SABA: IT-audit tooling 2.0

M.R.A.M. Smeets MSc
is junior adviseur bij KPMG en werkzaam in de unit ICT Security & Control. Hij is specialist op het gebied van beveiliging van besturingssystemen en netwerkinfrastructuren en voert onder andere penetratietests uit op publieke en interne IT-infrastructuren. Daarnaast is hij één van de kernpersonen in de ontwikkeling van SABA.

smeets.marc@kpmg.nl

Marc Smeets MSc

SABA is de nieuwe generatie IT-audit tooling van KPMG voor het verzamelen van systeemgegevens. SABA is beter afgestemd op de moderne eisen van de IT-auditors: automatisering is verder doorgevoerd waardoor nog meer tijdwinst kan worden gehaald en beoordelingen kunnen gemakkelijker klantspecifiek worden gemaakt door verbeterde rapportagemogelijkheden.

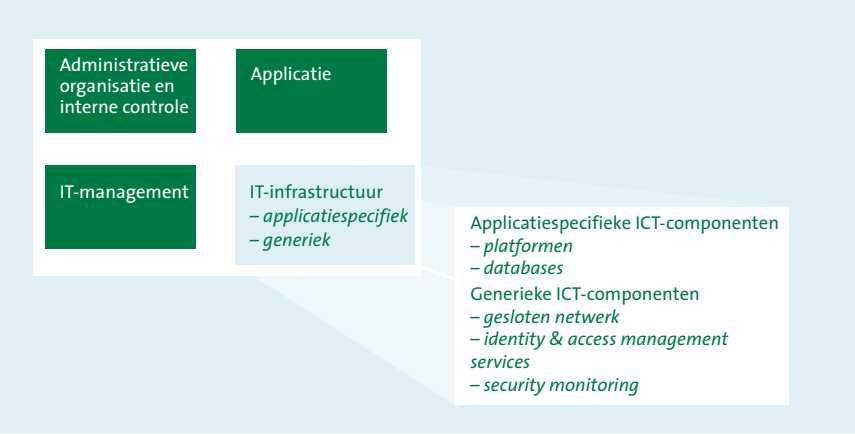
Inleiding

Door de jaren heen heeft KPMG IT Advisory diverse losse tools gebruikt ter ondersteuning van IT-audits. Hoewel deze tooling altijd goed heeft geholpen om snel systeeminstellingen te verzamelen, heeft deze oude tooling een aantal nadelen. Naast een uitleg over de achtergrond en de voor- en nadelen van deze tooling ter ondersteuning van IT-audit zal dit artikel verder ingaan op de kernpunten en het gebruik van de 'next generation' audit tooling die KPMG heeft ontwikkeld: SABA.

Achtergrond IT-audit tooling

Hoewel een IT-audit vaak over meer dan alleen IT-systemen gaat, is de component van deze IT-systemen zelf niet te onderschatten. Omdat IT-systemen nou eenmaal een belangrijk onderdeel zijn van de informatieverwerking (zie ook figuur 1), moeten deze systemen met de bijbehorende instellingen en autorisaties worden beoordeeld ([Korno7]). Door het toenemende gebruik van IT in de maatschappij, en daarmee ook in de klantenkring van KPMG, komen de auditors en adviseurs van KPMG ook steeds meer IT-systemen tegen bij klanten.

Alvorens de instellingen van IT-systemen kunnen worden beoordeeld, moeten deze eerst worden verzameld. Deze stap van verzamelen is uitermate geschikt om te automatiseren aangezien het hier puur het uitvoeren en samenvoegen van systeemcommando's betreft. Op het vlak van verzamelen van instellingen kan dus door de IT-auditor een flinke winst in tijd worden behaald omdat niet alle instellingen uit interviews of handmatige demonstratie hoeven te blijken. Let wel, interviews zijn nog steeds noodzakelijk om de instellingen te *beoordelen*. Een klant kan immers altijd compenserende maatregelen hebben getroffen om bepaalde risico's af te dekken.



Figuur 1. **Positie van IT-systemen in de bedrijfsvoering.**

In deze laatste stap van beoordelen zit dan ook meteen het risico voor de IT-auditor. Het verzamelen van de instellingen kan worden gedaan door iedereen die voldoende kennis heeft van het IT-landschap van de klant en de keuze kan maken om de juiste systemen te beoordelen (functioneel). Echter, voor het beoordelen van de uitkomst is nog steeds kennis nodig van de systemen zelf (versies van besturingssystemen en applicaties) en van de klant zelf (bijvoorbeeld voor compenserende maatregelen).

