Robert Fransen is consultant bij RCenter.

Windows XP na Service Pack 2

ALLE POORTEN DICHT

Windows XP Service Pack 2 (SP2) is meer dan een service pack. Met SP2 introduceert Microsoft een aantal veranderingen en uitbreidingen op het gebied van beveiliging. Deze verbeteringen moeten er voor zorgen dat Windows XP beter bestand is tegen aanvallen van virussen, wormen en andere kwaadwillende zaken. SP2 brengt behoorlijk wat veranderingen met zich mee en deze zijn niet alleen door de eindgebruikers te merken; beheerders en ontwikkelaars krijgen hier zeker mee te maken. Deze toegenomen veiligheid van Windows XP heeft namelijk wel een prijs. Sommige applicaties zullen niet zondermeer werken nadat SP2 is geïnstalleerd.

Reden genoeg om eens grondig te onderzoeken wat de doelstellingen en de gevolgen zijn van SP2. Een bekend probleem is dat veel organisaties de beveiligingspatches en updates niet onmiddellijk kunnen of willen uitrollen zodra deze beschikbaar worden. Elk beveiligingsbulletin dat Microsoft uitgeeft, bevat informatie die klanten kunnen gebruiken om risico's in te schatten. Deze informatie wordt echter ook misbruikt om malafide code te schrijven. De beveiligingstechnologieën die Windows XP SP2 introduceert zorgen er voor dat het moeilijker wordt een Windows XP-computer aan te vallen - ook als deze niet is voorzien van de laatste patches en updates. De beveiligingstechnologieën die Windows XP SP2 introduceert zijn in vier groepen te verdelen: betere netwerkbeveiliging, geheugenbeveiliging, betere beveiliging voor email- en instant messaging-applicaties, veiliger browsen. Bovendien zijn er nog diverse andere verbeteringen. In tabel 1 is te zien wat de implicaties zijn van de nieuwe beveiligingstechnologieën.

Betere netwerkbeveiliging

Deze beveiligingstechnologieën helpen bij een betere beveiliging tegen aanvallen via het netwerk, zoals Blaster. De belangrijkste verandering is dat Windows XP nu standaard voorzien is van een firewall en deze standaard aanstaat. Voor de komst van SP2 moest per internetverbinding de Internet Connection Firewall (ICF) aangezet worden. De Windows Firewall houdt voor alle verbindingen alle poorten gesloten als deze niet worden gebruikt. Het kwetsbare gebied van RPC-services wordt verkleind door geen anonieme calls meer te accepteren. Om een RPC-Service te gebruiken is authenticatie nodig. Hiermee wordt weerstand geboden tegen bijvoorbeeld Trojan Horses die anoniem een gevonden buffer-overrun gebruiken. In SP2 zijn twee wijzigingen aangebracht in het gedrag van DCOM (Distributed Component Object Model). Zo worden extra toegangsverificaties uitgevoerd bij elke aanroep, activering of startactie van een COM-server.

Geheugenbeveiliging

Sommige aanvallen van kwaadwillige software maken misbruik van een bekend trucje door te veel gegevens te kopiëren naar gebieden in het geheugen van de computer. Deze zwakke plekken worden buffer-overruns genoemd. Microsoft werkt samen met fabrikanten van microprocessoren aan de ondersteuning voor hardwarematige 'no execute'-functies (of NX) op microprocessoren met deze voorziening. NX gebruikt de CPU zelf om de scheiding tussen applicatiecode en gegevens af te dwingen. Zo wordt voorkomen dat een applicatie of Windows-component programmacode uitvoert die een worm of virus in een gedeelte van het geheugen heeft geplaatst dat alleen bestemd is voor gegevens.

Veiliger e-mail

De nieuwe beveiligingstechnologieën voor attachments helpen virussen buiten de deur te houden die zich verspreiden via e-mail en instant messaging. Service Pack 2 introduceert 'Attachment Execution Service'. Outlook Express en Windows Messenger maken hier gebruik van en bieden verbeterde controle van attachments. Mogelijk onveilige attachments worden geïsoleerd.

Veiliger browsen

De nieuwe beveiligingstechnologieën die deel uitmaken van Internet Explorer bieden verbeterde beveiliging tegen schadelijke webcontent. Eén van de veranderingen is het vergrendelen van de Local Machine Zone. Mocht een kwaadwillend script op de harde schijf terecht zijn gekomen, dan kan deze niet worden uitgevoerd. Bovendien is de gebruikersinterface verbeterd. Deze helpt voorkomen dat ongewenste ActiveX-controls en spyware worden uitgevoerd zonder dat de gebruiker dit in de gaten heeft; of de uitvoering expliciet heeft toegestaan.
Zoals je kunt zien hebben al deze veranderingen effect op applicaties - en dan vooral wanneer er communicatie is tussen applicaties. De belangrijkste veranderingen zullen nu in detail behandeld worden.

