Secure Computing

04 - 2014

W.Bosgra taakaccenthouder Digitale Criminaliteit

Downloadverbod

Open wifi gevaarlijk

Het rapport:
CYBER SECURITY PERSPECTIVES 2013

Zo bescherm je bestanden tegen onbevoegden (special)

Einde XP: stap over op Linux (special)

Besluit u Linux een kans te geven middels de handleiding in dit magazine, dan doet u dit op eigen verantwoordelijkheid !

Wat betekent het downloadverbod?

Nederland heeft per direct een downloadverbod, zo maakte het kabinet donderdagmiddag bekend. Hoe kan het kabinet dat zomaar besluiten? En wat betekent dit voor downloaders van films, muziek en e-books? Een aantal vragen en antwoorden op een rij.

Het Europese Hof heeft geoordeeld dat Nederland het downloaden van materiaal uit 'illegale bron' niet mag toestaan. Nederland beschouwde het kopiëren van een cd of dvd hetzelfde als het downloaden van een film van een torrentsite, maar volgens het Europese Hof is er wel degelijk een verschil.

Wat verandert er precies?

Het was in Nederland altijd toegestaan om voor eigen gebruik audiovisueel materiaal te downloaden uit 'illegale bronnen'. Dat mag nu niet meer. Een auteursrechtelijk beschermd werk komt uit illegale bron als het zonder toestemming van de auteursrechthebbende is verspreid, bijvoorbeeld via een torrentsite of nieuwsgroepen. Voor het downloaden van software verandert er niks; uit illegale bron mocht dat al niet. Hetzelfde geldt voor uploaden.

Krijgen we nu Amerikaanse toestanden, met downloaders die worden veroordeeld tot hoge schadevergoedingen?

De vraag is wat er voor Nederlandse downloaders verandert. Het Openbaar Ministerie gaat downloaders in ieder geval niet vervolgen; dat gebeurt alleen bij commerciële auteursrechtinbreuken. Het is aan organisaties als Stichting Brein om downloaders aan te pakken en Brein heeft al aangegeven dat ze dat niet zal doen. In plaats daarvan richt Brein zich op sites die illegaal materiaal aanbieden.

Desondanks kan een boze auteursrechthebbende je wel aanklagen als je zijn e-book, serie, film of album illegaal downloadt. Amerikaanse toestanden zullen we echter niet krijgen. Amerikaanse rechters leggen soms punitive damages op: schadevergoedingen die ook een afschrikwekkende werking hebben en niet alleen bedoeld zijn om de schade te vergoeden. Nederland kent die niet. Downloaders hebben dus waarschijnlijk niet veel te vrezen.

Hoe kan het downloadverbod per direct in werking treden?

Het kabinet heeft bekendgemaakt dat het downloadverbod per direct werkt. Dat is geen beslissing van het kabinet zelf, het komt door de uitspraak van het Europese Hof, dat heeft besloten dat bestaande wetgeving anders moet worden uitgelegd. Tot nu toe oordeelden het kabinet en rechtbanken altijd dat op basis van de Nederlandse auteurswet 'illegaal downloaden' is toegestaan.

Het Europese Hof oordeelt anders. Uitspraken van het Europese Hof zijn bindend en gaan bovendien boven die van nationale rechtbanken, zodat in de toekomst alle rechters ervan uitgaan dat Nederland een downloadverbod heeft. Er is dus niet zozeer een downloadverbod ingevoerd, het is meer dat het Europese Hof heeft bepaald dat er een downloadverbod ís.

Waarom bemoeit het Europese Hof zich met onze downloadwetgeving?

De Nederlandse auteurswet is gebaseerd op Europese wetgeving, waaraan Nederland heeft meegewerkt. Het Europese Hof bestaat onder meer om ervoor te zorgen dat Europese wetgeving in verschillende lidstaten op dezelfde manier wordt uitgelegd. Anders zou het ook weinig zin hebben om überhaupt Europese wetgeving in te voeren.

In dit geval boog het Europese Hof zich over downloaden in een rechtszaak die onder meer door Sony en Philips werd aangespannen. Zij waren het niet eens met de hoogte van de thuiskopieheffing. Voor de hoogte van de thuiskopieheffing is het downloadverbod van belang.

Wat hebben de thuiskopieheffing en het downloadverbod met elkaar te maken?

Nederland zag het downloaden van materiaal uit illegale bron als een thuiskopie. De thuiskopie is bedoeld voor het maken van - de naam suggereert het al - auteursrechtelijk beschermde werken voor eigen gebruik. De thuiskopieheffing is bedoeld om de inkomsten die auteursrechthebbenden door de thuiskopie mislopen, te compenseren. Het Europese Hof oordeelde echter dat downloaden helemaal geen thuiskopie is.

Dat betekent ook dat de thuiskopieheffing waarschijnlijk omlaag gaat. Daarvoor hoeft geen wet te worden gewijzigd. Deze zomer wordt duidelijk hoe hoog de nieuwe thuiskopieheffingen zullen zijn.

Kan de thuiskopieheffing niet gewoon worden verhoogd om downloaden toch toe te staan?

Nee, het Europese Hof vindt dat niet eerlijk voor mensen die niet downloaden. De hoogte van de thuiskopieheffing zou dan omhoog moeten, wat 'aanzienlijke extra kosten' zou betekenen, ook voor mensen die braaf betalen.

Europol en NCTV geven wifiwaarschuwing

Het versturen van gevoelige informatie via wifinetwerken in cafés of andere openbare plekken is zeer onverstandig. Die waarschuwing gaf Europol en de Nationaal Coördinator Terreurbestrijding en Veiligheid (NCTV) onlangs in het televisieprogramma Brandpunt. Het advies is gebruik te maken van een beveiligd en betrouwbaar netwerk.

Nationaal Coördinator
Terrorismebestrijding en Veiligheid
Ministerie van Veiligheid en Justitie

Veel mensen weten niet dat cybercriminelen allerlei inlogcodes en wachtwoorden kunnen buitmaken als ze internetten via een publiek wifinetwerk, al dan niet in de horeca. Beide organisaties signaleren dat de software waarmee dergelijke aanvallen worden uitgevoerd steeds professioneler wordt en spreken van 'een nieuwe industrie'.

l"Als je niet het risico wilt lopen dat jouw persoonlijke en financiële gegevens opgevangen en misbruikt worden, zorg er dan voor dat je thuis in een veilige omgeving internetbankiert of je e-mail ophaalt", zegt directeur cybercrime van Europol Jaap van Oss in het programma.

Identiteitsfraude

Ook identiteitsfraude is een risico, volgens de NCTV een groot gevaar. "Het is natuurlijk een bron voor criminelen om op deze wijze aan belangrijke gegevens te komen. Dat kunnen financiële gegevens zijn of gegevens die daarna gebruikt kunnen worden om in jouw naam transacties te doen of je identiteit te gebruiken", aldus directeur cybersecurity Wil van Gemert.

Nephotspot

Om een wifinetwerk aan te vallen creëren hackers een nephotspot die ongemerkt al het internetverkeer naar zich toetrekt. Bezoekers verkeren in de veronderstelling dat ze verbonden zijn met de hotspot van de horecagelegenheid, maar ondertussen zijn hun inlognamen en wachtwoorden eenvoudig te onderscheppen.

Ook de landelijke wifinetwerken van Ziggo, UPC en KPN zijn kwetsbaar, zegt Jaap van Oss van Europol. "Een provider kan proberen om zijn service zo veilig mogelijk te maken. Maar het blijft een open wifinetwerk en daar zijn risico's aan verbonden. Zo'n nephotspot is daar een van. Ik denk dat het minder makkelijk gaat maar ik denk dat het wel kan."

Bekijk hier de Brandpuntuitzending

‘CYBER SECURITY PERSPECTIVES 2013’: JAARLIJKS SECURITY REPORT DOOR KPN NL, THTC, TNO, NCSC

Recentelijk verscheen de eerste uitgave van een nieuw rapport over veiligheid in Nederland: ‘Cyber Security Perspectives 2013’. Vier partijen, die nauw samenwerken in het bestrijden van Cybercrime in Nederland, hebben bijgedragen aan dit rapport. Ieder geheel vanuit zijn eigen discipline en perspectief.

Het rapport neemt de lezer mee in de fascinerende wereld van cybersecurity vanuit een andere invalshoek. In plaats van het tonen van grafieken en cijfers, worden cyberaanvallen beschreven vanuit het perspectief van een betrokken partij: als slachtoffer of als bestrijder. Wat is er gebeurd? Welk effect heeft dit? Wat kunnen wij er in de samenleving aan doen?

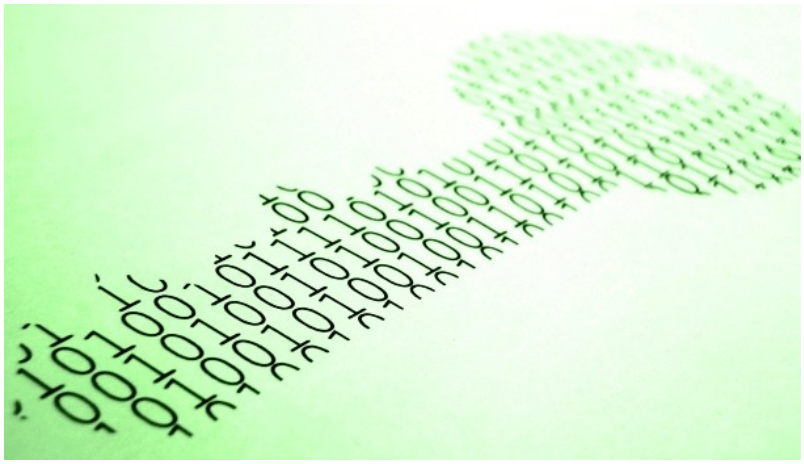
Het rapport geeft een overzicht van belangrijke cyberaanvallen die hebben plaatsgevonden in 2013 in Nederland. De grote diversiteit aan onderwerpen laat zien dat het voor cybercriminelen een druk jaar is geweest. Helaas moeten we ook constateren dat cyberaanvallen inmiddels onderdeel zijn geworden van het dagelijkse leven. De beste verdediging hiertegen is om te weten wat er mogelijk is en je eigen maatregelen te nemen. Er wordt in het rapport ook vooruit gekeken naar trends in 2014 met een grote impact op de gemeenschap, zowel in Nederland als wereldwijd.

De impact van cyberaanvallen wordt steeds groter en daarom hebben de vier partijen besloten om dit rapport jaarlijks te gaan uitgeven. Hiermee hopen zij de samenleving handvatten te bieden voor de bestrijding van cybercriminaliteit.

Trend #1: mainstream cyberattack increasingly become available to the masses

Trend #2: targeted and sophisticated attacks occur closer to home

Zo bescherm je bestanden tegen onbevoegden



Dankzij smartphones en laptops is het makkelijker dan ooit om altijd toegang te hebben tot je bestanden. Maar ben je de enige die altijd toegang heeft tot je bestanden of hebben veel meer mensen dat? Hoe beveilig je bestanden en schijven tegen ongeoorloofde toegang?

Tip 01: Authenticatie

De combinatie van een gebruikersnaam en wachtwoord zijn de bekendste manieren om bestanden te beveiligen. Helemaal correct is dat echter niet, gebruikersnaam en wachtwoord zijn geen methode voor beveiliging, maar voor authenticatie.

De combinatie van gebruikersnaam en wachtwoord kan wel enige zekerheid geven dat iemand ook echt de persoon is die hij zegt te zijn, maar het helpt op zichzelf niet de toegang tot een bestand te voorkomen. Daarvoor is een beveiligingstechniek nodig. Een bekende beveiligingstechniek is encryptie of versleuteling.

Daarvoor heb je in principe geen gebruikersnaam nodig, maar alleen een wachtwoord. Authenticatie en beveiliging zijn dus erg nauw met elkaar verbonden, maar het zijn toch verschillende onderdelen van dezelfde opdracht: gegevens beveiligen.

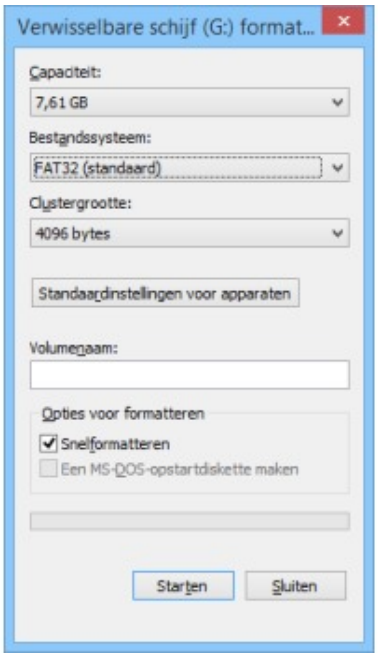
Tip 01 Een wachtwoord is een vorm om vast te stellen dat iemand de persoon is die hij zegt te zijn.

Tip 02: Beveiliging

Een tweede belangrijk punt voordat je begint met het beveiligen van je bestanden, is dat elke beveiligingsmaatregel voorwaarden stelt om succesvol te zijn. En die voorwaarden zijn vaak afhankelijk van de plek waar je de maatregel toepast.

Wil je echt niet dat iemand anders bij je bestanden kan, dan is de cloud niet de goede plek. Want in de cloud kan uiteindelijk altijd de beheerder van de server bij de bestanden. Een NAS in je thuisnetwerk is dan een betere plek, want daarvan ben je zelf de beheerder. En wil je je bestanden niet versleutelen maar alleen afschermen met een gebruikersnaam en wachtwoord, gebruik dan een bestandssysteem dat dit ook echt kan. Het FAT32-bestandssysteem dat Windows nog standaard gebruikt bij kleinere schijven en usb-sticks, kan dat bijvoorbeeld niet.

