Les D-06 Veilig internetten

Internet is niet meer weg te denken uit ons dagelijks leven. Er wordt heel wat informatie over het net verspreid, waaronder ook informatie die voor andere partijen interessant kan zijn. Er zijn dan ook veel kapers op de internetkust. Zo is het voor commerciële instellingen belangrijk om te weten wat een computergebruiker interesseert, zodat deze "op maat" advertenties voorgeschoteld kan krijgen. Om deze informatie te verzamelen verspreiden de instellingen tracing cookies. Criminelen zijn erg geïnteresseerd in bijvoorbeeld creditcardgegevens, zodat zij met die gegevens aankopen kunnen doen. Om deze informatie te verzamelen sturen zij spoofing mails. De opkomst van internet heeft dan ook wetgeving nodig gemaakt die aangeeft wat wel en niet mag bij internetverkeer.

Het is belangrijk om je als internetgebruiker bewust te zijn van mogelijke gevaren. In deze lesbrief wordt uitgelegd welke gevaren er zoal zijn en hoe je je computer tegen deze gevaren kunt beschermen.

6.1 Phishing en spoofing

Phishing is een vorm van internetfraude waarbij wordt geprobeerd persoonlijke informatie te verkrijgen, om daar vervolgens misbruik van te maken. Phishing vindt veelal plaats door het versturen van emails of het verwijzen naar websites die erg lijken op betrouwbare websites. Doordat de indruk wordt gewekt dat het om iets bekends en vertrouwds gaat, bent u er mogelijk van overtuigd om de gevraagde informatie in te vullen of toe te sturen. Deze informatie wordt dan door criminelen gebruikt om toegang te krijgen tot bijvoorbeeld een creditcard, bankrekening of mailbox. Phishing door het vervalsen van kenmerken (net doen of het om een betrouwbare mail of website) gaat wordt ook wel **spoofing** genoemd.
Misbruik van gegevens is buitengewoon vervelend. Het kan immers gebeuren dat je bankrekening wordt geplunderd of dat er een flink bedrag van je creditcard wordt gehaald.

Wat kan je tegen phishing doen? Reageer nooit op verzoeken per mail, op een website of via de telefoon waarin men naar jouw persoonlijke gegevens vraagt (bijvoorbeeld gebruikersnaam en wachtwoord van je email). Verder is het verstandig om een virusscanner en firewall op je computer te installeren en deze up-to-date te houden.

6.2 Spam

Spam is een verzamelnaam voor ongewenste digitale berichten via email, instant-messaging, websites of pop-ups. Het zijn berichten die ongevraagd worden verstuurd aan een grote groep geadresseerden.

Wat kan je tegen spam doen? Je kunt een **spamfilter** op je mailbox zetten. Ook is er software beschikbaar die e-mail en websites scant op spam. Meestal zit deze software ook in antivirusprogramma's.

6.3 Ongewenste websites

Op internet kun je veel nuttige en bruikbare informatie vinden. Soms kunt je echter geconfronteerd worden met zaken die je liever niet gezien had: pornografisch, racistisch en ander schokkend materiaal. Ook heb je vast wel eens last gehad van ongewenste pop-up schermen tijdens het surfen.

Wat kan je tegen ongewenste websites doen? Allereerst moet je niet te klikken op alles wat beweegt en er aantrekkelijk uit ziet of verdachte links in e-mailtjes. Je kunt ook een browser gebruiken die niet alle sites toestaan, in je firewall bepaalde websites blokkeren of een **contentfilter** gebruiken.

6.4 Malware

Malware is een verzamelnaam voor kwaadaardige en/of schadelijke software. Het woord is een samenvoeging van het Engelse malicious software (kwaadwillende software). Kwaadwillenden maken gebruik van onvolkomenheden (bugs) in software en het surf en downloadgedrag van gebruikers.

