlook, enz. Je kunt nuttige macro's maken maar je kunt met macro's ook virussen maken. Als je je wilt beschermen tegen macrovirussen dan kun je het beveiligingsniveau tegen macro's in Word , Excel, PowerPoint en Outlook aanpassen. Kies in de menubalk [Extra] -> [Macro] -> [Beveiliging].


Opdracht

Maak zelf een macro met de opdracht "Macro's" uit het menu-onderdeel "Opdrachten en Toetsen".

2.3b Java en Javascript

Java is een programmeertaal. Java wordt gecompileerd naar bytecode voor een virtuele machine, de Java Virtual Machine (JVM). Deze JVM is beschikbaar voor allerlei verschillende soorten computers, dat wil zeggen computers die draaien onder verschillende besturingssystemen, zoals MS Windows, Linux, Mac OS X. Men gebruikt voor dergelijke talen het begrip platformonafhankelijk: ze zijn niet afhankelijk van een bepaald besturingssysteem. Java en Javascript worden als begrippen wel eens met elkaar verward, maar in feite hebben de twee talen weinig met elkaar te maken. Hoewel beide talen op het eerste gezicht qua syntaxis (de gebruikte code) op elkaar lijken, zijn er grote verschillen.

Bepaalde eigenschappen van Java en zeker JavaScript maken deze talen kwetsbaar voor insluipers die daarmee de eigenschappen kunnen beïnvloeden.

Hackers misbruiken Firefox-lek met Javascript
Door: Niels de Rijk Bron: TechWorld, okt. 2006

Twee hackers hebben zaterdag aangetoond hoe een kritiek lek in Firefox kan worden misbruikt.

Dat meldt Cnet. Tijdens een presentatie op de Toorcon-hackersconferentie demonstreerden Mischa Spiegelmock en Andrew Wbeelsoi hoe kwaadwillenden de controle over een pc kunnen overnemen door gebruik te maken van een bepaalde Javascript-code.

Het lek ontstaat door de manier waarop Firefox Javascript implementeert, aldus Spiegelmock. Diverse codes kunnen volgens de hacker een stack overflow-fout veroorzaken. Volgens Spiegelmock is de Javascript-implementatie 'een zootje'. "Het is onbegonnen werk om het te patchen", zo verklaarde Spiegelmock tegenover Cnet.

Mozilla's veiligheidschef Window Snyder kondigde aan dat het bedrijf de kwetsbaarheid zal onderzoeken. Snyder is niet blij met het feit dat de hackers tijdens de presentatie ook een deel van de code van een exploit voor het lek toonden, aldus Cnet. Tegelijkertijd meent Snyder dat de presentatie genoeg aanknopingspunten biedt voor Mozilla om het lek te dichten.

De beveiligingschef vreest echter ook dat het lek moeilijker te dichten is dan andere kwetsbaarheden, omdat het zich bevindt in de Javascript Virtual Machine. De hackers beweerden tijdens hun presentatie zo'n dertig nog niet gedichte Firefox-lekken te kennen, maar ze willen informatie hierover niet aan Mozilla verstrekken.

"Het mes snijdt aan twee kanten, maar wat wij doen is eigenlijk in het belang van Internet. We creëren communicatienetwerken voor black hats", zo verklaarde Wbeelsoi in een reactie op het verzoek van Mozilla-beveiligingsmedewerker Jesse Ruderman om de kwetsbaarheden te melden.

2.3c ActiveX

Soms komt het voor dat je tijdens het surfen op Internet een waarschuwing krijgt dat een ActiveX-element iets wil doen op je pc. ActiveX is een moderne variant van wat door Microsoft OLE (Object Linking and Embedding) werd genoemd. OLE zorgt voor communicatie tussen verschillende applicaties binnen Windows. Dit maakt het in de praktijk bijvoorbeeld mogelijk om in Word andere

bestandstypen, zoals een plaatje in JPEG, in te voegen of als verwijzing op te nemen in het document. Een ander voorbeeld waarin OLE van pas komt, is wanneer secties in afzonderlijke documenten bewerkt worden en vervolgens als subdocumenten later gecombineerd worden in een hoofddocument. Deze toepassingen werden standaard in Windows-programma's meegeleverd.

ActiveX werd door Microsoft ontwikkeld om applicaties via het Internet te verdelen. Deze technologie is het antwoord van Microsoft op de Java-technologie van SUN Microsystems. Net zoals Java-applets kunnen ActiveX-objecten worden opgenomen in een webpagina. In tegenstelling tot Java-applets zijn ActiveX-objecten afhankelijk van het platform waarop ze draaien, hetgeen betekent dat ze opnieuw moeten worden gecompileerd om ze op een ander platform te kunnen gebruiken.

ActiveX bestaat uit de onderdelen ActiveX Controls, ActiveX Server Pages en ActiveX Server.

- ActiveX Controls zijn kleine programma's die een specifieke taak kunnen uitvoeren en worden aangeroepen door andere programma's zoals een browser. Met zo'n Control kan men bijvoorbeeld een pop-up menu op een pagina laten openen.
- ActiveX Server Pages, beter bekend onder het letterwoord ASP, is een applicatie die is ontwikkeld met behulp van ActiveX Controls en HTML. Dergelijke applicaties worden door een moderne browser herkend en voegen bijvoorbeeld interactiviteit toe aan de statische HTML-codering van een pagina.
- Met de ActiveX Server kan men bijvoorbeeld een database koppelen aan internet. Pagina's bevatten dan zowel statische gegevens (vaste teksten) als dynamische gegevens (de variërende inhoud van de database).

ActiveX kan dus heel nuttige functies verrichten, zoals bepaalde gegevens verzamelen, die je geheel op maat geleverd wilt hebben, bepaalde bestanden bekijken en animaties vertonen. Maar dat maakt een vreemd ActiveX-element ook tot een min of meer gevaarlijke toepassing. Immers, hoe kun je er zeker van zijn dat de ActiveX die iets voor je wilt doen, ook wel de juiste dingen doet en niet ongewenste? Zou het niet gegevens kunnen opsporen in een bestand dat op je pc staat, zonder dat je dat in de gaten hebt? ActiveX-elementen hebben "hogere bevoegdheden" in het Windows-domein dan Java-applets. Zo zie je gebeuren dat ActiveX-elementen als vervoermiddel van spyware en virussen kunnen fungeren.

 Opdracht

Maak nu de opdracht "Virusbestrijding " uit het menu-onderdeel "Opdrachten en Toetsen".

3 Ongewenste e-mail

3 Ongewenste e-mail

In dit thema worden de volgende onderwerpen besproken:

- Spam
- Hoaxes
- E-mailadressen
- Captcha
- Spamfilters

3.1 Spam

Ongevraagde berichten via e-mail, via de mobiele telefoon (SMS of MMS) of via een ander elektronisch kanaal worden spam genoemd.

"SPAM" is een merknaam uit de voedselindustrie: het is ingeblikte ham.
De makers van de Engelse televisieserie Monty Python gebruikten het in een sketch, die zich afspeelt in een café waarvan de menukaart vrijwel geheel uit gerechten met spam bestaat. Een groep Vikingen zingt voortdurend luidkeels: "Spam, spam, lovely spam, wonderful spam". Door het voortdurend gebruik van het woord spam wordt normaal converseren onmogelijk. Hierin zit de overeenkomst met elektronische spam: door de toename van e-mail spam wordt normaal e-mailen ook steeds moeilijker.