De nieuwe generatie audit tooling die door KPMG is ontwikkeld, is beter afgestemd op de moderne eisen van de IT-auditors: automatisering is verder doorgevoerd waardoor nog meer tijdwinst kan worden behaald en beoordelingen kunnen gemakkelijker klantspecifiek worden gemaakt door verbeterde rapportagemogelijkheden.

Tekortkomingen vorige versies KPMG-audit tooling

Door de jaren heen heeft KPMG diverse versies gehad van verschillende IT-audit tooling. De meeste tools waren zelf ontwikkeld, al werd en wordt nog steeds af en toe gebruikgemaakt van software van derden. Vaak is gebleken dat zelfgemaakte tooling meer flexibiliteit biedt en inzichtelijker is voor klanten. Software van derden wordt namelijk vrijwel altijd aangeboden als programma en niet als script[1]. Hierdoor heeft zelfgemaakte tooling dan ook de voorkeur boven software van derden. Desondanks kleven er diverse nadelen aan eigen tooling, welke vaak werden opgelost in nieuwere versies. Hieronder volgt een kort overzicht van de verschillende versies die we kennen binnen KPMG en de bijbehorende nadelen.

1) Een script is een aaneenschakeling van systeemcommando's die te lezen en aan te passen is met een tekstverwerker. Een applicatie is gecompileerde programmacode die niet te lezen en niet te wijzigen is zonder de broncode. Deze broncode wordt vrijwel nooit vrijgegeven door de fabrikant.

Versie 0

Versie 0 kenmerkt zich door het ontbreken van een feitelijk script. Deze allereerste versie mag dan ook eigenlijk geen echte versie heten. De manier van informatie verzamelen was puur gebaseerd op het vertellen door systeembeheerders van welke instellingen screenshots moesten worden gemaakt, of van welke systeemcommando's de output moest worden gekopieerd naar een tekstbestand. Dit gebeurde door middel van observaties van het ophalen van de systeeminstellingen.

De nadelen van deze methode werden al snel duidelijk en waren eindeloos: niet schaalbaar, foutgevoelig, veel specifieke kennis nodig bij auditor tijdens verzamelen, training-on-the-job kostbaar, et cetera. Al snel werd er dan ook gewerkt aan een opvolger.

Versie 1

De automatiseringsslag die volgde heeft geresulteerd in de scripts voor diverse smaken besturingssystemen en databases. De eerste generieke scripts zijn in 2002 ontwikkeld. De scripts waren een aaneenvoeging van een select aantal systeemcommando's waarvan de output werd geëxporteerd naar een HTML-document. Het resultaat was voor de auditor gemakkelijk te bekijken met een webbrowser. Deze scripts waren een enorme verbetering en zijn lange tijd gebruikt binnen KPMG, en soms zelfs daarbuiten.

De voordelen van deze eerste echte generatie audit tooling waren groot en zorgden voor een goede verspreiding. De scripts konden worden weggezet door een auditor zonder specifieke kennis van het platform, en de klant kon het script uitvoeren zonder de overhead van een gedetailleerd interview waarbij systeeminstellingen werden bekeken. Het script kon worden uitgevoerd door de klant wanneer het uitkwam, en de resultaten ervan waren gemakkelijk terug te mailen naar de auditor. De analyse kon vervolgens op een andere locatie en een ander moment worden gedaan, eventueel door een expert op het platform.

Echter, met de voordelen kwamen ook nadelen. De voornaamste nadelen van deze generatie audit tooling zijn hieronder genoemd in willekeurige volgorde:

- *Gebrek aan uniformiteit.* Doordat de verschillende scripts voor de diverse besturingssystemen en applicaties allemaal los van elkaar werden ontwikkeld, resulteerde dit in los van elkaar staande scripts die ieder een aparte manier van aanroepen, uitvoeren en rapporteren hadden. Bij het ene script was de output één bestand, bij andere scripts een hele directory vol met

bestanden. De opzet van de rapportage was niet altijd in dezelfde volgorde, wat de vertaalslag naar de samenvattende rapportage onnodig ingewikkeld maakte.