Het NTFS-bestandssysteem weer wel. Kies bij het formatteren daarom altijd voor Bestandssysteem / NTFS tenzij beveiliging niet nodig is of je de stick gaat gebruiken in combinatie met een pc met een oude versie van Windows, zoals Windows 95 of 98.



Tip 02 Het FAT32-bestandssysteem is niet ontworpen voor beveiliging en dus ongeschikt voor het afschermen van bestanden.

Tip 03: Gebruikersaccount

Beschermen van bestanden op de pc begint bij het maken van verschillende accounts voor de verschillende gebruikers van de pc. Ben je de enige gebruiker? Ook dan is het aan te raden één echt gebruikersaccount voor jezelf te maken en te voorzien van een wachtwoord.

Bij oudere versies van Windows is er bovendien ook nog een Administrator-of Beheerderaccount dat met een wachtwoord moet worden beveiligd. In alle gevallen dient het wachtwoord ervoor dat alleen jij kunt inloggen op de pc en het besturingssysteem dan ook weet dat je inlogt. Ga naar het Configuratiescherm, kies Gebruikersaccounts en Ouderlijk toezicht. Klik op Uw Windows-wachtwoord wijzigen wanneer je nog geen wachtwoord hebt of anderen je wachtwoord kennen. Klik dan op Een wachtwoord voor uw account instellen en typ het nieuwe wachtwoord inclusief de bevestiging.

Je kunt een geheugensteun opgeven voor als je het wachtwoord een keer niet direct herinnert. Bevestig met Wachtwoord instellen.

Tip 03 Pas met een wachtwoord is een gebruikersaccount ook echt een account voor één gebruiker.

Tip 04: Andere gebruikers

Deel je de pc met anderen, maak dan voor elke gebruiker een eigen account aan met een eigen wachtwoord. Open het onderdeel Gebruikersaccounts en Ouderlijk toezicht in het Configuratiescherm. Klik op Gebruikersaccounts toevoegen of verwijderen. Klik dan op Een nieuw account maken en geef het account een naam en kies voor Standaardgebruiker. Klik dan op Account maken.

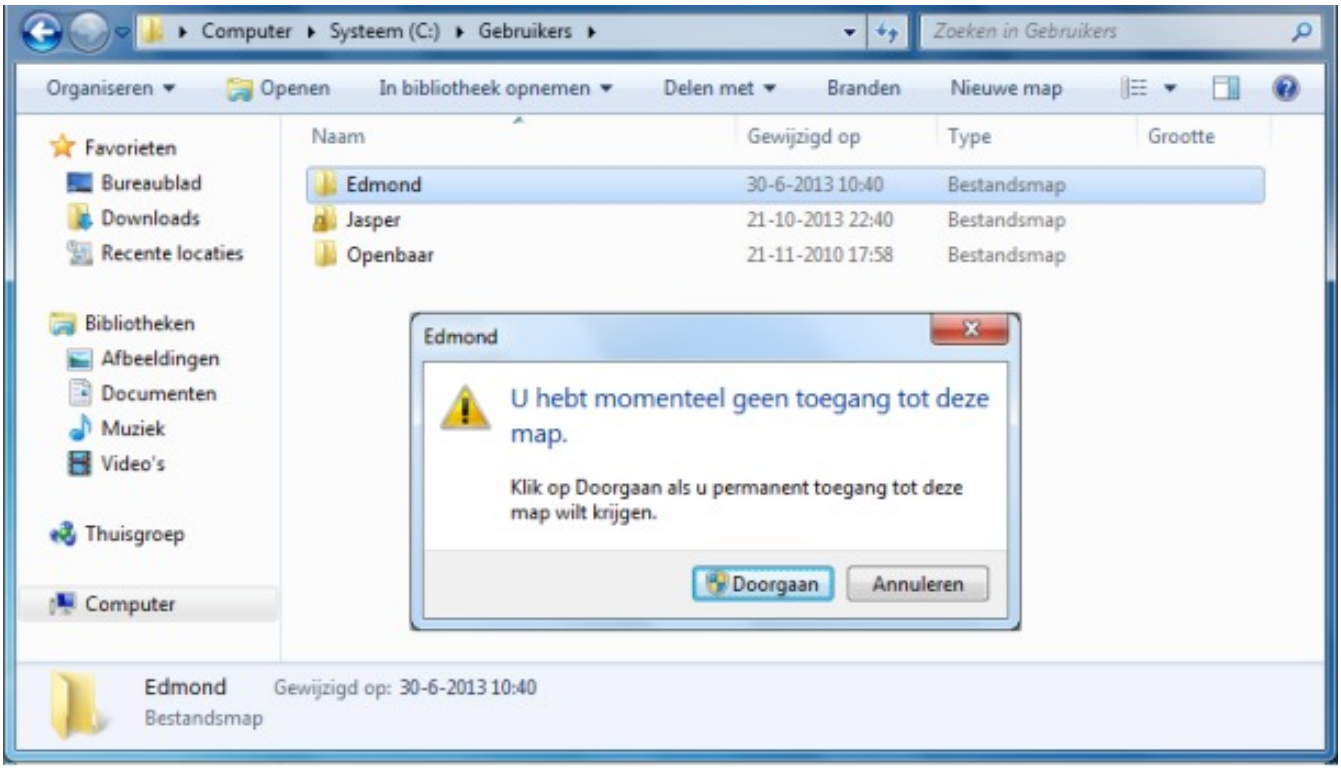
Klik daarna op het account in het scherm waar alle accounts staan weergegeven en kies voor Een wachtwoord instellen. Typ dan het wachtwoord, de herhaling en de geheugensteun. Dit laatste kun je ook aan de gebruiker zelf overlaten als hij de volgende keer de pc gaat gebruiken. Hij kan je account dan niet meer gebruiken, maar logt in met zijn eigen account en kan van daaruit een wachtwoord instellen.

Tip 04 Geef elke gebruiker een eigen wachtwoord.

Tip 05: De juiste mappen

Door je bestanden binnen Windows in de juiste mappen te bewaren, worden ze automatisch afgeschermd voor andere gebruikers in hetzelfde netwerk en van dezelfde pc. De veilige mappen zijn alle mappen die je ziet in de Windows Verkenner binnen de map met je Windows-gebruikersnaam. Dat zijn de mappen Documenten, Afbeeldingen, Downloads, Favorieten enzovoort.

Alle andere mappen zijn niet afgeschermd voor andere gebruikers. Heb je meerdere schijven in de computer of is de harde schijf opgedeeld in meerdere partities, dan zijn die extra locaties waar je bestanden kunt bewaren dus niet standaard afgeschermd voor andere gebruikers. Ze zijn juist ideaal om bestanden te delen.

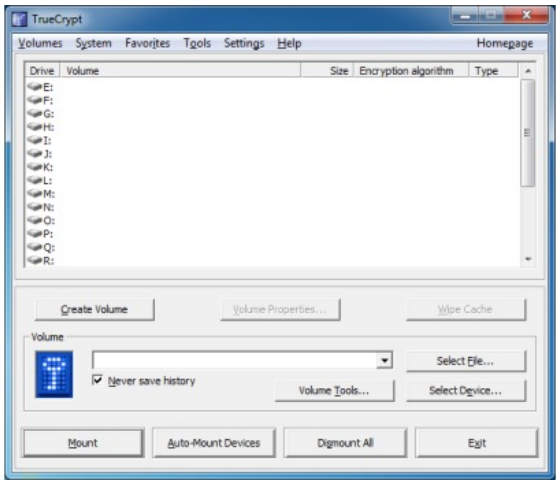


Tip 05 Andere gebruikers hebben geen toegang tot je standaardmappen.

Tip 06: Versleutelen

Wil je verder gaan dan bestanden afschermen, dan is versleuteling nodig. Krijgt iemand dan toch toegang tot de bestanden of tot een harde schijf, dan zijn de gegevens onleesbaar. Hét programma om hiervoor te gebruiken is TrueCrypt. Ga naar deze website en klik op Downloads. Klik op Download bij het besturingssysteem van je pc, dus Windows, Mac OS X of Linux.

Bewaar het bestand op de pc en start het om het te installeren. Tijdens de installatie kun je de standaardinstellingen laten staan. Met TrueCrypt maak je een groot bestand, liefst van vele gigabytes of zelfs terabytes groot. Dat bestand is onleesbaar zonder de sleutel (het wachtwoord) van de versleuteling. Heb je die sleutel, dan kun je met TrueCrypt het grote bestand (dit wordt een container genoemd) gebruiken alsof het een aparte harde schijf is. Je kunt er dus bestanden in opslaan. Ben je klaar, dan ontkoppel je de container en zijn alle bestanden in de container voor buitenstaanders volkomen onbruikbaar.



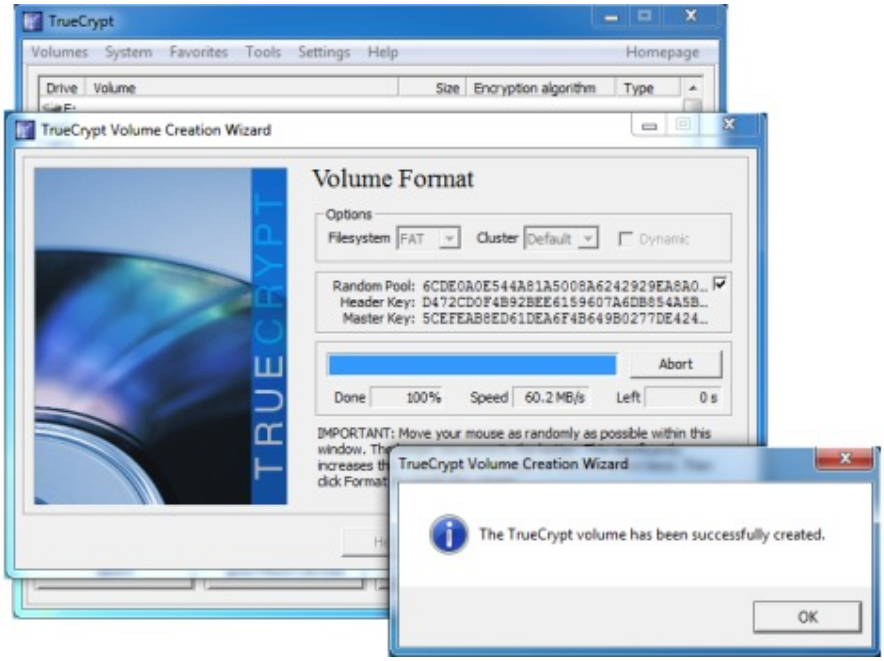
Tip 06 TrueCrypt ziet er behoorlijk lastig uit maar is na enige gewenning eenvoudig te gebruiken.

Tip 07: Container maken

Om bestanden in een onleesbare en dus superveilige versleutelde container te bewaren, maak je eerst die container. Klik in TrueCrypt op Create volume. Kies voor Create an encrypted file container en klik op Next. Vervolg met Standard TrueCrypt volume en klik dan op Select File.

Selecteer nu de map waar je het versleutelde bestand wil bewaren en typ in het vak Bestandsnaam de naam van de container. Bevestig via Opslaan. Klik twee keer op Next en geef dan de grootte van de container op, dit kan in KB, MB of GB, het liefste kies je een wat grotere container, zodat er meerdere bestanden in passen. Klik op Next. Nu moet je het wachtwoord voor de container opgeven. Typ het bij Password en nogmaals bij Confirm.

TrueCrypt wil graag dat je een sterk wachtwoord gebruikt dus met hoofdletters, leestekens en cijfers. Dit wachtwoord bewaar je dan weer in KeePass met erbij de naam van het bestand. Je kunt dan voor elke container een ander wachtwoord gebruiken. Klik dan op Next / Format om de container aan te maken. Het versleutelde gebied formatteren duurt langer naarmate de container groter is en kan bij enkele terabytes al snel een paar uur duren.



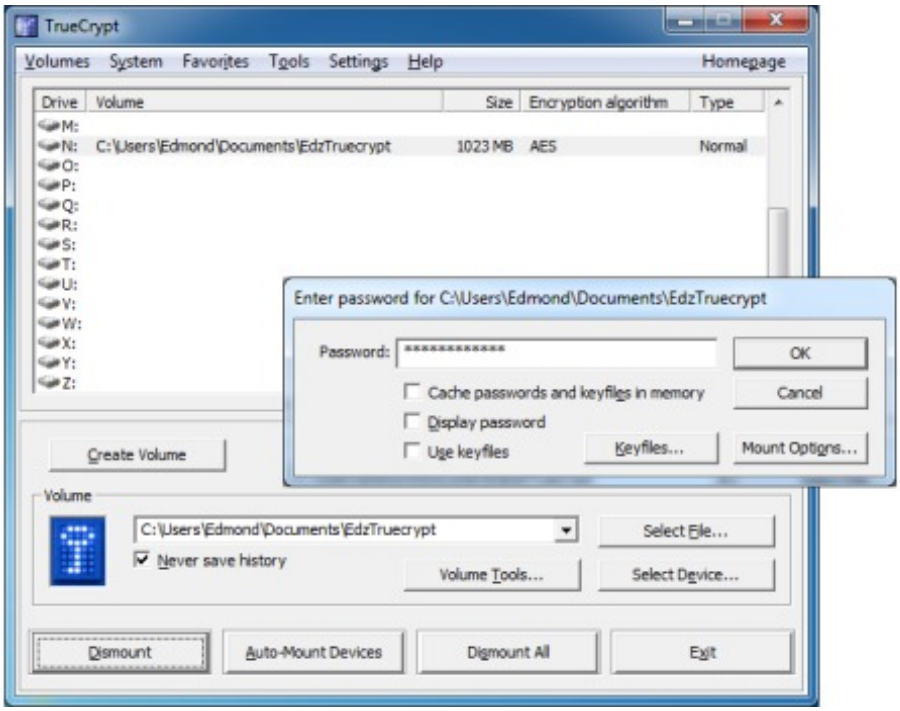
Tip 07 Maak in TrueCrypt een containerbestand aan waarin je je bestanden veilig kunt gaan opslaan.