Hieronder staan voorbeelden van malware:

Adware - infecteert de computer met reclamesoftware, en zorgt doorgaans voor pop-ups.
Bootsectorvirus - infecteert de bootsector op een harde schijf of diskette.
Backdoor - is in een programma geplaatst om toegang tot een systeem of programma te krijgen.
Computervirus - infecteert bestanden en richt vaak schade aan.
Computerworm - verspreidt zich direct over het netwerk en richt vaak schade aan.
Dialer - verbindt een modem met een duur telefoonnummer.
IRC-bot - verbindt de geïnfecteerde computer met een netwerk van waaruit de computer bestuurd kan worden.
Keylogger - kan de toetsaanslagen of de muisbewegingen en wat er op het scherm getoond wordt van een computergebruiker registreren.
Rootkit - software om een cracker toegang te geven tot een computer.
Spyware - verzamelt gegevens van de gebruiker en geeft deze door aan derden.
Rogueware – misleidt de gebruiker om geld te betalen voor het verwijderen van bedreigingen en waarschuwingen die nep zijn.
Tracking cookie - verzamelt informatie over websurfers.
Trojaans paard - doet zich voor als iets anders dan het daadwerkelijk is en richt dan schade aan of functioneert als spyware.

Wat kan je tegen malware doen? Pas op met het downloaden van (gratis) programma's en bestanden. Je kunt zomaar malware mee downloaden. Installeer antivirussoftware en/of firewall software. Deze software is in staat om malware te herkennen en ongedaan te maken. Gebruik bijvoorbeeld een USB-stick voor het downloaden van MP3-tjes, zodat je systeem niet wordt besmet.

