In The Boxing Ring

IN THIS ISSUE

Network Box Technical News from Mark Webb-Johnson, CTO Network Box

Welcome

歡迎您來閱讀2010年4月版“In TheBoxing Ring”期刊。在這一版，我們將看一看安全認證、漏洞掃描和對即將到上市的Apple iPad的支持。

在第二頁，Michael Gazeley（Network Box公司主席）將專為客人談談安全認證的重要性，以及世界各地的Network Box運營中心都一致遵循的ISO 27001:2005不斷改進過程。

在第三頁，我將花一些時間討論網絡脆弱性掃描的現狀。我將向您展現現有的三種類型的掃描，並討論Network Box如何能協助這個利用重要的機會，以積極地幫助您關注網絡防禦和保護你的信息。這是一篇含有兩部分的文章，下半部分將要在下個月的通訊中提供。

同樣還是在第三頁，我要宣布Network Box針對iPhone的應用程序3.1版正式發布，包括對即將到貨的蘋果iPad的支持。新的V3.2的版本（對iPad提供更高分辨率的支持）也正在進行中，並計劃在4月發布。

在第四頁，我們仍將介紹通常的每月提示給您（這個月是關于微軟停止對IE6的技術支持），並在本月進行了一些軟件版本的更新，它們將作為補丁星期二的一部分提供。

和以往一樣，如果有任何反饋，意見或者建議，我們都歡迎您隨時提出來。您也可以通過發送郵件到我們的郵件列表：

nbhq@network-box.com

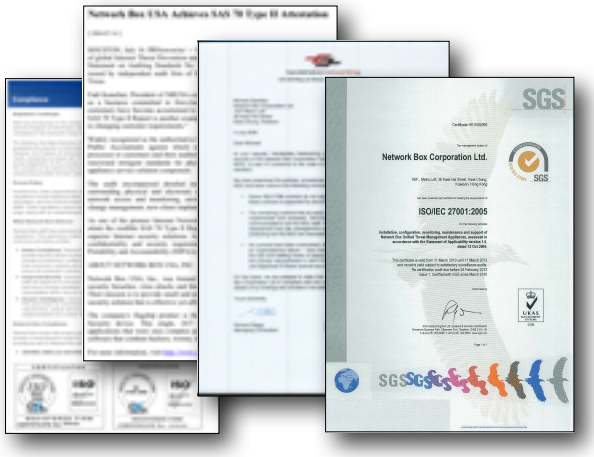
聯系我們。或者當您下次在香港市區的話來隨時來我公司辦公室進行參觀指導。

您也可以加入或訂閱我們的安全響應Twitter 和我們保持聯系，網址是：

twitter.com/networkboxhq

Mark Webb-Johnson
CTO, Network Box Corporation
April 2010

NETWORK BOX



ISO/IEC 27001:2005

By Michael Gazeley, Chairman Network Box

隨著信息安全管理日益成為一個交談的主流話題，在世界各地政府和公司董事會會議室，越來越多的IT經理發現自己需要積極地表明，他們的組織的IT安全解決方案已為到位，或者說已經“達到標准。”

現今IT安全新聞經常成為報紙、電台和電視台的頭條新聞，並且美國總統奧巴馬目前的外交政策倡議也是非常前沿，顯然已不再局限于利基電腦雜志和內幕博客的主題。

當然，大多數的IT經理現在明白，安裝一些“自己動手做”的防火牆，以及一些傳統的下拉式更新反病毒軟件，只是不會再“剪掉它”了。但什麼是真正 “符合標准”的意思？

在Network Box，我們相信，一個“達到標准"的很大一部分，是指確保在適當的地方安裝、配置、監控、維護和支持符合ISO / IEC 27001:2005標准的安全解決方案。

擁有最新的防火牆、入侵檢測和預防、虛擬專用網、反惡意軟件、反垃圾郵件、內容過濾、公司安全政策管理、業務連續性設施和自動化報告系統等統統到位但並不足夠；某人（或更准確地說是專家小組）需要全年24小時進行監督、管理和更新上述所有的網絡安全系統。

ISO / IEC 27001:2005已變得如此重要的原因，是因為雖然大多數組織有一定的信息安全控制類型，卻沒有一個正式的管理制度，甚至有的組織在理論上已經擁有在上面列出的一切，但仍然受到經常性的不平衡結果，或者是在執行上的不一致，因此只得到幾乎次優的定義。

安全永遠不應該是“臨時”性質。保持一致性和連續性，是每個標准的基石。

因此，全球各地的IT經理常面臨的問題正在迅速成為“我如何才能在有所需要地方部署有必要的安全系統，並確保他們的管理通過ISO/IEC 27001:2005的標准，但是如何在削減開支的實際的經濟環境下實現我們的這些目標？”

