Technology

ความก้าวหน้าอีกขั้นของ
ระบบรักษาความปลอดภัยของซิสโก้

เทคโนโลยีใหม่ๆ ของซิสโก้ช่วยให้องค์กรมีเครื่องมือสำหรับเพิ่มความปลอดภัยให้กับเครือข่ายด้วยการตรวจสอบผู้ใช้ที่ไม่ได้ดูแค่ MAC หรือไอพีแอดเดรสของไคลเอ็นต์เท่านั้น แต่ยังดูจากลักษณะเฉพาะส่วนบุคคลด้วย การตรวจสอบตัวตนของผู้ใช้ก่อนที่จะให้สิทธิ์ในการใช้งานระบบเครือข่ายขององค์กรเริ่มเป็นไปได้ภายใต้ข้อตกลงที่ชื่อ Cisco Identity-Based Networking Services (IBNS) ซึ่งเป็นเทคโนโลยีที่อิงกับ IEEE 802.1X ขณะนี้ IBNS ถูกนำไปใช้กับผลิตภัณฑ์ในกลุ่มแลนหลายๆ ตัวของซิสโก้ เพื่อใช้ในการตรวจสอบผู้ใช้ในการเข้าใช้งานแลนทั้งแบบใช้สาย และไร้สาย IBNS ได้รับการสนับสนุนทั้งในสวิตช์ตระกูล Cisco Catalyst, จุดติดต่อสำหรับเครือข่ายไร้สาย (Access Point) รุ่น Aironet 1100 และ 1200 series และใน Cisco Secure Access Control Server (ACS) ที่ทำหน้าที่เป็น RADIUS

เมื่อเร็วๆ นี้ ซิสโก้ได้วางจำหน่าย Secure ACS 3.2 ในรูปแบบของอุปกรณ์แร็กในชื่อว่า Cisco Secure ACS Solution Engine "อุปกรณ์นี้เป็นอีกออปชันหนึ่งที่ทำให้การเจาะระบบปฏิบัติการเซิร์ฟเวอร์ และแอพพลิเคชันของผู้ผลิตอื่นๆ ที่มักจะมีช่องโหว่ในระบบรักษาความปลอดภัยได้ยาก" Michel Chahine ผู้จัดการผลิตภัณฑ์ Secure ACS Product ในแผนก Secure Managed Networks Business Unit ของซิสโก้กล่าว

อะไรที่ขับเคลื่อนระบบเครือข่ายแบบมีการอิงตัวตนของผู้ใช้

ปัจจุบันระบบเครือข่ายภายในบริษัทเริ่มมีความเปราะบางมากขึ้น เปิดโอกาสให้ผู้ไม่ประสงค์ดีลอบเข้ามาใช้งานง่ายขึ้น สืบเนื่องจากสองสาเหตุหลักด้วยกันคือ หนึ่ง นโยบายที่เปลี่ยนไปของบริษัทส่วนใหญ่ที่หวังจะเพิ่มประสิทธิภาพในการทำงานและเพิ่มความสะดวกสบายในการใช้งานเครื่องโมไบล์ จึงยอมให้ผู้ใช้เปิดการทำงานของพอร์ตโดยตรง และอีกสาเหตุหนึ่ง คือการขอไอพีแอดเดรสง่ายขึ้นผ่านการกำหนดคอนฟิกโดยอัตโนมัติด้วย Dynamic Host Control Protocol (DHCP) เครือข่ายใดที่ไม่มีระบบรักษาความปลอดภัยที่ดีพอก็จะเปิดโอกาสให้ถูกโจมตีทำให้ระบบปฏิเสธการให้บริการ denial-of-service (DoS) หรือโดนขโมยไอพีแอดเดรส และแฮกเข้าไปเอาข้อมูลในเครือข่าย

