Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Stop met gebruik Windows XP

Factsheet FS-2013-04
versie 1.0 | 30 oktober 2013

In 2001 heeft Microsoft het besturingssysteem Windows XP op de markt gebracht. Op 8 april 2014 krijgt dit besturingssysteem na 13 jaar de status 'end-of-life'[1]. Microsoft zal dan niet langer updates uitbrengen voor Windows XP. Als beveiligingslekken in Windows XP worden gevonden, zullen deze niet worden gedicht. Computers met Windows XP zullen dan kwetsbaar blijven. Het NCSC adviseert daarom computers met Windows XP voor april 2014 te vervangen of te voorzien van een besturingssysteem dat nog wel wordt ondersteund met (beveiligings)updates.

De belangrijkste feiten

- Microsoft zal vanaf 8 april 2014 geen updates meer uitbrengen voor Windows XP. Het besturingssysteem krijgt de status 'end-of-life'.
- Een computer die na april 2014 nog Windows XP gebruikt als besturingssysteem, zal kwetsbaar zijn en blijven voor aanvallen van buitenaf.
- Het NCSC adviseert om computers met Windows XP voor april 2014 te vervangen of te upgraden naar een besturingssysteem dat nog wel wordt ondersteund met updates.
- Nieuwere versies van Windows, zoals Windows 7 en 8, worden nog wel ondersteund. Hetzelfde geldt voor Linux-gebaseerde besturingssystemen als Ubuntu en Red Hat. Ook Mac OS X wordt ondersteund. Omdat Mac OS X niet werkt op computers met Windows XP, zal voor een overstap naar Mac OS X de aanschaf van een nieuwe computer nodig zijn.
- Het upgraden kan voor problemen zorgen bij de werking van geïnstalleerde programma's. Begin daarom op tijd met het plannen, testen en uitvoeren van de upgrade.
- Computers voor beheer en aansturing van medische of industriële apparatuur zijn soms niet te upgraden: er bestaan alternatieve maatregelen, maar die vereisen vrij intensief beheer.

Achtergrond

Op 10 april 2012 heeft Microsoft aangekondigd vanaf 8 april 2014 niet langer updates uit te zullen brengen voor het besturingssysteem Windows XP en de kantoorsoftware Office 2003[2]. Vooral Windows XP is nog bij veel thuisgebruikers en organisaties in gebruik: 2,7 miljoen thuisgebruikers en 40% van de computers in bedrijven gebruikten in april 2013 nog Windows XP[3]. Momenteel wordt alleen de meest recente versie van Windows XP, Service Pack 3, nog van updates voorzien: eerdere versies worden al langer niet meer ondersteund[4].

Wat is er aan de hand?

Bij veel software, ook bij Windows XP, worden na publicatie programmeerfouten gevonden. Sommige van die fouten beperken de werking van een systeem of laten het vastlopen, andere vormen een beveiligingsrisico. Deze stellen kwaadwillenden in staat om op een computersysteem in te breken. De leverancier van de software repareert deze fouten in volgende versies van de software, maar in de tussentijd zijn systemen die de huidige versie gebruiken dus kwetsbaar. Daarom worden door leveranciers regelmatig updates voor hun software uitgebracht. Het installeren van updates verhelpt

1 http://windows.microsoft.com/en-us/windows/products/lifecycle

2 https://blogs.technet.com/b/msrc/archive/2012/04/10/ windows-xp-and-office-2003-count-down-to-end-of-support-and-the-april-2012-bulletins.aspx

3 http://www.nu.nl/gadgets/3393144/27-miljoen-nederlanders-gebruiken-nog-windows-xp.html

4 Het NCSC heeft hier ook op gewezen in het derde Cybersecuritybeeld Nederland: https://www.ncsc.nl/actueel/nieuwsberichten/cybersecuritybeeld-nederland-kwetsbaarheid-van-ict-onverminderd-hoog.html

de dan bekende kwetsbaarheden die het gevolg zijn van de programmeerfouten.