Tip 08: Container gebruiken

Om een versleutelde container te gebruiken als veilige plek om je bestanden te bewaren, moet je die container mounten oftewel koppelen. Start TrueCrypt en kies Select File. Selecteer dan het versleutelde bestand en kies in de lijst met stationsletters, de letter waaronder je het versleutelde bestand wil gebruiken. Klik dan op Mount. Typ nu het wachtwoord in en klik op OK of druk op Enter.

Start dan Windows Verkenner en zie dat er een harde schijf is bijgekomen, met de stationsletter die je net geselecteerd hebt. Je kunt deze schijf gewoon openen in de verkenner en er bestanden in opslaan en bewerken. Je hoeft bestanden die je wil gebruiken dus niet eerst uit de container te kopiëren om ze te bewerken. Je kunt de bestanden die in de versleutelde container zitten, precies zo behandelen als andere bestanden die op een gewone harde schijf staan.

Mits je de hele tijd het station gemount laat. Ben je klaar met de bestanden, sluit dan de container veilig af via Dismount of Dismount All wanneer je meerdere containerbestanden gebruikt.



Tip 08 Koppel de TrueCrypt-container aan een stationsletter om de bestanden toegankelijk te maken.

Tip 09: Windows Firewall

De Windows Firewall controleert elke uitgaande en binnenkomende verbinding op de pc. Wanneer vanaf een andere computer in het netwerk of via het internet geprobeerd wordt toegang te krijgen tot de bestanden op de pc, dan ziet de firewall dat en zal dat in de standaard configuratie afwijzen.

Je hoeft met de Windows Firewall ingeschakeld dan ook niet bang te zijn dat anderen zomaar bij de bestanden op je pc kunnen. Controleer de werking van de Windows Firewall via Configuratiescherm / Windows Firewall / Status van firewall controleren. De firewall moet zijn ingeschakeld. Is dit niet het geval, klik dan op Windows Firewall in- of uitschakelen en kies voor Windows Firewall inschakelen zowel bij de Instellingen voor netwerklocatie Thuis of Bedrijf als bij Instellingen voor netwerklocatie Openbaar.

Deze netwerklocaties zijn de profielen die de Windows Firewall gebruikt. Zodra je de pc met een nieuw netwerk verbindt, zal het vragen wat voor netwerk het is. Kies dan alleen voor Thuisnetwerk en Bedrijfsnetwerk wanneer je dat netwerk vertrouwt. Kies in alle andere gevallen voor Openbaar netwerk. De firewall is dan extra alert en zorgt ervoor dat anderen in hetzelfde netwerk je pc helemaal niet kunnen zien.

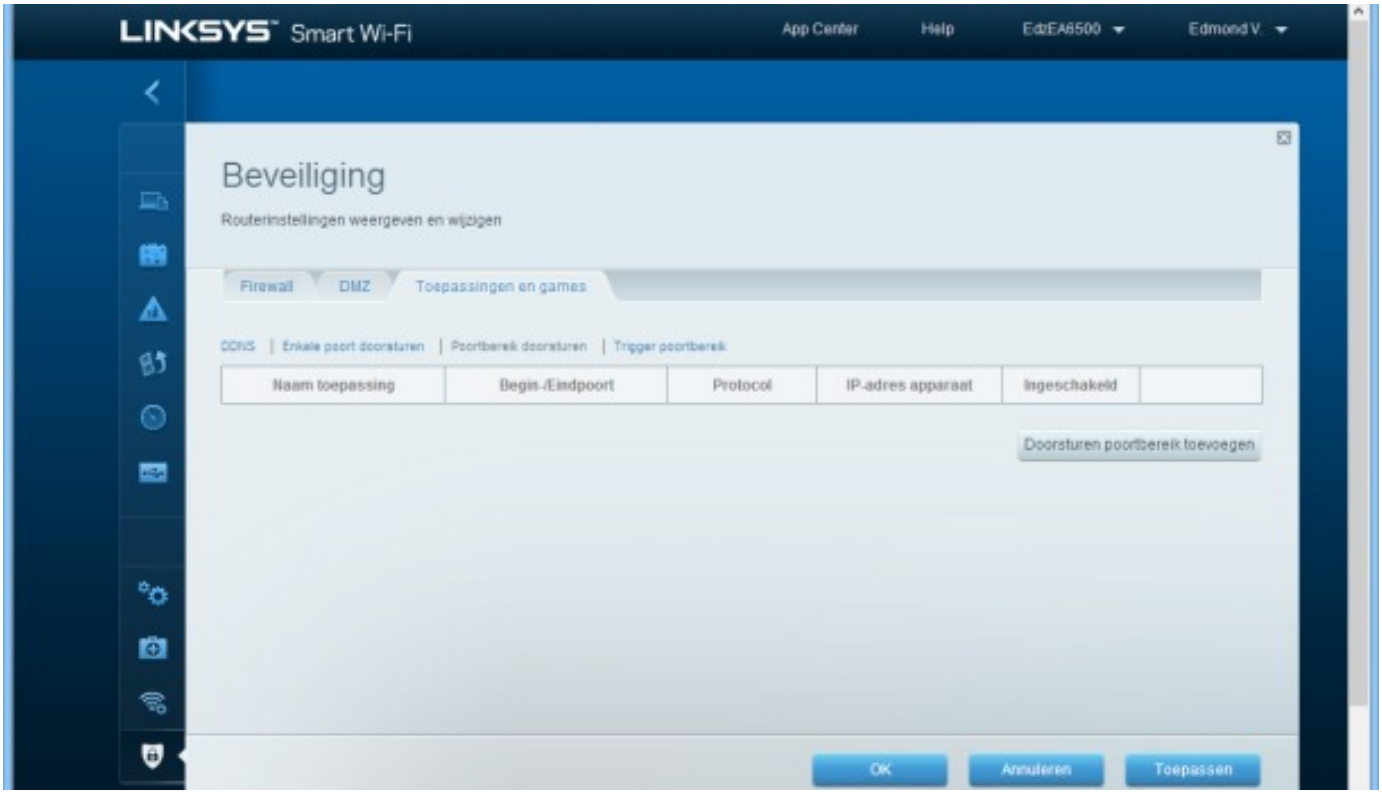
Tip 09 Wanneer je op een ander netwerk dan thuis bent, selecteer je het profiel Openbaar netwerk om de bestanden maximaal te beschermen.

Tip 10: Firewall router

Behalve de firewall op de pc is er nog een belangrijke firewall op het netwerk. Dat is de firewall op de router: de firewall die je pc's en tablets en alle bestanden op die apparaten, mede beschermt. Dat een onbekend persoon via het internet toegang krijgt tot je bestanden is wel de grootste nachtmerrie.

Deze firewall heeft een belangrijke rol om dit te voorkomen. Open de browser en ga naar de beheerpagina van je router. Typ de gebruikersnaam en het wachtwoord in en log in op de router. Waar de instellingen staan, is per merk/type router verschillend, er kunnen dus andere termen gebruikt worden. Ga naar het onderdeel Beveiliging of Firewall. Controleer of de firewall is ingeschakeld. Doe dat voor IPv4 en ook voor IPv6. Selecteer opties om je pc en thuisnetwerk te verbergen zoals Niet reageren op PING of Anonieme internetverzoeken filteren.

Kijk ook bij de DMZ en het onderdeel voor Portforwarding of Toepassingen en Games. Bij deze laatste onderdelen kun je systemen op het thuisnetwerk opgeven die wel vanaf het internet toegankelijk mogen zijn. Heel veel redenen zijn daar echter niet voor. Verwijder eventuele uitzonderingen die daar opgesomd staan of schakel een regel tijdelijk uit (disable) om te ervaren wat er dan niet meer werkt. Hoe minder uitzonderingen, des te veiliger de bestanden op het thuisnetwerk.

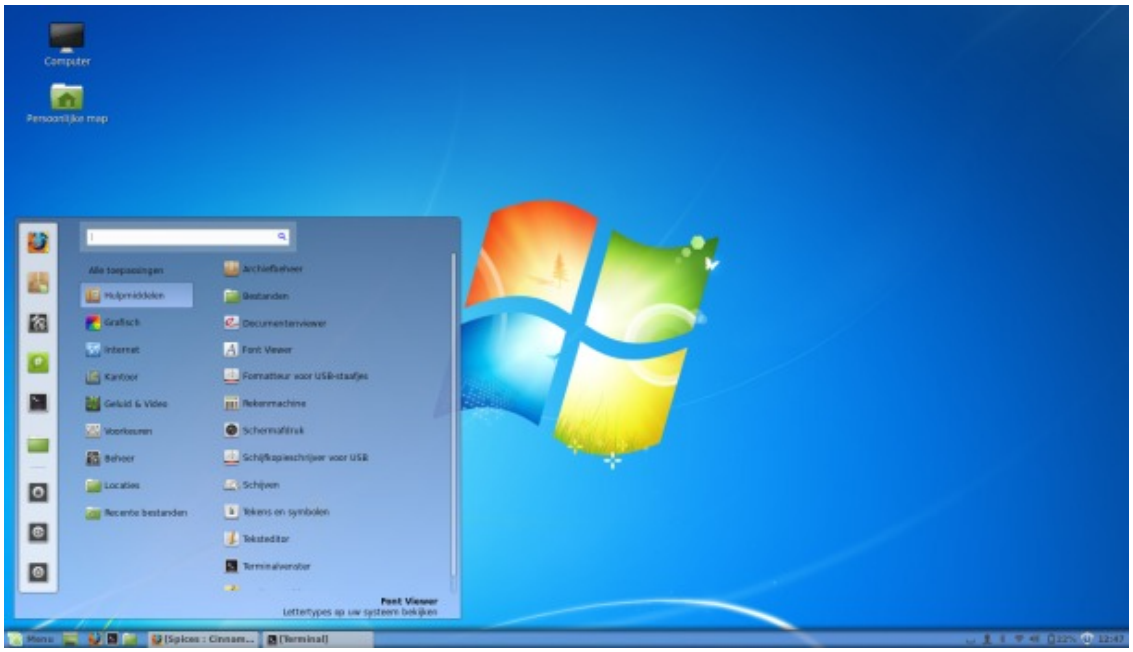


Tip 10 Elke DMZ en elke toepassing die je toestaat in de firewall, maakt het thuisnetwerk minder veilig.

Einde Windows XP-tijdperk: Overstappen op Linux ?

Nog steeds in het bezit van een reeds aantal jaren oude PC?Je werkt nog steeds met Windows XP? Nu Windows XP niet meer door Microsoft ondersteund wordt, zou je zeker ook eens een kijkje moeten nemen bij Linux. Je hebt geen nieuwe PC nodig, alleen een ander besturingssyteen. Het voordeel van een Linux systeem? Veilig en…….GRATIS ! Welke distributie het eenvoudigst is voor Windows-gebruikers, hoe je deze installeert en hoe je je bestanden overzet. En voor elk Windows programma is een Linux alternatief . GRATIS ! Zoals alles bij Linux.

Een eerste vraagstelling bij Linux is: welke distributie kiest je? Linux wordt immers door meerdere partijen aangeboden, met elk hun eigen versie. Mijn keuze voor een Windows XP-alternatief gaat echter naar een andere distributie: Linux Mint. Deze is gebaseerd op Ubuntu, maar gebruikt een gebruikersinterface die meer op Windows lijkt (Cinnamon) en bevat standaard veel multimediaprogramma's.



Met het juiste thema lijkt het of je van Windows XP naar Windows 7 bent overgeschakeld, maar dit is gewoon Linux Mint.

01 Systeemvereisten

Voordat je Linux Mint installeert, moet je eerst eens nagaan of je computer hiervoor geschikt is. Meestal is dat geen probleem, want Linux Mint heeft heel bescheiden systeemvereisten: 512 MB RAM (1 GB is wel aangeraden) en 8 GB ruimte op de harde schijf. De kans is dus groot dat Linux Mint probleemloos op je oude computer draait.

Important info:

- Recommended packages and 32-bit libraries
- DVD playback
- EFI Support
- PAE required for 32-bit ISOs
- mint4win

Make sure to read the "Release Notes" to be aware of important info or known issues related to this release.

System requirements:

- x86 processor (Linux Mint 64-bit requires a 64-bit processor. Linux Mint 32-bit works on both 32-bit and 64-bit processors).
- 512 MB RAM (1GB recommended for a comfortable usage).
- 5 GB of disk space
- Graphics card capable of 800×600 resolution
- CD/DVD drive or USB port

Upgrade instructions:

- To upgrade from a previous version of Linux Mint follow these instructions.
- To upgrade from the RC release follow these instructions.

