SAN Security นิยามที่เหนือกว่าคำว่าโซนนิง

โครงข่าย SAN และเทคโนโลยีการเข้าถึงข้อมูลผ่านไอพี ได้ทำให้การรักษาความปลอดภัยบน SAN กลายเป็นเรื่องสำคัญเร่งด่วนกว่าที่เคย

เมื่อไม่นานมานี้ โซลูชันรักษาความปลอดภัยสำหรับ Storage Area Network (SAN) มักได้รับการพิจารณาเป็นอันดับสองรองจากประเด็นเรื่องสมรรถนะ ความสามารถในการเชื่อมต่อ และจำนวนพอร์ต แต่ปัจจุบัน การรักษาความปลอดภัยบน SAN ได้กลายเป็นพระเอกกลางเวทีบ้างแล้ว สาเหตุหนึ่งก็เพราะเริ่มมีหลายๆ บริษัทขยายโครงข่าย SAN ออกไปนอกศูนย์ข้อมูลเพื่อสร้างภูมิต้านทานต่อภาวะล้มเหลว (เช่น การฟื้นสภาพระบบจากภัยพิบัติ) และยังเป็นการสนองตอบมาตรากฎหมายของสหรัฐอเมริกาในเรื่องความเป็นส่วนตัวของข้อมูล เช่น Gramm-Leach-Bliley Act, HIPPA, Sarbanes-Oxley Act, และ European Privacy Directive ซึ่งบังคับให้องค์กรต้องปกป้องข้อมูลลับของลูกค้าขณะที่วิ่งไปมาระหว่างวง SAN ต่างๆ

สำหรับปริมาณของม้าโทรจัน หนอนอินเทอร์เน็ต และการโจมตี DoS ที่เพิ่มขึ้นทุกเวลาก็เพิ่มความตระหนักในเรื่องการรักษาความปลอดภัยตัวอุปกรณ์ให้มากขึ้นด้วยเช่นกัน "โฮสต์บน SAN ที่มีจุดอ่อนแม้แค่เครื่องเดียวก็มีโอกาสทำให้โฮสต์อื่นที่เชื่อมต่ออยู่เกิดอันตรายได้" Lincoln Dale วิศวกรเทคนิคประจำแผนก Storage Group ของซิสโก้กล่าว "เสียงร่ำลือที่ว่าไฟเบอร์แชนแนลมีความปลอดภัยสูงกว่าไอพีหรืออีเทอร์เน็ตนั้นถูกลบล้างไปเรียบร้อยแล้ว แม้ผู้คนส่วนใหญ่ไม่เคยได้ยินปัญหาเกี่ยวกับไฟเบอร์แชนแนลเลย แต่ก็ไม่ได้หมายความว่าปัญหาจะไม่มี เหตุผลง่ายๆ คือการโจมตีบนระบบ SAN เกิดขึ้นในปริมาณที่น้อยมากเมื่อเทียบกับขนาดของเครือข่ายไอพีที่ใหญ่กว่าหลายเท่าตัว"

"อีกสาเหตุหนึ่งที่ประเด็นด้านความปลอดภัยบน SAN ถูกหยิบยกขึ้นมาพิจารณาก็คือ ความโน้มเอียงที่ผู้คนแห่กันใช้ไอพีส่งผ่านทราฟฟิกของระบบจัดเก็บข้อมูลกันมากขึ้น "การใช้โครงข่ายไอพีและ FCIP (Fibre Channel over IP) บนระบบ SAN ที่แผ่ขยายระหว่างศูนย์ข้อมูลต่างๆ เพื่อวัตถุประสงค์ด้านฟื้นสภาพระบบจากภัยพิบัติและความต่อเนื่องทางธุรกิจนั้นเสียค่าใช้จ่ายน้อยกว่าการใช้เส้นทางเชื่อมต่อแบบแยกใช้เฉพาะกิจ" Dale กล่าว "โซลูชันทำซ้ำ (เรพพลิเคต) ข้อมูลส่วนใหญ่จะส่งข้อมูลโดยไม่เข้ารหัสลับก่อน ทำให้ต้องหาทางปกป้องข้อมูลลับเพิ่มเติมหากจะส่งออกไปบนเครือข่ายสาธารณะ"