Windows Firewall

Windows Firewall - voorheen de Internet Connection Firewall genaamd - omvat een keur aan nieuwe voorzieningen en is standaard ingeschakeld. Dit kan van invloed zijn op bestaande appli-

Verandering van Windows XP SP2	Webontwikkelaars	Applicatie- ontwikkelaars	Netwerkbeheerders	Eindgebruikers
Betere netwerkbeveiliging	X	X	X	X
Nieuwe geheugenbeveiliging		X		
Verbeterde beveiliging van e-mail		X	X	X
Veiliger browsen	X	X	X	X

Tabel 1.
Overzicht van implicaties van de nieuwe beveiligingstechnologieën

caties als de applicatie niet standaard werkt met stateful filtering. Als bijvoorbeeld een applicatie berichten verwacht van een andere computer zonder eerst zelf de communicatie te initialiseren, zal deze vastlopen op de firewall. Voor veel applicaties is echter geen aanpassing nodig. Bij uitgaand verkeer wordt automatisch de juiste poort geopend. Tijdens het booten is Windows XP nu ook beveiligd. In eerdere versies van Windows is er een tijdsinterval tussen het starten van de netwerkstack en het inschakelen van Firewall. Een pakket kon dus worden ontvangen en afgeleverd bij een service zonder dat firewall het filterde: een mogelijke zwakke plek. In SP2 heeft de firewall driver een statische regel genaamd *boot-time policy* die direct zorgt voor stateful filtering, en die basisnetwerktaken zoals DNS en DHCP en communicatie met de domain controller toestaat. Zodra de firewall-service actief is, wordt de *run-time Windows Firewall policy* geladen en toegepast en worden de opstart-tijdfilters verwijderd. Mocht de firewall Service niet willen starten dan blijven de boot-time policies van kracht.

Applicaties die inkomend verkeer verwachten

Sommige applicaties werken als client en als server. Als een serverapplicatie binnenkomend netwerkverkeer kan verwachten, dan zullen we nu actie moeten nemen. Voorafgaand aan SP2 moesten applicaties de API's van de firewall aanroepen om de benodigde poorten te openen zodat berichten konden worden ontvangen. Dit bleek moeilijk in peer-to-peer situaties waarbij de poort niet van tevoren bekend was. Bovendien was het de verantwoordelijkheid van de applicatie om de poort weer te sluiten, wat de mogelijkheid bood tot het overbodig open staan van de poort als de applicatie onverwachts stopte. Overigens konden deze poorten alleen worden geopend door applicaties die werden gedraaid in de beveiligingscontext van een lokale beheerder. In SP2 moet een applicatie die naar het netwerk moet kunnen luisteren, worden toegevoegd aan de *Windows Firewall Exception List*. Als een applicatie voorkomt op deze lijst, worden alleen de benodigde poorten geopend én alleen gedurende de tijd dat de applicatie deze gebruikt om te luisteren. Dit voorkomt dat een applicatie een poort opent die niet wordt gebruikt en zo opzettelijk of per ongeluk een andere applicatie of service zichtbaar maakt voor netwerkverkeer via die poort. Bovendien kunnen applicaties die luisteren naar het netwerk op deze manier worden uitgevoerd onder normale rechten en niet als beheerder. Applicaties die niet naar netwerkpoorten luisteren, hoeven niet op deze Application Permission List te worden geplaatst. Alleen beheerders kunnen trouwens een applicatie toevoegen aan deze lijst; zie afbeelding 1.

Afbeelding 1. Windows Firewall exceptions

Afbeelding 2. Windows Firewall Security Alert

Gebruikers kunnen worden geconfronteerd met een dialoogscherm om aan te geven of ze de desbetreffende applicatie toestemming geven om bepaalde poorten te open. U zult er rekening mee moeten houden dat een gebruiker wel eens *nee* kan zeggen. Ook kan het gebeuren dat de gebruiker deze dialoogbox nooit ziet, denk maar aan games die de hele beeldschermaansturing overnemen; zie afbeelding 2.

Services met inkomend verkeer

In scenario's bij services zoals het delen van bestanden en printers en remote desktop, waarbij Windows XP een inkomende verbinding met een service moet accepteren, moet mogelijk een gedeelte van de code worden aangepast. Hoewel ontwikkelaars wordt geadviseerd de AuthorizedApplication-API's te gebruiken voor alle andere scenario's, worden de Global Port-API's van Windows Firewall aangeraden voor services die gebruikmaken van vaste poorten. Aangezien deze poorten altijd geopend zijn, is het nauwelijks voordelig om deze poorten dynamisch te openen. In plaats hiervan hebben gebruikers de mogelijkheid om de firewall-instellingen voor deze vaste poorten aan te passen wanneer de Global Port-API's worden gebruikt. Als een service moet luisteren naar een vaste poort, moet de gebruiker worden gevraagd of hij/zij de service wil toestaan om poorten in de firewall te openen.