作為一家提供全方位托管的安全服務，並且通過ISO / IEC 27001:2005標准的管理系統認證的公司，Network Box提供了最佳（和最經濟）的答案。

不僅是政府部門、大型跨國公司、醫院、銀行、上市公司的最佳答案，並且是有PCI要求的零售業務的選擇；同時對于世界各地所有的小型和中型規模的組織而言，在沒有第三方專業的幫助下，他們幾乎沒有什麼機會在公司內部負擔（或想要負擔）必需進行的工作。

Network Box的高度敬業的安全行動中心工程師的工作從不間斷，包括每天晚上、每一個假期，甚至在有龍卷風、颶風和洪水警告時，他們時時刻刻都在利用主動推進式更新技術，幫助保護您的計算機、網絡和組織，同時還符合ISO /IEC 27001:2005的標准。

最後，真正網絡安全是一種服務，而不僅僅是一個硬件和軟件的組合。這就是ISO / IEC 27001:2005標准給我們的啓示。

Vulnerability Scanning

在今天的安全環境，脆弱性掃描扮演著一個重要的角色，它對安全系統進行積極主動的測試和厘定基准。
今天主要有三種類型的網絡掃描：

1　網絡探測器（網絡映射的高級形式）——在其中包含掃描一個網絡發現其中連接的主機，然後掃描這些主機枚舉它們的操作系統信息（如版本，提供的服務，登錄的用戶，網絡共享等）。
2　網絡漏洞掃描器——這是一種深入的掃描，主要針對特定的主機和服務進行的，以確定是否存在任何已知的漏洞。
3　網絡應用掃描器——先進的網絡漏洞掃描和針對特定的應用進行深入的測試，經常使用通用啓發式測試以及已知的基于簽名的測試。
漏洞掃描工具經常被互聯網上的惡意黑客用來定位有脆弱性漏洞的機器以便攻陷。對您來講，使用的類似工具主動保護您的網絡具有重要的意義——在別人之前發現您的脆弱性漏洞。
這些漏洞掃描通常可以從外部發起的（來自互聯網上的掃描，顯示了互聯網角度的觀點）或從內部發起的（從局域網/非軍事區進行掃描，顯示了一個內部的、有特權的網絡用戶的觀點）。
調諧掃描來自特定環境和方向（內部或外部）是非常重要的。例如，我們經常看到外部掃描虛報有關開放代理的漏洞（如允許開放接入互聯網的SMTP或Web代理），這些代理不應該對外可訪問或開放，但對于從內部掃描來講，這種代理應該可用。同樣，我們看到一個特別脆弱的假設虛報漏洞，僅僅因為一個特定的服務是開放的（有效的漏洞掃描器應該測試弱點本身的真實性，而不是僅僅假設一個特定的版本是有漏洞的）。
自動化漏洞掃描的假報告率通常是非常高的。PCI等標准關于漏洞掃描的要求結合了自動掃描軟件的供應，導致了掃描服務的爆炸性出現。這些服務大多在一個預定的時間自動掃描您的網絡，然後提交給你一本未過濾的漏洞報告（真實可信的和想象中可能有的）。需要一個專家詳細分析這些報告，以確定各脆弱性漏洞的狀態，並提供建議以便執行後續的行動計劃。
這種自動化的漏洞掃描通常只來自外部，並不提供從網絡內部對漏洞的洞察力。他們無視已經在你的組織內部的惡意人員的威脅。
同樣重要的是能夠比較不同時間的掃描。看看上個季度的掃描和本季度的相比，既要重點查看新的安全漏洞，以及確保後續行動計劃得到正確的執行。
正確地使用和熟練地處理漏洞掃描是一種積極主動地保護您的網絡的寶貴工具。即使您的組織沒有遵守掃描的強制規定，請也考慮使用它們。Network Box世界各地的營運中心在那裏可以幫助你和協助您完成這項重要任務。
在接下來的幾個月的In The Boxing Ring通訊中，我計劃詳細解釋Network Box如何可以幫助您完成任務和管理漏洞掃描，以及我們所建議的建立有效的定期脆弱性評估的要求。