นี่เป็นแค่เหตุผลสองสามข้อที่ทำให้ต้องควบคุมการใช้งานเครือข่ายจากตัวตนของผู้ใช้ Ken Hook ผู้จัดการฝ่ายผลิตภัณฑ์ Cisco Catalyst 6500 Series ซึ่งมีส่วนร่วมในการพัฒนา IBNS กล่าว ภายใต้ข้อกำหนดนี้ ซิสโก้ได้เพิ่มเติมการตรวจสอบตัวตนตามมาตรฐาน 802.1X ไว้บนผลิตภัณฑ์ของตน ตั้งแต่สวิตช์ Catalyst 6500, 4500, 3550 และ 2950 series รวมทั้งในอุปกรณ์รับสัญญาณของระบบแลนไร้สาย Cisco Aironet series เมื่อผู้ใช้พยายามเชื่อมต่อกับเครือข่ายใช้สาย หรือไร้สายก็ตาม อุปกรณ์ตัวใดตัวหนึ่งนี้จะทำหน้าที่เป็นผู้ตรวจสอบ authenticator ในโมเดล 802.1X (กฎที่เกี่ยวข้องกับการส่งข้อความ และการตรวจสอบตัวตนระหว่างไคลเอ็นต์และเซิร์ฟเวอร์ตรวจสอบตัวตน (authentication server) Cisco Secure ACS 3.2 ทั้งที่เป็นแบบอุปกรณ์ (appliance) และเป็นเซิร์ฟเวอร์ของไมโครซอฟท์วินโดวส์ มีหน้าที่ทำตามกฎของเซิร์ฟเวอร์ตรวจสอบตัวตนตามเฟรมเวิร์กของ 802.1X และสามารถเชื่อมต่อกับข้อมูลหลายแบบที่ใช้เพื่อตรวจสอบตัวตนของผู้ใช้ (อย่างเช่น ไมโครซอฟท์ แอ็กทีฟไดเรกทอรี)

โพรโตคอล 802.1X ในการเข้าถึงเครือข่ายผ่านพอร์ตนั้นทำหน้าที่เสมือนเป็นตัวเชื่อมโยงเลเยอร์รับส่งข้อมูลเพื่อใช้กับข้อความที่ถูกส่งไปพร้อมกับโพรโตคอลตรวจสอบระดับสูง อย่างเช่น EAP หรือชื่อเต็มว่า Extensible Authentication Protocol (RFC 2284) โดยใช้เฟรมฟอร์แมตที่เหมาะสมของแลนเลเยอร์ 2 อย่างเช่น เครือข่ายอีเทอร์เน็ต (802.3) หรือแลนไร้สาย (802.11) จริงๆ แล้ว 802.1X สามารถนำไปใช้กับมีเดียแลนชนิดอื่นก็ได้ถ้าต้องการ Cisco Secure ACS สนับสนุน EAP ด้วยเช่นกัน

ปกติแล้ว Cisco Secure ACS จะติดตั้งไว้ที่ศูนย์ข้อมูล ทำหน้าที่กำหนด และตัดสินใจตามกฎที่ชาญฉลาด กรณีที่มีผู้ใช้พยายามเข้าไปใช้งานเครือข่าย การตรวจสอบไคลเอ็นต์สามารถใช้ยูสเซอร์/รหัสผ่านแมคแอดเดรสเลเยอร์

2 หรือไอพีแอดเดรสเลเยอร์ 3 ก็ได้ทั้งนั้น

ขั้นตอนการตรวจสอบ เริ่มต้นจากไคลเอ็นต์ร้องขอการเชื่อมต่อเครือข่ายผ่านทางอุปกรณ์ Authenticator ชั่วคราว ซึ่งมักจะเป็นอุปกรณ์ที่เข้าถึงเครือข่ายที่อยู่ปลายทางของเครือข่าย

Authenticator จะส่งใบแนะนำตัวของไคลเอ็นต์ (เช่น ยูสเซอร์เนมและรหัสผ่าน หรือใบรับรองโครงสร้างพื้นฐานแบบพับลิกคีย์ (Public Key Infrastructure (PKI) certificates) ไปยังซอฟต์แวร์ Cisco Secure ACS โดยที่ ACS มีหน้าที่หลักเป็นเซิร์ฟเวอร์ตรวจสอบตัวตนในเฟรมเวิร์ก 802.1X จากนั้นก็มีแลกเปลี่ยนข้อมูลกันหลายครั้งผ่านทาง authenticator ถ้าขั้นตอนประสบความสำเร็จ ACS พบว่าผู้ใช้นั้นเป็นบุคคลที่ถูกต้อง ก็ให้อำนาจเท่าที่จำเป็น พร้อมคำสั่งกำหนดนโยบายไปยังอุปกรณ์ปลายทางเพื่อกำหนดขอบเขตให้กับการทำงานของไคลเอ็นต์