Download:

Md5 sum:

- 32-bit: 5ba48b32861c62aebd44c5f310966ea3
- 64-bit: 21190d6baacbe106f145ca1ae44a0d88

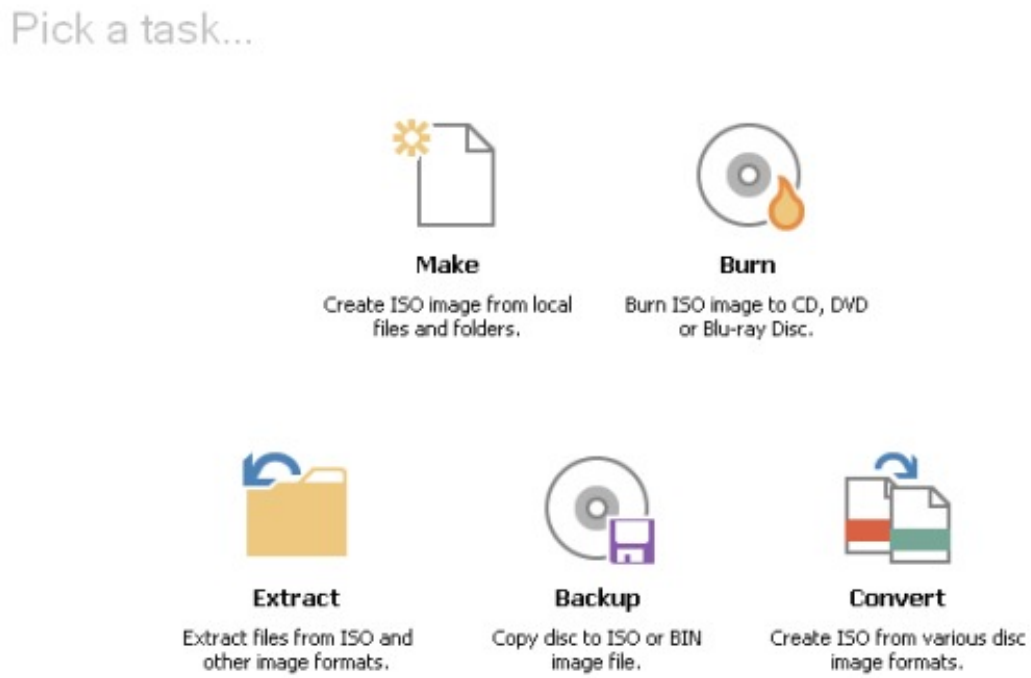
02 Download

Op de website van Linux Mint vind je een aantal versies om te downloaden. Allereerst moet je kiezen uit een 32- of 64bit-versie. Je vindt dit in XP in Configuratiescherm / Systeem / tabblad Algemeen. Staat hier Windows XP, dan heb je de 32bit-versie. Als je de toevoeging x64 ziet, gebruik je een 64bit-versie.

Daarnaast biedt Linux Mint allerlei versies met verschillende gebruikersinterfaces aan. We kiezen de standaardversie met Cinnamon. Op het moment van schrijven was de nieuwste versie Linux Mint 16 met codenaam Petra. Ieder halfjaar komt er een nieuwe versie uit.

03 Brand

Wat je juist gedownload hebt, is een iso-bestand dat je nog op een dvd-schijfje moet branden. Dat kan bijvoorbeeld met het gratis programma ISO Workshop. Zodra je dat geïnstalleerd hebt, kies je in het hoofdvenster Burn, waarna je de locatie van het gedownloade iso-bestand kiest.

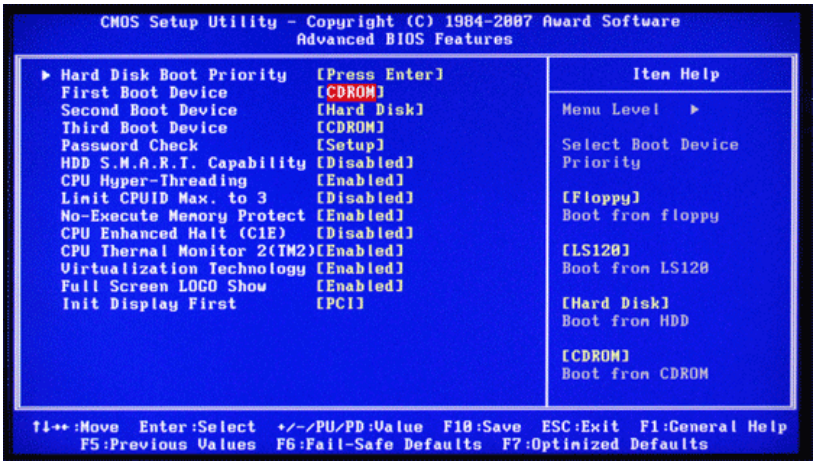


Back-up!

Voordat je Linux Mint installeert op de harde schijf van je computer waar nu Windows XP op staat, moet je een back-up van je harde schijf maken. Alle bestanden worden namelijk overschreven.

Kopieer dus al je bestanden naar een externe harde schijf. Sluit de schijf aan, selecteer in Windows Verkenner alle mappen die je nodig hebt en versleep ze naar de externe schijf. Denk ook aan de wachtwoorden die je door Windows hebt laten onthouden en andere nuttige informatie zoals je bladwijzers, e-mails enzovoort.

04 Start op van dvd



Start nu je computer op vanaf de dvd. Daarvoor moet je misschien eerst nog in het BIOS het dvd-station vooraan in de opstartvolgorde plaatsen. Afhankelijk van het merk van je computer ga je naar de instellingen van het BIOS met bijvoorbeeld F2, Esc of Del.

Sla de instellingen daarna op en herstart. Op sommige computers kun je tijdens het opstarten met een toets een menu oproepen waarin je kiest van welk opslagmedium je opstart. Als je het opstartmenu van Linux Mint te zien krijgt, weet je dat het werkt.

05 Eerste kennismaking

Na een tijdje is Linux Mint van de dvd-schijf opgestart en krijg je het bureaublad te zien. Hiermee krijg je ook al een eerste kans op een kennismaking met het systeem. Wat je nu ziet, is een volledig werkende Linux Mint-installatie, alleen werkt deze vanaf de dvd-schijf en nog niet vanaf je harde schijf.

Zo kun je bijvoorbeeld eenvoudig testen of je draadloze netwerkkaart ondersteund wordt en kijken of Linux Mint je ligt. Dubbelklik linksboven op het bureaublad op Install Linux Mint om het installatieprogramma te starten.

06 Kies je taal

Het installatieprogramma van Linux Mint bestaat uit zeven stappen. In de eerste stap kies je je taal, Nederlands is ook één van de opties. Na je keuze verandert de taal van het installatieprogramma en klik je op de knop Verder om door te gaan.

07 Installatietype

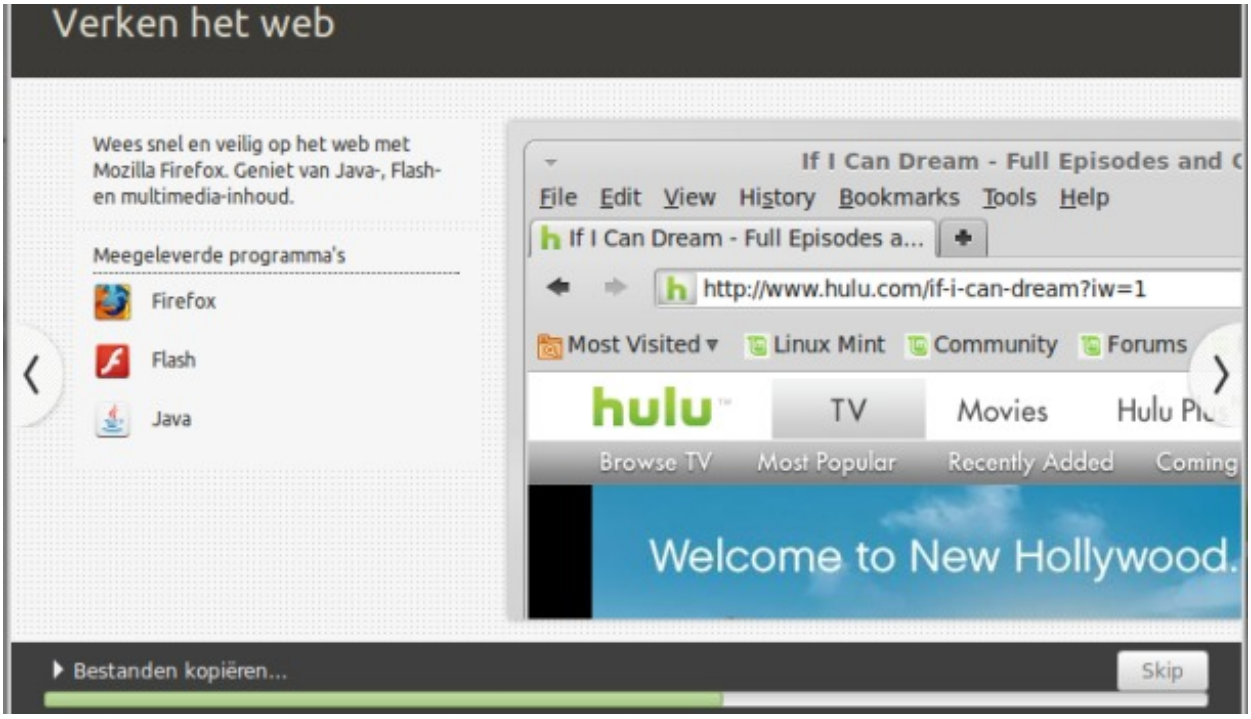
Als je Windows XP op de harde schijf hebt staan, ontdekt Linux Mint dat en vraagt je wat je wil doen. Standaard wordt voorgesteld om Windows XP door Linux Mint te vervangen. Daarbij wordt je hele harde schijf opnieuw geformatteerd, waardoor al je bestaande bestanden verloren gaan.

Verzeker je er dus eerst van dat je een back-up gemaakt hebt van al die bestanden! Optioneel kun je nog kiezen of je je Linux Mint-installatie wil versleutelen. Klik tot slot op Installeer nu.

08 Instellingen

Terwijl het installatieprogramma nu Linux Mint op je harde schijf installeert, kun je al enkele instellingen ingeven. Zo word je achtereenvolgens gevraagd in welke tijdzone je je bevindt, welke toetsenbordindeling je gebruikt (je kunt in het getoonde tekstveld typen om te controleren of je keuze correct is) en welke gebruikersnaam en wachtwoord je kiest.

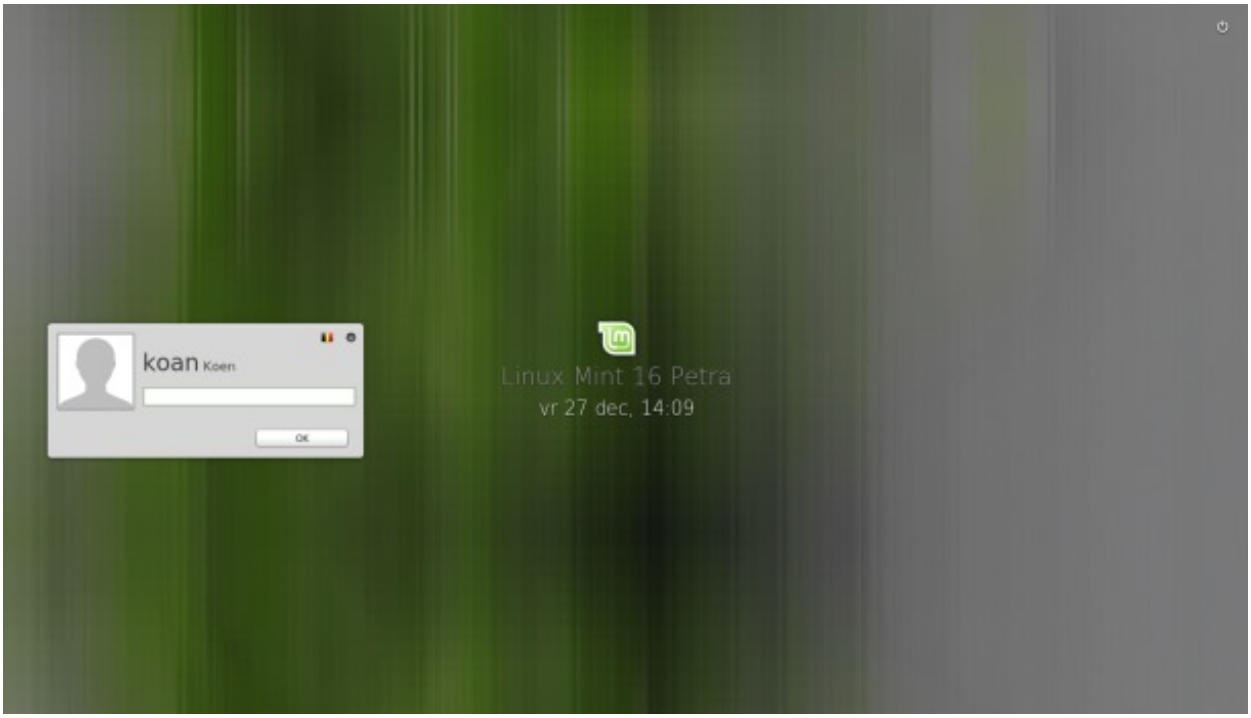
In het laatste venster krijg je ook de keuze om je persoonlijke map te versleutelen. Klik tot slot op Verder, waarna de installatie verdergaat en je een slideshow te zien krijgt. Na voltooiing klik je op Nu herstarten.



09 Aanmelden

Na de herstart krijg je het aanmeldvenster te zien. De gebruikersnaam die je hebt gekozen, wordt al getoond. Klik erop en vul het bijbehorende wachtwoord in, waarna je op Enter drukt om aan te melden.

Als je niet wil aanmelden, klik je rechtsboven op het icoontje van de powerknop. Dan krijg je de keuze om de computer uit te schakelen, in slaapstand te zetten of te herstarten.



10 Welkomstscherm

Zodra je aangemeld bent, krijg je een welkomstscherm te zien waarin de ontwikkelaars van Linux Mint je verwijzen naar verdere informatie op internet, zoals documentatie, internetfora en chatrooms en een database met ondersteunde hardware. Als je die informatie de volgende keren niet meer wil zien, vink dan het vakje met Dit dialoogvenster weergeven bij het opstarten uit.