ในทำนองเดียวกัน ยังมีความโน้มเอียงที่ผู้คนจะเข้าถึงระบบจัดเก็บข้อมูลที่เสียค่าใช้จ่ายถูกลงโดยใช้ SCSI over IP (iSCSI) อีกด้วย "iSCSI ได้รับความนิยมสูง เนื่องจากทั้งโฮสต์และเซิร์ฟเวอร์สามารถเชื่อมต่อกับเครือข่ายได้โดยใช้การ์ดอีเทอร์เน็ตที่มาพร้อมเครื่อง ช่วยให้ไม่ต้องเสียเงินซื้อ Host Bus

Packet_cisco.pmd 20 22/3/2549, 14:17

Adapter (HBA) และพอร์ตไฟเบอร์แชนแนลสำหรับสวิตช์อีก" Dale กล่าว "อย่างไรก็ตาม ถ้าข้อมูลในระบบจัดเก็บข้อมูลมีระดับความเป็นส่วนตัวสูงมาก เราก็จำเป็นที่จะต้องสร้างกลไกการปกป้องทราฟฟิก SAN บนเครือข่ายไอพีด้วย"

ประเด็นสุดท้ายเป็นเรื่องสำคัญพอๆ กับการป้องกันผู้บุกรุก ที่คุณจะต้องป้องกันภาวะข้อมูลเสียหายและสูญหายโดยบังเอิญด้วย "การคอนฟิกโซนนิงที่ผิดพลาดอาจเป็นเหตุให้เกิดความเสียหายได้มากเท่าๆ กับภัยอันตรายที่เกิดขึ้นแบบจงใจเลยทีเดียว" Dale ลงความเห็น

ปัจจัยต่างๆ ที่กล่าวมาข้างต้นได้กระตุ้นให้บุคลากรไอทีเพิ่มความสำคัญของการรักษาความปลอดภัยบน SAN ให้เท่าเทียมกับ LAN และ WAN ซึ่งก่อนหน้านี้วิธีหนึ่งที่นิยมปฏิบัติเพื่อเพิ่มความปลอดภัยของ SAN นั้นคือการทำโซนนิง (Zoning) หรือบังคับใช้แอ็กเซสคอนโทรลภายในไฟเบอร์แชนแนล "การทำโซนนิงอย่างน้อยดีกว่าไม่ทำอะไรเลย แต่ก็เป็นเรื่องง่ายที่จะฝ่าด่านป้องกันตรงนี้" Dale อธิบาย "ยกตัวอย่างเช่น การทำซอฟต์โซนนิงจะให้ 'ความปลอดภัยเหนือความคลุมเครือ' ซึ่งเปรียบเสมือนการพรางตำแหน่งศูนย์บัญชาการทหารบนแผนที่ แต่กลับปล่อยให้ไม่มียามคอยอารักขาในกรณีที่ข้าศึกค้นเจอ ส่วนฮาร์ดโซนนิงจะดีขึ้นมานิดหนึ่งกล่าวคือแต่ละเฟรมจะถูกตรวจสอบขณะวิ่งผ่านสวิตช์ แต่หากเจอเฟรมประเภทที่ปลอมแอดเดรสเข้ามา ฮาร์ดโซนนิงเองก็ไม่สามารถป้องกันได้เหมือนกัน"

เทคโนโลยีรักษาความปลอดภัยสำหรับ LAN และ WAN จำนวนมากที่ใช้กันอยู่ในปัจจุบันนั้นสามารถประยุกต์ใช้กับ SAN ได้เช่นเดียวกัน โดยเฉพาะเมื่อควบรวมกับเทคโนโลยีรักษาความปลอดภัยบน SAN ของซิสโก้แล้ว ก็ยิ่งเพิ่มความมั่นใจได้ว่าข้อมูลที่วิ่งบนเครือข่ายไอพีจะได้รับการปกป้องตลอดเส้นทาง "คุณลักษณะสำคัญที่สุดของแผนรักษาความปลอดภัยศูนย์ข้อมูลก็คือ ต้องปกป้องข้อมูลได้ตั้งแต่ต้นทางจรดปลายทาง" Dale กล่าว "และเราไม่อาจแยกการปกป้อง SAN ออกจาก LAN หรือ WAN ออกจากกันได้โดยเด็ดขาด"