- *Verschillende rapportages*. De rapportages van de verschillende scripts waren net allemaal wat anders. Hoewel allemaal opgesteld in HTML, week de manier van rapporteren steeds weer in een of meer opzichten af van andere rapportages. Denk hierbij aan de volgorde van de soorten controles, wel of geen beoordeling bij de resultaten en verschillende opmaakstijlen.
- *Handmatig kopiëren*. Doordat de rapportages niet in Microsoft Word waren opgesteld, moest de auditor vervolgens de relevante output van de scripts kopiëren en plakken naar de uiteindelijke Word-rapportage. Dit is erg tijdintensief.
- *Kennis in scripts*. De scripts bevatten naast de feitelijk uit te voeren systeemcommando's ook meteen het rapportagegedeelte. Hierdoor werd de kennis die erin zit (norm, systeemcommando en resultaat) ook meteen doorgegeven aan degene die de scripts ontving. Hoewel het geen 'rocket science'-kennis betreft, bleken deze scripts toch een gewild iets gezien het grote aantal plaatsen waar we als KPMG onze eigen scripting terug hebben gezien op andere plaatsen bij dezelfde klanten, totaal andere klanten en zelfs concurrenten.

Een ander nadeel hiervan was dat mocht de output van de scripts per ongeluk in handen komen van een derde, alle (wellicht gevoelige) data over klantsystemen kant-en-klaar werd gepresenteerd, inclusief hiaten in de beveiliging van deze systemen.

- *Statisch*. Door de manier waarop de scripts zijn opgezet, zijn ze onnodig statisch. Uitbreiding was niet altijd even snel gedaan en specifieke normen voor specifieke klanten moesten of overal worden doorgevoerd, of de rapportage moest achteraf worden aangepast.
- *Versiecontrole*. De scripts bevatten geen enkele manier van versiecontrole. Eventuele fouten of onvolkomenheden die in oude versies konden bestaan, bleven tot in lengte van dagen bestaan omdat auditors niet werden gedwongen periodiek een update van de scripts binnen te halen.

Kernpunten versie 2.0

Na enkele jaren van intensief gebruik en gewenning aan de nieuwe scripts maakten de voordelen plaats voor de nadelen. De roep om vernieuwde versies werd steeds sterker. In 2006 is de ontwikkeling van een nieuwe generatie gestart waarbij de volgende kernpunten werden aangehangen:

- *Uniformiteit*. Dezelfde tooling voor alle systemen en applicaties. De manier van rapporteren moet nauw aansluiten op onze manier van rapporteren naar de klant.

Bij deze uniformiteit moet ook rekening worden gehouden met mogelijkheden voor het gemakkelijk toevoegen van nieuwe platformen en nieuwe rapportagevormen (bijvoorbeeld voor specifieke klanten of voor specifieke dossiereisen).

- *Kennisscheiding*. Scheiding tussen kennis in scripts (KPMG) en de uitkomst daarvan (klant), waardoor beide veiliger worden voor luistervinken.
- *Versiecontrole*. Makkelijke manier van verplicht updaten van de scripts.
- *Procesoptimalisatie*. Minder 'dom' werk voor de auditor en automatiseer wat je kunt. Hierdoor veel tijdwinst en verminderde foutgevoeligheid.

De nieuwe generatie: SABA

SABA is het nieuwe platform voor IT-audit tooling voor het verzamelen en analyseren van systeeminstellingen dat KPMG IT Advisory sinds enige tijd gebruikt. Hoewel de ontwikkeling door één afdeling is gedaan, is het niet zo dat alleen deze afdeling hier verder aan kan werken. Doordat het nieuwe platform modulair is opgezet, is (internationale) samenwerking met andere units, of zelfs klanten, vrij gemakkelijk te bewerkstelligen.

Kernpunten SABA

Toen met de ontwikkeling van SABA werd begonnen, is een aantal ontwerpkeuzes gemaakt. Deze keuzes zijn gemaakt om de nadelen van de vorige generatie tooling zo optimaal mogelijk weg te werken. Hieronder volgt een uitleg van de belangrijkste kernpunten van SABA:

- *Tooling platform*. SABA moet een uniform platform worden dat gemakkelijk is uit te breiden met gewenste functionaliteit. Het toevoegen van een nieuw platform of nieuwe applicatie moet snel te doen zijn zonder dat dit consequenties heeft voor de rest van SABA. Tevens moet de manier van gebruik uniform zijn.
- *Spreiding van vergaren en rapporteren*. De scripts die worden uitgevoerd op het systeem van de klant mogen geen hapklare rapportage opleveren. Zonder de rapportageslag, die alleen kan worden gedaan op het KPMG-netwerk, is de SABA-output vrijwel onbruikbaar.