เพื่อใช้ประโยชน์จากฟังก์ชันเหล่านี้ อุปกรณ์ทั้งหมดในระบบจะต้องรองรับโพรโตคอล IEEE 802.1X และอัลกอริธึมในการพิสูจน์ตัวตน โดยเฉพาะ EAP ซึ่งมีอยู่หลายแบบ เช่น EAP-Transport Layer Security (TLS) ซึ่งใช้ระบบความปลอดภัยด้วย PKI crypto, Protected EAP (PEAP), EAP-MD5, Cisco LEAP, EAP-Generic Token Card (GTC) และ EAP-Microsoft Challenge-Handshake Authentication Protocol (MSCHAP) การเลือกใช้ EAP ที่เหมาะสมพร้อมกับรหัสผ่านแบบใช้ครั้งเดียว หรือการตรวจสอบพับลิกคีย์ด้วยการเข้ารหัส RSA อาจถูกนำมาใช้เพื่อตรวจสอบเครื่องไคลเอ็นต์บนเครือข่ายได้อย่างปลอดภัย Cisco IBNS ยังสนับสนุน PKI เพื่อการตรวจสอบที่แข็งแรงขึ้นโดยผ่านการใช้การเข้ารหัสพับลิกคีย์ด้วย x.509 v3

เหตุผลในการเลือกใช้อุปกรณ์

Cisco Secure ACS Solution Engine ใช้ฟอร์มแฟ็กเตอร์แบบแร็กเพียงตัวเดียว ทำงานด้วยโพรเซสเซอร์ความเร็ว 2.66 กิกะเฮิรตซ์ มีคุณสมบัติ และฟังก์ชันเหมือนกับ Cisco Secure ACS for Windows มีระบบความปลอดภัยที่แข็งแกร่งขึ้น การติดตั้งแบบปลั๊กแอนด์เพลย์ และการทำงานที่น่าเชื่อถือ จุดประสงค์หลักเพื่อปรับปรุงต้นทุนรวมในการเป็นเจ้าของ (total cost of ownership) ด้วยการลดค่าใช้จ่ายในการติดตั้งและดูแลรักษา ฟอร์มแฟ็กเตอร์แบบใหม่นี้ได้ตั้งคอนฟิกให้ระบบปฏิบัติการรีบูตเองโดยอัตโนมัติเมื่อระบบหยุดทำงาน serial console service ถูกตั้งคอนฟิกให้รีสตาร์ทเองโดยอัตโนมัติถ้ามันหยุดทำงานซอฟต์แวร์ Cisco Secure ACS เตรียมโปรแกรมเฝ้าติดตามดูการทำงานของระบบที่จะรีสตาร์ทบริการ Cisco Secure ACS กรณีที่มันหยุดทำงาน นอกจากนี้อุปกรณ์นี้ยังได้เตรียมระบบจัดการจากระยะไกลแบบบรรทัดคำสั่ง (command line interface - CLI) ที่รองรับการติดต่อทั้งทางซีเรียลและ Telnet ตัวบริการ Cisco Secure ACS เองสามารถใส่อิมเมจใหม่ รีโหลด อัพเกรด และรีบูตจากระยะไกลผ่านทาง CLI ได้ด้วย

