Nationaal Cyber Security Centrum
Ministerie van Veiligheid en Justitie

Software heeft een houdbaarheidsdatum

Hoe om te gaan met End-of-Life-aankondigingen

Factsheet FS-2015-03
versie 1.0 | 3 april 2015

Leveranciers kondigen regelmatig aan dat bepaalde versies van software niet langer ondersteund worden na een bepaalde datum. Deze datum wordt End-of-Life genoemd. Het is raadzaam om aankondigingen over End-of-Life van software in de gaten te houden en hier zo snel mogelijk actie op te ondernemen.

Software is na End-of-Life niet meer houdbaar en kan dan niet langer als veilig beschouwd worden. Werk daarom systemen zo snel mogelijk bij en vervang uitgefaseerde software.

Het is belangrijk voor een bedrijf om een goed beeld van de gebruikte software te hebben, zodat snel de impact van een End-of-Life-aankondiging kan worden ingeschat. Wanneer het overzicht van gebruikte software wordt uitgebreid met afhankelijkheden tussen de verschillende toepassingen, is er een beter beeld van de impact van een migratietraject.

De belangrijkste feiten

- Leveranciers doen regelmatig aankondigingen dat een bepaald product niet meer ondersteund zal worden. Deze datum wordt ook wel End-of-Life genoemd.
- Een softwarepakket waarin na de End-of-Life een kwetsbaarheid bekend wordt, zal kwetsbaar zijn en blijven voor aanvallen.
- Wanneer een End-of-Life-aankondiging wordt gedaan, begin dan zo snel mogelijk met het upgradeproces.
- Het upgraden kan mogelijk voor problemen zorgen bij de werking van andere programma's. Begin daarom op tijd met het plannen, testen en uitvoeren van upgrades.
- Voor veel software zijn alternatieven beschikbaar, al dan niet van andere leveranciers.
- Sommige systemen zoals medische of industriële apparatuur zijn niet te upgraden: er bestaan alternatieve maatregelen, maar die vereisen intensief beheer.

Wat is End-of-Life van software?

End-of-Life is de datum waarna een bepaald software product geen updates meer ontvangt. Regelmatig kondigen leveranciers End-of-Life van software aan. Het kan gaan om besturingssystemen, maar ook om andere soorten soft- en firmware. Vaak wordt een aankondiging van End-of-Life ruim van tevoren gedaan. Na die datum zal de leverancier geen updates meer verzorgen voor dit product.

Eerder is er bijvoorbeeld een aankondiging geweest voor het einde van ondersteuning van Windows XP.[1] Voor andere software geldt ook dat er aankondigingen worden gedaan, bijvoorbeeld Windows Server 2003[2], Ubuntu-distributies[3] of software van Adobe[4].

Samenwerkingspartners

Deze factsheet is tot stand gekomen in samenwerking met Microsoft, Agentschap Telecom, Belastingdienst en Nederlandse banken.

Doelgroep

Deze factsheet richt zich op beheerders van software en systemen. Heeft u de ondersteuning van uw werkplekken en servers uitbesteed, treed dan in overleg met uw leveranciers over hoe u hier het beste mee om kunt gaan.

[1] Zie ook de Factsheet 'Stop met gebruik Windows XP' (2013-04) https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/factsheets/factsheet-stop-met-gebruik-windows-xp.html
[2] Windows Server 2003 aankondiging: http://www.microsoft.com/en-us/server-cloud/products/windows-server-2003/
[3] Ubuntu release end of life: http://www.ubuntu.com/info/release-end-of-life
[4] Adobe Lifecycle Policy: https://www.adobe.com/support/products/enterprise/eol/

Bij veel software wordt na publicatie programmeerfouten gevonden. Sommige van die fouten beperken zich tot de werking van het systeem, andere vormen een beveiligingsrisico. Deze laatstgenoemde fouten stellen kwaadwillenden bijvoorbeeld in staat om op het 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 brengen leveranciers regelmatig updates uit voor hun software. Het installeren van updates verhelpt de dan bekende kwetsbaarheden die het gevolg zijn van die programmeerfouten.

Nieuw ontdekte kwetsbaarheden zullen na End-of-Life vaak niet meer worden gerepareerd. Antivirussoftware kan slechts een deel van de aanvallen op deze kwetsbaarheden tegenhouden. 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.

Wat kan er gebeuren?