Behalve e-mailadressen, is het ook mogelijk om het internet te spammen. Dit kan bijvoorbeeld worden gedaan met een zogenaamde googlebom. Een googlebom is een methode om een bepaalde pagina hoog in de resultaten van Google te laten verschijnen terwijl de trefwoorden waar je op zoekt, niet eens voorkomen in de pagina. Probeer het maar eens met bijvoorbeeld de woorden "raar kapsel" of "miserable failure". Google bombing is mogelijk doordat Google niet alleen de frequentie van woorden op een pagina telt, maar ook het aantal links dat naar die pagina verwijst. Als veel mensen dus een link naar een bepaalde pagina plaatsen en daarbij trefwoorden gebruiken, dan zal Google deze pagina hoger ranken wanneer deze trefwoorden worden opgegeven in de zoekopdracht.

Naast SPAM bestaan er ook SPIM (ongewenste berichten via instant messaging) en SPIT (automatische oproep via de internettelefoon).

3.2 Hoaxes

Een hoax is een nepwaarschuwing. Meestal is het geschreven als een e-mailbericht. De e-mail probeert zich te verspreiden als een kettingbrief. Dit betekent dat in de boodschap de lezer wordt aangespoord om zoveel mogelijk mensen te informeren en de mail dus door te sturen. Het woord hoax komt uit het Engels, waar het zoveel betekent als nep, bedrog, truc of oplichterij.

Bekende voorbeelden van hoaxes zijn:

November 2005
heey iedereen,
vanaf 1 november moet je gaan betalen voor je MSN en mail van hotmail,
tenzij je dit mailtje doorstuurt naar 18 mensen. als je het niet gelooft
kijkt dan op www.msn.com. als je dit naar 18 mensen doorstuurt word je
MSN-poppetje blauw.

Maart 2006
Music Top 50, een nieuw tv-programma dat binnenkort op SBS6 komt, deelt gratis I-pods uit! Wanneer je dit mailtje doorstuurt naar ten minste 15 vrienden (of kennissen) krijg je een gratis I-pod thuisgestuurd. Je moet het mailtje ter controle ook naar bart@musictop50.com sturen, administratief medewerker Bart van Domburg die registreert wie er allemaal een gratis I-pods moeten krijgen.
Music Top 50 doet dit om aan meer naamsbekendheid te komen. Stuur je dit mailtje door naar 15 vrienden maak je dus reclame voor Music Top 50 en krijg je een gratis i-pod.
Als je het zelfs doorstuurt naar 50 vrienden, dan krijg je alle singles uit de Top 50 bijgeleverd met I-pod!
Stuur het door!

Januari 2003
Onderwerp: Waarschuwing voor virus !!
We hebben een boodschap ontvangen van een van onze contacten dat ons adresboek wel eens geïnfecteerd kan zijn door een virus (genaamd jdbgmgr.exe) dat niet gedetecteerd wordt door de

Norton of McAfee antivirus scanners. Het virus slaapt ongeveer een 14 dagen voordat het je computer gaat beschadigen. Het wordt automatisch doorgestuurd naar je contacten uit je adresboek, of je nu hen een e-mail stuurt of niet. Als het aanwezig is op uw PC is het mogelijk geïnstalleerd in c:\Windows\system.

Wat moet u doen:
1.. Ga in Windows Verkenners naar Extra, Zoeken, Bestanden of mappen, of gewoon in het start menu "zoeken" etc.
2.. In het "Naam:" venster schrijft u "jdbgmgr.exe"
3.. In het "Zoeken in:" venster gaat u naar "Drive_c (C:)"
4.. Klik op "Nu zoeken"
5.. Het virus heeft een klein beertje als icoon en de naam "jdbgmg.exe" OPEN DIT NIET !!!!!!!!!
6.. Aanklikken met uw RECHTER muisknop en verwijderen (het gaat dan naar je Prullenbak)
7.. Ga nu naar de Prullenbak en verwijder het bestand of maak de Prullenbak helemaal leeg

ALS U HET VIRUS VINDT, MOETEN ALLE ADRESSEN IN UW ADRESBOEK GEWAARSCHUWD WORDEN, OOK AL HEEFT U DE LAATSTE TIJD GEEN E-MAILS GESTUURD, ZIJ KUNNEN DAN OP HUN BEURT OOK HUN CONTACTEN WAARSCHUWEN.

Een hoax herken je aan de volgende punten:

- Ze roepen op om het bericht door te sturen naar alle contactpersonen.
- Er wordt vaak gewezen op een groot gevaar of een beroep gedaan op medelijden.
- Er is overmatig gebruik gemaakt van leestekens.
- Er staan vaak spelfouten in.

Op de site www.nepwaarschuwing.nl kun je zien welke e-mailberichten hoaxes zijn.


Opdracht

Schrijf nu zelf een (onschadelijke!) hoax met de opdracht "Hoax" uit het menu-onderdeel "Opdrachten en Toetsen".

3.3 E-mailadressen

Ongewenste e-mail kan alleen maar verstuurd worden als bedrijven weten waar ze het naar toe moeten sturen. Hoe komen spammers nu aan deze e-mailadressen? Als je weet hoe bedrijven aan je e-mailadres komen dan weet je ook gelijk hoe je dit kunt voorkomen. Spammers en phishers hebben e-mailadressen nodig waar ze hun berichten naar toe kunnen sturen. Er zijn verschillende manieren om aan e-mailadressen te komen.

De eerste manier waarop spammers aan adressen kunnen komen is door gebruik te maken van een zogenaamde spider. Een spider is een programma dat het hele internet afzoekt naar @ symbolen. Dus op elke pagina die de spider tegenkomt zoekt hij naar het @-symbool. De spider slaat het woord voor en na het apenstaartje op in een bestand en zo vindt de spider een hoop e-mailadressen. Spiders zijn krachtige programma's, dus als je geen ongewenste e-mailberichten wilt kun je het beste je e-mailadres geheim houden en het in ieder geval niet op internet zetten.

Een tweede manier waarop spammers aan adressen komen is door te gokken. Er bestaan computerprogramma's die miljoenen adressen kunnen genereren: zoals jan1@hotmail.com, jan2@hotmail.com enzovoort. Je kunt dus overwegen om niet een standaard e-mailadres te nemen,

maar een e-mailadres dat moeilijk te raden is door dit soort programma's. Spammers hoeven niet eens zelf deze programma's te gebruiken. Er zijn op internet dvd's te koop vol met e-mailadressen.

Als spammers een adres gokken weten ze natuurlijk niet of dat adres bestaat. Wat ze daarom vaak doen is in een spam bericht een unieke verwijzing naar een plaatje of pagina opnemen. Zodra deze wordt geopend weten ze dat het adres dat hoort bij die unieke verwijzing bestaat. Het is dus verstandig om niet altijd alle plaatjes en links te bekijken als je een bericht niet vertrouwt.