โซลูชันคุณภาพเกรด A++

ภายใน Cisco MDS 9000 Series Multilayer SAN Switch ซิสโก้ได้ผสมผสานความรู้ความชำนาญในเรื่องการรักษาความปลอดภัย LAN และ WAN ที่สั่งสมมานานกับ SAN อย่างมีประสิทธิภาพ จนการ์ทเนอร์ได้จัดอันดับคุณภาพการรักษาความปลอดภัย SAN ของ Cisco MDS 9000 สูงถึงเกณฑ์ A++ ทั้งนี้ สิ่งที่ทำให้ Cisco MDS 9000 โดดเด่นเหนือคู่แข่งก็คือความใส่ใจในประเด็นด้านความปลอดภัยของ SAN ในหกหัวข้อ (ดูภาพที่ 1) ได้แก่:

- Fabric Access Security – การเข้าถึงบริการบนโครงข่าย SAN อย่างปลอดภัย
- Target Access Security – การเข้าถึงอุปกรณ์เป้าหมายและ Logical Unit Number (LUN) อย่างปลอดภัย
- SAN Fabric Protocol Security – โพรโตคอลสื่อสาร และพิสูจน์ตัวตนระหว่างสวิตช์ไฟเบอร์แชนแนลด้วยกัน
- IP Storage Security – ครอบคลุมถึง FCIP ที่ใช้เชื่อมต่อระหว่าง SAN ในศูนย์ข้อมูลสองแห่งอย่างปลอดภัย เพื่อเพิ่มสภาพทนต่อภาวะล้มเหลว เช่นเดียวกับบริการ iSCSI สำหรับการเข้าถึงเซิร์ฟเวอร์ที่มีความสำคัญน้อยลงมา (และเสียค่าใช้จ่ายถูกลง) อย่างปลอดภัย
- Data Integrity and Secrecy – การเข้ารหัสลับข้อมูลในระหว่างการเดินทาง
- SAN Management Security – การเข้าถึงบริการด้านการจัดการอย่างปลอดภัย

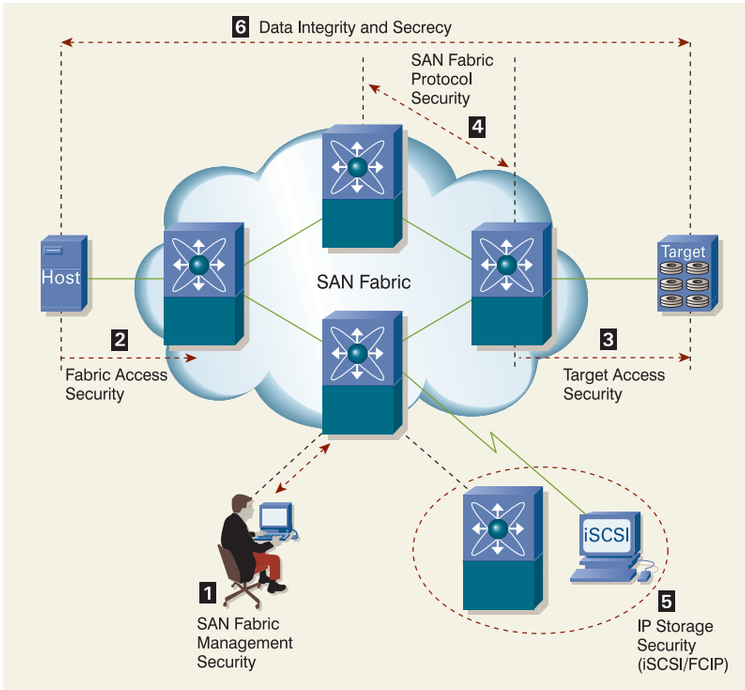
"คุณคงไม่มีวันได้โซลูชันที่เปี่ยมประสิทธิภาพหากข้อใดข้อหนึ่งในหกหัวข้อดังกล่าวขาดหายไป" Dale กล่าว "ยกตัวอย่างเช่น ถ้า SAN Management Security มีจุดอ่อน ผู้บุกรุกก็สามารถเข้าไปปิดกลไกรักษาความปลอดภัยอื่นๆ หรือแก้ไขคอนฟิกูเรชันเพื่อวิ่งเลี่ยงด่านป้องกันได้"