Kijk ook eens naar dit venster: naast de titelbalk bovenaan het venster staan helemaal rechts twee knopjes. Met een druk op het minteken minimaliseer je het venster en met het kruisje sluit je het, net zoals je dit gewend bent.

11 Draadloos netwerk

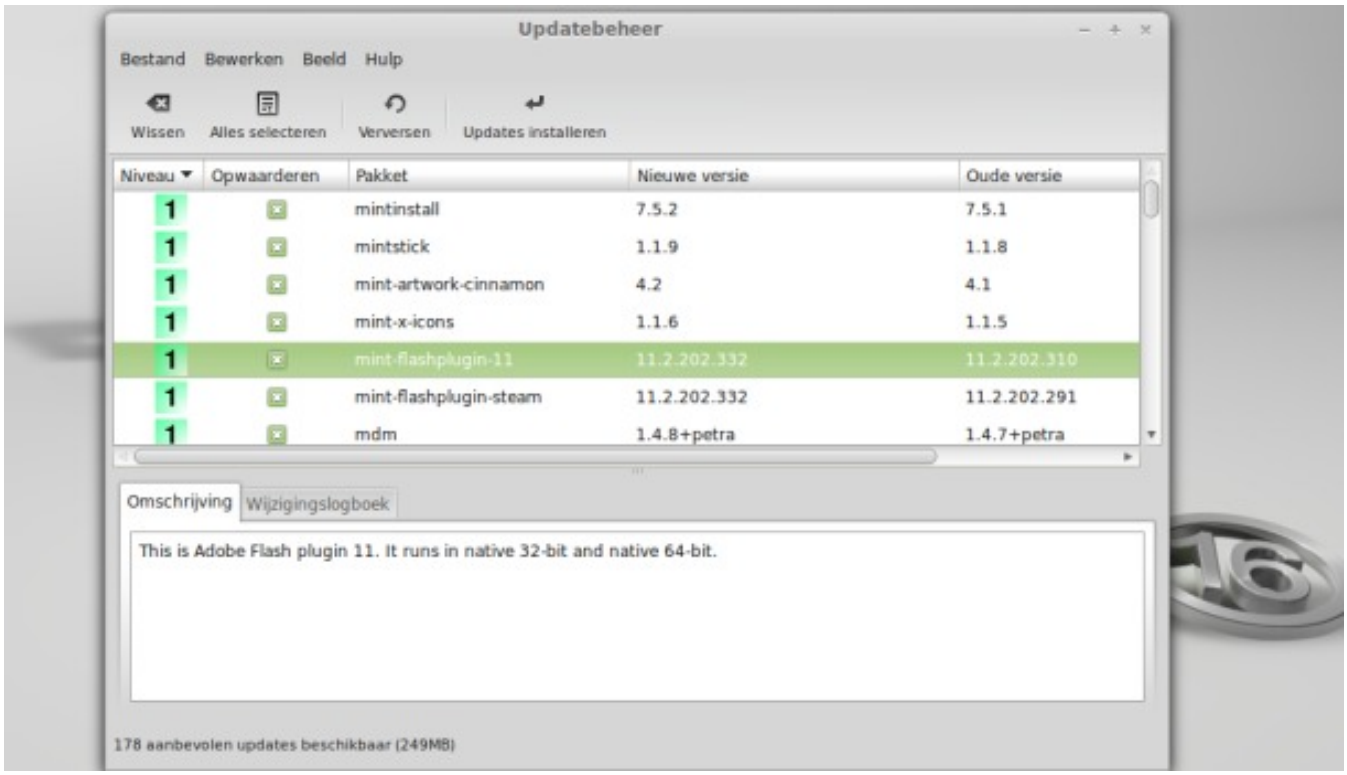
Het wordt tijd voor een kleine rondleiding. Onder in het scherm zie je het paneel. We beginnen aan de rechterkant, waar je een aantal icoontjes ziet in het systeemvak. Waarschijnlijk zie je links in dit systeemvak een icoontje van een tekstballon met een 1. Klik erop om de melding te zien: in ons geval de melding dat er draadloze netwerken beschikbaar zijn.

Klik daarna op het icoontje van de twee gebroken kabels om de draadloze netwerken te zien. Kies een netwerk en geef het wachtwoord in. Daarna wordt de draadloze internetverbinding opgezet en verandert het icoontje.

12 Updaten

De volgende stap die je het beste uitvoert is het updaten van Linux Mint. Normaal gesproken krijg je in het systeemvak al een icoontje van een blauw schild met een i te zien, dat je aanmaant om te updaten. Klik erop en geef dan je wachtwoord, waarna het updatebeheer wordt gestart.

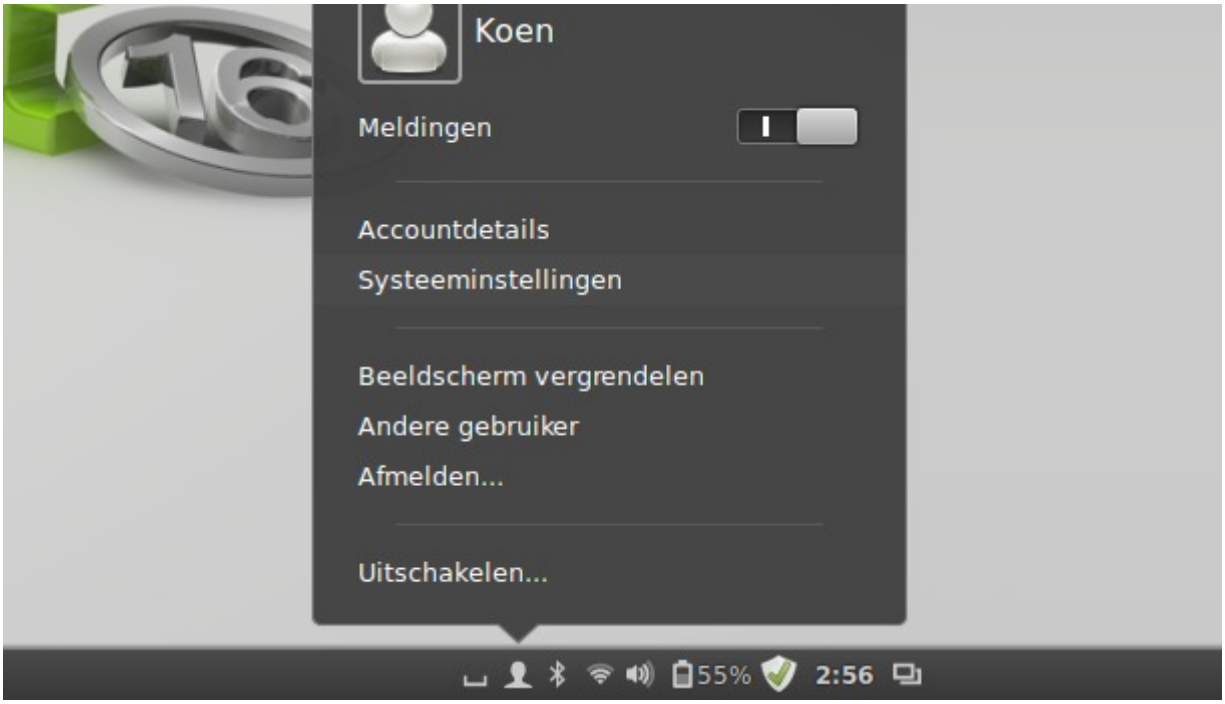
Klik daarna bovenaan op Updates installeren. Mogelijk komen er na het installeren van updates nog meer nieuwe updates beschikbaar en moet je nogmaals op Updates installeren klikken tot er geen updates meer beschikbaar zijn.



13 Systeemvak

Wanneer Linux Mint up-to-date is, kun je je systeem verder ontdekken. In het systeemvak vind je verder nog een knop om alle vensters te bekijken, de datum en tijd, de batterijstatus, het audiovolume, een knop voor de bluetooth-verbinding en een menu waarmee je de computer uitschakelt, het beeldscherm vergrendelt of de systeeminstellingen opent.

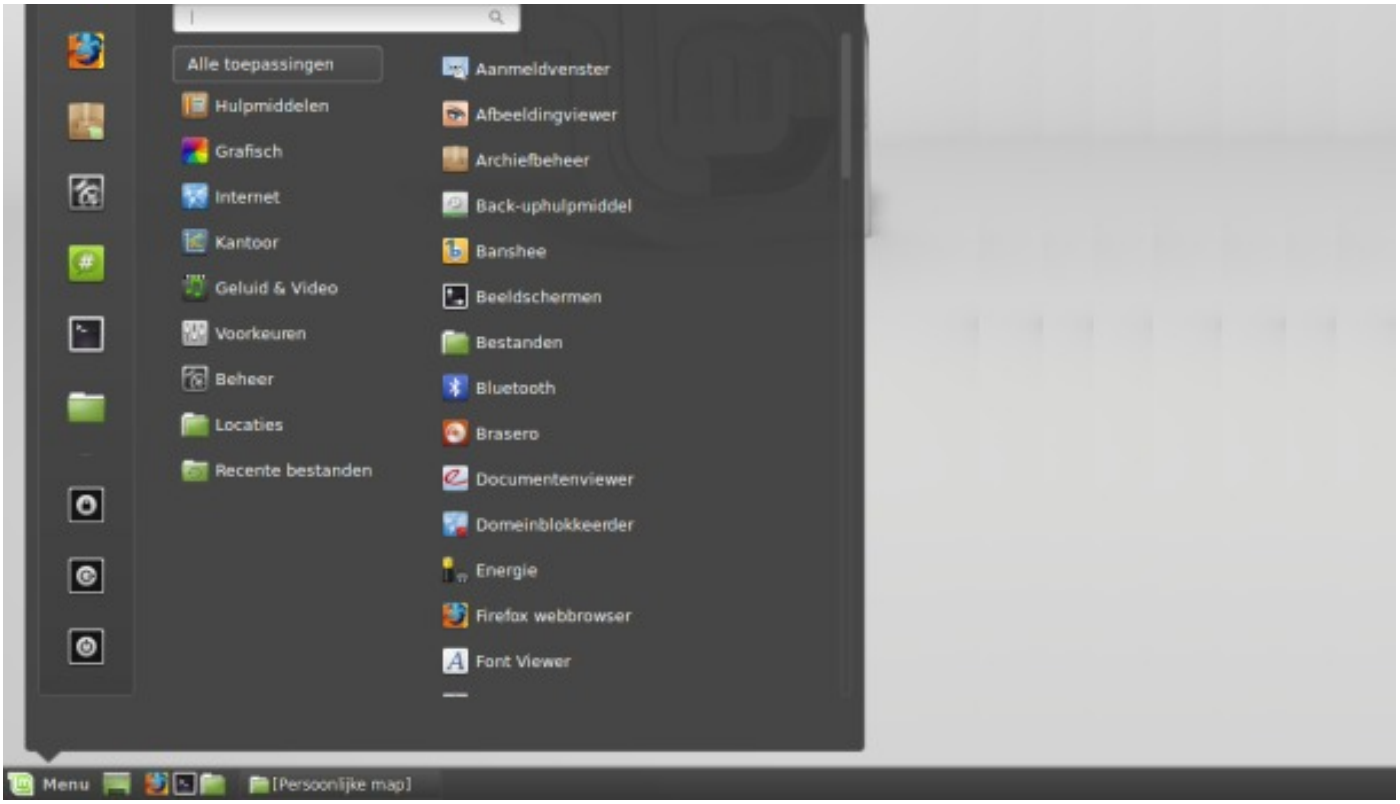
Klik of rechtsklik gerust eens op alle icoontjes om te zien wat je ermee kunt doen, want je zult ze dagelijks vaak gebruiken.



14 Programma's

Klik je linksonder op Menu, dan opent zich het hoofdmenu, waarvandaan je toegang krijgt tot alle programma's. Links staan wat icoontjes van populaire programma's, de instellingen en om het scherm te vergrendelen en de computer af te sluiten. Daarnaast staan menu-onderdelen voor verschillende categorieën programma's.