3.4 Captcha

Als je een spam of phishing bericht wilt sturen, wil je dat natuurlijk niet van je gewone e-mailadres doen. Je wilt liever anoniem zijn. Daarom schakelen professionele spammers programma's in om heel veel e-mailaccounts aan te maken bij een gratis webmaildienst zoals Hotmail of Gmail. Een computerprogramma dat dit automatisch kan doen wordt een bot genoemd. Een bot kan ook gebruikt worden om op gastenboeken of weblogs reclame achter te laten. Bots zijn voor spammers dus heel krachtige programma's die veel werk in korte tijd kunnen doen.

Om te voorkomen dat een bot automatisch een formulier kan invullen kan op het formulier gebruik gemaakt worden van een captcha. Captcha is een afkorting voor "Completely Automated Public Turingtest to tell Computers and Humans Apart".

De bekendste voorbeelden van captcha's zie je hieronder. Het is de bedoeling dat je de tekst overtypt. Pas als je de tekst goed overtypt kan je het formulier inleveren. Een bot heeft heel veel moeite om de teksten te lezen.

Hoewel Captcha's nog veel worden gebruikt, werken ze niet meer zo goed als vroeger. De bots worden steeds slimmer en met behulp van patroonherkenning is het mogelijk voor de bots om de captcha's te lezen.

Opdracht

Maak nu de opdracht "Captcha" uit het menu-onderdeel "Opdrachten en Toetsen".

3.5 Spamfilters

Men schat dat tegenwoordig bijna 90 procent van de e-mails die worden verzonden spam is. Daarom wordt er erg veel gedaan aan het bestrijden van spam. Een manier om dit te doen is gebruik te maken van spamfilters. Als gebruiker heb je dan weinig last van de spam, omdat die er voor je uit wordt gefilterd. Maar hoe werkt dat filteren precies?

De makkelijkste manier om mail te filteren is gebruik maken van een woordfilter. Alle berichten die binnenkomen, worden door de computer gescand. Als er een bepaald woord uit het woordfilter in voorkomt (bijvoorbeeld viagra), dan bestempelt de computer het bericht als spam.

Woordfilters kunnen werken met verboden woorden, zoals hierboven, en ook met toegestane woorden. Door te tellen hoeveel toegestane en verboden woorden een bericht bevat, kan de computer bepalen of

een bericht wel of geen spam is. Dit heet een heuristisch filter. Zo een filter bepaalt eigenlijk de kans dat een bericht spam is.

Nog slimmer is het om geen vaste woordenlijsten te gebruiken, maar de woordenlijsten steeds aan te passen. In zo een geval wordt een spamfilter Bayesiaans genoemd. Bayesiaanse filters moeten worden getraind. Dit betekent, dat je het filter van tevoren moet vertellen welke berichten wel spam zijn, en welke berichten geen spam zijn. Het programma scant dan alle berichten, en maakt een lijst van alle woorden die in die berichten voorkomen.

Voor elk woord wordt geteld in hoeveel spamberichten het voorkomt en in hoeveel ham-berichten het voorkomt. Een *ham-bericht* is hetzelfde als een *niet-spam bericht*. Dit levert dus een lijst op met voor elk woord dat in de berichten voorkomt twee getallen: het aantal spamberichten waar het in voorkomt in en het aantal ham-berichten waar het in voorkomt. Een spamfilter wordt natuurlijk steeds beter als je het traint met meer berichten.

Voorbeeld

Bijvoorbeeld: Het filter is getraind met 1000 berichten, waarvan er 700 spam zijn en 300 ham. De lijst ziet er als volgt uit:

woord	**aantal keer in spam**	**aantal keer in ham**
Aanbieding	200	30
!	500	100
boeken	7	6
twee	7	50

Het filter krijgt nu het volgende bericht binnen:
Aanbieding! Koop nu gloednieuwe boeken bij ons. Op is op. Betaal over twee jaar.

Is dit bericht nu spam of ham? Met de formule van Bayes kunnen we dit berekenen.

$$P(spam \mid woord) = \frac{P(woord \mid spam)P(spam)}{P(woord)}$$

De formule is het makkelijkst uit te leggen aan de hand van een voorbeeld. Stel dat we alleen kijken naar woord aanbieding dat voorkomt in ons binnengekomen bericht en we willen weten of het bericht spam of ham is.

- **P(spam|aanbieding)** = De kans dat een bericht spam is als het woord aanbieding voorkomt. Dit is wat we gaan berekenen.
- **P(aanbieding|spam)** = de kans dat het woord aanbieding voorkomt in een spambericht = aantal keer dat het woord aanbieding in een spambericht voorkomt gedeeld door het totaal aantal spamberichten = 200/ 700 = 0.29
- **P(spam)** = de kans dat een bericht spam is = aantal spamberichten gedeeld door het totaal aantal berichten = 700/1000 = 0.7
- **P(aanbieding)** = de kans dat het woord aanbieding voorkomt = totaal aantal keer dat het woord aanbieding voorkomt gedeeld door totaal aantal berichten = 230/1000 = 0.23

We krijgen nu dus:

$$P(spam \mid 'aanbieding') = \frac{P('aanbieding' \mid spam)P(spam)}{P('aanbieding')} = \frac{0.286x0.7}{0.23} = 0.87 = 87\%$$

De kans dat een bericht met het woord aanbieding erin spam is, is 87%.

Naïeve Bayes

We hadden niet alleen een bericht waar het woord aanbieding in voorkwam maar we hadden een langer bericht. Hier komen de woorden aanbieding, !, boeken en twee voor in de lijst van het spamfilter. Je krijgt nu de naïeve Bayes formule:

$$p(spam|'aanbieding' \wedge '!' \wedge 'twee' \wedge 'boeken') \approx \frac{x}{x+y}$$

Voor x en y geldt:

$$x = P('aanbieding'|spam)P('!'|spam)P('twee'|spam)P('boeken'|spam)P(spam)$$

$$y = P('aanbieding'|ham)P('!'|ham)P('twee'|ham)P('boeken'|ham)P(ham)$$

We kunnen nu berekenen of het bericht met deze 4 woorden spam is.

- **P(aanbieding|spam)** = aantal keer dat het woord aanbieding in een spambericht voorkomt gedeeld door het totaal aantal spamberichten = 200/ 700 = 0.29
- **P(!|spam)** = aantal keer dat het woord ! in een spambericht voorkomt gedeeld door het totaal aantal spamberichten = 500/ 700 = 0.72
- **P(boeken|spam)** = aantal keer dat het woord boeken in een spambericht voorkomt gedeeld door het totaal aantal spamberichten = 7/ 700 = 0.01
- **P(twee|spam)** = aantal keer dat het woord twee in een spambericht voorkomt gedeeld door het totaal aantal spamberichten = 7/ 700 = 0.01
- **P(spam)** = aantal spam berichten gedeeld door het totaal aantal berichten = 700/1000 = 0.7
- **P(aanbieding|ham)** = aantal keer dat het woord aanbieding in een hambericht voorkomt gedeeld door het totaal aantal hamberichten = 30/ 300 = 0.1
- **P(!|ham)** = aantal keer dat het woord ! in een hambericht voorkomt gedeeld door het totaal aantal hamberichten = 100/ 300 = 0.33
- **P(boeken|ham)** = aantal keer dat het woord boeken in een hambericht voorkomt gedeeld door het totaal aantal hamberichten = 6/ 300 = 0.02
- **P(twee|ham)** = aantal keer dat het woord twee in een hambericht voorkomt gedeeld door het totaal aantal hamberichten = 50/ 300 = 0.17
- **P(ham)** = aantal ham berichten gedeeld door het totaal aantal berichten = 300/1000 = 0.3

De uitkomst is nu:

$$p(spam|'aanbieding' \wedge '!' \wedge 'twee' \wedge 'boeken')$$

$$\approx \frac{0.29*0.72*0.01*0.01*0.7}{(0.29*0.72*0.01*0.01*0.7)+(0.1*0.33*0.02*0.17*0.3)} = 0.3 = 30\%$$

Opdracht

Maak nu de opdracht "Ongewenste e-mail " uit het menu-onderdeel "Opdrachten en Toetsen".