นอกจากนี้ สิ่งที่ทำให้โซลูชันรักษาความปลอดภัย SAN ของซิสโก้มีความโดดเด่น คือการที่คุณสมบัติด้านความปลอดภัยเกือบทั้งหมดจะได้รับการผนวกอยู่ใน Cisco MDS 9000 Series Switch เรียบร้อยแล้ว ช่วยให้ไม่ต้องจัดซื้อโมดูลที่จำเป็นอื่นๆ เพิ่มเติมอีก

Fabric & Target Access Security

การเข้าถึงโครงข่าย SAN รวมถึงอุปกรณ์เป้าหมายโดยไม่ได้รับอนุญาตสามารถก่อ

SAN VULNERABILITIES REQUIRING SECURITY MEASURES



ภาพที่ 1: Cisco MDS 9000 Series Switch สามารถตอบโจทย์ความต้องการ 6 ข้อในเรื่องการรักษาความปลอดภัยโครงข่าย SAN อย่างครบถ้วน จนได้รับรางวัลคุณภาพระดับสูงสุดจากการ์ทเนอร์

Packet_cisco.pmd 21 22/3/2549, 14:17

อันตรายให้ข้อมูลแอพพลิเคชัน หมายเลข LUN และประสิทธิภาพโดยรวมของแอพพลิเคชัน ซึ่งมัลติเลเยอร์สวิตช์ Cisco MDS 9000 Series จะให้คุณสมบัติที่ช่วยป้องกันความเสี่ยงที่จะเกิดเหตุการณ์ข้างต้น ดังนี้:

■ Fibre Channel Zoning – โซนนิงเป็นกลไกจำกัดการสื่อสารระหว่างอุปกรณ์ที่อยู่บนโครงข่ายไฟเบอร์แชนแนลเดียวกัน ซึ่งป้องกันไม่ให้โฮสต์เข้าถึงดิสก์ที่กำลังถูกใช้โดยอีกโฮสต์หนึ่งและทำให้ข้อมูลเสียหายโดยไม่ได้ตั้งใจ ทั้งนี้สวิตช์ Cisco MDS 9000 Series จะสนับสนุนการทำโซนนิงแบบ Software-based Zoning (ซอฟต์โซนนิง) และ Hardware-based Zoning (ฮาร์ดโซนนิง – โดยใช้ Hardware Access Control List กับทุกๆ เฟรมที่วิ่งผ่านสวิตช์) ได้มากถึง 2000 โซน และ 20,000 สมาชิกของโซนเลยทีเดียว

■ LUN Zoning และ Read-only Zoning – LUN Zoning ซึ่งเป็นความสามารถที่มีเฉพาะใน Cisco MDS 9000 Series คือผลผลิตจากการผสมผสานกลไกตรวจสอบเฟรมเชิงลึก (Deep Frame Inspection) และฮาร์ดโซนนิงเข้าด้วยกัน โดยผู้บริหารระบบไอทีสามารถใช้ LUN Zoning จำกัดสิทธิ์การเข้าถึง LUN ภายในอาร์เรย์ระบบจัดเก็บข้อมูลได้ ส่วน Read-Only Zoning จะมีประโยชน์สำหรับควบคุมมัลติมีเดียเซิร์ฟเวอร์ ซึ่งไม่มีความจำเป็นที่ต้องเขียนข้อมูลลงดิสก์แต่อย่างใด

■ VSAN – VSAN ช่วยเพิ่มระดับความปลอดภัยตลอดจนเสถียรภาพของโครงข่ายไฟเบอร์แชนแนลได้ โดยการแบ่งแยกอุปกรณ์ต่างๆ ที่เชื่อมโยงสายเข้ากับสวิตช์กลุ่มเดียวกันแบบลอจิคอล "ความผิดพลาดภายในโครงข่ายจะถูกจำกัดอยู่แค่ใน VSAN วงเดียวและไม่แพร่กระจายไปยังวงอื่น" Dale อธิบาย "ไม่มีการสื่อสารใดที่เกิดขึ้นระหว่าง VSAN คนละวง เว้นแต่ได้รับการยกเว้นผ่านการใช้คุณสมบัติ Inter-VSAN Routing ของ Cisco MDS 9000 เท่านั้น"

