Tool-gebaseerde beveiligingsscans van besturingssystemen

Drs. H. IJkel en ing. F.A. Giesing

De beveiliging in organisatie, applicatie en databasemanagementsysteem kan eenvoudig worden ondermijnd door beveiligingslekken in het besturingssysteem. Interne en externe hackers proberen met zo min mogelijk inspanning ongeautoriseerde toegang te bewerkstelligen en pas als de geijkte wegen niet begaanbaar zijn, zal verder worden gezocht naar andere ingangen. Waarom zouden we het hackers makkelijk maken, als het ook moeilijk kan? Ofwel, op welke manier kan een organisatie de risico's van de veelal onveilige configuratie van haar besturingssystemen beperken?

Inleiding

In overeenstemming met de wijzigingen in regelgeving zullen organisaties steeds beter moeten aantonen dat operationele risico's adequaat worden beheerst. Voorts zal de controlerende externe accountant (en overigens ook de interne auditor) als reactie op (recente) fraudegevallen de risico's die hij loopt verder willen beperken. Hij zal dan ook niet alleen meer aandacht aan de financiële administratie en de inrichting van de interne controles moeten geven, maar ook aan de informatiesystemen en aan de infrastructuur die de processen en interne controles ondersteunt.

Daar waar traditioneel gezien minder aandacht werd gegeven aan de werkelijke technische inrichting van het aan een informatiesysteem ten grondslag liggende besturingssysteem, neemt de behoefte toe om een meer gedetailleerd inzicht te verkrijgen in het beveiligingsniveau van deze besturingssystemen. Het dient immers niet mogelijk te zijn dat op organisatie- en applicatief niveau alles voldoende beveiligd lijkt, terwijl via een openstaande achterdeur (het besturingssysteem) eenieder met voldoende kennis alsnog toegang weet te verkrijgen tot gevoelige gegevens en deze weet te manipuleren.

De extra zekerheid die kan worden verkregen met het onderzoeken van het beveiligingsniveau van besturingssystemen, mag natuurlijk niet leiden tot hoge kosten. De beoordeling van de technische inrichting van besturingssystemen dient dan ook bij voorkeur met geautomatiseerde hulpmiddelen plaats te vinden. Interne en externe ICT-auditors kunnen met dergelijke hulpmiddelen op efficiënte wijze de beveiligingsstatus van een besturingssysteem inventariseren zodat verbeteringen kunnen worden doorgevoerd.

Drs. H. IJkel
is werkzaam bij KPMG Information Risk Management T&E als specialist op het gebied van technische beveiliging van IT-infrastructuren. Zijn primaire aandachtsgebieden zijn perimeter-, netwerk- en platformbeveiliging. Voorts voert hij regelmatig penetratietests uit op zowel publieke als interne IT-infrastructuren.

ijkel.hans@kpmg.nl

Ing. F.A. Giesing
is werkzaam bij KPMG Information Risk Management T&E als specialist op het gebied van IT-infrastructuurbeveiliging en beveiliging van Windows- en Unix-(internet)omgevingen. Daarnaast is hij betrokken bij audit- en adviesopdrachten inzake Information Security Services.

giesing.feico@kpmg.nl

In dit artikel wordt aan de hand van een casusbeschrijving verder ingegaan op de wijze waarop een organisatie via een selectietraject tot een keuze is gekomen voor ondersteunende tooling bij het onderzoeken van randvoorwaardelijke beveiligingsmaatregelen van het Microsoft Windows-besturingssysteem. Dit platform werd bij die organisatie veelvuldig toegepast voor kleine en middelgrote gegevensverwerkende informatiesystemen. Tevens wordt de daadwerkelijke toepassing van deze tooling beschreven.

Doelstelling beveiligingsscan

Denkt u dat uw kritieke systemen en gegevens adequaat beveiligd zijn, dat ongeautoriseerde personen nooit toegang kunnen verkrijgen tot 'geheime' memo's of vertrouwelijke e-mail van bijvoorbeeld de directie? Het zal u verbazen hoe vaak uit onderzoeken blijkt dat bestanden door iedereen kunnen worden geraadpleegd en/of gewijzigd, en hoeveel gebruikeraccounts er bestaan die

geen of uiterst eenvoudig te raden wachtwoorden hebben, zelfs als men een wachtwoordbeleid heeft ingevoerd.

Uit ervaring is gebleken dat de kwaliteit van de randvoorwaardelijke beveiligingsmaatregelen binnen organisaties vaak (onbewust) van onvoldoende niveau is en dat de hieruit voortvloeiende risico's niet worden onderkend. Wij zien in de praktijk een gebrek aan beveiligingskennis zowel bij de interne ICT-afdeling als bij vele consultancybureaus die zich met de implementatie van nieuwe informatiesystemen bezighouden. Dit kan in veel situaties leiden tot de installatie van standaard ingerichte systemen. En 'standaard' blijkt in veel gevallen gelijk aan 'vrijwel onbeveiligd'.