4 Cryptografie

4 Cryptografie

In dit thema worden de volgende onderwerpen besproken:

- Cryptografie

4.1 Inleiding

Cryptografie houdt zich bezig met het omzetten van een bericht of bestand in geheimtaal. Het voordeel hiervan is dat pottenkijkers niet meer mee kunnen lezen. Alleen de ontvanger, die de beschikking heeft over de juiste sleutel, kan uit het geheimschrift de originele boodschap terugkrijgen. Cryptografie wordt tegenwoordig veel toegepast: bijvoorbeeld in gsm's, pinautomaten, de chipknip of de decoder van de TV. Cryptografie wordt ook gebruikt om bestanden te versleutelen, e-mails te coderen of om afgeschermde websites mee te bekijken. In dit hoofdstuk houden we ons vooral bezig met het versleutelen van e-mailberichten. Welke mogelijkheden zijn er om je e-mailberichten te vertalen in geheimtaal zodat niemand mee kan lezen?

Drie belangrijke begrippen in de cryptografie zijn:
Encryptie : het versleutelen van de informatie door de zender
Decryptie : het weer ontcijferen van de informatie door de ontvanger.
Sleutel : De sleutel wordt gebruikt om de informatie te encrypten en ook om de informatie te decrypten

4.2 Simpele methodes

Julius Caesar was de eerste die op vrij grote schaal gebruik maakte van cryptografie. Hij gebruikte geheimschrift om zijn leger te informeren. De methode die Julius Caesar gebruikte is een van de simpelste vormen van cryptografie en werkt als volgt: Elke letter in een bericht werd in het alfabet drie plaatsen opgeschoven, dus een A werd een D, een B werd een E enzovoort. Een X werd weer een A. Deze methode van Julius Caesar is te makkelijk te kraken en wordt niet meer gebruikt in cryptografie.

In de Tweede Wereldoorlog dachten de Duitsers na over een betere encryptiemethode en kwamen met de Enigma. De Enigma is een soort typemachine die uit drie onderdelen bestaat: drie code-wielen, het toetsenbord en een paneel met lampen waarbij elke lamp bij een letter hoort.

Eerst moest een begininstelling van de enigma gekozen worden. Deze begininstelling werd uit een codeboek gehaald waar voor elke dag een andere instelling stond. Daarna kon de boodschap ingetoetst worden. De drie code-wielen vertaalden elke letter drie keer naar een geheime letter die werd aangegeven op het paneel van lampen.

Het voordeel van deze methode was dat na elke letter de code-wielen draaiden. Een letter W werd dus elke keer in een andere geheime letter vertaald. Het nadeel van deze methode was dat iedereen die de berichten wilden ontcijferen hetzelfde codeboek voor de begininstelling moesten hebben. Deze codeboeken moesten dus verspreid worden over het hele Duitse leger.

Uiteindelijk werd de code van de Enigma toch gekraakt door de Polen en de Britten. Ook de Enigma wordt niet meer gebruikt in hedendaagse cryptografie. Tegenwoordig heb je een betere beveiliging nodig.

Klik hier om naar de bron van de afbeelding te gaan.

Opdracht

Op deze pagina kun je de werking van de enigma-machine bekijken. Wat is het gecodeerde bericht van het woord Hallo?

Verander nu onder de knop settings de volgorde van de codewielen in 123 i.p.v. 312. Wat is nu het gecodeerde bericht van het woord hallo?

4.3 RSA

De voorbeelden die we tot nu toe gezien hebben zijn voorbeelden van symmetrische cryptografie. Dit betekent dat je dezelfde sleutel nodig hebt voor het encrypten en decrypten van een bericht. Het probleem hiervan is dat je de sleutel moet doorgeven en hierdoor kan deze onderschept worden. De onderschepper kan de berichten dan meelezen.

Tegenwoordig wordt gebruikt gemaakt van asymmetrische cryptografie. Bij asymmetrische cryptografie zijn twee verschillende sleutels nodig: een sleutel om de informatie te encrypten, en een andere sleutel om de informatie te decrypten.

De meest bekende encryptiemethode tegenwoordig is RSA. Deze methode maakt gebruik van asymmetrische cryptografie en van priemgetallen. Dit maakt de RSA methode heel veilig. RSA is genoemd naar de initialen van de uitvinders: Rivest, Shamir en Adleman.

Priemgetallen

RSA maakt gebruik van de eigenschappen van priemgetallen, daarom gaan we eerst in op wat dat precies zijn. Priemgetallen zijn getallen, die alleen door 1 en zichzelf deelbaar zijn. Het getal 9 is geen priemgetal want 9 is deelbaar door 3. Het getal 17 is wel een priemgetal. Er is geen getal denkbaar waar 17 een geheel aantal malen door te delen is.

Er is niet één priemgetal aan te duiden als het grootste. Er bestaat wel het grootste priemgetal dat tot nu toe bekend is. De Duitse oogarts Martin Nowak heeft in maart 2005 het grootste priemgetal tot nu toe ontdekt. Dit priemgetal bestaat uit maar liefst 7.816.230 cijfers. De eerste persoon die een priemgetal van 10 miljoen cijfers vindt, wint 100.000 dollar.

Priemgetallen hebben een speciale eigenschap: elk geheel getal kan worden gemaakt door bepaalde priemgetallen te vermenigvuldigen. Dit kan maar op één manier. Zo kun je het getal 42 maken door de priemgetallen 2,3 en 7 met elkaar te vermenigvuldigen (2 * 3 * 7 = 42). Er is geen andere combinatie van priemgetallen mogelijk die je met elkaar kunt vermenigvuldigen en die 42 oplevert.