iPhone App v3.1

Network Box iPhone應用程序3.1版本目前可在蘋果App Store獲得。在這個版本所作的更改包括：

1．內容兼容3.2版的操作系統（添加支持蘋果公司的ipad 1X和2X變焦模式）

2．提升本地緩存用以改進性能

3．改進首頁面視圖自動更新（顯示之前緩存的內容，而從服務器最新的檢索內容）

4．全球地圖自動更新增強（顯示之前緩存的地圖，而從服務器檢索的最後狀態情況）。

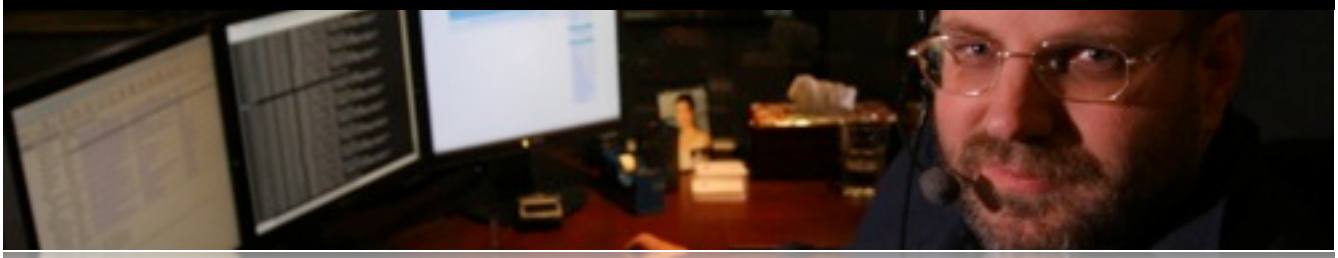
5．小錯誤的修正

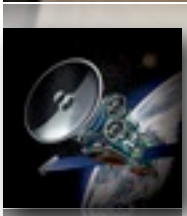
我們正在對我們的應用做進一步的更新，下一個版本的升級將是一個“普遍應用”支持iPhone，iPod Touch和iPad。下一個新版本（暫定的已知為3.2）將于本月（2010年4月）內公布，一旦蘋果開始接受這些普遍應用並且最終iPad硬件開始發貨。

我們也會加強對iPad的1024x768分辨率的支持，新版本增加了對更大的鍵盤（以及外部/藍牙鍵盤）的大力支持。

3.2版的更新將通過蘋果應用商店交付一個標准的更新。

Network Box v3.2 iPad App





April 2010 Features

On Tuesday, 6th April 2010, Network Box will release our patch Tuesday set of enhancements and fixes. The regional NOCs will be conducting the rollouts of the new functionality in a phased manner over the next 7 days. This month, these include:

- Further firmware support for new box models.
- Enhancements to the Box Office portal, to support the v3.2 iPhone/iPad application.
- Enhancements to the POP3 acceleration system, to improve compatibility with some non-standards compliant POP3 servers.
- Support for per-domain routing in our transparent SMTP proxy. Also add support for fail-safe session timeouts in this.
- Performance improvements to our web proxy URL categorisation and policy enforcement system.
- Minor security patches to the NTP service we offer (normally accessible to LAN/DMZ but not to NET).
- Minor sensor adjustments for some box models, in the health monitoring system.
- Minor cosmetic changes to some my.network-box.com administrative screens.

In most cases, the above changes should not impact running services or require a device restart. However, in some cases (depending on configuration), a device restart may be required. Your local NOC will contact you to arrange this if necessary.

April Hint: Internet Explorer v6 RIP

現在應該是Internet Explorer的安息時間了，真的。該產品一直運作良好，但現在只是太老了，太不符合現代標準，另外太不安全。

微軟公司已經在過去幾年裏，投入了巨大的工作改善他們的Internet Explorer浏覽器的安全，但是，這些改進主要為最新的版本，而IE6卻滯後了。例如，看看下面的表格，關于微軟最近MS10-018進行帶外的安全更新宣布的10個漏洞。其中，8個影響IE6，7個影響IE7，只有3個影響IE8。

Web開發人員，以及大型公共服務，為日益降低對IE6的支持，因為這證明了純粹是為了支持這項古老的浏覽器，降級現代 Web 2.0體驗變得越來越難。

目前，10%的Network Box用戶還在使用IE6，我們需要下降到0%，真的。

Mark Webb-Johnson,
CTO, Network Box Corporation

CVE	IE 6	IE 7	IE 8
CVE-2010-0267	Critical	Critical	NA
CVE-2010-0488	Important	Important	NA
CVE-2010-0489	Critical	Critical	NA
CVE-2010-0490	Critical	Critical	Critical
CVE-2010-0491	Critical	NA	NA
CVE-2010-0492	NA	NA	Critical
CVE-2010-0494	Critical	Important	Important
CVE-2010-0805	Critical	NA	NA
CVE-2010-0806*	Critical	Critical	NA
CVE-2010-0807	NA	Critical	NA

MS10-018 Simplified View (source: Microsoft)

MARCH 2010 NUMBERS

Key Metric)	#	% difference (since last month)
PUSH Updates	1,022	-23.7
Signatures Released	257,006	+2.3
Firewall Blocks (/box)	628,606	-5.6
IDP Blocks (/box)	161,793	-19.9
Spams (/box)	45,820	-14.8
Malware (/box)	767	-70.0
URL Blocks (/box)	78,214	-2.6
URL Visits (/box)	3,255,137	-4.3

NEWSLETTER STAFF

Mark Webb-Johnson
Editor

Michael Gazeley
Jason Law
Nick Jones
Production Support

Network Box Australia
Network Box Hong Kong
Network Box UK
Contributors

SUBSCRIPTION

Network Box Corporation
nbhq@network-box.com
or via mail at:

Network Box Corporation
16th Floor, Metro Loft,
38 Kwai Hei Street,
Kwai Chung, Hong Kong

Tel: +852 2736-2078
Fax: +852 2736-2778
www.network-box.com