เรื่อง : ภัยคุกคามจากช่องโหว่แบบ Zero Day
เรียบเรียงโดย : ชวลิต ทินกรสุติบุตร
เผยแพร่วันที่ : 23 พฤศจิกายน 2548

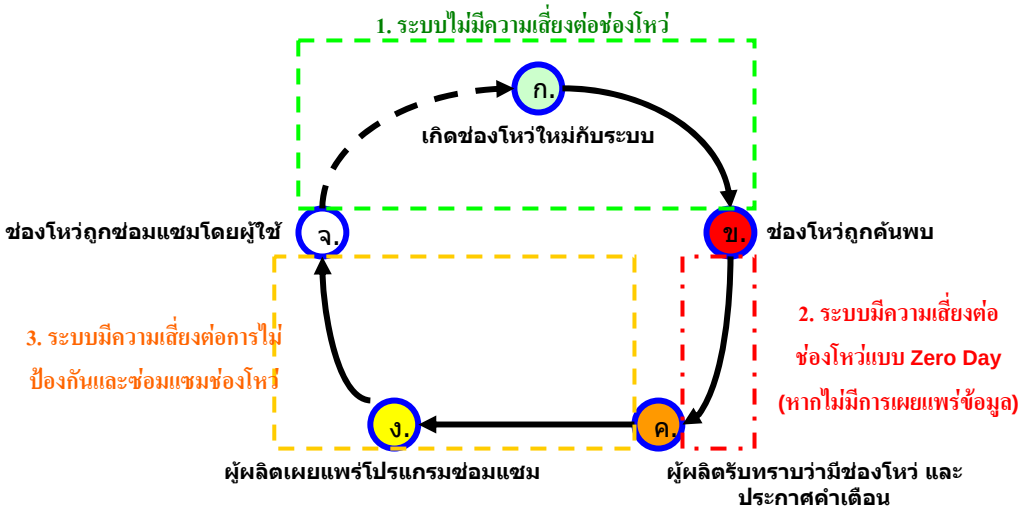
กล่าวนำ

การซ่อมแซม และปรับปรุงช่องโหว่ถือเป็นพื้นฐานหลักที่สำคัญมากสำหรับการสร้างความมั่นคงปลอดภัยให้กับระบบเครือข่าย และคอมพิวเตอร์ การเฝ้าระวังตรวจสอบข่าวสารช่องโหว่ใหม่ๆ ถือเป็นหน้าที่ที่ต้องปฏิบัติอย่างสม่ำเสมอของผู้ดูแลระบบ และผู้ใช้งานคอมพิวเตอร์ ช่องทางหนึ่งในการติดตามข่าวสารจากเว็บไซต์ หรือ Mailing List ทางด้านความมั่นคง ปลอดภัย (ศึกษาได้จาก [1]) และสามารถตรวจสอบฐานข้อมูล CVE (Common Vulnerability Exposure) ของช่องโหว่ (ดูรายละเอียดเพิ่มเติมจาก [2]) ในบทความนี้จะกล่าวถึงความหมาย และกรณีศึกษาความเสี่ยงชนิดใหม่ที่เกิดจากช่องโหว่แบบ Zero Day รวมทั้งแนวทางป้องกัน และระงับความเสี่ยงดังกล่าว

อะไรคือช่องโหว่แบบ Zero Day

หากอ้างอิงคำว่า Zero Day กับสาขาความรู้ทางด้านระบบสารสนเทศ (Information) แล้วจะหมายถึง ข่าวสารข้อมูลที่ไม่มีการเผยแพร่ให้กับสาธารณชนรับรู้ (อ้างอิงจาก [3]) ซึ่งในด้านความมั่นคงปลอดภัยนั้นจะอธิบายถึงช่องโหว่ที่ถูกนำไปสร้างเป็นโปรแกรมบุกรุก (exploit code) โดยช่องโหว่นี้ไม่ได้รับการเผยแพร่ให้กับสาธารณชนรับรู้ รวมทั้งเจ้าของผลิตภัณฑ์เองก็ไม่ทราบข้อมูลดังกล่าวเช่นเดียวกันจึงไม่มีการสร้างโปรแกรมซ่อมแซมช่องโหว่ โดยมากแล้วช่องโหว่นี้มักจะถูกค้นพบจากแฮกเกอร์เพียงไม่กี่คน และข้อมูลของช่องโหว่นี้จะรับทราบเฉพาะกลุ่มคนเหล่านั้นเท่านั้น

