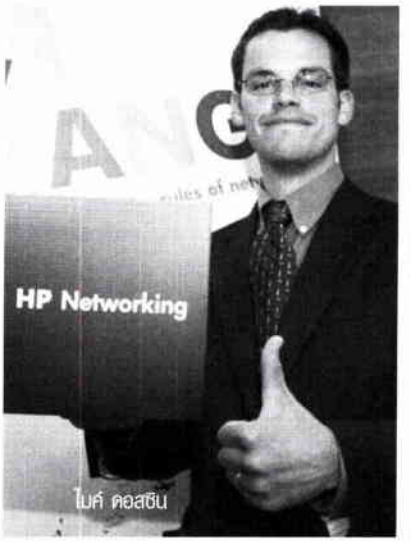
MATICHON INFORMATION CENTER | Subject Heading :
Source : เทคคอม เจอร์นัล
Date : 21 มิ.ย. 2554 Page : 19 No : 54329493

เอชพีชี้ภัยคุกคามเจาะระบบผ่านเว็บไซต์

อันดับ 1 การประกอบอาชญากรรมบนโลกไซเบอร์

19 เอชพี เผยรายงานล่าสุด นำเสนอภูมิคุ้มกันปกป้องระบบไอทีขององค์กรได้อย่างมีประสิทธิภาพ ชี้การเจาะระบบผ่านเว็บไซต์ คือภัยคุกคามอันดับหนึ่งในการประกอบอาชญากรรมบนโลกไซเบอร์ พร้อมเผยรายงานเรื่องปัจจัยเสี่ยงด้านการรักษาความปลอดภัยของโลกไซเบอร์ในปี 2553 ซึ่งระบุว่า อาชญากรรมบนโลกไซเบอร์มีปริมาณเพิ่มขึ้นอย่างเห็นได้ชัด โดยเฉพาะอย่างยิ่งการบุกรุกระบบศูนย์ข้อมูลและเครือข่ายต่างๆ ซึ่งเป็นสาเหตุให้องค์กรต้องสูญเสียเงินและข้อมูลเป็นอย่างมาก



ไมค์ คอสซิน

ในขณะที่มีรายงานด้านการโจมตีบนโลกไซเบอร์เพิ่มสูงขึ้น แต่จำนวนช่องโหว่ที่ถูกค้นพบยังคงเป็นอัตราที่อยู่ในระดับทรงตัว แต่ก็ยังนับเป็นตัวเลขที่สูงทีเดียว ทั้งนี้ รายงานดังกล่าวเผยว่า อาชญากรในโลกไซเบอร์ส่วนใหญ่ จะเน้นโจมตีไปที่ช่องโหว่ของระบบรักษาความปลอดภัยที่เป็นที่รู้จักและได้ปิดรูรั่วของระบบ (patched) แล้ว ขณะที่อาชญากรที่มีความเชี่ยวชาญสูง มักจะเลือกโจมตีไปที่ช่องโหว่ใหม่ๆ ก่อนที่ผู้ให้บริการจะจัดทำเครื่องมือแก้ไขและป้องกันต่างๆ ได้ทันท่วงที

เพื่อตอบโต้การโจมตีจากอาชญากรทั้งสองประเภท ภาครัฐและธุรกิจสามารถลดความเสี่ยงได้โดยยกระดับมาตรฐานการรักษาความปลอดภัย เช่น การปรับปรุงระบบรักษาความปลอดภัยของข้อมูลให้ทันสมัยอยู่เสมอ และหากมีการนำข้อมูลจากรายงานผลการวิจัยเรื่อง Zero Day initiative ของหน่วยธุรกิจ HP Digital Vaccine Labs (DVLabs) มาใช้จะเป็นประโยชน์อย่างยิ่งต่อองค์กรนั้นๆ

ทั้งนี้ รายงานเรื่อง ปัจจัยเสี่ยงด้านการรักษาความปลอดภัยของโลกไซเบอร์ในปี 2553 ใหม่ดังกล่าวเป็นการขยายผลการศึกษาจากรายงานที่เอชพีจัดทำไปเมื่อกลางปี 2553 โดยมีจุดมุ่งหมายเพื่อเผยแพร่ข้อมูลสำคัญแก่องค์กรต่างๆ สำหรับนำไปใช้ในการวางนโยบาย

การรักษาความปลอดภัยเพื่อปกป้องสินทรัพย์ด้านไอทีของตน นอกจากนี้ รายงานดังกล่าวยังช่วยพัฒนาระบบรักษาความปลอดภัยสำหรับพอร์ตโฟลิโอระบบโครงสร้างแบบผนวกของเอชพีให้ทันสมัย โดยผนวกรวมเทคโนโลยีดาต้าเซ็นเตอร์เข้าไว้ด้วยกัน เพื่อยกระดับสภาพแวดล้อมด้านไอทีให้มีการทำงานที่ง่ายดาย ทั้งยังมีความยืดหยุ่นและคล่องตัวยิ่งขึ้น และสามารถปรับขยายระบบได้มากขึ้น ตลอดจนมีต้นทุนในการเป็นเจ้าของทั้งหมดลดลง

รายงานดังกล่าวบ่งชี้ว่า เครื่องมือสำเร็จรูปในการเจาะระบบผ่านเว็บไซต์ (web exploit toolkits) มีปริมาณเพิ่มขึ้นอย่างน่าตกใจ และที่สำคัญมีการซื้อขาย "แพ็คเกจ" การโจมตีเช่นนี้ผ่านระบบออนไลน์ ทำให้นักโจมตีทั้งหลายสามารถเข้าถึงระบบไอทีระดับองค์กรพร้อมทั้งขโมยข้อมูลสำคัญต่างๆ ไปได้อย่างง่ายดาย นอกจากนี้ รายงานชิ้นนี้ยังระบุอีกว่า การเจาะระบบผ่านเว็บไซต์ ถูกเลือกนำไปใช้เป็นอาวุธในการจู่โจม เนื่องจากใช้งานง่าย และมีโอกาสสำเร็จสูง ◉