ยิ่งไปกว่านั้นอุปกรณ์นี้ยังรันระบบปฏิบัติการเฉพาะของตัวเอง พนักงานแผนกไอทีไม่ต้องกังวลในเรื่องการติดตั้งซอฟต์แวร์และการอัพเกรดเวอร์ชันระบบ ระบบปฏิบัติการเป็นระบบปิด ส่วนบริการทั้งหมดที่มักจะโดนโจมตีเรื่องความปลอดภัยก็ถูกลดขนาดลง หรือไม่ก็ถอดทิ้ง และนี่เองเป็นเหตุผลหนึ่งที่ทำให้แฮกเกอร์โจมตีอุปกรณ์นี้ได้ยาก ตัวอย่างเช่น NetBIOS เป็นที่รู้จักกันดีถึงความเปราะบางที่ถูกโจมตีง่าย และได้ถูกถอดออกจากแพลตฟอร์มนี้ (NetBIOS เป็นโปรแกรมระดับเลเยอร์รับส่งข้อมูลที่ใช้กันมาก ซึ่งยอมให้แอพพลิเคชันที่อยู่บนคอมพิวเตอร์ที่ต่อกับแลนคนละระบบสามารถติดต่อกันได้) อุปกรณ์นี้ได้ปิดพอร์ต TCP ทั้งหมดที่ไม่ถูกใช้งานโดย Cisco Secure ACS ด้วยเพื่อป้องกันไม่ให้แฮกเกอร์ใช้ในการโจมตีเครือข่าย

802.1X Extension ใน Cisco IBNS

ซิสโก้ได้เพิ่มความสามารถให้กับมาตรฐานเฟรมเวิร์ก IEEE 802.1x เพื่อรองรับความต้องการใช้งานบนเครือข่ายระดับองค์กร เช่น นอกจากการตรวจสอบตัวตนของผู้ใช้และเปิดพอร์ตให้ทำงานแล้วสวิตซ์ Catalyst ยังเตรียมการใช้งานแลนเสมือนจริง (virtual LAN - VLAN) ที่เหมาะสมให้กับผู้ใช้ด้วย Hook ให้คำอธิบายถึงเรื่องนี้ว่า “สิ่งนี้มีความหมายว่า ผู้ใช้จะเชื่อมโยงเข้ากับ VLAN ที่เกี่ยวกับการเงิน หรือวิศวกรรมเองโดยอัตโนมัติ นอกจากนี้ที่ปรึกษา หรือคนอื่นๆ อาจได้รับการต้อนรับจาก guest VLAN หรือจาก VLAN ที่จำกัดการใช้งานมากขึ้น ซึ่งอาจยอมให้เข้าไปใช้งานอินเทอร์เน็ต และเข้าถึงทรัพยากรบางอย่างของบริษัทได้ ทั้งนี้ก็ขึ้นกับความสัมพันธ์ของเขากับองค์กร

นอกจากนี้ การใช้งานโทรศัพท์ไอพีมากขึ้นทำให้หลายองก์กรสร้าง voice VLANs (VVLANs) ขึ้นมา จุดประสงค์เพื่อให้วอยซ์ทราฟฟิกหรือข้อมูลเสียงถูกจัดอันดับความสำคัญในคิว 802.1p ไว้ที่ลำดับสูงสุด เพื่อหลีกเลี่ยงการเกิดความล่าช้า (latency) และคุณภาพที่ด้อยลง สวิตซ์ Cisco Catalyst รองรับ VVLAN เช่นกัน โดยจะตรวจสอบโทรศัพท์ไอพีของซิสโก้ให้เองโดยอัตโนมัติ และเข้าไปใช้งานใน VVLAN นอกจากนี้เมื่อเวิร์กสเตชันเชื่อมต่อไปยังพอร์ตสวิตซ์บนโทรศัพท์ไอพีของซิสโก้ จะต้องได้รับการตรวจสอบตัวตนก่อนถึงจะเข้าไปใช้งานระบบเครือข่ายได้

กรณีที่ต่อโทรศัพท์พ่วง และมีการเชื่อมต่อพีซีไปยังสวิตซ์ Catalyst ตัวสวิตซ์จะตรวจพบพีซี และต้องมีการตรวจสอบตัวตนก่อนถึงจะเข้าไปใช้งานเครือข่ายได้ ความสามารถนี้ทำให้โทรศัพท์ไอพี และ IBNS ทำงานพร้อมๆ กันบนพอร์ตของสวิตซ์ Catalyst เดียวกันได้