Voor Windows XP zal Microsoft vanaf april 2014 niet langer updates uitbrengen. Nieuw ontdekte kwetsbaarheden zullen dan dus blijven bestaan. Antivirussoftware zal slechts een deel van de aanvallen op deze kwetsbaarheden kunnen tegenhouden. Het is echter ondenkbaar dat men alle aanvallen met behulp van antivirussoftware zal kunnen weerstaan. Hetzelfde geldt voor een firewall of een Intrusion Detection/Prevention System (IDS/IPS): het zal mogelijk een deel van de aanvallen tegenhouden, maar lang niet allemaal. Hoe dan ook is het nog maar de vraag of leveranciers van beveiligingssoftware die geschikt is voor Windows XP ook na april 2014 voor hun software op Windows XP ondersteuning zullen blijven bieden.

Sinds 2001, het jaar dat Windows XP werd uitgebracht, hebben clouddiensten en mobiele apparaten een vlucht genomen. In andere factsheets en whitepapers heeft het NCSC op de bijbehorende risico's gewezen. Van een besturingssysteem van de leeftijd van Windows XP valt niet te verwachten dat het met al deze nieuwe technologie en bijbehorende risico's om kan gaan.

Wat kan er gebeuren?

Een computer die na april 2014 nog Windows XP gebruikt als besturingssysteem, zal kwetsbaar zijn en blijven voor aanvallen van buitenaf. Zo lang Windows XP nog veel gebruikt wordt, valt te verwachten dat kwaadwillenden software zullen blijven ontwikkelen waarmee op grote schaal aanvallen kunnen worden uitgevoerd op computers met Windows XP. Het Team High Tech Crime van de politie signaleert dat dergelijke aanvallen momenteel worden voorbereid. De verwachting is dat kwaadwillenden deze willen uitvoeren nadat Windows XP de status 'end-of-life' heeft bereikt.

Een aanval op een kwetsbaar Windows XP-systeem kan op meerdere manieren plaatsvinden. Geïnfecteerd raken door het bezoeken van een besmette website of het openen van gevaarlijke e-mailbijlages komt veel voor, maar er zijn meer aanvalspaden. Elke computer die op enige manier met de buitenwereld in verbinding staat, kan in principe worden besmet. Deze verbinding kan direct zijn, via een netwerk- of internetverbinding, of indirect, via een besmette USB-stick of een met het netwerk verbonden printer.

Een aanvaller die een computer met malware besmet, heeft daarna vaak toegang tot alle informatie op de computer. Hij kan deze informatie naar believen inzien, wijzigen of verwijderen. De computer is dan niet meer geschikt voor het uitvoeren van vertrouwelijke handelingen zoals internetbankieren: transacties kunnen door de aanvaller worden ingezien en aangepast. Zonder dat de gebruiker het direct merkt, kan zo zijn bankrekening worden leeggeroofd. Daarnaast kan de aanvaller het computersysteem opdrachten uit laten voeren zoals het verzenden van spam of het inbreken op andere computersystemen: het lijkt dan of de eigenaar van de computer deze handelingen heeft verricht. De geïnfecteerde computer kan ook dienen als springplank voor verdere aanvallen op het interne computernetwerk. De aanvaller kan de computer tot slot ook lid maken van een botnet, een netwerk van geïnfecteerde computers. Een botnet kan worden gebruikt bij het uitvoeren van massale gedistribueerde aanvallen, zogeheten DDoS-aanvallen.

Een typische aanval: Ransomware

- Een computer die na april 2014 nog Windows XP gebruikt, is kwetsbaarder voor aanvallen met malware, zoals ransomware.
- Ransomware is software die bepaalde functionaliteit of informatie van de computer 'gijzelt' en om een geldbedrag vraagt. Betalen heeft echter geen zin.
- Het upgraden naar een besturingssysteem waarvoor wel updates uitkomen, helpt aanvallen met ransomware en andere malware voorkomen.
- Bent u besmet met ransomware? Raadpleeg het artikel 'Mijn computer is gekaapt en er wordt losgeld geëist, wat nu?' van de Waarschuwingsdienst.

