

ERNW Newsletter 30a / Februar 2010

Liebe Partner, liebe Kollegen,

willkommen zur 30. Ausgabe des ERNW-Newsletters mit dem Thema:

Drei IT-Security 'Bits' und ein White Paper zu Cisco WLAN Enterprise Security

Version 1.0 vom 15. Februar 2010

von:

Friedwart Kuhn (fkuhn@ernw.de)

Enno Rey (erey@ernw.de)

Roger Klose (rklose@ernw.de)

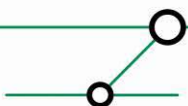
Olliver Röschke (oroeschke@ernw.de)

Abstract

In diesem Newsletter werden drei Security ‚Appetizer‘ und eine Studie zur Sicherheit von Cisco WLAN Enterprise-Lösungen vorgestellt.



1	DREI IT-SECURITY ‚BITS‘ ...	3
2	UNTERNEHMENSWEIT SICHERE INTERNET EXPLORER 8-KONFIGURATION	3
3	SICHERE SERVER UND APPLIKATIONS-KONSOLIDIERUNG IN VIRTUELLEN UMGEBUNGEN	3
4	WINDOWS SERVER 2008-OPERATIONS COMPLIANCE.....	4
5	...UND EIN WHITE PAPER ZU CISCO WLAN ENTERPRISE SECURITY	4
6	TROOPERS: IT-SICHERHEITSKONFERENZ	5



1 DREI IT-SECURITY ‚BITS‘...

Liebe Partner, liebe Kollegen,

wir möchten Ihnen mit drei ‚Security-Appetizern‘ Appetit auf mehr machen: mehr Wissen und mehr Sicherheit durch dieses Wissen, das Ihnen über die Erfahrung und das Know-How unserer Mitarbeiter zur Verfügung steht. Die folgenden drei ‚Security-Bits‘ stellen Themengebiete dar, die in den letzten Monaten verstärkt im Interessensfokus unserer Kunden standen und die unseres Erachtens aktuelle Themenkomplexe im Bereich der IT-Sicherheit mittlerer und großer Unternehmen und Organisationen treffen. Das separat verschickte Newsletter 30b ist eine (technisch orientierte) umfassende Studie aus einer ERNW GmbH-internen Untersuchung zur Sicherheit der Wireless LAN Enterprise-Lösungen von Cisco.

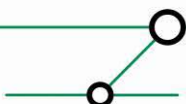
2 UNTERNEHMENSWEIT SICHERE INTERNET EXPLORER 8-KONFIGURATION

...ist eines der großen Themen, mit denen sich viele Unternehmen sprichwörtlich herum schlagen: Als eines der größten Einfallstore für Malware dient der Internet Explorer dort gleichzeitig als der am weitesten verbreitete Browser. Er sowie seine Konkurrenten (allen voran Mozilla Firefox) ermöglichen die bequeme Ansicht nicht nur von ‚einfachen‘ Webseiten, sondern ebenso das Abspielen von Videos, die Anzeige von Dokumenten verschieden(st)er Formate und das Ausführen von Skripten. Dazu steht dem Browser eine ganz Armada von Erweiterung – sog. ‚Add-ons‘ – in Form von *ActiveX-Controls* und *Browser Helper Objects* zur Verfügung. Diese Armada *angemessen* zu domestizieren, d. h. zu entscheiden, welches Add-on mit welchen Parametern verwendet werden darf, damit der Business Impact – sprich der unternehmensweite Einsatz – möglichst klein, der Sicherheitsgewinn jedoch möglichst hoch ist, erfordert Erfahrung, technisches Know-How und Kenntnis der Unternehmenskultur. Gleiches gilt für die vielen Sicherheitseinstellungen, die im Internet Explorer vorgenommen werden können: sei es etwa die Konfiguration des Zonenmodells, sei es das Verhalten gegenüber Java-Script oder sei es der Umgang mit Zertifikaten¹. Alles zusammen stellt für IT-Verantwortliche und -Personal in den meisten Umgebungen eine große Herausforderung dar. Die ERNW GmbH verfügt in diesem Gebiet über Erfahrung aus mehreren Projekten.

3 SICHERE SERVER UND APPLIKATIONS-KONSOLIDIERUNG IN VIRTUELLEN UMGEBUNGEN

Virtualisierung von Servern, aber auch Applikations-Konsolidierung in virtuellen Umgebungen haben bereits über die letzten zwei Jahre an Fahrt gewonnen. Dabei ermöglichen verschiedene Virtualisierungsplattformen (VMWare, Xen, Hyper-V) nicht nur die Konsolidierung von Serverhardware in virtuellen Maschinen, sondern auch die Konsolidierung von Anwendungen (etwa XenApp, App-V). Implementierung von Sicherheit beginnt – auch hier – bei der Konzeption und dem Design der virtuellen Umgebung und umfasst viele technische Aspekte wie etwa virtuelle Netz-

¹ Der im Firefox durch die aufwendige Konfiguration für Zertifikatsvalidierungen deutlich ‚uneleganter‘ als im Internet Explorer gelöst ist.