De doelstelling van een beveiligingsscan van besturingssystemen is dan ook het verkrijgen van inzicht in de mate waarin voldoende randvoorwaardelijke technische maatregelen zijn getroffen teneinde de vertrouwelijkheid, integriteit en continuïteit vanuit het besturingssysteem geredeneerd te kunnen garanderen en daarmee dus een slot te zetten op de spreekwoordelijke achterdeur.

Pakketkeuze

Om in een grote complexe infrastructuur efficiënt en effectief randvoorwaardelijke beveiligingsmaatregelen te kunnen onderzoeken, is het gebruik van geautomatiseerde hulpmiddelen een vereiste. Immers, onderzoeken die handmatig door specialisten moeten worden uitgevoerd, kosten veel tijd en dus geld, geld waarvoor betere bestedingsdoeleinden bestaan.

Overigens kunnen geautomatiseerde hulpmiddelen vaak niet efficiënt en effectief door organisaties zelf worden toegepast. Niet alleen de licentiekosten van de geautomatiseerde hulpmiddelen zelf, maar ook de te onderhouden kennis en beheerorganisatie zorgen ervoor dat alleen organisaties met voldoende schaalgrootte zelf effectief en efficiënt tot inzet van deze hulpmiddelen kunnen overgaan. Andere organisaties kunnen gebruikmaken van een tijdelijke softwarelicentie van bijvoorbeeld hun externe ICT-auditor of gespecialiseerde ICT-beveiligingsbureaus[1].

Hierdoor heeft de organisatie die in deze casus centraal staat, besloten tot het doorlopen van een pakketselectie- en implementatietraject, hetgeen heeft geleid tot de implementatie van een pakket dat adequate ondersteuning biedt bij het uitvoeren van beveiligingsonderzoeken van Microsoft Windows-besturingssystemen. Teneinde ervoor te zorgen dat dit pakket kwalitatief voldoende toegevoegde waarde levert, is een aantal selectie-eisen gedefinieerd, waarvan in tabel 1 een aantal essentiële eisen is weergegeven.

1) Zogenaamde traveling license.

Tabel 1. Uittreksel uit overzicht van gehanteerde selectiecriteria.

Gehanteerde selectie-eis	Beschrijving
Gerenommeerd softwarepakket	De werking van het pakket dient bij voorkeur reeds in de praktijk bewezen te zijn, alsmede dienen het voortbestaan van de leverancier en goede en bijtijdse ondersteuning te zijn gegarandeerd.
Zo min mogelijk impact van gebruik pakket op de IT-omgeving van een organisatie	Veel pakketten werken op basis van een client-server-principe. Dit is voor beveiligingsonderzoeken die door externe partijen worden uitgevoerd complicerend, aangezien dit de installatie van client software op de te onderzoeken systemen met zich meebrengt. Voorts dient de mogelijkheid te bestaan om het geautomatiseerde beveiligingsonderzoek op voor de klant acceptabele tijdstippen uit te voeren, teneinde eventuele negatieve bedrijfsinvloed zoveel mogelijk te beperken.
Uit te voeren beveiligingstests aanpasbaar aan specifieke organisatie- en KPMG-normen	Het pakket dient zodanig flexibel te zijn dat de mogelijkheid bestaat deze aan de individuele organisatie aan te passen.

De werking van de oplossing

In samenwerking met de organisatie wordt bepaald voor welke systemen de randvoorwaardelijke beveiligingsmaatregelen zullen worden getest; zo nodig worden klantspecifieke beveiligingsbaselines opgesteld en in het tool ingevoerd. Een laptop, waarop de gekozen oplossing is geïnstalleerd, wordt vervolgens op het netwerk van de organisatie aangesloten en de oplossing wordt zodanig geprogrammeerd dat deze buiten kantooruren de uit te voeren beveiligingstests uitvoert. Dit om ervoor te zorgen dat de beveiligingsscan een minimale impact heeft op de ICT-omgeving.

De resulterende rapportage bestaat uit een combinatie van een managementsamenvatting en een bijlage met daarin specifieke, technische aanbevelingen ten behoeve van de systeembeheerder. De managementsamenvatting laat op een hoog niveau zien in hoeverre per aandachtsgebied uit de baseline wordt gescoord en geeft specifiek aan waar verbeterpunten bestaan (zie kader 2). Deze bijlage kan voor een belangrijk deel door de software worden gegenereerd.

Conclusie

Organisaties maken in hoge mate gebruik van besturingssystemen voor hun kritieke gegevensverwerkende informatiesystemen. Teneinde vast te stellen dat voldoende aandacht is besteed aan randvoorwaardelijke beveiligingsmaatregelen is, mede door de omvang van de te testen omgevingen, de inzet van geautomatiseerde hulpmiddelen onontbeerlijk.

Met behulp van een geautomatiseerde beveiligingsscan van besturingssystemen kan op een efficiënte en effec-

tieve wijze het huidige beveiligingsniveau worden vastgesteld en indien noodzakelijk worden verbeterd. Dit zal dan moeten leiden tot een reductie in operationele risico's en dus bijdragen aan de naleving van regelgeving en een verhoging van de veiligheid en beheersbaarheid van de eigen ICT-omgeving.