■ Port Security – เมื่อผู้บริหารฝ่ายไอทีเปิดใช้คุณสมบัตินี้ที่พอร์ตใดพอร์ตหนึ่ง อุปกรณ์เครือข่ายจะสามารถเข้าถึงพอร์ตนั้นได้ก็ต่อเมื่อมีรายชื่ออนุญาตอยู่ในฐานข้อมูลแล้วเท่านั้น

■ Port Mode Security – โหมดนี้สร้างขึ้นเพื่อจำกัดหน้าที่ของพอร์ตใดพอร์ตหนึ่ง เช่น ดูแลไม่ให้ Edge Port ถูกใช้เป็น Inter-Switch Link (ISL) โดยไม่ได้ตั้งใจ เป็นต้น

■ FC-SP DH-CHAP – FC-SP DH-CHAP มีหน้าที่ป้องกันการแก้ไขข้อมูลโดยไม่ได้รับอนุญาต และพิสูจน์ยืนยันการสื่อสารระหว่าง Host-to-switch และ Switch-to-switch ซึ่งปัจจุบันผู้ผลิต HBA และ SAN Switch รายใหญ่บางแห่งเริ่มสนับสนุนเทคโนโลยีนี้แล้ว ในการพิสูจน์ยืนยันนั้นสามารถกระทำได้จากภายในสวิตช์โลคอล หรือสั่งจากระยะไกลผ่าน RADIUS หรือ TACACS+ Server และ FC-SP DHCHAP เป็นเทคโนโลยีหนึ่งเดียวขณะนี้ที่สามารถป้องกันระบบจากทราฟฟิกที่ปลอมแอดเดรสเข้ามาได้

SAN Fabric Protocol Security

คุณสมบัติส่วนใหญ่ของ Cisco MDS 9000 Series ที่ได้กล่าวถึงในหัวข้อ Fabric & Target Access Security ยังสามารถรองรับโพรโตคอลสื่อสาร และพิสูจน์ตัวตนระหว่างสวิตช์ไฟเบอร์แชนแนลด้วยกันได้ด้วย โดยเหลือเพียงคุณสมบัติเพิ่มเติมที่ยังไม่ได้เอ่ยถึง ดังนี้:

■ Disruptive Reconfigure Fabric Rejection – คุณสมบัตินี้ช่วยป้องกันความอันตรายอันเกิดจากมือมนุษย์ โดยปฏิเสธคำขอแก้ไขคอนฟิกูเรชันใดๆ ก็ตามที่จะทำให้ระบบขัดข้อง ซึ่งอาจเกิดจากการคอนฟิกที่ผิดพลาด หรือการเพิ่มสวิตช์ตัวใหม่ที่ยังไม่ผ่านการคอนฟิกเข้าไปในโครงข่ายที่มีอยู่เดิม

■ IBM Fiber Connection (FICON) Fabric Binding –Cisco MDS 9000 สามารถจำกัดสิทธิ์การติดต่อกับโครงข่าย FICON ได้ตามหมายเลขสวิตช์ และ Domain ID

IP Storage Security

iSCSI ให้การเชื่อมต่อ SAN ในราคาถูกกว่าที่ไฟเบอร์แชนแนลสามารถทำได้ ยิ่งเมื่อประกบกับโมดูลไอพีเซอร์วิส หรือโมดูลมัลติโพรโตคอลเซอร์วิสแล้ว Cisco MDS 9000 ก็จะสามารถรองรับคอนเน็กชัน iSCSI จากโฮสต์ที่เรียกว่า iSCSI Initiator ได้ ตลอดจนรองรับการใช้ FCIP สำหรับการขยายโครงข่าย IP SAN ด้วย โดยคุณสมบัติด้านความปลอดภัยในแง่ IP Storage Security ของ Cisco MDS 9000 จะมีดังนี้:

■ iSCSI Authentication – ก่อนสร้างเซสชันการติดต่อ iSCSI สวิตช์ Cisco MDS 9000 จะพิสูจน์ยืนยัน iSCSI Initiator ก่อนโดยใช้โพรโตคอล CHAP

■ iSCSI Initiator Persistent Dynamic WWN และ Static WWN Allocation – สวิตช์ Cisco

เทคนิครักษาความปลอดภัยโครงข่าย SAN

เทคนิคที่ใช้	สนองความต้องการในด้าน	คุณสมบัติของ CISCO MDS 9000 SERIES ที่รองรับ
การแยกทราฟฟิกที่ใช้ไปยังเซิร์ฟเวอร์ฟาร์มคนละแห่งออกจากกัน	Fabric and Target Access Security	Virtual SAN (VSAN) Hard Zoning Fibre Channel Port Security
การพิสูจน์ยืนยันกันระหว่างสวิตช์ทั้งสองฝั่ง	Fabric and Target Access Security SAN Fabric Protocol Security Fibre Channel Port Security	Fibre Channel Security Protocol (FC-SP) Diffie-Hellman Challenge Handshake Authentication Protocol (DH-CHAP)
การเข้ารหัสลับ เพื่อป้องกันการโจรกรรมข้อมูล	Data Integrity and Secrecy	Integrated IP Security (IPSec)
การเฝ้าติดตามทราฟฟิก เพื่อสืบหาพฤติกรรมที่มุ่งร้าย	SAN Management Security SAN Management Security	SPAN RSPAN Fibre Channel Flow Statistics Call Home RMON Threshold Alarms
การบริหารที่รัดกุม เพื่อลดโอกาสเสี่ยงที่คนร้ายจะเข้าครอบงำอุปกรณ์ SAN		Authentication, Authorization, and Accounting (AAA) Secure Shell Protocol version 2 (SSHv2) Simple Network Management Protocol version 3 (SNMPv3) Syslog Network Time Protocol version 3 (NTPv3) Role-Based Access Control (RBAC)

Packet_cisco.pmd 22 22/3/2549, 14:17

MDS 9000 จะจับคู่ iSCSI Initiator กับ Virtual Fibre Channel Initiator ที่เหมาะสมได้ทั้งแบบไดนามิกหรือเชิงสถิติ ช่วยให้อาร์เรย์ระบบจัดเก็บข้อมูลสามารถระบุตัวโฮสต์ที่เชื่อมต่อผ่าน iSCSI ในวิธีเดียวกับที่ใช้ระบุโฮสต์ที่เชื่อมต่อผ่าน Fibre Channel HBA

■ **iSCSI Access Control** – ผู้บริหารฝ่ายไอทีสามารถใช้แอ็กเซสคอนโทรลกับ iSCSI Initiator ได้บนพื้นฐานของอุปกรณ์เป้าหมาย VSAN อุปกรณ์ระบบจัดเก็บข้อมูล หรืออินเทอร์เฟซ โดยเฉพาะกรณีหลังสุด อุปกรณ์ iSCSI เป้าหมายจะได้รับการป่าวประกาศออกไปยังอินเทอร์เฟซกิกะบิตอีเทอร์เน็ต ซับอินเทอร์เฟซ หรือ VLAN ได้

■ **FCIP** – Cisco MDS 9000 ยังสนับสนุนเทคโนโลยี FCIP ซึ่งนิยมใช้สำหรับทราฟฟิกแบบ SAN-to-SAN โดยแม้ FCIP ไม่มีคุณสมบัติด้านความปลอดภัยเป็นของตัวเอง แต่ก็อาจยืมกลไกทั้งหมดที่มีสำหรับไฟเบอร์แชนแนลใช้แทนได้ เช่น Port Security หรือ FC-SP DH-CHAP เป็นต้น