Hiermee gaan we tegen dat de scripts gevoelige informatie kant-en-klaar presenteren aan iedereen die de output onderschept. Tevens gaan we hiermee tegen dat de scripts buiten ons medeweten worden gebruikt.

- *Rapportage in gewenst formaat*. Rapporteren in het Word-formaat heeft grote voordelen. Niet alleen is het omzetten naar de uiteindelijke eindrapportage gemakkelijker, maar ook is het een stuk gemakkelijker om het rapport te bewerken.
- *Inhoud van rapportage aanpasbaar*. Door gebruik te maken van rapportagetemplates kan de auditor kiezen wat er uiteindelijk wordt gerapporteerd. Dit geeft de vrijheid om voor klanten met specifieke eisen een aparte template te maken waar specifieke controles worden weggelaten of juist worden toegevoegd. Tevens is het hierdoor gemakkelijk een 'quick-scan' rapport te maken dat alleen de basale controles (versiecontrole en autorisaties) bevat.

Een ander voordeel is dat de taal van de rapportage kan worden aangepast. Bij het genereren van de rapportage moet de auditor de keuze hebben om het rapport in het Nederlands of Engels te genereren. In de toekomst kunnen hier gemakkelijk nieuwe talen aan worden toegevoegd.

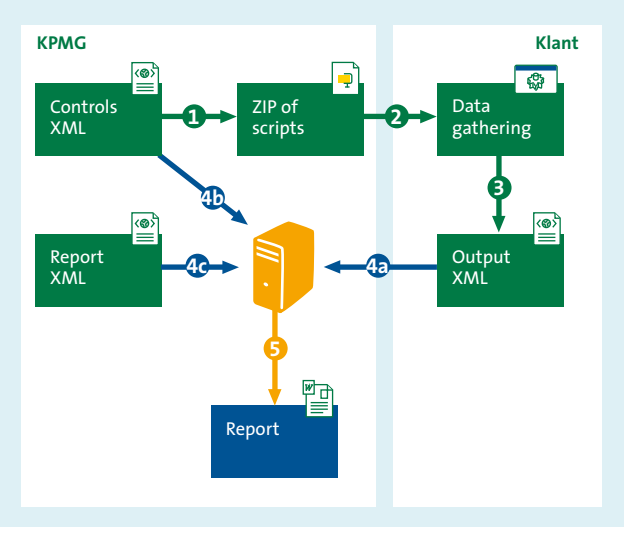
De architectuur van SABA

In de architectuur van SABA onderscheiden we een aantal componenten. Zoals in figuur 2 te zien is kent SABA een duidelijke scheiding tussen wat bij de klant gebeurt en wat bij KPMG gebeurt. Tevens is te zien dat gebruik wordt gemaakt van drie XML-bestanden, die alle drie nodig zijn alvorens een rapport te kunnen genereren.

Het eerste XML-bestand, genaamd 'controls XML', bevat de definitie van de feitelijke controles die moeten worden uitgevoerd met de daarbij behorende scriptcommando's per besturingssysteem en/of applicatie. Dit 'controls XML' is dan ook het bestand dat wordt gebruikt voor het maken van het script.

Het tweede XML-bestand dat we zien is genaamd 'output XML'. Dit bestand bevat de resultaten en de uitvoer van het uitvoeren van de scripts. Hoewel een XML-bestand gewoon platte tekst is, is het niet presenteerbaar als een rapport en daardoor minder bruikbaar mocht het in de verkeerde handen vallen. Alleen de resultaten zitten in dit XML-bestand. De commando's waar deze resultaten bij horen zijn hierin niet vermeld, wat het voor een luistervink een stuk moeilijker maakt om het bestand te interpreteren.

Het derde XML-bestand, genaamd 'report XML', bevat de definitie van de verschillende rapportagetemplates. Hierin staat welke hoofdstukstructuur het rapport kent en welke controles in welke volgorde terugkomen in het rapport.