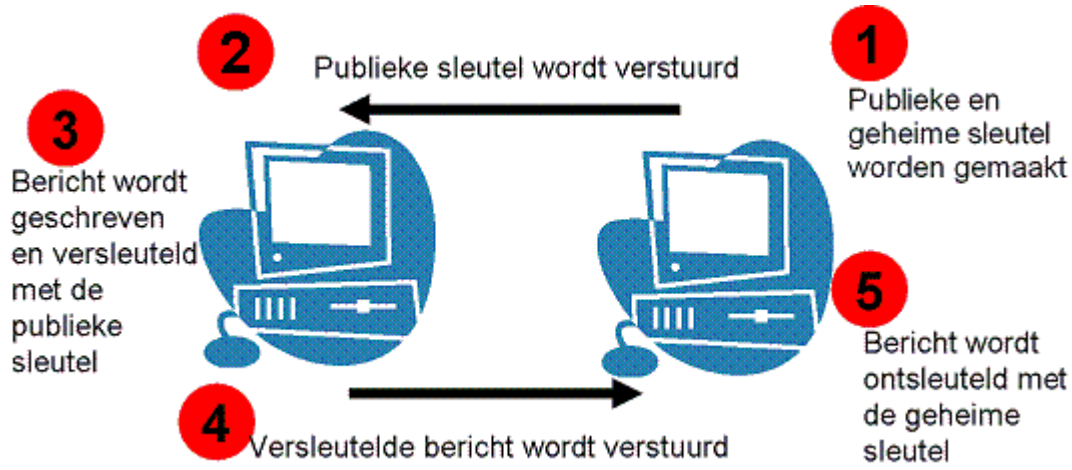
RSA en priemgetallen

RSA maakt gebruik van deze eigenschap van priemgetallen. Zoals we al eerder hebben gezien maakt RSA gebruik van twee sleutels: een publieke sleutel en een geheime sleutel. De publieke sleutel mag iedereen weten en deze sleutel is nodig om een bericht te encrypten. De geheime sleutel moet je goed geheim houden en met behulp van deze sleutel kun je een bericht decrypten. De publieke sleutel kun je maken door twee priemgetallen met elkaar te vermenigvuldigen. Bijvoorbeeld 2027 * 6359 = 12889693. de publieke sleutel is dus nu 12889693. Met deze sleutel kun je een bericht encrypten.

Om het bericht vervolgens te decrypten heb je de getallen 2027 en 6359 nodig.Het is niet makkelijk om erachter te komen welke priemgetallen je met elkaar moet vermenigvuldigen om de publieke sleutel te krijgen. Bij kleine getallen is dit nog wel mogelijk zoals je hebt gezien. Maar bij heel grote getallen is dit niet mogelijk - tenminste met de computers die we tot nu hebben. Als je een bericht veilig wilt versturen heb je een heel grote publieke sleutel nodig.

4.4 Versleutelde E-Mail

Welke stappen moet je nu ondernemen om een beveiligde e-mail te sturen? Hieronder zie je de vijf stappen:



Om publieke en geheime sleutels te genereren kies je twee heel grote priemgetallen. De getallen noemen we P en Q. Aan de hand van deze priemgetallen genereert de computer drie getallen.

1. Getal N : N = P * Q
2. Getal D
3. Getal E

Als je wil weten hoe de getallen D en E gegenereerd worden kijk dan op Wikipedia. Getal N en E zijn je publieke sleutels. Je publieke sleutel is openbaar en iedereen mag deze weten. Getal D is de geheime sleutel. Hoe langer deze sleutel is, hoe betrouwbaarder de codering zal zijn.

Om een bericht veilig te versturen kun je het coderen met behulp van iemand anders zijn publieke sleutel. Hierna kan de ontvanger het bericht decoderen met zijn geheime sleutel. De publieke sleutel van de ontvanger moet dus bekend zijn. De geheime sleutel wordt echter nooit verzonden, wat deze methode behoorlijk veilig maakt.

Opdracht

Maak nu de opdracht "Cryptografie" uit het menu-onderdeel "Opdrachten en Toetsen".

5. RFID

5. RFID

Radio Frequency Identification (RFID) is een automatische identificatiemethode. Een RFID chip is een minuscule chip die je ergens op kunt plakken of aan kunt hangen (bijvoorbeeld aan dingen, mensen of dieren). Een RFID lezer kan draadloos de informatie uit de chip halen. Elke chip heeft een unieke code.

Omdat er relatief veel informatie op een RFID chip kan, ze geen batterij nodig hebben en ze goedkoop gemaakt kunnen worden, worden RFID chips nu al veel toegepast. In de toekomst zal dat alleen maar meer gaan worden.

Hieronder staan enkele toepassingen waar de RFID chip gebruikt wordt in Nederland:

- **Baja beach club**: RFID chips worden gebruikt in de Rotterdamse discotheek Baja Beach Club. Een vaste klant met een RFID chip in zijn arm kan op deze manier afrekenen. Een chipknip in je arm dus.
- **Bibliotheekboeken**: Alle bibliotheekboeken in Nederland bevatten een chip. Hierdoor kunnen ze makkelijker uitgeleend en gevonden worden.
- **Paspoorten**: Alle Europese paspoorten die na augustus 2006 worden uitgegeven bevatten een chip. Op deze chip staan al je gegevens en zelfs je foto. Dit is om fraude tegen te gaan.
- **Dieren**: Denk maar aan de gele oormerken van de koeien. Hierin zitten RFID chips.
- **Bagage**: Schiphol wil alle koffers uitrusten met een RFID chip. De bagage blijkt zo namelijk veel beter te volgen. Dit project is nog in de testfase.
- **OV-chippas**: De OV-chipkaart heeft ook een RFID chip. Op deze manier kunnen mensen reizen met de metro, tram of bus en wordt de oude strippenkaart overbodig.
- **WK-voetbal**: Tijdens het Wereldkampioenschap voetbal van 2006 zijn in de toegangskaarten RFID-chips verwerkt. Op deze manier waren de kaarten veel moeilijker na te maken.

Op de pagina http://www.rfidnederland.nl/ kun je heel wat informatie vinden over het gebruik van RFID op dit moment in Nederland.

Deze nieuwe techniek is heel handig maar brengt ook problemen met zich mee. Op de VU in Amsterdam hebben ze het eerste virus geschreven voor een RFID-chip. Dit heeft toen op veel plaatsen het nieuws gehaald. Kijk voor een overzicht op deze pagina.

Een nadeel van virussen op de chips wordt beschreven in het volgende scenario:
Een persoon komt een supermarkt binnen en koopt een pot pindakaas met een RFID chip. Thuis aangekomen haalt hij de chip van de pot af en hij plakt een nieuwe met een virus geïnfecteerde chip terug op de pindakaas. Hij neemt de pot pindakaas weer mee naar de supermarkt en rekent deze opnieuw af. Als de pot pindakaas nu gescand wordt, dan wordt het supermarktsysteem geïnfecteerd met een virus. Dit kan een hoop problemen tot gevolg hebben, bijvoorbeeld dat alle prijzen van de producten veranderen. Supermarkten gebruiken nu nog geen RFID chips maar streepjescodes. Supermarkten zijn wel van plan om over te stappen omdat RFID scanners veel sneller zijn.

6 De wet

6 De wet

Sinds 1993 bestaat er in Nederland een wet om computercriminelen aan te pakken. In deze nieuwe wet werden onder andere computervredebreuk, virusverspreiding, gegevensbeschadiging, het onbevoegd aftappen van gegevensverkeer en het vervalsen van betaalpassen strafbaar gesteld. Deze wet heet de Wet computercriminaliteit I.

De wet uit 1993 bleek snel verouderd door de snelle ontwikkelingen op computergebied. Daarom is per 1 september 2006 de Wet computercriminaliteit II ingegaan.

In dit hoofdstuk zullen we een aantal artikelen uit de Wet computercriminaliteit II bekijken.

6.1 Computervredebreuk

De bekendste vorm van computercriminaliteit is hacken, de wet noemt dit computervredebreuk. Met het wetsartikel 138 kunnen hackers bestraft worden. Onder de oude wetgeving was computervredebreuk alleen strafbaar wanneer een beveiliging werd doorbroken. Deze eis is komen te vervallen. Computerinbraak is nu strafbaar wanneer de dader wist of had kunnen weten dat hij op verboden terrein was. In Nederland zijn er nog niet zoveel mensen veroordeeld voor het plegen van computervredebreuk.