Data Integrity and Secrecy

ไม่มีเทคโนโลยีใดเลยระหว่าง iSCSI หรือ FCIP ที่สามารถปกป้องข้อมูลที่กำลังเดินทางข้ามเครือข่ายไอพีสำเร็จ "หากอุปกรณ์ของผู้ประสงค์ร้ายเกิดดักดูข้อมูลตามรายทางได้ แน่นอนว่าข้อมูลระบบจัดเก็บข้อมูลก็ย่อมถูกดักดูกลางทางได้เช่นกัน" Dale กล่าวเตือน "ในการปกป้องข้อมูลตามทางเหล่านี้ Cisco Multiprotocol Switching 14+2 (MPS 14+2) Line Card และ Cisco MDS 9216i Multilayer Fabric Switch จะใช้คุณสมบัติ Hardware-Based IPSec เข้ารหัส/ถอดรหัสลับข้อมูลด้วยอัลกอริทึม Advanced Encryption Standard (AES) และ Triple Data Encryption Standard (3DES) อันทรงประสิทธิภาพ"

SAN Management Security

การเข้าถึงส่วนบริหาร SAN โดยไม่ได้ผ่านกลไกขออนุญาตก่อนนั้นคือความเสี่ยง เนื่องจากคนร้ายจะสามารถแก้ไขคอนฟิกูเรชันเครือข่ายให้เกิดช่องโหว่ขึ้นได้ ซึ่งความเปราะบางของการเข้าถึงส่วนบริหาร SAN มีสาเหตุหลักๆ ที่เป็นไปได้สามข้อ ได้แก่ ความล้มเหลวของสวิตช์โพรเซสซิงเสถียรภาพของโครงข่ายที่ไม่ดีพอ และสภาพป้องกันการแก้ไขข้อมูลระหว่างทางที่ขาดความรัดกุม Cisco MDS 9000 ก็จะช่วยบรรเทาความเสี่ยงเหล่านี้ได้โดยใช้:

■ **AAA** – Cisco MDS 9000 สามารถใช้ TACACS+ หรือ RADIUS อย่างใดอย่างหนึ่งในการพิสูจน์ยืนยัน และทำรายการการเข้าถึงส่วนบริหารแบบรวมศูนย์ แต่หากไม่มี AAA Server ก็อาจใช้ฐานข้อมูลของชื่อผู้ใช้/รหัสผ่านภายในตัว Cisco MDS 9000 แทนก็ได้

■ **RBAC** – RBAC ทำให้ผู้ใช้แต่ละรายได้รับการกำหนดสิทธิหน้าที่บนพื้นฐานของ VSAN ที่ประจำอยู่ ซึ่ง Dale กล่าวว่า "วิธีนี้ช่วยให้บริษัทต่างๆ สามารถควบรวมระบบจัดเก็บข้อมูล พร้อมจำกัดสิทธิ์แอ็ดมินแต่ละคนให้เข้าถึงเกาะ VSAN ที่ตัวเองเคยมีสิทธิ์จัดการได้ก่อนหน้าการควบรวมนั้นด้วย"

■ **SSHv2** – เป็นทางเลือกใหม่ที่มาแทนโพรโตคอลที่มีความปลอดภัยต่ำกว่า อย่าง Telnet, rlogin และ FTP โดย SSHv2 ให้การเข้าถึงจากระยะไกลที่ปลอดภัยผ่านกระบวนการพิสูจน์ยืนยันและเข้ารหัสลับ อีกทั้งสามารถใช้งานร่วมกับ TACACS+ และ RADIUS ได้ด้วย

■ **SSL Version 2 และ TLS 1.0** – Cisco MDS 9000 จะสนับสนุนมาตรฐาน Storage Management Initiative Specification (SMI-S) ซึ่งเป็นชุดอินเทอร์เฟซบนพื้นฐานของ Common Information Model (CIM) ที่อนุญาตให้อุปกรณ์จากต่างผู้ผลิตทำงานร่วมกันได้บนโครงข่าย SAN และการเข้าถึงส่วนบริหารผ่าน SMI-S นั้นจะได้รับการปกป้องผ่าน SSL อีกทีหนึ่ง

■ **SNMPv3** – ในฐานะโพรโตคอลบนแอพพลิเคชันเลเยอร์ SNMP จะอำนวยความสะดวกในเรื่องการแลกเปลี่ยนข้อมูลเชิงบริหารระหว่างอุปกรณ์เครือข่ายต่างๆ ซึ่งสวิตช์ Cisco MDS 9000 ทุกรุ่นสามารถรองรับ SNMPv1, v2c, และ v3 ได้อย่างครบครัน ทั้งนี้ SNMPv3 (RFC 2271-2275) มีความพิเศษตรงการทำหน้าที่พิสูจน์ตัวตนโดยใช้อัลกอริทึม MD5 MAC หรือ SHA HMAC พร้อมเข้ารหัสลับผ่าน DES ที่ขึ้นชื่อเรื่องความแข็งแกร่ง