Ondersteuning van Remote Procedure Calls (RPC)

Bepaalde applicaties en/of services gebruiken voor inkomende verbindingen RPC-poorten, hetzij via DCOM hetzij direct via RPC. Gezien de aanzienlijke gevolgen voor de beveiliging bij het openen van RPC-poorten, worden deze poorten op een aparte manier behandeld. In eerdere versies van Windows blokkeerde Internet Connection Firewall alle RPC-communicatie, waardoor functies zoals het delen van bestanden en printers en remote beheer niet werkten. De oorzaak hiervan was dat de bestandsnaam van het RPC process-image dezelfde was voor veel RPC-servers (svchost.exe). Op een gemiddeld werkstation draaien standaard ongeveer 60 RPC-servers die allemaal luisteren naar client-opdrachten. Ontwikkelaars wordt aangeraden RPC via firewall alleen in te schakelen als dit absoluut noodzakelijk is. In SP2 bevat de Windows-firewall een expliciete instelling waarmee poorten voor RPC automatisch kunnen worden geopend en gesloten. Applicaties en services hoeven dus niet specifieke poorten te openen om RPC te kunnen gebruiken voor inkomende verbindingen. RPC wordt echter wel standaard geblokkeerd door firewall. SP2 biedt fijnmazig toezicht over welke RPC-services de Windows Firewall mag doorkruisen. Wanneer een poort wordt geopend, kan een oproeper beweren dat de poort zal worden gebruikt voor RPC. De Windows Firewall accepteert deze bewering alleen wanneer deze vanuit de beveiligingscontext Lokaal systeem, Netwerkservice of Lokale service wordt aangeroepen. De Windows Firewall ondersteunt een registry-key die toestaat dat RPC-poorten worden geopend, zelfs als de oproeper niet voorkomt op de Application Permission List: *PrivilegedRpcServerPermission*. Dankzij de modulaire structuur kunnen beheerders regelen welke RPC-services zichtbaar zijn op het netwerk, zodat de communicatie kan worden beperkt tot die services die het nodig hebben.

'On with no exceptions' modus

In het geval een zwakke plek wordt ontdekt, en een kwaadwillende applicatie wordt los gelaten voordat een beveiligingsupdate beschikbaar is, introduceert SP2 een instelling voor firewall genaamd 'On with no exceptions' modus. Met deze modus kunnen gebruikers zichzelf eenvoudig beschermen door de firewall zo in te stellen dat al het ongewenste inkomende verkeer wordt tegengehouden tot er een patch beschikbaar is, zonder de firewall opnieuw te hoeven configureren. In deze modus zal de computer niet luisteren naar aanvragen die afkomstig zijn van het netwerk. Uitgaande verbindingen zijn de enige verbindingen die kunnen worden gemaakt.

Support voor IPv6

Service Pack 2 voorziet Windows XP nu ook standaard met het internetprotocol versie 6 (IPv6). Dit was voorheen onderdeel van het 'Advanced Networking Pack for Windows XP'. De Windows Firewall ondersteunt ook IPv6, voorheen was er een aparte firewall-service voor IPv6. De instellingen van de firewall zijn voor beide protocollen gelijk.

File Sharing

Op het gebied van *File and Printer Sharing* zijn er ook veranderingen waar we rekening mee moeten houden. Normaal gesproken als we File and Printer Sharing aanzetten geldt dat globaal voor alle netwerkverbindingen en ongeacht waar het verkeer vandaan komt; het locale netwerk of van het internet. Na installatie van SP2 kunnen we per poort opgeven van welk netwerkadres we verkeer toestaan. De standaardinstelling voor file-sharing is *local subnet*. Hierdoor wordt in eerste instantie het delen van bestanden tot de directe omgeving beperkt. Voor een thuisnetwerk of afdeling is dit natuurlijk prima, maar dit kan toch al gauw tot problemen leiden bij simpele toepassingen als Access, dBASE of FoxPro of waar databasebestanden gezamenlijk gebruikt worden. Zelfs een klein netwerk bestaat vaak uit meer subnets, denk bijvoorbeeld aan een netwerkomgeving die bestaat uit UTP-bekabeling en een wireless netwerk. We kunnen via de NetShare-API, Network Setup Wizard of de firewall-gebruikersinterface aangeven welke netwerkadressen we allemaal toestaan.

RPC-interface-restrictie

In SP2 heeft Microsoft een aantal wijzigingen aangebracht in de RPC-infrastructuur (Remote Procedure Calls) dat RPC-interfaces standaard veiliger maakt en dit kwetsbare gebied verkleinen. Interface-restrictie, die is bepaald door een nieuwe registry-key met de naam RestrictRemoteClients, wijzigt het gedrag van alle interfaces voor RPC-oproepen op het systeem en voorkomt standaard alle anonieme externe toegang tot RPC-interfaces op het systeem, enkele uitzonderingen daargelaten. In de praktijk vereist RPC-interface-restrictie dat alle oproepers worden geverifieerd. Als u COM alleen gebruikt voor in-process COM-componenten, heeft SP2 geen invloed op de applicatie.