Wat adviseert het NCSC?

De belangrijkste maatregel om te voorkomen dat een computer met Windows XP kwetsbaar blijft, is het installeren van een besturingssysteem dat nog wel wordt voorzien van updates. Microsoft heeft sinds Windows XP nog drie andere versies van Windows uitgebracht (Windows Vista, Windows 7 en Windows 8). Microsoft adviseert[5] om te upgraden naar Windows 7 of Windows 8.

Naast nieuwere versies van Windows bestaan er andere besturingssystemen die ook regelmatig van updates worden voorzien. Er zijn verschillende Linux-distributies die geschikt zijn voor persoonlijk en zakelijk gebruik. Ubuntu en Red Hat zijn hiervan twee populaire voorbeelden. Het is ook mogelijk om de computer zelf te vervangen. Dan kunt u ook kiezen voor een computer met besturingssysteem Mac OS X. Deze worden door Apple geleverd en ondersteund. Ook oudere versies van Mac OS X of Linux-gebaseerde systemen krijgen van tijd tot tijd de status 'end-of-life'. Ook voor gebruikers van deze besturingssystemen is het daarom van belang om een actuele versie te gebruiken.

Het is van belang te beseffen dat een upgrade ervoor kan zorgen dat sommige geïnstalleerde software het niet langer doet, omdat deze niet werkt op het nieuwe besturingssysteem. Software die is geschreven voor Windows zal niet zonder meer werken op Mac OS X of Linux-gebaseerde besturingssystemen. Ook werkt oudere software voor Windows XP soms niet op nieuwere versies van Windows[6]. De leverancier van uw software kan u hier verder over informeren.

5 https://www.microsoft.com/en-us/windows/endofsupport.aspx

6 Compatibiliteit tussen Windows-versies: http://technet.microsoft.com/en-us/library/ee461265%28v=ws.10%29.aspx

Nieuwere versies van Windows vereisen van een computer betere specificaties dan Windows XP vraagt. Het kan dus zijn dat een computer met Windows XP niet geüpgraded kan worden naar een nieuwere Windows-versie. Linux-distributies vergen soms[7] een minder krachtige computer. Wilt u toch Windows blijven gebruiken, dan zult u in voorkomende gevallen over moeten stappen naar een krachtiger computer.

Voor bedrijven die Windows XP gebruiken, is het migreren naar een ander besturingssysteem een aanzienlijk project. Men dient van alle applicaties die in gebruik zijn na te gaan of deze ook op het nieuwe besturingssysteem werken: software die niet werkt onder het nieuwe besturingssysteem moet worden herschreven, of er moeten alternatieven voor worden gevonden. Mogelijk gaat oudere hardware worden vervangen. Medewerkers hebben training nodig om met het nieuwe besturingssysteem overweg te kunnen. Een migratie zal, afhankelijk van de omvang en aard van de organisatie, al snel zes tot twaalf maanden vergen. Gebruikt uw organisatie nog Windows XP en bent u nog niet begonnen met de overstap, dan is nu het moment daarvoor. Uw IT-afdeling en -leveranciers zijn belangrijke partners in dit project: betrek hen bij elk onderdeel ervan.

Alternatieven voor upgraden

Het NCSC adviseert alle gebruikers en beheerders van computers met Windows XP met klem om over te stappen naar een ander besturingssysteem. Toch is dit voor sommige computers niet haalbaar. Aansturings- en beheersystemen voor medische of industriële apparatuur maken vaak gebruik van verouderde besturingssystemen. Het belang van de werking van deze computers maakt dat de beveiliging ervan extra aandacht vraagt. Aan de andere kant kunnen de besturingssystemen van deze computers soms eenvoudigweg niet worden bijgewerkt naar de laatste versie. Men zal dan alternatieve maatregelen moeten treffen om deze computers alsnog veilig te kunnen gebruiken.