■ **Syslog** – แมสเซจ Syslog เป็นข้อความแจ้งเหตุที่อุปกรณ์เครือข่ายสามารถเก็บบันทึกลงใน Log File และ/หรือส่งต่อไปยังเซิร์ฟเวอร์อย่าง CiscoWorks Resource Manager Essentials (RME) โดยแมสเซจเหล่านี้จะรวมถึงการประทับเวลาจาก Syslog Server ชื่ออุปกรณ์ หมายเลขลำดับ การประทับเวลาจากอุปกรณ์เครือข่ายและแม้แต่ตัวแมสเซจเอง

■ **Accounting Log** – Cisco MDS 9000 สามารถเก็บบันทึกรายการคำสั่งคอนฟิกูเรชันไว้ได้ นอกจากนี้คำสั่งต่างๆ ยังอาจเก็บบันทึกไว้ใน Syslog Server และ AAA Server ผ่านตัวแอ็กเคาน์ติงแมสเซจ RADIUS หรือ TACACS+ และจะเก็บไว้ในส่วนของ NVRAM ที่ข้อมูลจะไม่หายไปไหนแม้สวิตช์จะรีสตาร์ตหรือไฟดับก็ตาม

■ **Call Home** – คุณสมบัตินี้สามารถใช้ในการแจ้งเหตุผ่านอีเมล์หรือเพเจอร์ไปยังเจ้าหน้าที่ผู้เกี่ยวข้องได้ (รวมถึง Cisco Technical Assistance Center หรือ TAC) เมื่อเกิดเหตุการณ์ที่สำคัญขึ้นในระบบ

■ **Fabric Consistency Checker** – คุณสมบัตินี้จะฟ้องถึงคอนฟิกูเรชันที่ผิดเพี้ยนไปจากนโยบายของสวิตช์ และหาทางแก้ไขให้ถูกต้อง

■ **ACL** – ผู้บริหารโครงข่ายสามารถกำหนดไอพีแอดเดรสที่มีสิทธิ์เข้าจัดการระบบได้ โดยบังคับใช้ ACL ทางแมเนจเมนต์อินเทอร์เฟซ และกิกะบิตอีเทอร์เน็ตอินเทอร์เฟซ

ปลอดภัยเท่าไหร่ถึงจะพอ?

ระดับความปลอดภัยของ SAN ที่บริษัทหนึ่งต้องการ จะขึ้นอยู่กับพื้นฐานความเสี่ยงที่ตนเองมีเป็นหลัก "โปรดถามตัวเองถึงมูลค่าความเสียหายที่เกิดขึ้น หากคู่แข่งหรือแฮกเกอร์เกิดขโมยข้อมูลสำคัญของคุณได้" Dale แนะนำ "โดยปกติมูลค่าความเสียหายจะมีปนกันๆ ระหว่างเสียหายหนักมาก เช่น ธนาคารจำเป็นต้องออกหมายเลขบัตรเครดิตใหม่แก่ลูกค้า และเสียหายน้อยลงมา เช่น การสูญเสียความเชื่อมั่นจากลูกค้า ดังนั้นจึงเป็นเรื่องสำคัญที่ควรเข้าใจถึงภัยคุกคามที่มีต่อตัวคุณก่อนที่จะรู้ถึงมูลค่าในการลงทุนเรื่องความปลอดภัยของระบบ"

เมื่อถึงคราวต้องลงมือปกป้องภัยคุกคามจากภายนอก ภายใน และความไม่ตั้งใจในรูปแบบต่างๆ ซิสโก้ขอแนะนำแนวทางปฏิบัติที่พิมพ์ไว้ในตารางข้างบน เพื่อให้องค์กรของคุณได้รับประโยชน์สูงสุด ■

อ่านเพิ่มเติม

- Cisco Storage Networking Solutions
  cisco.com/go/storagenetworking

Packet_cisco.pmd 23 22/3/2549, 14:17