De registry-key RestrictRemoteClients dwingt RPC enkele extra beveiligingscontroles uit te voeren voor alle interfaces, zelfs als de interface geen geregistreerde beveiligings-callback heeft. Als de RPC-applicatie oproepen verwacht te ontvangen van anonieme externe RPC-clients, kan deze wijziging van invloed zijn op de applicatie. U hebt drie opties om ervoor te zorgen dat de applicatie op de gewenste manier blijft werken:

1. U kunt eisen dat RPC-clients RPC-beveiliging gebruiken als zij contact opnemen met de serverapplicatie. Dit is de beste methode om beveiligingsrisico's te beperken.
3. U kunt een uitzondering maken voor een interface door RPC_IF_ALLOW_CALLBACKS_WITH_NO_AUTH op te geven tijdens de registratie van de interface. Hiermee configureert u RPC zo dat anonieme verbindingen worden toegestaan, maar alleen voor de interface in kwestie.
4. U kunt de registry-key instellen op RPC_RESTRICT_REMOTE_CLIENT_NONE (0) om af te dwingen dat RPC zich gedraagt zoals in eerdere versies van Windows.

De RestrictRemoteClients Registry Key (\\HKLM\SOFTWARE\Policies\Microsoft\Windows NT\RPC\) kent nog de volgende waarden: RPC_RESTRICT_REMOTE_CLIENT_DEFAULT (1) dit is de standaardwaarde ook als die niet aanwezig is. En RPC_RESTRICT_REMOTE_CLIENT_HIGH (2) zorgt er voor dat er ook geen anonieme RPC-calls binnenkomen. Ook uitzonderingen als RPC_IF_ALLOW_CALLBACKS_WITH_NO_AUTH worden niet doorgelaten.
Door toevoeging van de vlag RestrictRemoteClients is de endpoint mapper-interface standaard niet meer anoniem toegankelijk. Dit is een aanzienlijke verbetering van de beveiliging, maar zorgt ook voor een probleem bij het bepalen van een dynamisch endpoint. Momenteel voert een RPC-client eerst een anonieme call naar de endpoint-mapper om een dynamisch endpoint te bepalen. Deze vraag wordt normaal anoniem uitgevoerd, zelfs als de oproep van RPC-client daarna wordt uitgevoerd met RPC-beveiliging. Anonieme oproepen naar de endpoint mapper-interface mislukken in Windows XP SP2 als gevolg van de standaardwaarde voor de nieuwe key RestrictRemoteClients. Om dit probleem op te lossen is het noodzakelijk de RPC-client aan te passen zodat deze een verifieerbare oproep doet naar de endpoint-mapper. Als de key EnableAuthEpResolution wordt ingesteld, gebruikt de RPC-client NTLM authenticatie om zich bij de endpoint mapper te laten verifiëren. Deze verifieerbare aanvraag vindt alleen plaats als de daadwerkelijke RPC-clientoproep die wordt gemaakt, ook gebruikmaakt van RPC-verificatie. Kortom, anonieme Remote Procedure Calls behoren tot het verleden.

Wijzigingen in DCOM

In SP2 zijn twee wijzigingen aangebracht in het gedrag van DCOM (Distributed Component Object Model) te weten: restricties voor de hele computer en modulaire COM-machtigingen. Als u COM alleen gebruikt voor in-process COM-componenten, heeft SP2 geen invloed op de applicatie.

Restricties voor de hele computer

Restricties voor de hele computer bieden een extra controle waarbij elke oproep, activering of startactie van een COM-server op de computer worden gecontroleerd op basis van een Access Control List (ACL). Als de toegangscontrole mislukt wordt de oproep, activering of startactie geweigerd. Deze restricties beperken het risico van de zwakke instellingen die worden gebruikt door veel COM-applicaties en bieden beheerders een beter begrip van de beveiligingsinstellingen voor alle registreerde COM-applicaties op een computer. Bovendien geven ze de beheerder de mogelijkheid om inkomende DCOM-activering, -startactie en -oproepen uit te schakelen. De eenvoudigste manier om deze toegangscontroles voor te stellen is als een extra controle die wordt uitgevoerd op basis van een Access Control List voor elke oproep, activering of startactie van een COM-server op de computer. Als de toegangscontrole mislukt wordt de oproep, activering of startactie geweigerd. Deze controle biedt een minimale verificatiebarrière die moet worden genomen om toegang te krijgen tot COM-servers op het systeem. Er is een ACL voor de hele computer voor startmachtigingen (ter bescherming tegen activerings- en startacties) en een ACL voor de hele computer voor toegangsmachtigingen (ter bescherming tegen oproepen). Deze kunnen worden geconfigureerd via de Component Services MMC snap-in. Deze wijzigingen in DCOM-aanroepen kunnen van invloed zijn op bepaalde applicaties. Vooral als een applicatie ervan afhankelijk is dat iedereen standaard RCP-machtigingen heeft, kan SP2 het onmogelijk maken waarvoor ongeverifieerde externe oproepen nodig zijn. Na installatie van SP2 zijn de meeste COM-clientscenario's mogelijk, waaronder het gangbare geval waarbij een COM-client een lokale verwijzing doorgeeft aan een externe server, waarbij

de client eigenlijk een server wordt. Met SP2 zouden alle lokale scenario's moeten werken zonder aanpassing van de software of het besturingssysteem.