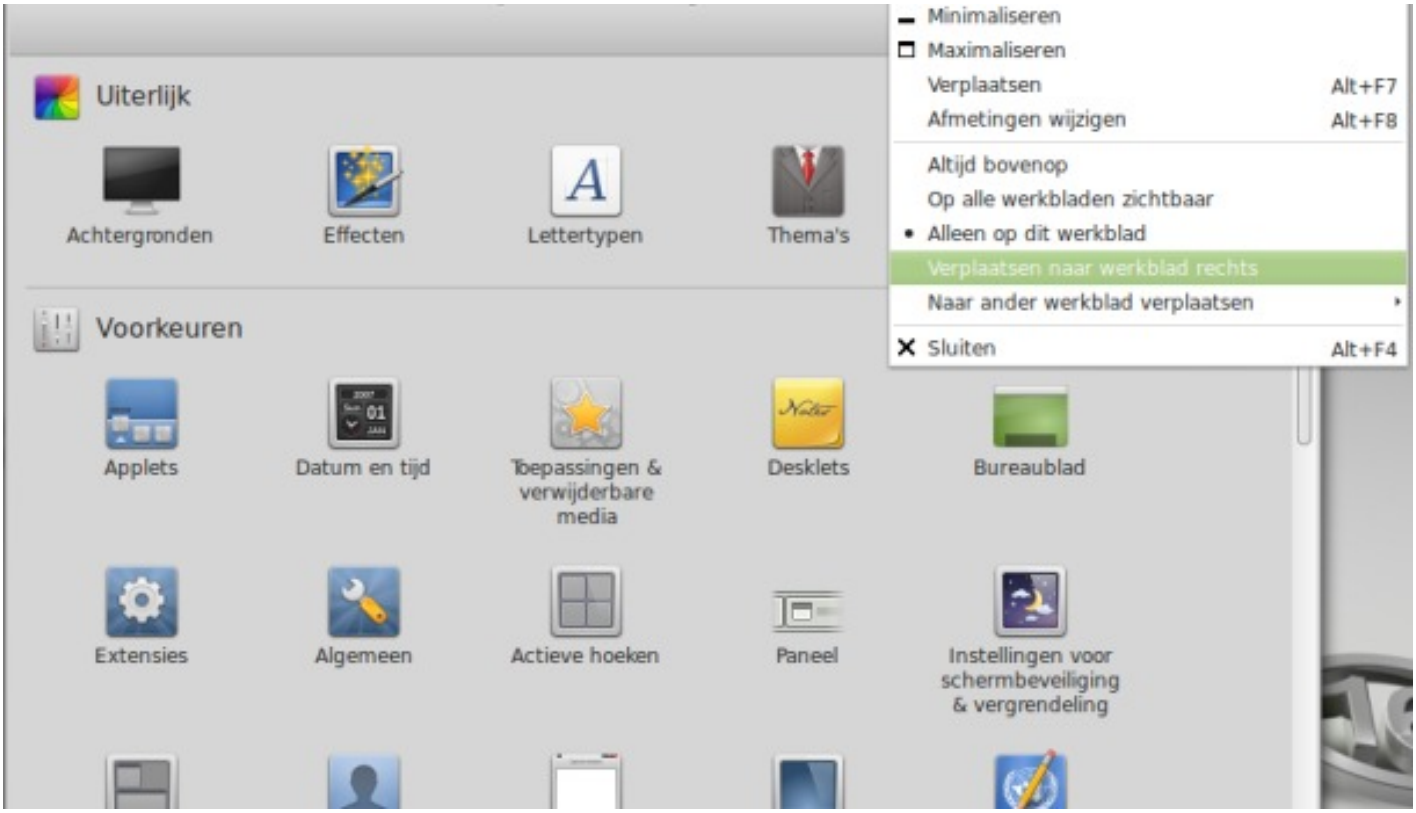
Standaard is al heel wat software geïnstalleerd, zoals het kantoorpakket LibreOffice, de browser Firefox, de instant messenger Pidgin, de mediaspeler VLC enzovoort. Naast het hoofdmenu staan wat snelkoppelingen en je vindt er de taakbalk met geopende vensters.



15 Vensters

Open eens een aantal vensters. Met het minteken in een venster minimaliseer je een venster met het kruisje sluit je het venster, dat weet je al. De meeste vensters hebben ook een plusteken, waarmee je het venster maximaliseert of zijn normale grootte teruggeeft. Rechtsklik op de titelbalk voor meer mogelijkheden.

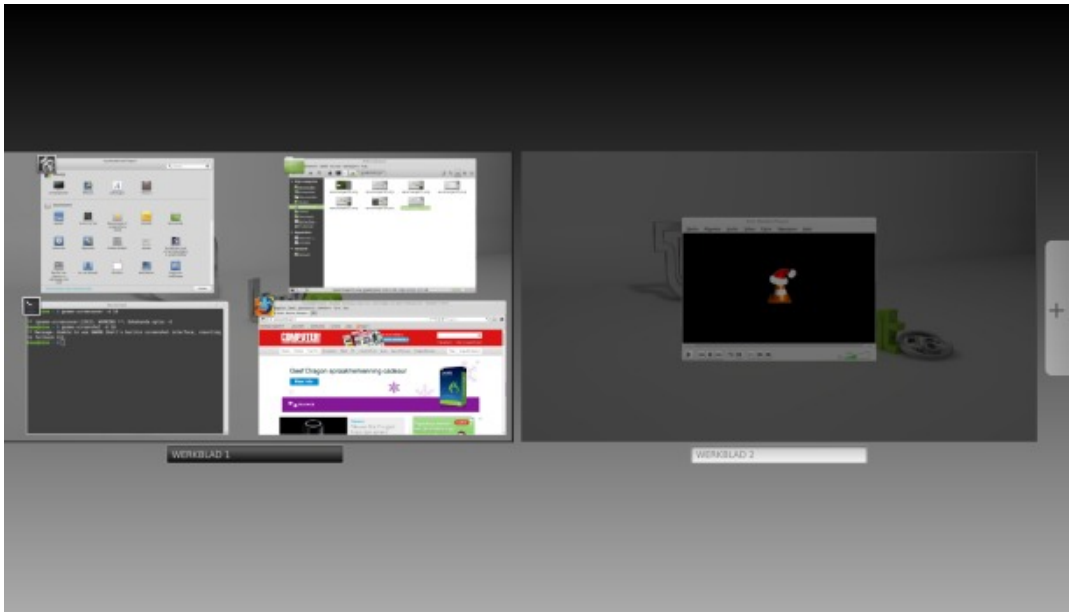
Kies bijvoorbeeld Verplaatsen naar werkblad rechts om het venster naar het tweede werkblad te verplaatsen. Druk je daarna op de toetsen Ctrl+Alt+PijlRechts, dan wordt het tweede werkblad getoond. Door je vensters over verschillende werkbladen te verdelen, houd je wat orde.



16 Werkbladen

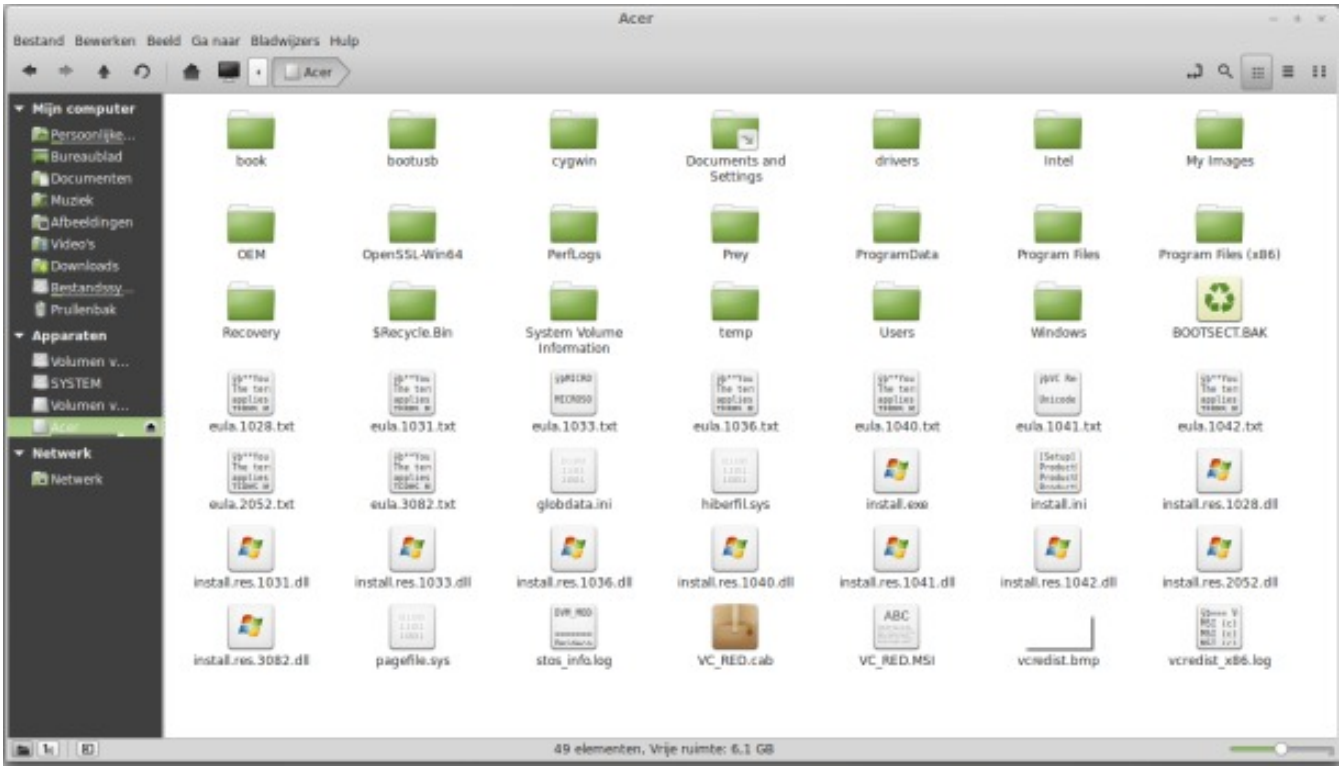
Heb je heel wat vensters openstaan, druk dan de toetsen Ctrl+Alt+PijlOmlaag, waarna je alle vensters op het huidige werkblad tegelijk in het klein te zien krijgt en op een venster klikt om het naar voren te brengen.

Druk je op Ctrl+Alt+PijlOmhoog, dan wordt een miniatuurversie van beide werkbladen met alle vensters erin getoond. Klik op een werkblad of venster om het te selecteren of klik op het plusteken helemaal rechts om een extra werkblad aan te maken.



17 Schijf aansluiten

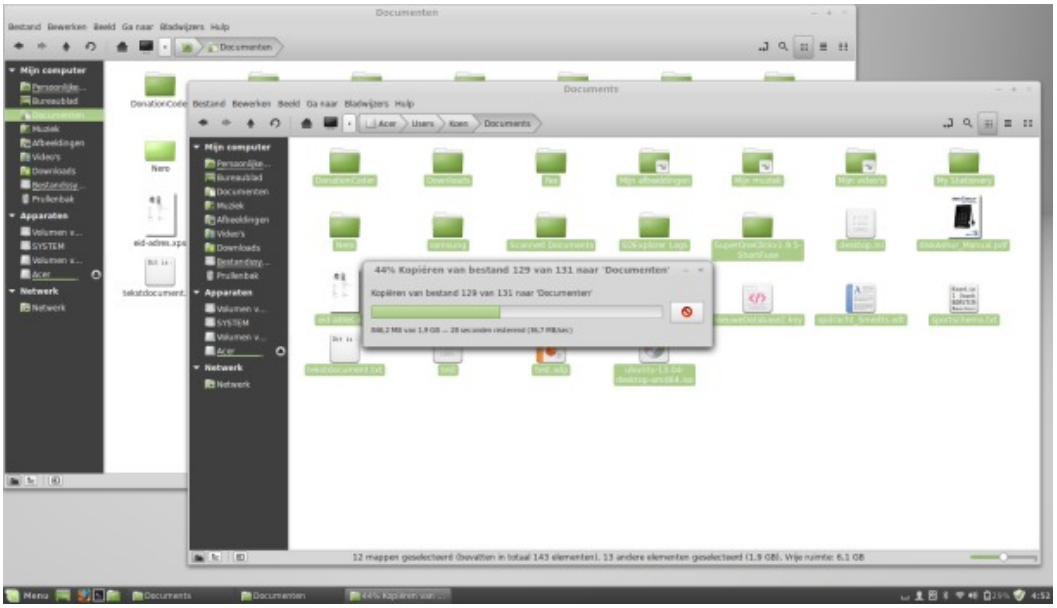
Nu je een beetje je weg weet in Linux Mint, is het tijd om je bestanden uit Windows te kopiëren. Sluit de externe harde schijf aan en klik daarna bovenaan links op het bureaublad op Computer. Je krijgt nu alle partities op de (interne en externe) harde schijven te zien. Dubbelklik op de schijf waarop je in Windows je back-up gemaakt hebt om de inhoud te bekijken.



18 Bestanden kopiëren

Heb je eenmaal beslist wat je wil kopiëren, open dan een tweede venster met je Persoonlijke map door op het gelijknamige icoontje op je bureaublad te dubbelklikken. Open dan het venster van de bestanden op je externe schijf en selecteer de te kopiëren bestanden. Dit doe je door met een ingedrukte muisknop een rechthoek rond de gewenste bestanden te slepen.