Figuur 2. **Fasen bij gebruik van SABA.**

Alle drie de XML-bestanden zijn nodig om het uiteindelijke rapport te kunnen genereren. Dit genereren van het rapport gebeurt op een webserver in het KPMG-netwerk. Bij het genereren van het rapport kan de auditor de taal van het rapport bepalen en welke rapportagetemplate moet worden gebruikt.

Voordelen voor auditor en klant

De nieuwe opzet van SABA heeft een aantal voordelen voor zowel auditor als klant. Naast de eisen voor uniformiteit en kennisscheiding die als grote nadelen werden gezien bij de vorige generatie audit tooling, is er nu ook eindelijk grip op de verschillende versies die in omloop zijn. De webserver die het rapport genereert kan controleren welke versie is gebruikt en of deze nog toegestaan is. Tevens is het aantal mogelijkheden voor het genereren van rapporten flink vergroot. Zo kan bijvoorbeeld een aantal systemen in één rapport worden verwerkt.

Voor de klant is het gemakkelijker geworden om de scripts te analyseren alvorens deze uit te voeren omdat deze scripts uniform en duidelijk zijn opgezet. Tevens is het voor de klant fijner om te weten dat de uitvoer van het script niet alle gevoelige data kant-en-klaar presenteert; de rapportgenerator is daar nog voor nodig en deze staat in het KPMG-netwerk.

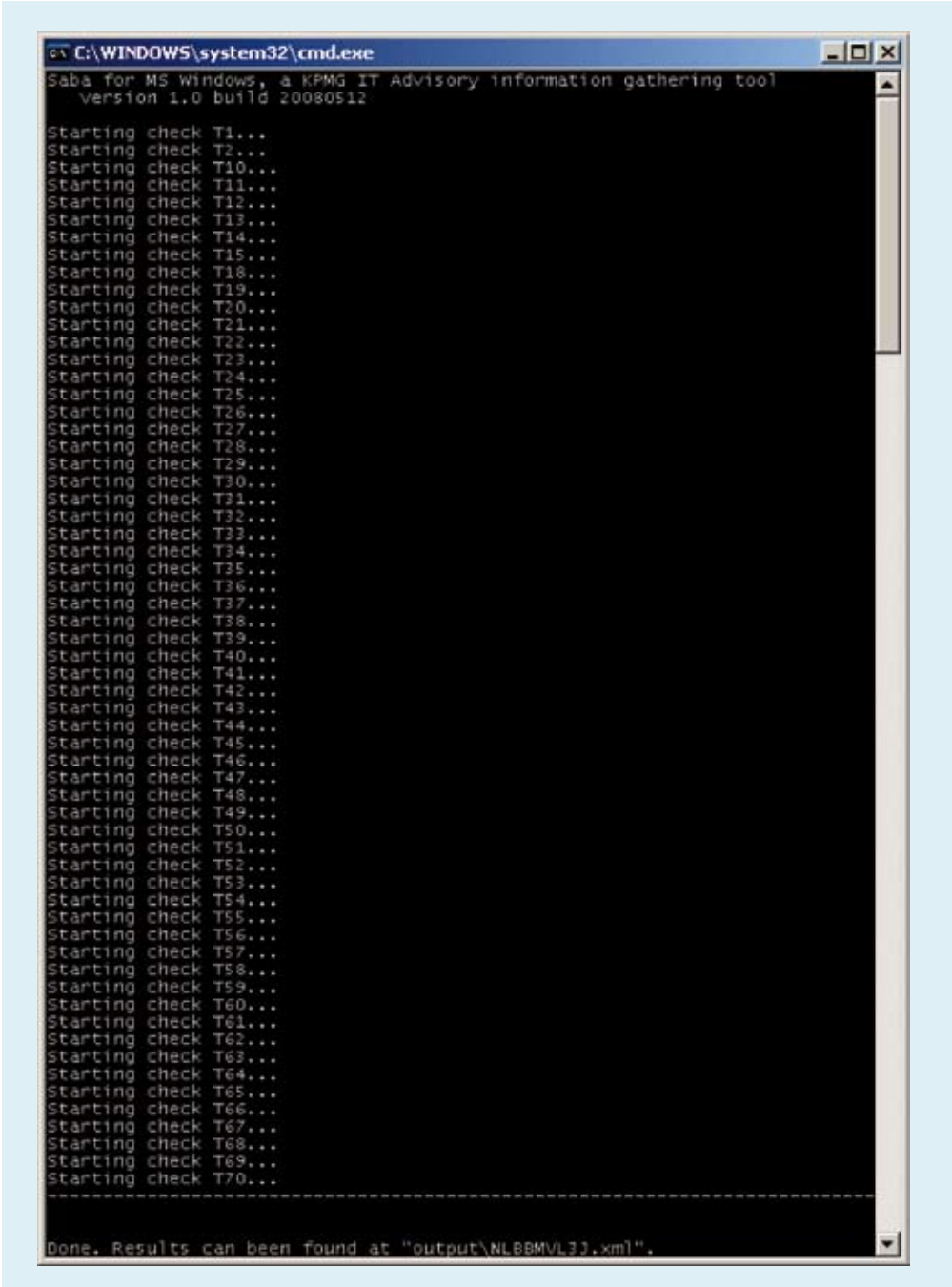
Als laatste grote voordeel kan het feit worden genoemd dat de ontwikkeling van de scripts (zowel inhoud van checks als uitbreidbaarheid van het aantal besturingssystemen en applicaties) veel gestructureerder kan worden aangepakt. Het SABA-platform is namelijk modulair opgezet. De reacties vanuit technische units uit andere landen zijn volmondig positief, wat veel goeds belooft voor de toekomst.