Literatuur

[Korn03] Ir. P. Kornelisse, *Zuinig beveiligen?*, Compact 2003/4.

[Wolf00] Ir. R. de Wolf, *Infrastructure Services – Tool-based auditing in open heterogene ICT-infrastructuren*, Compact 2000/4.

Binnen het in dit artikel behandelde onderwerp bestaat een beveiligingsbaseline uit een minimaal aantal benodigde instellingen met betrekking tot de volgende onderwerpen:

- *logische toegangsbeveiliging*: maatregelen ter voorkoming van ongeautoriseerde toegang via het authenticatiemechanisme;
- *systeembeveiliging*: maatregelen ter voorkoming van ongeautoriseerde toegang door misconfiguraties en zwakheden in de gebruikte software;
- *logging*: maatregelen teneinde ongeautoriseerde toegangspogingen achteraf te kunnen vaststellen.

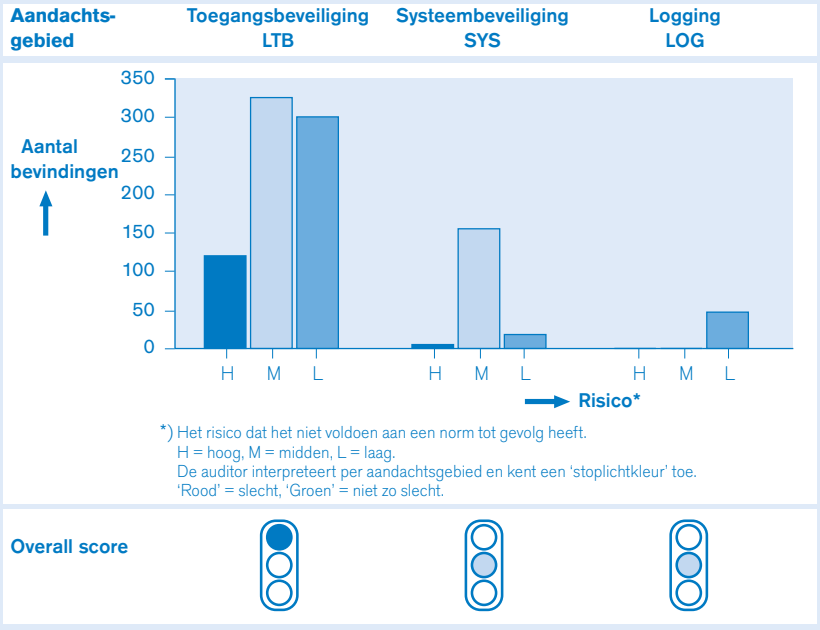
Kader 1. Waaruit bestaat een beveiligingsbaseline?

Leveranciers van besturingssystemen hebben de afgelopen jaren onder druk van de markt de beveiliging van hun producten moeten verbeteren. Echter, de verantwoordelijkheid voor het veilig configureren van besturingssystemen blijft liggen bij de organisatie zelf. De praktijk leert dat organisaties vaak niet over de kennis beschikken of de tijd nemen om het toereikend beveiligen van besturingssystemen vorm te geven. In dergelijke organisaties levert het hier besproken softwarehulpmiddel veel bevindingen op die op basis van interviews en/of documentatie niet zouden zijn vastgesteld. Een bijkomend voordeel van het inzetten van een dergelijk hulpmiddel is dat het onbetwistbare evidence levert. Hieronder een voorbeeld van de gedane bevindingen:

Nr.	Norm	Bevinding	Risico	Aanbeveling
1.	Geen accounts waarbij gebruikersnaam gelijk is aan het wachtwoord.	Een groot aantal accounts (79, waarvan 67 zijn geactiveerd) is aanwezig waarbij het wachtwoord gelijk is aan de gebruikersnaam.	Deze accounts vormen een gemakkelijke manier om functiescheidingen te doorbreken.	Accounts dienen van een nieuw, moeilijk te raden wachtwoord te worden voorzien.
2.	Beperk het aantal accounts met uitgebreide privileges.	Op de systemen is een groot aantal accounts (circa 100, waarvan 98 geactiveerd) met uitgebreide privileges aangetroffen.	Gebruikers beschikken wellicht onnodig over ruime bevoegdheden.	Beperk het aantal accounts dat deel uitmaakt van ingebouwde groepen met uitgebreide privileges.

Deze gedane bevindingen worden vervolgens per aandachtsgebied vanuit de beveiligingsbaseline gegroepeerd, waarna de toereikendheid van geïmplementeerde maatregelen wordt weergegeven.

Deze overzichten helpen het management bij het verkrijgen van inzicht in de mate waarin beveiligingsmaatregelen in het besturingssysteem zijn geïmplementeerd en in welke gebieden aanvullende maatregelen moeten worden getroffen om restrisico's verder te verkleinen.



Kader 2. Praktijkvoorbeeld.