Modulaire COM-machtigingen

Modulaire COM-machtigingen (permission) geven beheerders de flexibiliteit om de COM-permission policy van een computer te regelen op basis van het concept 'afstand'. In huidige Windows XP-systemen hebben gebruikers, als zij toegang hebben tot een COM-serverapplicatie, toegang voor zowel lokaal als extern gebruik. De COM-serverapplicatie biedt geen mogelijkheid voor nauwkeuriger controle. Met SP2 kunnen beheerders wel de COM-permission policy regelen op basis van het concept 'afstand'. De twee afstanden in SP2 zijn *lokaal* en *extern*. Bij lokaal komt het COM-bericht binnen via het LRPC-protocol, terwijl bij extern COM-berichten binnenkomen via een extern RPC-protocol zoals TCP. De wetenschap dat een RPC-oproep afkomstig is van een externe bron en dus minder (of geen) toestemming moet krijgen, beperkt het risico van aanvallen via het netwerk.
In SP2 is COM ook aangepast met een onderscheid tussen oproep- en activeringspermissie. Bovendien zijn de activeringsmachtigingen verplaatst van de lijst met ACL naar de ACL met startmachtigingen. Dit biedt ondersteuning voor COM-servers waarvoor ongeverifieerde toegang nodig is ter ondersteuning van callbacks terwijl er wel beperkingen gelden voor wie een eerste objectverwijzing kan krijgen in de vorm van beperkte activeringsrechten. In plaats van slecht onderscheid tussen lokaal en extern te maken, worden vier rechten onderscheiden: lokaal starten (LL: local launch), extern starten (RL: remote launch), lokaal activeren (LA: local activate) en extern activeren (RA: remote activate). Dit geeft maximale compatibiliteit, waarbij externe activering toch is beperkt tot de beheerder. Dit geeft een flexibel, consistent model. Bovendien kan het systeem hiermee worden ingesteld op het toestaan van anonieme oproepen terwijl activering toch kan worden geregeld. Aangezien zowel activerings- als startacties zijn gerelateerd aan het verkrijgen van een interface-pointer, horen activerings- en startacties logischerwijs thuis in dezelfde ACL. Aangezien startmachtigingen altijd worden opgegeven via configuratie in tegenstelling tot toegangsmachtigingen, die vaak programmatisch worden opgegeven, geeft plaatsing van de activeringsmachtiging in de lijst met startmachtigingen de beheerder de controle over activering. Er zijn geen compatibiliteitsproblemen met COM-applicaties die de standaard beveiligingsinstellingen gebruiken.

Geheugenbeveiliging in SP2

Memory protection of execution protection (NX of no execute) is een voorziening van het besturingssysteem die gebruikmaakt van de hardware van de processor om geheugen te markeren met een attribuut dat aangeeft dat geen code mag worden uitgevoerd vanuit dat geheugen. Dit biedt een beveiliging tegen misbruik van bufferoverruns. Memory protection werkt per pagina virtueel geheugen en maakt gebruik van een bit in de PTE-tabel (Page Table Entry) om de geheugenpagina te markeren. Memory protection voorkomt dat code wordt uitgevoerd vanuit gegevenspagina's zoals de heap, diverse stacks en geheugenpools. Beveiliging kan worden toegepast in zowel gebruikers- als kernel-modus. Aangezien memory protection voorkomt dat gegevens worden uitgevoerd vanuit de stack, zou de specifieke zwakke plek waarvan de laatste MSBlaster-worm misbruik maakt, hebben geresulteerd in een schending van de toegang tot het geheugen en zou het proces zijn beëindigd.

Op een systeem met execution protection, zou MSBlaster beperkt zijn gebleven tot een DoS-aanval (Denial-of-Service), maar zou het virus niet de mogelijkheid hebben gehad om zich te vermenigvuldigen en te verspreiden naar andere systemen.

De eigenlijke hardwarematige implementatie van execution protection en markering van virtuele geheugenpagina's verschilt per processorarchitectuur. Processoren die execution protection ondersteunen zorgen voor een exception wanneer code wordt uitgevoerd vanaf een pagina die is gemarkeerd met het betreffende attribuut. De 32-bits versie van Windows maakt momenteel gebruik van de NX-voorziening van processoren, zoals gedefinieerd in de AMD64 Architecture Programmer's Manual. Voor deze processorvoorziening moet de processor worden gebruikt in PAE-modus (Physical Address Extension). Hoewel op het moment alleen de AMD K8-serie en de Intel Itanium Processor-serie geschikt zijn voor hardwarematige ondersteuning van memory protection, ligt het in de lijn der verwachtingen dat toekomstige 32- en 64-bits processoren memory protection bieden. Microsoft loopt vooruit op deze trend en moedigt deze aan door execution protection te ondersteunen in de toonaangevende Windows-besturingssystemen.
Het gedrag van bepaalde applicaties is naar verwachting niet compatibel met execution protection. Applicaties die dynamische code genereren - en de gegenereerde code niet expliciet markeren met execution permission - kunnen compatibiliteitsproblemen ondervinden met execution protection. Ook applicaties die code vanuit de process-stack of heap uitvoeren moeten extra aandacht besteden aan de vereisten van execution protection. Zoals bekend maakt Microsoft .NET gebruik van een JIT-compiler (Just In Time). De oude versie van de CLR (Common Language Runtime) is niet compatibel met execution protection. SP2 zal een geüpdate versie van het .NET Framework leveren die zonder probleem werkt als de NX-bit is ingesteld. Er zijn managed applicaties en componenten die een speciale versie van de CLR vereisen. SP2 zorgt dat deze applicaties blijven werken op de 'oude' CLR door de NX-bit uit te zetten. Het advies is echter om zo de laatste versie van de CLR te gebruiken.