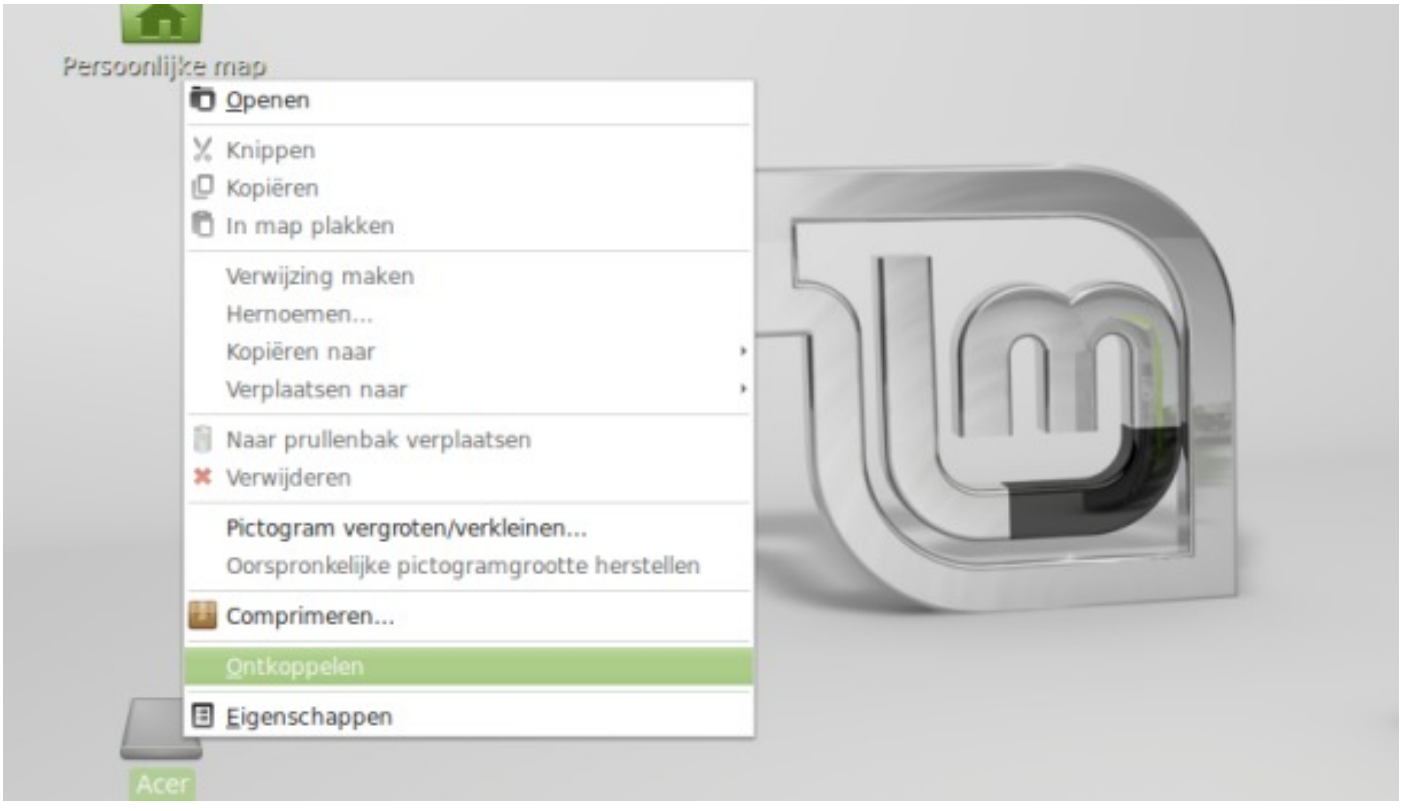
Versleep de bestanden naar de map op je interne schijf terwijl je de muisknop ingedrukt houdt. Het kopiëren kan overigens wel even duren.



19 Schijf ontkoppelen

Nadat je de bestanden van de externe schijf gekopieerd hebt, moet je die eerst ontkoppelen in Linux Mint voor je de usb-kabel uit de computer haalt of de schijf uitschakelt. Dubbelklik daarvoor op Computer op het bureaublad en klik dan op het icoontje naast de schijf om die te ontkoppelen. Je kunt ook op het icoontje van de schijf op het bureaublad rechtsklikken en dan Ontkoppelen kiezen.

Vanaf nu staan al je documenten op je computer met Linux Mint en kun je zonder Windows XP veilig aan de slag.



Linux Mint-programma's voor Windows XP-gebruikers

Veel van je Windows-programma's zijn niet beschikbaar voor Linux. Maar er is Linux-software die minstens even goed presteert.

De grootste uitdaging voor Windows XP-gebruikers die willen overstappen op Linux Mint is om de programma's die je al jaren gebruikt te vervangen. Gelukkig zijn sommige programma's beschikbaar op Linux en Windows. Daarnaast is er heel wat Linux-software met dezelfde functionaliteit als je favoriete Windowsprogramma's. Ik ga je niet voorhouden dat al je software beschikbaar is op native Linux. Dat is niet zo.

Maar er zijn methodes om Windows-applicaties te draaien op Linux. Je kunt Windows zelfs draaien op Linux. Maar dat vergt specialistische kennis.

Grafisch: Linux heeft een geweldige fotobewerker, Gimp. Dat is het goede nieuws. Het slechte nieuws is dat het totaal niet lijkt op Adobe Photoshop. Als je de moeite wil doen om een nieuw programma onder de knie te krijgen, dan is Gimp zeker de moeite waard.

Office-pakket: Je kunt Microsoft Office niet zomaar draaien op een Linux-desktop. Je kunt het daarentegen wel vervangen door LibreOffice. Ik gebruik dit pakket al sinds het zich afsplitste van OpenOffice.org, en het gedraagt zich zo erg als Microsoft Office dat ik zonder problemen kan afwisselen tussen de twee pakketten zonder me ooit te moeten afvragen met welke software ik ook alweer bezig ben. Als je weet hoe je Office moet gebruiken, dan kan je zo al met LibreOffice uit de voeten. Daarenboven kan de nieuwste versie van het kantoorpakket, LibreOffice 4.2, zonder al te veel problemen bestanden bewaren in Microsofts eigen bestandstypes.

E-mail: Als jeverknocht bent aan Exchange en Outlook, dan kan je Evolution groupware gebruiken. Evolution kun je combineren met Exchange. Je kunt uiteraard elke webmailclient gebruiken op Linux.

Browser: Je krijgt bij Mint standaard Firefox. Gebruik je liever Chrome, dan download je de 32- of 64-bitversie voor Debian/Ubuntu, afhankelijk van waarop je systeem draait. Als je die hebt gedownload, open je het bestand, waarna je het Package Installer-programma ziet verschijnen. Klik gewoon op Install Package, en binnen een paar minuten kan je verder surfen in Chrome.

Antivirus: Eén belangrijke categorie van programma's zul je trouwens niet meer nodig hebben: antivirussoftware. Bij Windows duiken er, wat is het, zo ongeveer om het uur wel nieuwe en gevaarlijke virussen op. Bij Linux mag je gerusten rekenen in weken of maanden. Er is vrijwel geen malware op Linux die je parten kan spelen. En als je toch het zekere voor het onzekere wil nemen, download je gewoon het gratis antivirusprogramma ClamAV.

Gamen: Bijna geen van je games zal native kunnen draaien op Linux. Veel van Valve Softwares Steam-games draaien tegenwoordig echter wel op Linux. Om Steam-spellen te draaien op Mint moet je hardware, naar XP-standaarden, behoorlijk krachtig zijn. Je hebt een 64 bit-processor nodig, 4 GB werkgeheugen en een grafische kaart van AMD, Intel of Nvidia. Als je aan de hardwarekant goed zit, dan zal je de SteamLauncher moeten opstarten in Mints Software Manager. Daarna volg je gewoon de instructies van de Steamclient en kan je binnen de kortste keren je spel beginnen spelen. Linux heeft trouwens ook een heleboel native spellen. Voor een goede selectie neem je een kijkje op Linuxgames. Veel van deze games vind je via de softwaremanager.

Firewall: In Linux heb je ook een firewall die heet Gufw. In mint moet die apart geinstalleerd worden via het softwarecenter.

Defragmenteren: van die defragmentatie ben je voorgoed verlost met Linux. Het bestandsysteem in Linux is anders waardoor er nooit gedefragmenteerd hoeft te worden.

Updates: updates komen automatisch binnen en kun je zelf installeren wanneer je het uitkomt. En dus niet als je wil afsluiten, zoals bij Windows.

Kunt u geen goed Linux-alternatief vinden voor een bepaald Windowsprogramma?

Installeer in uw Linux de Windows-nabootser Wine. Hiervoor gebruikt u in Ubuntu softwarecentrum de zoekterm wine en installeert u Wine Windows-programmalader.

Wine is een programma dat Linux in staat stelt om veel (niet alle) Windowsprogramma's te draaien. Het is dus een technologisch wondertje.

Keerzijde: veiligheidsrisico's :echter, wel een wondertje met een keerzijde: niet alleen gewone Windowsprogramma's kunnen ineens opstarten in Linux, maar ook.... Windowsvirussen en andere gevaarlijke rotzooi.

Die kunnen uw systeembestanden weliswaar niet aantasten (Wine heeft immers slechts gewoon gebruikersrecht), maar wel uw persoonlijke bestanden (documenten, foto's, muziek)! En dat is natuurlijk veel erger.

Daarom ben ik niet zo'n voorstander van Wine. Ik houd Linux liever zuiver. Veiligheid voor alles.

Wine beveiligen

Kiest u er toch voor om Wine te installeren? Beperk dan de mogelijke schade die Windowsvirussen kunnen aanrichten. Als volgt:

1. Klik op het grijze Ubuntulogo (Snelzoeker), bovenin de uitklapbare zijbalk. Gebruik de zoekterm wine

Klik op Wine configureren

(het opstarten daarvan kan de eerste keer erg lang duren, wacht rustig af)

Tabblad Stations

Verwijder hier alle stations, behalve C: (drive_c), D: (/media/cdrom0) en Z:.

Klik op Toepassen.

Klik op OK.

Sluit het configuratieprogramma van Wine.

2. Beperk de integratie van Wine in uw werkomgeving:

(opmerking: maak deze ingreep weer ongedaan wanneer het de werking van Wine teveel belemmert).

a. Maak eerst in uw persoonlijke map een nieuw mapje aan, genaamd wijnazijn. Ik ga even uit van gebruiker Karel, die een persoonlijke map heeft genaamd karel. Voor gebruiker karel is dat dus:

/home/karel/wijnazijn

Maak daarna in wijnazijn de volgende submapjes aan:

Bureaublad

Documenten

Afbeeldingen

Muziek

Video's

b. Klik op het grijze Ubuntulogo (Snelzoeker), bovenin de uitklapbare zijbalk. Gebruik de zoekterm wine

Klik op Wine configureren

Tabblad Desktop Integratie - onderdeel Folders

klik op Bureaublad

...en wijzig het bestandpad in:

/home/karel/wijnazijn/Bureaublad

klik op Mijn Documenten

... en verander daarbij het bestandpad in:

/home/karel/wijnazijn/Documenten

Enzovoorts, bij alle categorieën.

Klaar? Klik op Toepassen.

Klik op OK.

Hiermee verkleint u de kans, dat Wine zich bemoeit met uw belangrijke documenten: in het voorbeeld beperkt hij zich nu in principe tot /home/karel/wijnazijn (en de submapjes die daarin zitten).

Let op: gebruikersinstellingen: herhalen per gebruikersaccount.

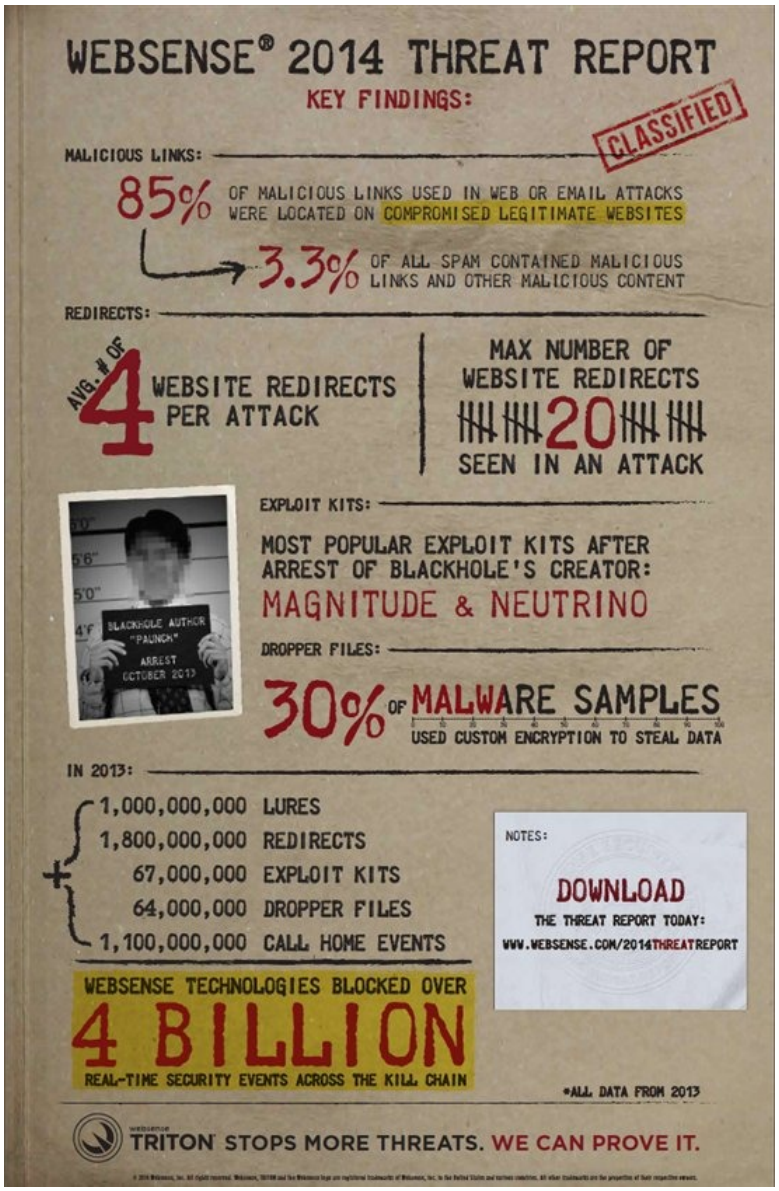
Cybercrimineel maakt steeds meer gebruik van legitieme websites

Volgens het Websense Security Labs 2014 Threat rapport stonden maar liefst 85% van alle kwaadaardige links in web en e-mail aanvallen op gecompromitteerde legitieme websites.

Websites in de categorieën bedrijf en economie, ICT, winkelen en reizen staan in de top 10 van gecompromitteerde sites. Daarnaast lijken Magnitude en Neutrino de toorts over te nemen van Blackhole als meest gebruikte exploit kits. Waarschijnlijk komt dit door de arrestatie van de maker van de Blackhole exploit kit.

Vice-president Charles Renert merkt op dat cybercriminelen constant de planning en uitvoering van hun aanvallen aanpassen teneinde beveiligingsmaatregelen voor te zijn. Hoewel volhardende aanvallers nog altijd succes boeken met geavanceerde aanvallen en zero-day exploits lijkt cybercriminaliteit op grote schaal steeds meer op te bloeien. Volgens Renert worden minder geavanceerde aanvallen vaak niet opgemerkt door organisaties waar real-time bescherming ontbreekt.