SABA gebruiken

Voor de klant verandert er weinig als SABA wordt gebruikt in plaats van oude scripts. In essentie is het nog steeds een script

dat moet worden uitgevoerd. Het bestand met de uitvoer, in dit geval een XML-bestand, moet nog steeds worden teruggestuurd naar de auditor. In figuur 3 is te zien wat de klant zal zien bij het uitvoeren van de scripts.

Voor de auditor is er een klein aantal veranderingen in het gebruik van SABA ten opzichte van de oude scripts. Allereerst moet de auditor ervoor zorgen dat hij de laatste versie heeft van de scripts alvorens deze uit te sturen naar de klant. In essentie is dit niet anders dan bij de oude scripts. Echter, in tegenstelling tot bij vorige generaties tooling zijn bij SABA de gevolgen groter als de auditor niet de juiste versie stuurt; oude versies zullen niet worden geaccepteerd door de rapportgenerator waardoor er geen rapport kan worden gemaakt zonder hulp van de ontwikkelaars. De laatste versies van de scripts zijn altijd te vinden op het KPMG-netwerk.



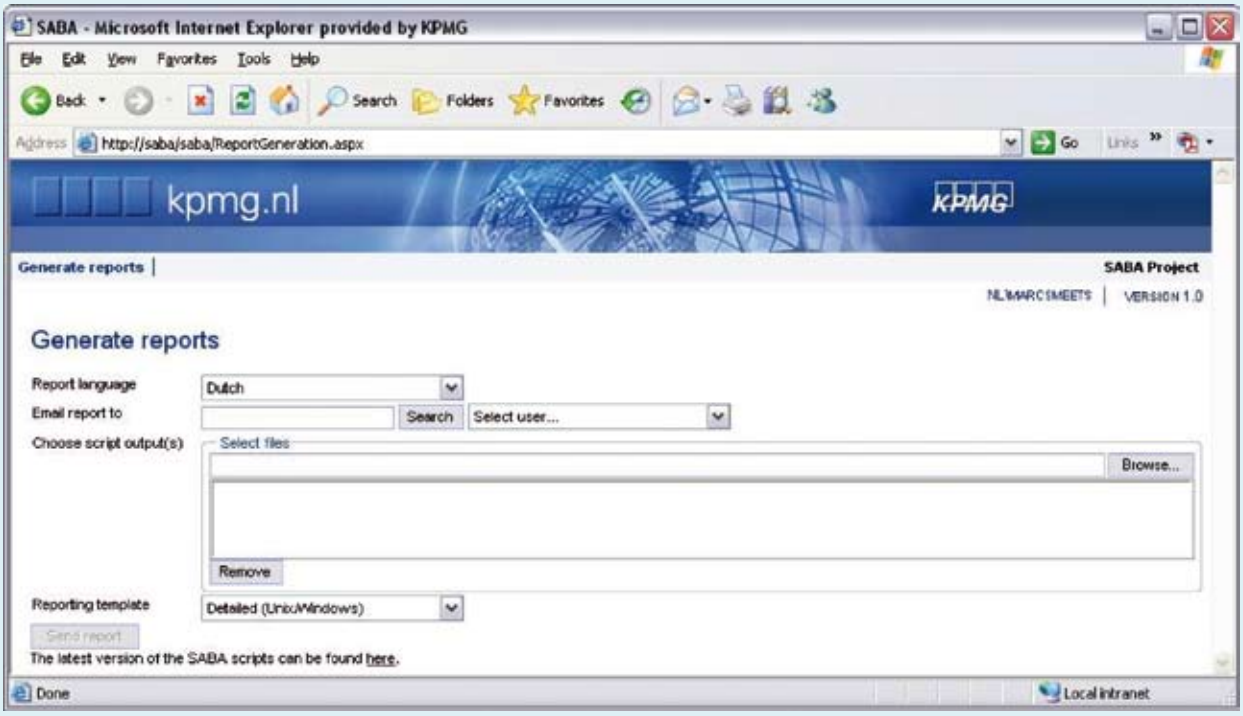
Figuur 3. **Schermafbeelding van succesvol uitvoeren SABA op doelsysteem.**