Om een computer met Windows XP ook na april 2014 veilig te kunnen gebruiken, is het belangrijk om verbindingen met de buitenwereld tot een minimum te beperken. Idealiter betekent dit dat deze computer geen verbinding heeft met het internet, niet verbonden is met het kantoornetwerk en dat er geen externe media zoals USB-sticks in worden geplaatst. Is het toch nodig de computer met het kantoornetwerk of het internet te verbinden, gebruik deze verbinding dan alleen voor de strikt noodzakelijke handelingen. Installeer updates voor geïnstalleerde software als deze beschikbaar zijn. Schakel alle niet-noodzakelijke netwerkservices op de computer uit. Monitor de netwerkverbinding actief met een IDS of IPS (Intrusion Detection/Prevention System). Is het gebruik van externe media zoals USB-sticks noodzakelijk, formatteer deze dan voor gebruik op een vertrouwde (andere) computer. Scan gebruikte externe media ook regelmatig, bijvoorbeeld voor elk gebruik, op virussen met een vertrouwde (andere) computer.

Tot slot:

Na meer dan een decennium van trouwe dienst is de tijd gekomen om afscheid te nemen van Windows XP. Er zijn gelukkig meerdere goede alternatieven van verschillende leveranciers beschikbaar, maar de overgang zal moeite kosten, zowel voor zakelijk als thuisgebruik. Niets doen is geen optie: het vormt een groot risico om na april 2014 dit besturingssysteem te blijven gebruiken. De vraag is dus niet óf, maar wanneer u overstapt. Als u op 8 april klaar wilt zijn, is vandaag de beste dag om te beginnen. «

Handelingsperspectief:

1. Ga na of uw omgeving computers bevat met Windows XP. Zo ja, dan adviseert het NCSC u om te upgraden naar een ander besturingssysteem.
2. Inventariseer welke software er op uw computers met Windows XP geïnstalleerd is. Informeer bij de leverancier op welke andere besturingssystemen deze software ook werkt.
3. Kies een besturingssysteem dat nog wordt voorzien van updates, zoals Windows 7, Windows 8, Ubuntu of Red Hat. Baseer de keuze onder meer op de geschiktheid om software te draaien die u wilt gebruiken.
4. Overweeg om de computer zelf te vervangen. Naast de genoemde besturingssystemen is dan ook het gebruiken van Mac OS X een optie.
5. Richt een testcomputer in met het beoogde besturingssysteem. Test of gebruikte software ook op deze testcomputer werkt.
6. Kies een alternatief voor software die niet op het nieuwe besturingssysteem werkt. Laat software herschrijven voor het nieuwe besturingssysteem als alternatieven niet voldoen.
7. Start in overleg met uw IT-afdeling en uw IT-leveranciers een migratieproject om over te stappen van Windows XP naar uw nieuw gekozen besturingssysteem.
8. Bevat uw omgeving computers die, ongeacht de nadelen, niet kunnen worden geüpgraded? Pas dan aanvullende maatregelen toe om deze computers zoveel mogelijk af te schermen van het internet en potentiële aanvallers.

7 Systeemeisen voor Ubuntu: https://help.ubuntu.com/community/Installation/SystemRequirements

Uitgave van Nationaal Cyber Security Centrum, DefCERT, Microsoft en Team High Tech Crime.
Verder hebben bijgedragen: Atos, Capgemini, KPN (vanuit de MSP-ISAC) en Rabobank
Turfmarkt 147 | 2511 DP Den Haag
Postbus 117 | 2501 CC Den Haag
www.ncsc.nl | info@ncsc.nl
T 070 888 75 55 | F 070 888 75 50
Publicatienr: FS2013-04 v1.0 | Aan deze informatie kunnen geen rechten worden ontleend.