Segmentierung und sichere Konfiguration der virtuellen Switches, Definition und Implementierung von Zugriffsberechtigungen zwischen Host und virtueller Maschine, Hardening des Hosts, sicheres Management von Host und virtuellen Maschinen sowie deren Logging und Monitoring. Weitere Aspekte wie die sichere Bereitstellung von Anwendungen sowie die Umsetzung von Mandantentrennung innerhalb einer virtualisierten Applikation müssen ggf. ebenso bei der Sicherheitsbetrachtung berücksichtigt werden. Darüber hinaus kann auch die Firewall-Umgebung selbst virtualisiert werden. Wir verfügen über vieljährige Erfahrung in diesem Bereich und unterstützen Sie bei sämtlichen Schritten von der Planung bis zur Implementierung sowie dem Auditing von Server- und Applikationsvirtualisierung.

4 WINDOWS SERVER 2008-OPERATIONS COMPLIANCE

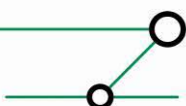
Sowohl für Behörden als auch größere und vor allem DAX-notierte Unternehmen stellt Compliance des IT-Betriebs eine wichtige Anforderung und gleichzeitig ein Gütesiegel für ihre Partner und Kunden dar. Relevante Standards für IT-Sicherheit werden durch die ISO 27000-Reihe sowie durch den Grundschatz (IT-Grundschatz-Standards) des Bundesamtes für Sicherheit in der Informationstechnik (BSI) definiert. International operierende Unternehmen stützen sich dabei meistens auf die Normen ISO 27001/2, während Behörden den BSI-Standards verpflichtet sind². Da ISO 27001 keine konkreten Konfigurationsanweisungen gibt und da die Grundschatzkataloge noch nicht die für Windows Server 2008-basierte Umgebungen relevanten Maßnahmen enthalten³, stellt sich für Behörden wie Unternehmen häufig die Frage, wie eine Windows Server 2008-basierte Umgebung konkret denn compliant zu betreiben ist. Dabei kommt dem (Windows Server 2008-, Active Directory- und Microsoft Infrastruktur-Komponenten-) Hardening eine wichtige Teilrolle zu. Wirkungsvoll wird das (technische) Hardening jedoch erst durch die Implementierung von Prozessen wie (Risikoanalyse, Dokumentation, Patchmanagement, Business Continuity-Management und Incident Response). Die Einbettung der Technik in diese organisatorischen Prozesse bereitet den Weg für Compliance zu den genannten Standards. Wir begleiten Unternehmen und Behörden schon länger auf diesem Weg und haben vor kurzem eine Behörde erfolgreich auf die Abnahme ihrer Windows Server 2008-Umgebung durch das BSI vorbereitet.

5 ...UND EIN WHITE PAPER ZU CISCO WLAN ENTERPRISE SECURITY

der separat verschickte ERNW-Newsletter 30b enthält eine detaillierte Analyse der in vielen Unternehmen ausgerollten Cisco WLAN Enterprise-Lösungen: Signifikante Designfehler im Structured Wireless Aware Network (SWAN) ermöglichen etwa das Auslesen des Master Keys, mit dem Access Point und Node (Kommunikationspartner /Computer) ihre Kommunikation verschlüsseln. Weitere Schwächen des Unified. Weitere Schwächen des Cisco Unified Wireless Networks betreffen das Trustmodell

² Im Zuge der Internationalisierung ist es seit 2006 möglich, eine ISO 27001-Zertifizierung auf Basis von IT-Grundschatz zu erwerben; das Zertifizierungsverfahren nach IT-Grundschatz wurde dafür grundlegend überarbeitet.

³ Dabei sei angemerkt: schon jetzt ist es für Nicht-Grundschatzspezialisten schwierig, die geeigneten Maßnahmen aus den mittlerweile 4000 Seiten umfassenden Grundschatzkatalogen auf die eigenen Umgebung anzuwenden; darüber hinaus dürfte die Integration von Windows Server 2008 erfahrungsgemäß noch auf sich warten lassen.



und die Management-Protokolle. Maßnahmen-Empfehlungen zeigen Möglichkeiten auf, sich gegen die durch diese Schwächen hervorgerufenen Bedrohungen zu schützen.

6 **TROOPERS: IT-SICHERHEITSKONFERENZ**

Last but not Least möchten wir unseren Leser die von uns **in Heidelberg vom 8.-12. März** im dritten Jahr veranstaltete internationale IT-Sicherheitskonferenz *Troopers* ans Herz legen. Es sind noch Plätze frei. Darüber hinaus werden für Kunden, Behörden und Fachjournalisten Nachlässe gewährt.

Eine Agenda mit dem vollständigen Programm finden Sie unter:

http://www.troopers.de/content/e3/index_eng.html

Für Fragen rund um die genannten Themen sowie zur Konferenz steht Ihnen ein Team erfahrener Sicherheitsspezialisten gern zur Verfügung.

Mit freundlichen Grüßen,

Friedwart Kuhn, Enno Rey, Roger Klose und Olliver Röschke.

ERNW GmbH
Friedwart Kuhn
Senior Security Consultant

ERNW Enno Rey Netzwerke GmbH
Breslauer Str. 28
69124 Heidelberg
Tel. +49 6221 480390
Fax +49 6221 419008
Mobil +49 15152411855
www.ernw.de