Het advies is om de laatste versie van de CLR te gebruiken na installatie van SP2

Ontwikkelaars van drivers moeten rekening houden met execution protection en de vereisten van de software die wordt uitgevoerd op een ondersteunend platform. De meeste drivers voor Windows XP 64-bit Edition zijn getest door Microsoft. Bij 32-bits drivers echter die code generen of DMA gebruiken kunnen we problemen verwachten.

Applicaties (in user-mode) die de execution protection schenden, ontvangen een exception met statuscode STATUS_ACCESS_VIOLATION (0xC0000005). Applicaties die uitvoerbaar geheugen nodig hebben, moeten het kenmerk PAGE_EXECUTE, PAGE_EXECUTE_READ, PAGE_EXECUTE_READWRITE of PAGE_EXECUTE_WRITECOPY gebruiken bij de toewijzing van geheugen zodat ze compatibel zijn met NX.

Populaire copy-protection-programma's zoals Safedisk en SecureROM die veel bij games en educatieve software wordt gebruikt geven ook een probleem op systemen met execution protection. Deze programma's gaan op zoek naar de originele sleutel op de CD-ROM en plaatsen vervolgens versleutelde code (de loader) in virtueel geheugen en beginnen met ontcijferen, waarna deze code wordt gestart. Dit geheugen is niet voorzien van de flag PAGE_EXECUTE, zodat de code niet uitgevoerd kan worden op systemen met execution protection. Windows XP Service Pack 2 zal beide

CheckPolicy()	Vervangt de **AssocIsDangerous()** en onderzoekt beschikbaar bewijs 'evidence' en vergelijkt dit met de aanwezige policy
PromptUser()	Biedt een consistente dialoog box en vervangt eigen implementaties. Kan aangeroepen worden voordat het bestand gekopieerd wordt.
Execute	Vervangt een call naar **ShellExecute()**. Garandeert **CheckPolicy()** en roept PromptUser() aan indien nodig. Aanroep van IAttachment-Execute::PromptUser() met de EXEC actie.
Save()	Garandeert aanroep van **CheckPolicy()**. Bewaart bewijs met de attachment.

Tabel 2. IAttachmentExecute-interface

programma's herkennen en zal NX uitzetten zodat beide programma's probleemloos draaien. Er zijn echter meer copy-protection-programma's in omloop en die zal SP2 niet herkennen. Ook andere applicaties die acties uitvoeren die niet compatibel zijn met execution protection, moeten worden geüpdate.

Veiliger e-mail

Het delen en uitwisselen van bestanden via computer is de normaalste zaak van de wereld. Het brengt echter wel het gevaar van een besmetting van computervirussen met zich mee. Om gebruikers te beschermen tegen deze gevaren blokkeren sommige applicaties riskante bestandtypes. Elke applicatie doet dat op zijn eigen manier. Het is vrij lastig om op basis van de bestandsextensie een inschatting te maken. Bovendien is soms de uiteindelijke extensie nog niet bepaald; denk aan Office XML-document en MIME-sniffing. Er staat een functie ter beschikking om een inschatting te maken of een bestand risicovol is. Deze functie genaamd *AssocIsDangerous* is onderdeel van IE 6.01 en zit standaard in Windows XP SP1 en Windows Server 2003. De gebruiker krijgt een mededeling dat de betreffende attachment 'zeer gevaarlijk' kan zijn of slechts dat er 'een mogelijk gevaarlijk' bestaat. Eigenlijk zegt dit nog niet veel, en het is onverstandig de eindgebruiker de keuze te laten maken of een bestand potentieel gevaarlijk is of niet. Service Pack 2 introduceert: *'Attachment Execution Service'* met als doel het uitwisselen van bestanden op een veilige manier mogelijk te maken. Op basis van het bestand en de instellingen van de computer maakt de Attachment Execution Service (AES) een afweging en geeft duidelijke aanwijzingen aan de gebruiker. Intern geeft AES het bestand een risico-rating die is gebaseerd op de extensie, het soort bestand, handles, afkomst en meer. Ook wordt het bestand vergeleken met de instelling van de IE-zones (restricted, internet, intranet, local en trusted) en wordt vervolgens gekoppeld aan het bestand. Attachment Execution Services kunnen we gebruiken in onze eigen applicatie met de IAttachmentExecute interface met vier nieuwe API's; zie tabel 2.

Zowel Outlook als Windows Messenger maken na SP2 gebruik van Attachment Execution Services. Wanneer we nu in Outlook een potentieel gevaarlijke attachment ontvangen zal Outlook deze niet vrijgeven. Standaard is het ook niet mogelijk om deze op te slaan. Als we bij instellingen hebben aangegeven dat we het opslaan van potentieel gevaarlijke bestanden toch toestaan,

Afbeelding 3. De waarschuwing van de Attachment Execution Service blijft aan het bestand gekoppeld wanneer deze is opgeslagen.

wordt de waarschuwing van Attachment Execution Service aan het bestand gekoppeld. Als we het bestand later openen krijgen we opnieuw de waarschuwing; zie afbeelding 3. Het advies is om hiervan in eigen applicaties ook gebruik te maken bij het ontvangen van bestanden, zodat er een eenduidige en veilige manier komt om bestanden uit te wisselen.