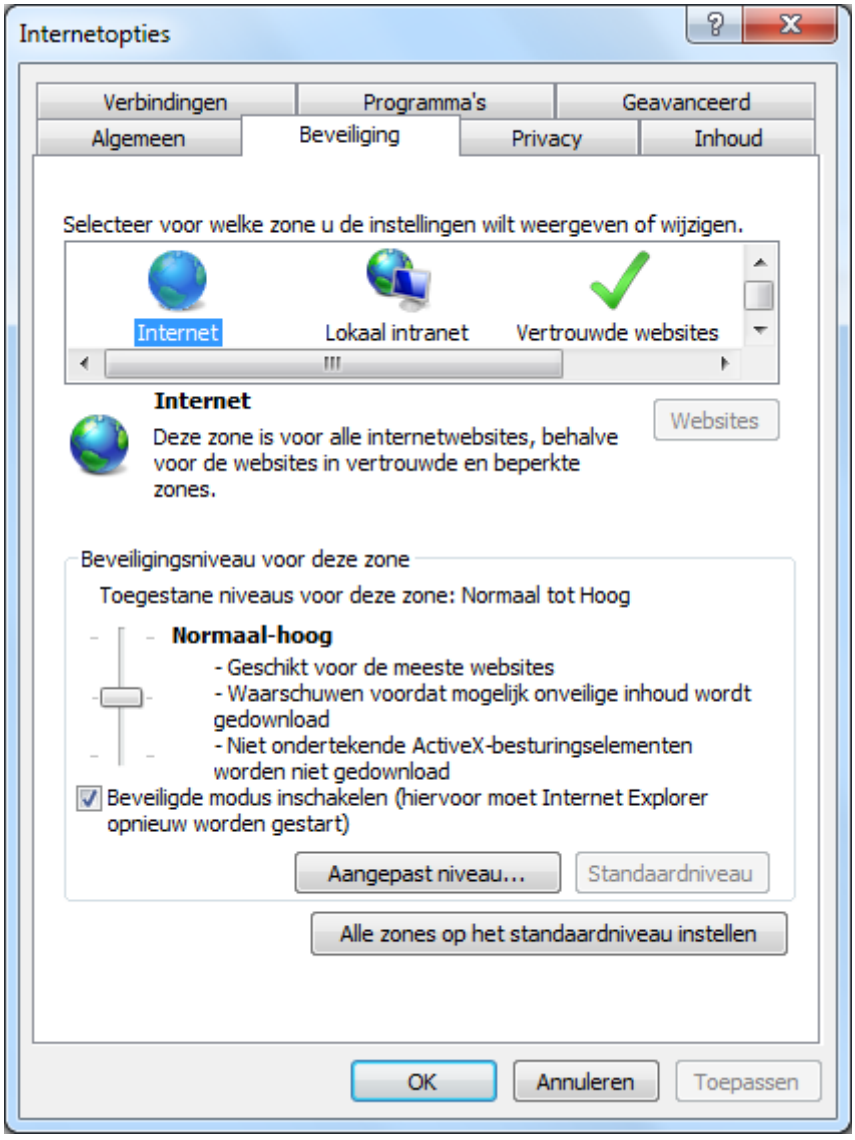
6.5 Hacking en cracking

Onder **hacking** verstaan we het vinden van toepassingen die niet door de maker bedoeld zijn. Een vorm van hacking is **cracking**. Onder cracking verstaan we het wederrechtelijk toegang verschaffen tot (al dan niet beveiligde) computersystemen. Toch spreekt iedereen over hacking daar waar cracking bedoeld wordt.

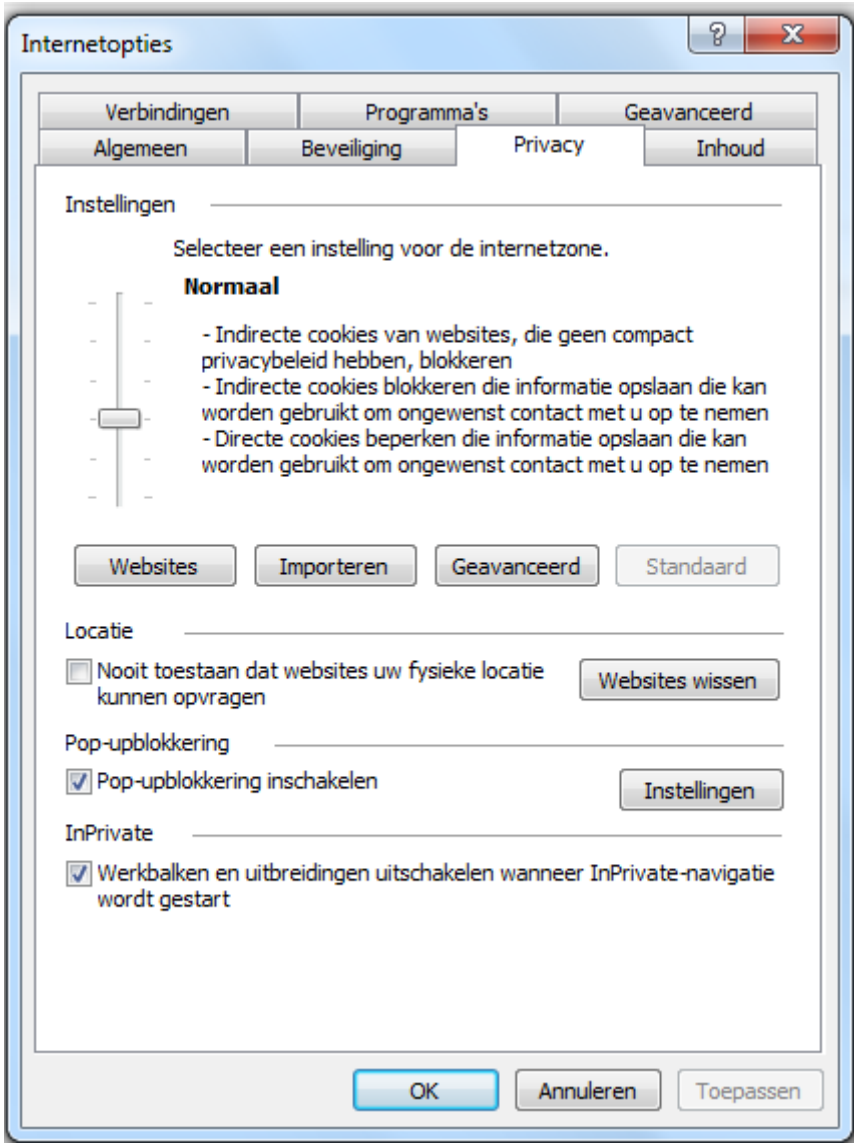
Bij hacking kan op technische of sociale wijze de beveiliging van een systeem worden gekraakt, dat wil zeggen er kan via de poorten van het netwerk of via de gebruikers van het netwerk worden ingebroken.