เมื่ออ้างอิงกับวงจรของการซ่อมแซมช่องโหว่ (Patching Life Cycle) จะมองเห็นภาพของช่องโหว่แบบ Zero Day มากยิ่งขึ้น



รูปที่ 1 แสดงวงรอบของการซ่อมแซมช่องโหว่ (Patching Lifecycle)

ขั้นตอนต่างๆ ของวงจรของการซ่อมแซมช่องโหว่ดังนี้

ก. ระบบเกิดช่องโหว่ : เป็นที่ทราบกันดีว่าไม่มีระบบใดไม่มีช่องโหว่ ซึ่งอาจจะเกิดจากความผิดพลาดของการตั้งค่าของระบบจากผู้ดูแลระบบเอง หรือเกิดจากซอฟต์แวร์เอง
ข. ช่องโหว่ถูกค้นพบ : เมื่อมีช่องโหว่เกิดขึ้นผู้ค้นพบอาจเป็นผู้ใช้งานระบบ/ซอฟต์แวร์ ผู้พัฒนาระบบ/ซอฟต์แวร์ รวมทั้งแฮกเกอร์ ซึ่งหากข้อมูลไม่ได้รับการเผยแพร่ และแฮกเกอร์นำไปสร้างโปรแกรมบุกรุกจะถือว่าช่องโหว่ดังกล่าวเป็น zero day
ค. ผู้ผลิตรับทราบ และแจ้งเตือน : เมื่อมีการเผยแพร่ข้อมูลของช่องโหว่ ผู้ผลิต หรือผู้เชี่ยวชาญจะต้องทำการแจ้งเตือนข้อมูลข่าวสารเกี่ยวกับช่องโหว่ รวมทั้งอาจจะมีคำแนะนำเบื้องต้นในการป้องกันก่อนเผยแพร่โปรแกรมซ่อมแซมช่องโหว่

ง. ผู้ผลิตเผยแพร่โปรแกรมซ่อมแซมช่องโหว่ : ผู้พัฒนาจะเผยแพร่โปรแกรมซ่อมแซมช่องโหว่ออกสู่สาธารณะ
จ. ผู้ใช้งานติดตั้งโปรแกรมซ่อมแซมช่องโหว่ : เป็นช่วงที่ผู้ใช้งาน หรือผู้ดูแลระบบจะต้องทำการติดตั้งโปรแกรมซ่อมแซมช่องโหว่ดังกล่าว

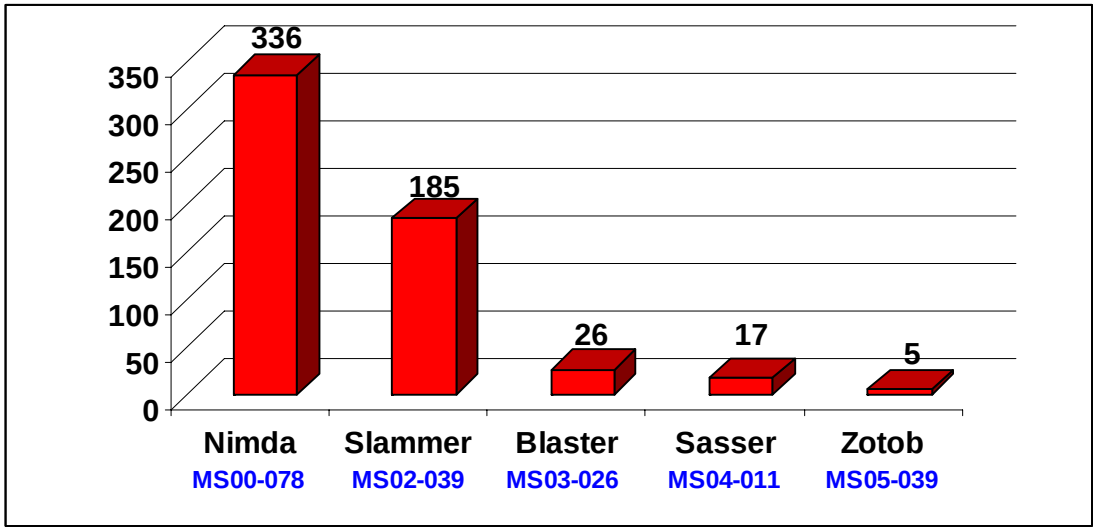
1. จากวงจรข้างต้นพบว่าช่วงที่ระบบจะปลอดภัยต่อความเสี่ยงของช่องโหว่คือช่วงระหว่างหลังการติดตั้งโปรแกรมซ่อมแซมช่องโหว่ จนถึงก่อนการค้นพบช่องโหว่ใหม่ ยิ่งช่วงนี้กว้างเท่าไรระบบยิ่งมีความมั่นคงปลอดภัยมากยิ่งขึ้น