Een paragraaf uit een wetsartikel wordt een lid genoemd. Hieronder staan twee leden uit **artikel 138a**.

- **Lid 1** Hierin is vastgelegd dat het inbreken in iemand anders zijn computer strafbaar is.
  Straf : Gevangenisstraf van ten hoogste een jaar of geldboete van 16.750 euro.
- **Lid 2** Wie na het opzettelijk binnendringen ook nog eens gegevens kopieert, kan een straf van maximaal vier jaar cel krijgen

Om een computer binnen te dringen wordt vaak gebruik gemaakt van software. **Artikel 139** zegt over deze software :

- **Lid 2a** Het maken, vervaardigen, verkopen, verwerven, invoeren, verspreiden of anderszins ter beschikking stellen of voorhanden hebben van dergelijke software is een strafbaar feit.
  Straf : 1 jaar cel of een boete van 16.750 euro.

Sinds september 2006 is er niet alleen een artikel 138a maar ook een **artikel 138b** , in dit artikel staat :

- Het is niet toegestaan een systeem plat te leggen door er grote hoeveelheden data naar toe te sturen.
  Straf : maximaal 1 jaar cel of geldboete van 16.750 euro

Met behulp van deze nieuwe wet is het nu mogelijk om het uitvoeren van een denial of service aanval (ook wel verstikkingsaanval genoemd) te bestraffen. Een denial of service aanval is een actie waarbij wordt geprobeerd een server uit de lucht te halen. Een voorbeeld hiervan is de mislukte chatsessie met Willem-Alexander en Maxima in 2002. Een groep van acht zeer ervaren hackers voerde een massale aanval uit op de computers van KPN. In enkele seconden tijd bezweken deze onder de grote hoeveelheid data die via internet aankwam hierdoor kon de chatsessie niet meer doorgaan.

6.2 Gegevensbeschadeging

Een ander belangrijk wetsartikel in de computerwetgeving is artikel 350a. In artikel 350a staat dat het verboden is om opgeslagen gegevens te vernielen.

Artikel 350a

- **Lid 1** : Het is verboden om gegevens te veranderen, wissen of toe te voegen.
  Straf : twee jaar cel of een boete van 16.750 euro
- **Lid 2** : Lid 2 zegt dat er nog een extra straf is voor degenen die eerst in een computer inbreken voordat ze gegevens wijzigen.
  Straf : vier jaar cel of een boete van 16.750 euro
- **Lid 3** : Het verspreiden van virussen, wormen of Trojaanse paarden is verboden.
  Straf : maximaal vier jaar cel
- **Lid 4** : Lid 3 mag wel als als de verspreider goede bedoelingen heeft.

De eerste persoon die in Nederland veroordeeld is voor het schrijven van een virus was Jan de W. in het jaar 2001. Hij maakte Het Kournikova-virus met behulp van een virusmaker die hij gedownload had van internet. Het Kournikova virus was een van de meest verspreide virussen in 2001.

Een artikel dat lijkt op het artikel 350a is artikel 161sexies:

Artikel 161sexies

- **Lid 1** : Het is verboden om opzettelijk een computersysteem te vernielen, beschadigen of

onbruikbaar te maken.
Met het vernielen van een computer wordt niet het fysiek vernielen van een computer bedoeld.
Straf : een jaar cel
Straf : zes jaar cel als goederen of diensten in gevaar worden gebracht
Straf : negen jaar cel als er levensgevaar door wordt veroorzaak
Straf : vijftien jaar cel als er iemand door komt te overlijden

Opdracht

Maak nu de opdracht "De wet" uit het menu-onderdeel "Opdrachten en Toetsen".

7 Hacken

7 Hacken

In dit thema worden de volgende onderwerpen besproken:

7.1 Waarom wordt er gehacked

Hackers en crackers doen hetzelfde: inbreken op een andere computer. Maar toch is er een groot verschil tussen hacken en cracken.

Een hacker is iemand die om idealistische redenen de beveiliging van systemen test op fouten en daar verbeteringen voor probeert te vinden. Een cracker is een kwaadwillend persoon, die zich bezig houdt met illegale toegang tot een andere computer.

Een hacker wordt ook wel een white-hat hacker genoemd en een cracker een black-hat hacker. Deze termen komen uit cowboyfilms waarin de "kwaden" zwarte hoeden droegen en de "goeden" witte hoeden.

Een white-hat hacker is geliefd in het bedrijfsleven. Bedrijven huren ze in om de beveiliging van hun systemen te testen. Zo hopen ze de black-hat hackers buiten de deur te houden.

Naast hackers en crackers is er ook nog de categorie scriptkiddies. Scriptkiddies zijn personen zonder kennis van programmeren die het leuk vinden om virussen te maken en verspreiden. Het is mogelijk om van het internet software te downloaden waarmee je zonder enige kennis van zaken een virus kunt maken. Het blijkt dat veel virussen door scriptkiddies gemaakt zijn.

Maar hoe werkt hacken dan? De meeste hackers, crackers en scriptkiddies maken gebruik van exploits. Een exploit is een kwetsbaarheid in de hardware of software. Een zero-day exploit is een net ontdekte kwetsbaarheid. Zero-day exploits zijn extra gevaarlijk omdat de makers van de software waarin de exploit zit vaak nog niet eens weten hoe ze de software moeten beveiligen.

Naast exploits gebruiken crackers vaak ook sociaal hacken oftewel social engineering. Dit is een techniek waarbij de hacker een inlognaam en wachtwoord probeert te achterhalen via een mens. Een methode is bijvoorbeeld om een bedrijf te bellen en de receptioniste te vertellen dat alle computers besmet zijn met een ernstig virus en dat je nu het wachtwoord nodig hebt om de informatie op de computers te kunnen redden. Als de secretaresse dan toehapt en het wachtwoord geeft, ben je als cracker binnen.

7.2 Wardriven

Wardriving is rondrijden met een auto met de bedoeling draadloze netwerken te vinden.

Een draadloos netwerk is een computernetwerk waarbij de aangesloten apparaten niet via kabels met elkaar communiceren maar via radiogolven. Het voordeel van een draadloos netwerk is dat je geen kabels hoeft te leggen en dat je op elke willekeurige plek in je huis kan internetten. Voor een draadloos netwerk heb je een basisstation nodig. Dit apparaat zorgt voor de verbinding. Meestal is dit basisstation een draadloze router (zie het plaatje hiernaast). Als je een computer hebt die draadloze netwerken ondersteunt dan kun je contact maken met het basisstation en op die manier bijvoorbeeld gebruik maken van internet.

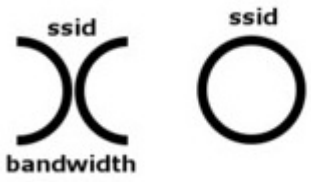
Het nadeel van een draadloos netwerk is dat radiogolven door muren en ramen gaan dus dat ook je buurman contact kan maken met jouw basisstation. De meeste draadloze netwerken maken zich bekend door continu hun naam te versturen. Deze naam noemen we het SSID. SSID staat voor Service Set Identifier. Wardrivers zijn in hun auto continu op zoek naar SSID's.