6.6 Beveiliging via de browser.

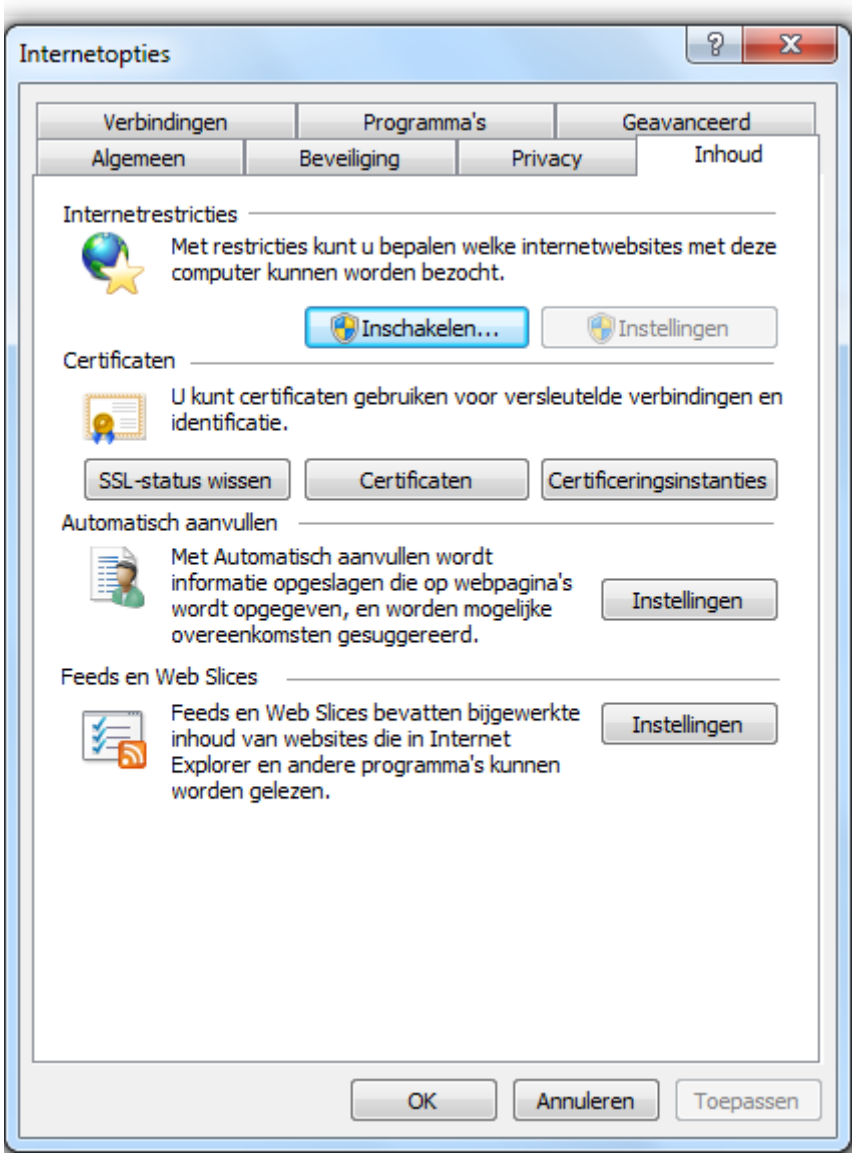
Een eerste mogelijkheid om je te beveiligen tegen gevaren van buitenaf is beveiligen via de browser. Bij Internet Explorer vind je mogelijkheden voor Beveiliging, Privacy en Inhoud onder “Extra” / “Internetopties”. Op het tabblad “Beveiliging” kan je het beveiligingsniveau instellen, dat wil zeggen dat je de mate van controle op onveilige sites door Internet Explorer instelt.