Veiliger browsen

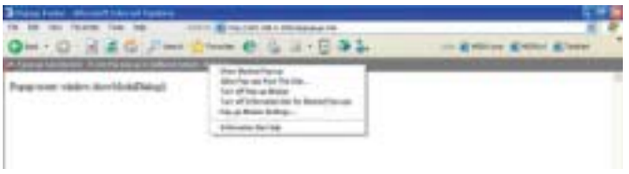
SP2 zorgt ook voor een aantal veranderingen op het gebied van de Internet Explorer. Nieuw is een pop-up-blokker en het dichtzetten van de Local Machine Zone.

Local Machine Zone Lockdown

IE kent een aantal security-zones: internet, local *intranet, restricted sites, trusted sites*. Afhankelijk van de zone worden bepaalde zaken – gebruik van ActiveX, plug-ins, Scripts, Authenticode - wel of niet toegestaan. Een speciale zone is de *local computer*, deze zone heeft de minste beveiliging. Deze zone is niet in het configuratiemenu van IE te vinden en heeft altijd een speciale status gehad. Alle content op de computer werd als 'veilig' bestempeld en uitgevoerd. Hier werd misbruik van gemaakt, door bijvoorbeeld te zorgen dat kwalijke scripts op de harde schijf terecht kwamen en gestart werden. Met SP2 wordt de *Local Machine Zone* afgegrendeld. De beperkingen zijn zelfs strenger zijn dan die van de *internet zone*. De gevolgen hiervan zijn dat locale HTML-applicaties zeer beperkt zijn in hun mogelijkheden en waarschijnlijk niet volledig zullen draaien. Ook even een pagina op de desktop zetten om hem lokaal te testen gaat niet meer. Een oplossing hiervoor is om in de HTML-code de volgende verwijzing op te nemen **<!—saved from url=(0018)http://www.msn.nl/ -->** waarbij 0018 de string-lengte van de URL is. Het gevolg hiervan is dat de opgeslagen webpagina in de security context van genoemde website draait. Het is niet mogelijk om te verwijzen naar een *trusted site* en zo toch alle rechten te krijgen.

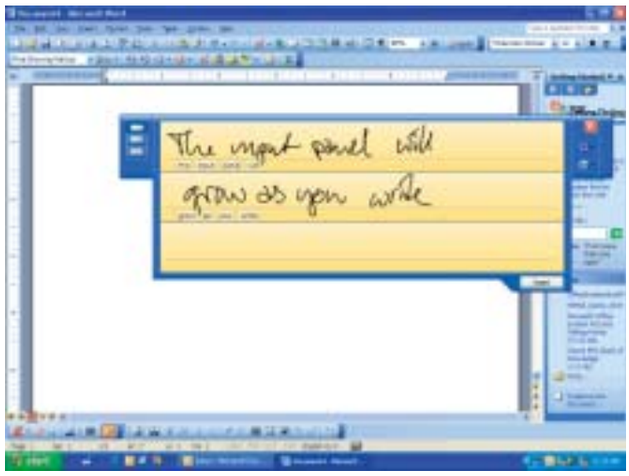
Geen binaire behaviors meer

Wat zijn behaviors? IE 5.0 introduceerde Dynamic HTML 'behaviors' en daarna zijn er veel bijgekomen zoals VLM en HTML+TIME. Vanaf Internet Explorer 5.5 hebben we ook binaire behaviors. Behaviors bieden een oplossing waar scripts te kort schieten. Zelf een behavior maken is natuurlijk mogelijk. Er zijn drie soorten behaviors: HTML components (HTC), Windows Script Components (WSC) en COM objects. De eerste twee zijn scripts en de laatste is een COM-object. De interactie tussen Internet Explorer en de behavior geschiedt altijd via COM; ook voor de scripts. Behaviors zijn vrij eenvoudig te schrijven in HTC of WSC, er is gedegen kennis is nodig om een COM-object te schrijven. Binaire behaviors zijn zeer krachtig en niet zonder gevaar. Tot nu toe was er in IE geen enkele mogelijkheid om binaire behaviors te beperken of te beheren. SP2 brengt daar verandering in, per zone kunnen behaviors worden beperkt. Gebruikt u in uw applicatie beha-



Afbeelding 4. Mogelijke acties na het blokken van een pop-up

Afbeelding 5. Beveiligingscentrum voor thuisgebruikers



Afbeelding 6. Nieuw inputpanel voor de TabletPC

vior dan moeten deze worden toegestaan aan de client. Dit kan in de registry door de volgende key op te nemen: HKLM\Software\Microsoft\Internet Explorer\Main\FeatureControl\FEATURE_BEHAVIORS "mijnapp.exe" met REG_DWORD 0.