Software die na End-of-Life nog gebruikt wordt, zal meer en meer kwetsbaar worden en blijven voor aanvallen. Een aanval op een kwetsbaar systeem kan op meerdere manieren plaatsvinden, afhankelijk van het type software. Dit kan bijvoorbeeld door het bezoeken van een besmette website of het openen van een gevaarlijke e-mailbijlage, maar er zijn meer aanvalspaden mogelijk. 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, maar ook indirect, via een besmette USB-stick of via andere apparaten die op hetzelfde netwerk zijn aangesloten, zoals printers.

Een aanvaller die een computer met kwaadaardige software infecteert, heeft daarna vaak toegang tot alle informatie op de computer, en vanaf daar kan hij proberen de aanval door te zetten naar alle aangesloten computers en/of apparatuur in het netwerk. Hij kan informatie naar believen inzien, wijzigen of verwijderen. De computer is dan niet meer geschikt voor het uitvoeren van vertrouwelijke handelingen of financiële transacties; deze transacties kunnen door de aanvaller worden ingezien en aangepast.

Wat kunt u doen?

De belangrijkste maatregel om te voorkomen dat een computer met niet-ondersteunde software kwetsbaar blijft, is het tijdig vervangen van deze niet-ondersteunde software.

Het is raadzaam om een goed overzicht bij te houden van gebruikte software. Houd End-of-Life-aankondigingen van software bij op basis van deze lijst. Deze aankondigingen worden vaak op de website van de leverancier gedaan of via een nieuwsbrief. Als een aankondiging gedaan wordt, start dan zo snel mogelijk met het plannen van migratietrajecten.

Leveranciers van software kondigen vaak tijdig aan dat een softwarepakket niet meer ondersteund zal worden, en bieden dan ook zelf alternatieven aan. Naast nieuwere versies van de software zijn er vaak alternatieven van andere leveranciers. Mocht een systeem software bevatten die niet te vervangen is, dan kan het te overwegen zijn het systeem in het geheel te vervangen.

Er zijn ook risico's verbonden aan het upgraden van software. Een upgrade kan ervoor zorgen dat andere afhankelijke software niet goed meer functioneert. Denk bijvoorbeeld aan software die afhankelijk is van een oudere versie van het besturingssysteem. Ook tussen verschillende programma's kunnen afhankelijkheden bestaan, bijvoorbeeld door de manier waarop informatie tussen programma's uitgewisseld wordt. De leverancier van uw software kan u hier verder over informeren.

Software Lifecycle Management

Software Lifecycle Management (SLM) is een continu proces dat speelt bij het aankopen, installeren, gebruiken en uitfaseren van software. Goed doordacht SLM zorgt voor voorspelbaarheid in softwarebeheer en verkleint de kans op misbruik van kwetsbaarheden.

SLM bestaat uit verschillende fases die de hele levenscyclus van software omvatten. Het gaat dan om de aanschaffase, de implementatie- en configuratiefase, de productiefase, met daarbij een wijzigingsproces, de onderhoudsfase en uiteindelijk het uitfaseren. Aan het einde van de levensduur van de software begint deze cyclus weer van voren af aan.

End-of-Life speelt een rol bij verschillende fases van SLM:

- Betrek bij de keuze van **aan te schaffen software** welk proces de leverancier heeft om fouten en kwetsbaarheden op te lossen.
- Installeer tijdens de **productiefase** updates zo spoedig mogelijk. Geef beveiligingsupdates de hoogste prioriteit om zo kwetsbaarheden in de software te verhelpen.
- Houd tijdens de **onderhoudsfase** de berichtgeving van de leverancier bij. Deze zal aankondigingen van updates en End-of-Life publiceren. Ontvangt u een aankondiging van End-of-Life terwijl u de betreffende software nog gebruikt, vervang dan de software door een nieuwe versie of alternatief om te voorkomen dat uw organisatie kwetsbaar wordt na het verstrijken van End-of-Life.

Het migreren van software kan een aanzienlijk project zijn. Men dient voor alle software te bekijken wat de afhankelijkheden zijn tussen de verschillende software, en daarna te bekijken of deze nog steeds werken met de nieuwere versies. Mogelijk moet er dan naar alternatieven gezocht worden, of zelfs hardware vervangen worden. Medewerkers hebben vaak training nodig om met de nieuwe software om te kunnen gaan.

Een softwaremigratietraject kost meer of minder tijd afhankelijk van de aard van de software en van de omvang van de organisatie. Bij kleine pakketten kan het binnen een maand gebeuren, bij grotere pakketten, zoals besturingssystemen, kan dit in de orde van zes tot twaalf maanden zijn. Uw IT-afdeling en –leveranciers zijn belangrijke partners in dit soort migratietrajecten: betrek hen bij elk onderdeel.