Op het tabblad “Privacy” stel je het privacy niveau instellen, dat wil zeggen aangeven in hoeverre cookies jouw surfgedrag kunnen volgen.



Op het tabblad “Inhoud” kan je restricties instellen, aangeven welke sites wel en niet mogen worden bezocht.



6.7 Beveiliging via antivirussoftware

Met behulp van antivirusprogramma’s kunnen computervirussen en andere malware worden herkend, tegengehouden en verwijderd. Antivirusprogramma’s bekijken bestandscode en het gedrag van programma’s. Als verdachte code of gedrag wordt herkend kan de virusscanner:

- de verdachte code uit het bestand verwijderen
- het bestand/programma in quarantaine plaatsen
- het geïnfecteerde bestand/programma verwijderen

Bekende antivirusprogramma’s zijn AVG, McAfee en Norton.

6.8 Beveiliging via een firewall

Een firewall is een systeem dat een enkele computer (personal firewall) of een compleet netwerk (network firewall) beschermt tegen aanvallen van buitenaf.

Er worden vier typen firewalls onderscheiden:

Stateless firewall
Een stateless firewall bekijkt elk pakketje op zichzelf en slaat geen informatie op van de connecties die over de firewall lopen.

Stateful firewall
Een stateful firewall houdt wel tussentijdse informatie bij van connecties die over de firewall lopen. Hierdoor is de firewall makkelijker in staat onderscheid te maken tussen pakketjes die wel toegestaan en niet toegestaan mogen worden.

Als je bijvoorbeeld bestanden download (volgens het FTP-protocol) zijn soms verbindingen op willekeurige poorten nodig. Een stateless firewall zal dan verkeer op alle poorten toestaan, terwijl een stateful firewall kan volstaan met het tijdelijk openen van één enkele poort waarover de FTP-sessie plaatsvindt. Stateless firewalls komen dan ook weinig voor.

Packet filtering firewall
Een packet filtering firewall bekijkt datapakketjes op het niveau van de netwerklaag. Het IP-adres waar het pakket vandaan komt bepaalt of het pakket wordt doorgelaten of niet. De producent van de firewall en de netwerkbeheerder kunnen instellen welke IP-adressen worden doorgelaten en welke niet.

Een packet filtering firewall wordt bijvoorbeeld gebruikt bij het inloggen op een bedrijfsnetwerk via de telnetpoort. Alleen bekende IP-adressen kunnen inloggen.

Application layer firewall
Een application layer firewall bekijkt datapakketjes op het niveau van de applicatielaag. De inhoud van de pakketjes (bestanden en programma's) wordt bekeken. Deze firewall moet over meer informatie beschikken dan een packet filtering firewall.

Een application layer firewall wordt bijvoorbeeld gebruikt bij het gebruik van een mailserver (om spam te herkennen) of proxyserver (om ongewenst internetgedrag, virussen enz te herkennen).

6.9 Een draadloos netwerk beveiligen.

In les D-01 is uitgelegd hoe je een draadloos netwerk met SSID en WEP\WPA encryptie kunt beveiligen.

6.10 Wet Computercriminaliteit

Ook door de wet wordt de computergebruiker beschermd tegen computercriminaliteit. Sinds 1993 is er een **Wet Computercriminaliteit**. Regelmatig vinden er in deze wet aanpassingen plaats ten gevolge van het ontstaan van nieuwe technologieën.

6.11 Samenvatting

Als computergebruiker ben je blootgesteld aan gevaren van buitenaf:

- **phishing / spoofing**

- **spam**

- **ongewenste websites**

- **malware** (oa. adware, dialer, keylogger, virus, worm, spyware, cookies, trojan horse)

- **hacking / cracking**

Op verschillende manieren kan je je computer/netwerk tegen deze gevaren beschermen:

- **browser**

- **antivirussoftware**

- **firewall** (we onderscheiden: **stateless, stateful, packet filtering, application layer**)

Een draadloos netwerk kan je met **SSID** en **WEP\WPA** encryptie beveiligen.

Ook de **Wet Computercriminaliteit** beschermt de computergebruiker tegen computercriminaliteit.