Pop-up Manager

Nieuw bij SP2 is een pop-up manager in IE. Eindelijk zult u zeggen. Net als bij de privacysettings voor het toestaan van cookies, kan per site worden opgegeven of pop-ups worden toegestaan of geblokkeerd. Het resultaat hiervan is dat openen van een venster – met een van deze methods window.open(), window.showModeless Dialog(), window.showModalDialog(), window.navigateAndFind() en window.showHelp() - waarschijnlijk geblokkeerd wordt. Gebleken is dat veel webapplicaties niet correct zullen werken als de pop-up-blokker aanstaat. Door de strengere security-policies zal ook het automatisch starten van downloads – zoals op download.com - en het starten van ActiveX-controls niet altijd zonder problemen gaan. Voor de gebruiker wordt het blokkeren van content en pop-ups zichtbaar gemaakt met een gele balk direct onder de toolbar; zie afbeelding 4.

Naast de pop-up manager is het nu ook eenvoudiger om ActiveX-controls, browser-extensions, Browser Helpers, en toolbar-extensions te beheren. Eigenwijze controls die we niet wensen kunnen we nu voor altijd tegenhouden.

Nieuwe voorzieningen

Een van de in het oog springende nieuwe voorzieningen van SP2 is ondersteuning van Bluetooth en het beveiligingscentrum. In een oogopslag kunnen eindgebruikers zien of ze goed beveiligd zijn. Zie afbeelding 5. De ondersteuning van Bluetooth is vrij breed. Communicatie met groot aantal apparaten zoals keyboards, muizen, printers, telefoons, PDA's, GPS-ontvangers, enzovoort behoort nu tot de mogelijkheden. Een Personal Area Netwerk (PAN) tussen twee computer en het inbellen (Dial-Up Networking) met behulp van een Bluetooth-telefoon is standaard mogelijk.

Windows XP SP2 Newsgroups

Voor vragen over Windows XP Service Pack 2 kunt u terecht op de verschillende nieuwsgroepen die Microsoft heeft ingericht voor SP2. Er zijn twee manieren om deze nieuwsgroepen te bereiken:

1. **Met een browser:**
   http://communities.microsoft.com/newsgroups/default.asp?icp=xpsp2&slcid=us
2. **Met een NNTP-Newsreader**
   - **Server: privatenews.microsoft.com**
   - **Account name: privatenews\sp2user**
   - **Password: password**
   - **Let op: het wachtwoord is case-sensitive.**

Windows XP TabletPC Edition

SP2 brengt, naast alle genoemde veranderingen nog een paar specifiek voor de Tablet PC, zoals een nieuw TabletPC inputpanel met *'Write Where You Are'*. Dit betekend dat we direct in elk invoerveld met de pen gegevens kunnen invoeren. Automatisch verschijnt er op die plek het Tablet PC inputpanel; zie afbeelding 6. Hierdoor werkt het inputpanel nu ook beter in combinatie met inputvelden op HTML-formulieren Ook de onderliggende engines voor het herkennen van handschriften zijn verbeterd en is het nu mogelijk de tekst te corrigeren voordat het naar de onderliggende applicatie wordt gestuurd.

Meer dan een service pack

In dit artikel zijn enkele belangrijke wijzigingen beschreven die worden doorgevoerd in Windows XP Service Pack 2 om de beveiliging en veiligheid van het besturingssysteem te verbeteren. De meeste van deze voorzieningen zijn ontworpen om het risico van kwaadwillende aanvallen op systemen te beperken, zelfs als de laatste patches niet zijn geïnstalleerd. SP2 is meer dan een simpele service pack. Het zorgt dat Windows eindelijk op slot gaat. De wijzigingen en verbeteringen kunnen gevolgen hebben voor Windows- en webapplicaties die je hebt ontwikkeld. Evalueer de veranderingen en test uw toepassingen.

En nu de grote vraag; wanneer komt Service Pack 2 voor Windows XP? Daar SP2 een ingrijpende release is, wordt er door Microsoft zorgvuldig getest en staat er eigenlijk geen datum achter deze Serivce Pack. Veiligheidshalve kunnen we zeggen dat we deze zomer SP2 kunnen verwachten. Service Pack 2 voor Windows XP 64-bit Edition komt later samen met Service Pack 1 voor Windows Server 2003.

Nuttige internetadressen

www.microsoft.nl/windowsxp/sp2
msdn.microsoft.com/security/productinfo/xpsp2/
www.microsoft.com/technet/prodtechnol/winxppro/deploy/reinsp2.mspx
www.microsoft.com/technet/prodtechnol/winxppro/default.mspx
www.microsoft.com/windows/appcompatibility
www.microsoft.com/technet/community/columns/cableguy/cg0204.mspx

Memory protection:

http://www.intel.com/ca/pressroom/2004/0218b.htm
http://www.intel.com/technology/security/index.htm
http://www.amd.com/us-en/Processors/DevelopWithAMD/0,,30_2252_875_7044,00.html

Robert Fransen is freelance consultant. Hij is de beheerder van de Nederlandse MSDN- en TechNet-portal en geestelijk vader van het .NET Magazine.