Alternatieven voor upgraden

Het NCSC adviseert alle gebruikers en beheerders van computers met uitgefaseerde software met klem om over te stappen naar andere wel-ondersteunde software. Toch is dit voor sommige systemen niet haalbaar. Aansturings- en beheersystemen voor medische of industriële apparatuur maken vaak gebruik van verouderde software. Het belang van de werking van deze computers maakt dat de beveiliging ervan extra aandacht vergt. Tref waar nodig alternatieve maatregelen om risico's te mitigeren.

Smartphones en tablets

Mobiele apparaten, zoals smartphones en tablets, hebben ook een eigen besturingssysteem dat regelmatig moet worden bijgewerkt. Fabrikanten kondigen regelmatig nieuwe versies aan en geven daarbij aan welke apparaten wel en niet meer ondersteund worden. Voor mobiele apparaten waarvan het besturingssysteem niet meer zal worden geüpdatet, geldt hetzelfde advies als voor computers: zo snel mogelijk vervangen.

Voor software op mobiele apparaten ('apps') geldt ook het advies dat updates zo snel mogelijk geïnstalleerd moeten worden. Deze updates komen regelmatig uit en worden via de 'app-stores' of op het apparaat aangekondigd.

Helaas worden er voor niet meer ondersteunde apps meestal geen aankondigingen van End-of-Life uitgestuurd. Hiervoor adviseren we de website van de leverancier in de gaten te houden en bij twijfel contact op te nemen met de leverancier.

Mocht het onmogelijk zijn om een computer met uitgefaseerde software te updaten of te vervangen, dan zijn er verschillende maatregelen die de kans op besmetting of inbraak kunnen verkleinen:

- Het is belangrijk om verbinding 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 netwerk en dat er geen externe media zoals USB-sticks in worden geplaatst.
- Mocht het noodzakelijk blijken de computer met het kantoornetwerk of het internet te verbinden, gebruik deze verbinding dan alleen voor de strikt noodzakelijke handelingen of plaats het systeem in een gesegmenteerd deel van het netwerk.
- Installeer updates voor de andere geïnstalleerde software als deze beschikbaar zijn.
- Schakel niet-noodzakelijke netwerkservices op de computer uit.
- Laat de computer alleen gebruiken met lokale accounts; log niet meer in met bedrijfs- en beheerdersaccounts.
- 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

Software heeft net als andere producten een beperkte levensduur. Tijdens de levensduur van een softwarepakket brengt de leverancier periodiek updates uit om software bij te werken. Het is van belang updates zo snel mogelijk te installeren. Voor veel software geldt dat de levensduur niet oneindig is. Leveranciers beëindigen dan een productlijn, of maken een nieuw alternatief. Voor het oude product zal dan een aankondiging van End-of-Life worden gedaan. Zorg dat er een goed overzicht van de gebruikte software is, zodat aankondigingen opgemerkt worden en er tijdig migratietrajecten gestart worden.

Handelingsperspectief

1. Zorg voor een goede inventarisatie van gebruikte software op alle systemen.
2. Breng in kaart wat de afhankelijkheden zijn van én tussen de gebruikte software en systemen. Zorg dat dit overzicht continu bijgewerkt blijft.
3. Kies bij aanschaf van software voor producten die nog worden onderhouden. Baseer de keuze onder meer op de compatibiliteit met andere gebruikte software.
4. Houd aankondigingen van de sofwareleverancier in de gaten om tijdig op de hoogte te zijn van de End-of-Life.
5. Start in overleg met uw IT-afdeling en uw IT-leveranciers tijdig een migratieproject om over te stappen van software waar een aankondiging van End-of-Life voor is gedaan.
6. Bevat uw omgeving computers die, ongeacht de nadelen, niet kunnen worden geüpgraded? Neem dan aanvullende maatregelen om deze computers zoveel mogelijk af te schermen van het lokale netwerk, het internet en potentiële aanvallers.

Uitgave van **Nationaal Cyber Security Centrum**
Turfmarkt 147 | 2511 DP Den Haag
Postbus 117 | 2501 CC Den Haag
www.ncsc.nl | info@ncsc.nl | T 070-751 55 55
Publicatienr: FS-2015-03 1.0 | Aan deze informatie kunnen geen rechten worden ontleend.