Het rapport gaat verder in op de manier waarop aanvallers de infrastructuur van een aanvalscampagne ontwikkelen, gedurende de aanval aanscherpen en hergebruiken. Zo zagen de Websense onderzoekers dat het gebruik van de Zeus malware weer een sterke groei doormaakte toen deze omgevormd werd van keylogger en bedreiging voor financiële diensten tot malware die gebruikt kon worden om andere sectoren op de korrel te nemen, zoals bijvoorbeeld de overheid.



XP-gemeenten onderworpen aan test burgerprivacy

Minister Plasterk wil de privacy van burgers bij gemeenten aan een test onderwerpen voordat die belangrijke sociale taken van het Rijk overnemen. Het gaat daarbij dan vooral om de veiligheid van gegevensuitwisseling.

De gegevensuitwisseling die gemeenten gaan doen in het kader van de uitvoering van nieuwe taken die zij krijgen van het Rijk in het sociale domein, moet aan een Privacy Impact Assessment onderworpen worden. Daarin zal het ministerie van Binnenlandse Zaken het voortouw nemen.

Dat schrijft minister Plasterk aan de Tweede Kamer in antwoord op vragen van het CDA over de beveiliging van burgergegevens bij gemeenten. Tweede Kamerlid Van Toorenburg maakt zich grote zorgen over die beveiliging aangezien een groot aantal gemeenten ook na 8 april met Windows XP werken.

CBP maakt zich grote zorgen over burgerprivacy

Het College bescherming persoonsgevens heeft daarover aan de bel getrokken omdat gemeenten steeds meer privacygevoelige informatie over hun burgers in beheer krijgen. Bij een oud besturingssysteem als Windows XP bestaat het risico dat die informatie op straat komt te liggen.

Plasterk schrijft dat voor die nieuwe gemeentelijke praktijk "een beperkt aantal modellen" worden ontwikkeld om de nieuwe sociale taken (Jeugdzorg, zorg aan langdurig zieken en bijstand) vorm te geven. Als die modellen klaar zijn, wil Plasterk die aan een PIA onderwerpen.

In dit voorjaar wil Plasterk verder ook nog met een beleidsvisie komen over die gegevensuitwisseling en privacy. Op vragen over Windows XP bij gemeenten en de afhankelijkheid van leverancier Microsoft zegt Plasterk kortweg dat het de verantwoordelijkheid van de gemeenten zelf is.

Snapshots:

Philips smart TV kwetsbaar via wifi

Alle modellen van Philips Smart TV die in 2013 verschenen zijn kwetsbaar voor een aanval via wifi, waardoor een aanvaller cookies en andere bestanden kan stelen. Het probleem wordt veroorzaakt door Miracast, een Bluetooth-achtige feature die recente Philips Smart televisies gebruiken om een wifi-verbinding met de apparaten van de gebruiker op te zetten, zonder dat hiervoor een wifi-router is vereist. Miracast gebruikt echter een vast wachtwoord. Door de kwetsbaarheid kan iedereen in de buurt van de televisie toegang tot het apparaat krijgen.

Zodra een aanvaller toegang tot de televisie heeft kan die bestanden van aangesloten USB-apparaten lezen en cookies van websites stelen waar de gebruiker via de televisie op is ingelogd. Verder zou een aanvaller zijn eigen video of foto's op de televisie kunnen tonen en het kanaal dat de gebruiker aan het kijken is wijzigen, zo blijkt uit een demonstratievideo die ReVuln op Vimeo plaatste. De kwetsbaarheid zou in de meest recente firmware van de televisies aanwezig zijn.

Kabinet dient wetsvoorstel in dat cookieregels voor websites versoepelt

De cookiewet wordt zo aangepast dat er geen toestemming meer hoeft te worden gevraagd voor cookies die niet privacygevoelig zijn. Het gaat dan onder andere om cookies die de werking van websites verbeteren, de zogeheten analytic cookies.

Minister Kamp van Economische Zaken (EZ) heeft daartoe een wetsvoorstel ingediend. "Het beschermen van de privacy van internetters is belangrijk", aldus minister Kamp. "Tegelijkertijd moeten we ervoor zorgen dat deze bescherming niet doorslaat. Burgers moeten ook kunnen profiteren van het gemak van het gebruik van internet."

Voor cookies die het surfgedrag van internetgebruikers volgen verandert er niets. Hiervoor moet nog steeds vooraf toestemming worden gegeven.

Gebruik mobiele anpr-camera's goedgekeurd

De Kamer heeft donderdag unaniem een wettekst goedgekeurd die het de politie toelaat gebruik te maken van mobiele camera's voor automatische nummerplaatherkenning - de zogenaamde anpr-camera's. De tekst kreeg eerder groen licht in de Senaat.

Anpr staat voor "Automatic Numberplate Recognition". De camera's worden meestal ingezet als middel om de criminaliteit te bestrijden en de verkeersveiligheid te verbeteren, door middel van een koppeling aan allerlei databanken. Mobiele camera's die op voertuigen gemonteerd staan voor automatische nummerplaatherkenning, konden evenwel als onwettig worden beschouwd omdat ze volgens de camerawet enkel gebruikt mogen worden bij grote volkstoelopen.

Het wetsontwerp past daar nu een mouw aan. Wanneer de politie beslist om de mobiele anpr-camera's te gebruiken, moet ze de Privacycommissie daarvan op de hoogte brengen en elk trimester een omstandig verslag bezorgen over hoe vaak en waar de toestellen zijn gebruikt.

Populaire Virus Shield App blijkt scam

Security bewuste Android gebruikers kwamen deze week bedrogen uit toen bleek dat hun Virus Shield anti-virus app niets meer was dan een simpele afbeelding op het scherm van hun mobiele telefoon of apparaat.

Volgens maker Deviant Solutions voorkomt Virus Shield dat schadelijke apps op het mobiele apparaat van de gebruiker terecht komen. Daarnaast zou het apps, instellingen, bestanden en media real time scannen en zou de app de privé gegevens van de eigenaar beschermen. Dit alles, met een minimale impact op de batterij en zonder vertoon van advertenties.

Google Play Store

De app kreeg maar liefst 4.7 sterren in de officiële Google Play Store, kostte 3,99 dollar en was binnen een week de beste verkochte betaalde app in de Store.

Scam

Helaas bleek de belofte te mooi om waar te zijn. Toen de Android Police een blik wierp op de broncode, bleek dat de enige functionaliteit van de app bestond uit een afbeelding van een schild met een kruis en een schild met een checkmark waar de gebruiker tussen kon schakelen door op het scherm te tappen. Dit zou vervolgens de zogenaamde beveiliging uit of in moeten schakelen. Deviant Solutions bleek echter "ver-zuimd" te hebben om een daadwerkelijke anti-virus applicatie achter de aan- en uitknop te hangen.

Virus Shield is inmiddels verwijderd uit de Google Play Store.

Kabinet trekt richtlijn bewaarplicht telecomgegevens nog niet in

Het kabinet is nog niet van plan de bewaarplicht voor telecomgegevens in te trekken, ook al is de Europese richtlijn die er aan ten grondslag ligt vandaag met terugwerkende kracht door het Europese Hof vernietigd. Het kabinet wil eerst het arrest van het Europees Hof van Justitie bestuderen en wil geen beslissingen nemen op basis van slechts een perscommunicee, aldus staatssecretaris van Veiligheid en Justitie Fred Teeven in het wekelijkse vragenuur in de Tweede Kamer. Hij verwacht hier 8 weken voor nodig te hebben.

Liesbeth van Tongeren (GroenLinks) vroeg de staatssecretaris of de intrekkingswet deze week naar de kamer gaat en zo nee, waarom niet. Ook wilde ze weten of de systemen al zijn stilgelegd en wat de gevolgen van de uitspraak van het Europese Hof heeft voor lopende strafzaken en het verzamelen van meta-data door de inlichtingendiensten.

Staatssecretaris Teeven antwoordde dat het volledige arrest eerst bestudeerd moet worden alvorens er een uitspraak kan worden gedaan omtrent een intrekkingswet of het stilleggen van systemen. Op de vraag over de gevolgen voor lopende strafzaken op basis van reeds verzamelde gegevens en het opslaan van meta-data door de inlichtingendiensten antwoordde hij dat er geen gevolgen zijn omdat deze gegevens op basis van andere wetgeving worden verzameld.

Cops in cyberspace Blog

Even wat nieuws van het openbronnen-front: sinds 1 april 2014 is het openbare register met ‘bewinden’, oftewel wie er onder curatele is gesteld, uitgebreid. Nieuw is dat ook gevallen worden opgenomen waarin over het vermogen van personen bewind is uitgesproken, mits die vermogens onder bewind gesteld zijn vanwege ‘verkwisting’ en/of ‘problematische schulden’.

Actievoerders maken foto’s van politiemensen, beveiligers maken foto’s van actievoerders en de politie fotografeert iedereen. Maar de politie moet nog leren hoe ze met dit soort nieuwe media moeten omgaan, vindt ‘activist journalist’ Margo Kinston. Zij maakte foto’s toen demonstranten betoogden tegen de aanleg van een nieuwe kolenmijn. Kingston is nu aangeklaagd voor smaad en intimidatie. Op haar weblog zette ze onder meer een lijst met namen en foto’s van politiemensen in het Leard State Forest. In totaal werden bij de actie 82 actievoerders opgepakt. Kingston ontkent de dienders te willen beschadigen. ‘Iedereen wil gewoon vastleggen wat de ander doet’, zegt ze, verwijzend naar transparantie, openheid en mogelijke rechtszaken. Volgens de politie zijn agenten weliswaar ‘accountable to the public’ maar mag niet zomaar iedereen op de foto. ‘Police will not tolerate being harassed or intimidated’. Tja.

Computerbeveiliger Kaspersky Lab heeft een interactieve kaart gemaakt waarop – real time – te zien is waar cyberbedreigingen plaatsvinden. De kaart toont onder meer kwaadaardige objecten die tijdens on-access en on-demand scans, web antivirusdetecties en in e-mails worden ontdekt. Op de wereldbol blijkt Rusland het ‘#1 most-infected country’; Nederland staat (vandaag althans) 63e.

‘Dit kan iedereen overkomen’, waarschuwt Dallas Miller (21, uit White Creek, Tennessee) die haar grootste vrees zag uitkomen: haar facebookfoto’s werden ‘pontificaal’ in een escortadvertentie gebruikt. Millers foto’s stonden op advertentiesite Backpage.com, met de tekst ’100% satisfaction guaranteed’. Niks nieuws, vrijwel alle profielfoto’s op (nep-dating)sites die ‘seks met je buurvrouw’ beloven dan wel dat de afzendster ‘op zoek is naar jou’, staan al jarenlang op verschillende websites in verschillende landen. Hoe dan ook, Millers foto’s waren volgens haar gemaakt tijdens een benefiet-evenement voor misbruikte kinderen. Ze deed aangifte en vroeg Backpage de advertentie te verwijderen. Kopieën ervan zwerven, vermoedelijk nog vele jaren, over internet. Volgens de politie is de zaak lastig op te lossen ‘omdat internetmisdrijven vaak via valse accounts worden gepleegd. Van andere facebook’ers krijgt Miller vooral het advies beter op te letten: foto’s die privé zijn moet je privé houden. Ook de FBI zegt dat gebruikers vaker hun privacyinstellingen op netwerksites moeten controleren.

Volgens twee experts in cybercrime is de pakkans van cybercriminelen veel te laag. En dat kan tot gevolg hebben dat landen hun opsporingsbevoegdheden in het buitenland zelfstandig gaan uitbreiden: als de Nederlandse politie een server in Rusland hackt, mogen de Russen dan ook een Nederlandse server hacken? John Higgins, directeur van Digital Europe, en Lotte de Bruijn, directeur Nederland ICT, pleiten voor internationale afspraken om een veiliger digitaal domein te realiseren. Ze stellen dat het ‘internet of things’ – vrijwel alles is op internet aangesloten – behalve kansen ook gevaren in zich draagt: welke informatie wordt opgeslagen, wie beheert die data en wie heeft er toegang toe. Volgens Higgins en De Bruijn zijn de kansen die internet en ICT bieden, niet te benutten zonder goede afspraken hierover.

Een man (50, uit Weert) die wordt verdacht van het bezit van een half miljoen kinderpornoplaatjes is vrijgelaten. Volgens de rechter is de aanklacht van het OM ‘niet concreet genoeg’. In de stukken stond slechts globaal beschreven wat er op de plaatjes te zien is. Volgens de advocaat van de verdachte is het daarom onduidelijk waartegen de man zich moet verdedigen. De man werd in oktober 2013 aangehouden tijdens opnamen voor het tv-programma Undercover. SBS6-journalist Albert Stegeman had hem seks met een jong meisje beloofd.

De politierechter in Zwolle heeft een man (25, uit Rheezerveen) een voorwaardelijke straf opgelegd voor internetsmaad. De man had een financieel conflict met iemand, waarover hij op facebook schreef dat die man een dief was en onder meer webcamseks met minderjarige meisjes zou hebben. Het slachtoffer deed aangifte, maar de verdachte had er geen spijt van. ‘Ik zou het zo weer doen’. Voor de rechter was met name die opmerking reden om ‘een duidelijk signaal’ af te geven. Om te voorkomen dat de verdachte nogmaals zulke berichten op internet zet, kreeg deze een week voorwaardelijk en moet hij zijn slachtoffer zeshonderd euro schadevergoeding betalen.