Om te voorkomen dat je buurman of wardrivers gebruik kunnen maken van je draadloze netwerk is het belangrijk dat je je draadloze netwerk goed beveiligt.

Naast wardriving zijn er ook mensen die aan warwalking (wandelen), warcycling (fietsen) en warstorming (rondvliegen) doen. En er zijn ook mensen die niet op zoek zijn naar draadloze internetverbindingen maar naar bijvoorbeeld telefoons met een bluetooth verbinding.

Als je als wardriver een netwerk hebt gevonden, wil je dat aan andere wardrivers laten weten. Dat kan op twee manieren:

Warchalking is het met krijt aangeven in publieke ruimtes of er een draadloos netwerk in de buurt is. Ook geven ze aan of het goed of slecht beveiligd is. De twee belangrijke tekens die ze gebruiken zie je hieronder.



Het rechterteken geeft een onbeveiligd netwerk aan. Het linkerteken een beveiligd netwerk.

De andere manier om aan te geven waar onbeveiligde netwerken zijn is natuurlijk via internet. Er zijn diverse internetsites die aangeven waar je draadloze netwerken kunt vinden en of ze beveiligd of onbeveiligd zijn.

7.3 Phishing

Phishing is een variant op het Engelse woord fishing, wat "vissen" betekent. Phishing is een vorm van oplichterij. Het doel van phishing is het verkrijgen van gevoelige informatie zoals creditcard nummers, wachtwoorden of inloggegevens. Een phisher doet zich meestal voor als een bekende organisatie, bijvoorbeeld een bank of online winkel. De phisher verstuurd miljoenen nep e-mails naar willekeurige mensen. In deze e-mail verzoekt de phisher de mensen om een site te bezoeken en er persoonlijke gegevens achter te laten. De link in het bericht verwijst echter niet naar de officiële site van de bank of winkel, maar naar een vervalste website. Als een bezoeker van de nepsite dan zijn of haar gegevens invult, krijgt de phisher ze op een presenteerblaadje aangereikt.

Het plaatje hieronder laat een voorbeeld van een phishing e-mail zien:

Lieve Postbank Klant,

Deze email werd verzonden door de Postbank server om uw identiteit vast te stellen. Je moet dit proces afmaken door de link beneden aan te klikken om door te gaan in het volgende menu en daar je gebruikersnaam en wachtwoord invullen. Dit is gedaan voor je eigen veiligheid - omdat sommige van onze leden niet langer toegang hebben tot hun emailadres en wij het moeten verifieren.

http://www.postbank.nl/q6GmCDVHkdOCtbhcD8ZsYS51ASSLFqxpmG4faOdRpjRVibHeu4zc1c8n0n5l9w50k

Wij hopen u hiermee voldoende te hebben geinformeerd.
Met vriendelijke groet,
Postbank.nl

Veel voorkomende zinnen in een phishing e-mail zijn:

- "Geachte klant."
- "Controleer uw account."
- "Klik op de onderstaande link om toegang te krijgen tot uw account."

Vaak is de boodschap van de mail dat het bedrijf de klanten gegevens aan het bijwerken zijn. Daarom moeten klanten hun gegevens nogmaals opsturen. Maar let op: een bank of internetbedrijf zal nooit om persoonlijke gegevens vragen via een e-mail. Dus als je zo'n e-mail binnenkrijgt dan kun je deze het beste weggooien!

7.4 Spoofing

In een phishing e-mail wordt vaak verwezen naar een nagemaakte website. Er wordt meestal gebruik gemaakt van URL-spoofing, dit is het nabootsen van een bekend internetadres, zodat de gebruiker denkt de echte site te bezoeken, terwijl de website die van de bedrieger is. Voorbeelden zijn:

http://wwwbank.com	i.p.v.	http://www.bank.com
http://www.microsoft.com@ebay.com	i.p.v.	http://www.microsoft.com/
http://www.gogle.nl	i.p.v.	http://www.google.nl
http://www.micosoft.com/	i.p.v.	http://www.microsoft.com

Niet alleen het internetadres lijkt op de echte site, ook de opmaak van de website lijkt erg op die van de echte site. Het is dus niet makkelijk te ontdekken dat je als bezoeker op een gespoofde site zit.

Zorg ervoor dat als je betrouwbare informatie van jezelf intypt (bijvoorbeeld een wachtwoord), dat er gebruik is gemaakt van een beveiligde site. Een beveiligde website maakt gebruik van een SSL certificaat. SSL staat voor Secure Sockets Layer en beveiligt data tegen onderschepping door derden door middel van een codering (encryptie). Een SSL beveiligde website is te herkennen aan:

1. "https://" voor het internetadres, en
2. het slotje onderaan de betreffende pagina

Je kunt op een SSL certificaat ook controleren van wie de site is.

Op Internet Explorer 7 en Firefox 2.0 zit een phishing-filter. Dit filter controleert of sites betrouwbaar zijn. De melding die je in Firefox krijgt zie je hieronder:

Ook spammers maken gebruik van spoofing. Dit heet e-mailheaderspoofing. Het adres van de afzender (de header) is daarbij vervalst, waardoor het lijkt alsof het bericht van een bekende komt. Dit verleidt gebruikers niet alleen om de mail toch te openen, maar verbergt tevens de identiteit van de echte afzender. E-mailspoofing is simpel. Verander in je e-mailprogramma je naam en e-mailadres in de naam en het e-mailadres van een ander.

Opdracht

Maak nu de opdracht "Veilig bankieren" uit het menu-onderdeel "Opdrachten en Toetsen".

7.5 Firewall

Bekijk eerst onderstaande video:

https://youtu.be/PBWhzz_Gn10

Bron: http://www.youtube.com/watch?v=PBWhzz_Gn10

Iedere computer in een netwerk heeft zijn eigen unieke Internet Protocol adres, het IP-adres. Om data naar een computer te kunnen sturen heb je zijn IP-adres nodig. Om er voor te zorgen dat de data bij het juiste programma terecht komt heeft elk IP-adres 65536 virtuele poorten. Als je bijvoorbeeld met een browser aan de slag gaat zullen de pagina's die je opvraagt via poort 80 (http) binnen komen. Het laden van je mail gaat via poort 110 (pop3).

Een hacker maakt gebruik van deze poorten om een computer binnen te komen. Met behulp van een poortscanner bekijkt de hacker alle poorten van een computer en controleert op deze manier of er een open staat.

Om een computer te beveiligen tegen hackers moeten we er voor zorgen dat er geen ongewenste bezoekers binnen komen, maar ook dat er niet zo maar informatie naar buiten gaat. Kortom, we hebben een poortwachter nodig die al het verkeer, naar binnen en naar buiten, controleert en zo nodig blokkeert: een firewall. Met behulp van de firewall kun je poorten openen en afsluiten.

Er zijn twee soorten firewalls: een hardware- en een softwarematige. De hardwarematige variant is een apart apparaat dat als firewall fungeert. Een softwarematige firewall is een programma dat op de computer draait.

7.6 Buffer Overflow

Een hacker kan door middel van een poortscanner controleren welke poorten open staan. Maar met een poortscanner is de hacker de computer nog niet binnen. De technieken die gebruikt worden om een computer binnen te komen, noemt men exploits. Deze heten zo omdat ze vaak gebruik maken van een beveiligingsgat, die ze dus exploiteren. Er zijn sites waarop gevonden exploits te vinden zijn. Toch is hacken niet makkelijk. Om de exploits te begrijpen is een aardige kennis over computers nodig. En echte hackers gebruiken niet alleen exploits van anderen maar ontdekken zelf ook regelmatig nieuwe exploits.