Om een output-XML-bestand van de klant te verwerken hoeft de auditor alleen maar te surfen naar de SABA-rapportgenerator, welke is te vinden op het KPMG-netwerk. In figuur 4 is weergegeven wat de auditor krijgt te zien.

De auditor moet hier een aantal keuzes maken: de taal, naar wie het rapport moet worden gemaild (inclusief zoekmogelijkheid), welke output-XML-bestanden in het rapport moeten worden verwerkt (maximum van acht output-XML-bestanden) en ten slotte welke rapportagetemplate moet worden gebruikt. Vervolgens verschijnt het rapport in de e-mailbox van de auditor die is opgegeven als ontvanger.

Toekomst

De basis die met SABA is gelegd, is op dit moment al uiterst effectief voor de auditors. De reacties zijn dan ook erg positief. Maar zoals altijd zijn er punten die nog verder kunnen worden verbeterd. In de toekomst zal SABA dan ook worden verbeterd op een divers aantal punten.



Figuur 4. **KPMG SABA-rapportgenerator.**

Op dit moment worden de voornaamste besturingssystemen reeds ondersteund: Windows Server 2000 en 2003, HP-UX, Solaris, AIX, SUSE Linux en Red Hat Linux. Naast een uitbreiding naar Windows Server 2008 zal er ondersteuning komen voor een aantal veelgebruikte applicaties zoals webservers en DNS-servers. Voor deze applicaties zal een aantal kritieke instellingen worden gecontroleerd door SABA.

Naast een verbreding in het aantal ondersteunde platformen zal er ook een verdieping komen in de controles die worden uitgevoerd. Dit houdt concreet in dat de basiscontroles die nu door SABA worden uitgevoerd, zullen worden aangevuld met steeds gedetailleerdere controles. Tevens kan voor een aantal basale controles de uitvoer automatisch worden geëvalueerd en in het rapport worden voorzien van een beoordeling.

Om dit alles spoedig te laten verlopen zal SABA beschikbaar worden gesteld voor diverse auditteams in binnen- en buitenland. Tevens zal samenwerking worden gezocht met deze teams om de ontwikkeling gezamenlijk verder op te kunnen pakken.

Samenvatting

SABA is de nieuwe standaard-tooling van KPMG ter ondersteuning van IT-audits waarbij de configuraties van IT-systemen worden onderzocht. Door de uniforme opzet heeft SABA een groot aantal voordelen boven de oude losse scripts, voor zowel auditor als klant. De voornaamste voordelen zijn te vinden op het gebied van tijdwinst, procesoptimalisatie en uniformiteit. De nieuwe opzet van SABA zorgt er namelijk voor dat het gebruik weer voldoet aan de huidige eisen van klant en auditor en dat toekomstige uitbreidingen (zowel in de breedte als in de diepte) geen invloed hebben op de werking van oudere versies.

Literatuur

[Korno7] Ir. P. Kornelisse RE CISA, *Jaarrekeningcontrole en technische IT-beveiliging*, Compact 2007/3.