De bekendste categorie van exploits is de buffer overflow. Om deze techniek te begrijpen moet we eerst weten wat een buffer is. Een buffer is een stukje geheugen op de computer dat wordt gebruikt voor tijdelijke opslag. Als je bijvoorbeeld een document afdrukt voordat je de printer hebt aangezet, worden de gegevens in de printbuffer gezet totdat de printer klaar is. Deze stukjes geheugen kun je zien als bakjes, met allemaal een nummer.

Als een hacker constant informatie naar een computer blijft sturen dan is het mogelijk dat de buffer overstroomt. Dit kun je vergelijken met het bakje dat overstroomt als je er teveel water in laat lopen. Het programma krijgt meer gegevens te verwerken dan het eigenlijk aan kan. Een goed geschreven programma veroorzaakt bij een buffer overflow een foutmelding of een crash. Sommige programma's voeren de commando's die buiten de buffer vallen toch uit. Van dit soort programma's maakt een hacker gebruik. De hacker laat de buffer overstromen en dwingt de computer om op het eind het door de hacker geschreven programma uit te voeren. Op deze manier kan een hacker de andere computer binnenkomen.

7.7 Voorbeeld

Stel we schrijven een webserver die van een browser (bijvoorbeeld Firefox, of Internet Explorer) een aanvraag krijgt voor een bepaalde webpagina. Bijvoorbeeld http://www.e-klassen.nl/. Laten we er vanuit gaan dat er ergens een stukje van het programma bestaat die de URL kopieert in een buffer waarin 20 tekens kunnen.

Belangrijk om te weten is dat functies, stukjes van een programma ook een bakje in het geheugen hebben, net als buffers. Zo'n functie verwijst dan weer terug naar het volgende deel van het programma. Deze verwijzing staat opgeslagen na de buffer. Het stukje geheugen waar de buffer staat ziet er dan zo uit:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
Buffer																				**Verwijzing**
																				-->

Nu gaan we met de functie de URL in de buffer plaatsen. Als deze URL bijvoorbeeld 'http://www.google.nl/' is,dan komt de 'h' in geheugencel 1, de 't' in 2, de volgende t in 3, de 'p' in 4, enz. Het geheugen ziet er dan zo uit:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
Buffer																				**Verwijzing**
h	t	t	p	:	/	/	w	w	w	.	g	o	o	g	l	e	.	n	l	-->

Maar wat nu als de URL langer is dan wat in deze 20 geheugencellen past? Stel je bijvoorbeeld voor dat hij een lengte heeft van precies 21 geheugencellen, zoals http://www.google.com. Een slordig geschreven programma controleert daar niet op met als gevolg dat er 21 geheugencellen worden

geschreven. Met andere woorden: het returnadres wordt overschreven, kijk maar:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
Buffer																				**Verwijzing**
h	t	t	p	:	/	/	w	w	w	.	g	o	o	g	l	e	.	c	o	m

Door een handige URL te maken kun je nu het programma laten doen wat je maar wilt! Stel dat je aan het eind van je URL bijvoorbeeld het adres van het begin van de buffer invult (in de vorm die computers begrijpen, d.w.z., nullen en enen). Dat betekent dat wanneer het programma de verwijzing uitvoert, niet wordt teruggesprongen naar het programma, maar naar de instructie die in bakje 1 staat. En laat dat nu net het begin van de buffer zijn die door de aanvaller wordt ingevuld. Dat betekent dus dat een aanvaller zijn eigen instructies kan laten uitvoeren. Deze instructies noem je de *payload* ofwel de lading van een exploit. Je kunt als aanvaller nu alles doen wat mogelijk is: de harde schijf formatteren, botsoftware downloaden en installeren, etc.

Het klinkt ongelooflijk, maar deze onzettend domme programmeerfout is schuld aan een enorme hoeveelheid wormen en virussen. Natuurlijk is het iets ingewikkelder met echte programmeertalen, maar verder is alles precies zoals hierboven is beschreven.

Opdracht

Maak nu de eindopdracht "What the hack?". Download hiervoor het volgende Word document:

Opdracht What the hack
kn.nu/ww.88336f9 (doc, maken.wikiwijs.nl)

In deze opdracht ga je zelf aan de slag als hacker. Dit doe je natuurlijk niet in een echt netwerk op echte computers, maar in een gesimuleerde omgeving.

Om te starten met de opdracht moet er een netwerk worden gesimuleerd met virtuele computers die kunnen worden aangevallen. Hiervoor gebruik je een programma dat op een bootable usb-stick staat die je docent in bezit heeft. Vraag je docent om verdere instructies.

D-toets

Eindopdracht

Over deze module

Over dit lesmateriaal

Colofon

Auteur	Its Academy
Laatst gewijzigd	17 september 2013 om 13:20
Licentie	Dit lesmateriaal is gepubliceerd onder de Creative Commons Naamsvermelding-GelijkDelen 3.0 Nederland licentie. Dit houdt in dat je onder de voorwaarde van naamsvermelding en publicatie onder dezelfde licentie vrij bent om: • het werk te delen - te kopiëren, te verspreiden en door te geven via elk medium of bestandsformaat • het werk te bewerken - te remixen, te veranderen en afgeleide werken te maken • voor alle doeleinden, inclusief commerciële doeleinden. Meer informatie over de CC Naamsvermelding-GelijkDelen 3.0 Nederland licentie

Aanvullende informatie over dit lesmateriaal

Van dit lesmateriaal is de volgende aanvullende informatie beschikbaar:

Leerniveau	; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;
Leerinhoud en doelen	; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;
Eindgebruiker	leerling/student
Moeilijkheidsgraad	gemiddeld
Studiebelasting	40 uur en 0 minuten
Trefwoorden	e-klassen rearrangeerbaar

Gebruikte Wikiwijs Arrangementen

Academy, Its. (z.d.). *1 Index*. https://maken.wikiwijs.nl/45979/1_Index

Academy, Its. (2013). *2 Inleiding*. https://maken.wikiwijs.nl/45971/2_Inleiding

Academy, Its. (2013). *3 1 Virussen*. https://maken.wikiwijs.nl/45972/3_1_Virussen

Academy, Its. (2013). *4 2 Virusbestrijding*. https://maken.wikiwijs.nl/45973/4_2_Virusbestrijding

Academy, Its. (2013). *5 3 Ongewenste e-mail*. https://maken.wikiwijs.nl/45974/5_3_Ongewenste_e_mail

Academy, Its. (2013). *6 4 Cryptografie*. https://maken.wikiwijs.nl/45975/6_4_Cryptografie

Academy, Its. (2013). *7 5 RFID*. https://maken.wikiwijs.nl/45976/7_5_RFID

Academy, Its. (2013). *8 6 De wet*. https://maken.wikiwijs.nl/45977/8_6_De_wet

Academy, Its. (2013). *9 7 Hacken*. https://maken.wikiwijs.nl/45978/9_7_Hacken

Academy, Its. (z.d.). *Basis e-klassen - verzamel*. https://maken.wikiwijs.nl/44455/Basis_e_klassen

___verzamel