2. ช่วงของการเกิดช่องโหว่ Zero Day จะเกิดระหว่างการค้นพบช่องโหว่ใหม่จนถึงผู้ผลิตรับทราบว่ามีช่องโหว่เกิดกับระบบ โดยเวลาจะสั้นหรือยาวนั้นขึ้นกับว่าช่องทางการแพร่กระจายข่าวสารรวดเร็วเพียงใด อีกทั้งขึ้นกับว่าข้อมูลเหล่านั้นถูกค้นพบโดยใคร ซึ่งหากเป็นแฮกเกอร์ก็ย่อมมีความเป็นไปได้ที่จะเกิด Zero Day

3. หลังจากการค้นพบช่องโหว่ถือเป็นช่วงที่สำคัญมากสำหรับผู้ใช้งานระบบ และผู้ดูแลระบบ เพราะช่วงนี้จะเป็นช่วงที่มีการแพร่กระจายของไวรัสคอมพิวเตอร์ และหนอนอินเทอร์เน็ตที่อาศัยช่องโหว่นี้เป็นจำนวนมาก ระบบจะได้รับความเสียหายมากหากไม่สามารถป้องกันหรือซ่อมแซมช่องโหว่ได้ทันเวลา

กรณีศึกษาผลกระทบจากช่องโหว่แบบ Zero Day

โดยมากแล้วช่องโหว่ที่มีผลต่อความมั่นคงปลอดภัยมักจะถูกนำไปสร้างเป็นไวรัสคอมพิวเตอร์หรือหนอนอินเทอร์เน็ต แผนภูมิแท่งที่ 1 แสดงระยะเวลาที่เกิดไวรัสคอมพิวเตอร์ หรือหนอนอินเทอร์เน็ตที่สำคัญ หลังจากประกาศการค้นพบช่องโหว่ ซึ่งรวบรวมสถิติโดยทีมงาน ThaiCERT



แผนภูมิแท่งที่ 1 แสดงจำนวนวันที่ไวรัสคอมพิวเตอร์ หรือหนอนอินเตอร์เน็ตเกิดหลังจากประกาศการค้นพบช่องโหว่

เห็นได้ชัดว่าระยะเวลาของการเกิดไวรัสคอมพิวเตอร์ หรือหนอนอินเตอร์เน็ตเร็วขึ้นเรื่อยๆ หลังจากประกาศการค้นพบช่องโหว่ ซึ่งแน่นอนว่ายิ่งเวลาดังกล่าวสั้นเท่าไร การป้องกัน และซ่อมแซมช่องโหว่ของระบบก็จำเป็นจะต้องทำให้รวดเร็วมากยิ่งขึ้นเท่านั้น จากสถิติแสดงให้เห็นว่ามีความเป็นไปได้สูงที่จะมีไวรัสคอมพิวเตอร์ หรือตัวหนอนอินเตอร์เน็ตกับช่องโหว่แบบ Zero Day ที่ไม่มีการประกาศจากผู้ผลิต ออกมาสร้างความเสียหายอีกจำนวนมากในอนาคต

นอกจากนี้กรณีศึกษาของช่องโหว่ของโปรแกรม Internet Explorer หมายเลข CVE-2005-1790 [4] ชื่อ Microsoft Internet Explorer JavaScript "windows()" Code Execution Vulnerability [5] ถือเป็นช่องโหว่แบบ Zero Day ได้เช่นเดียวกัน เนื่องจากมีการเผยแพร่ข่าวสารจากผู้เชี่ยวชาญของช่องโหว่นี้ พร้อมทั้ง Proof Of Concept ของ Exploits Code ก่อนออกโปรแกรมซ่อมแซมช่องโหว่

แนวทางป้องกัน

ความเสี่ยงที่เกิดจากช่องโหว่แบบ Zero Day ถือได้ว่าเป็นความเสี่ยงที่ใหม่และท้าทายมากสำหรับผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย การติดตั้งโปรแกรมซ่อมแซมช่องโหว่เพียงอย่างเดียวไม่ใช่แนวทางแก้ไขความเสี่ยงดังกล่าว การกำจัดความเสี่ยงชนิดนี้ถือได้ว่าทำได้ยาก แต่ทำได้โดยการลดระดับความเสียหายของความเสี่ยงชนิดนี้ ซึ่งมีแนวทางดังต่อไปนี้

- ควรใช้ซอฟต์แวร์เสริมสร้างความมั่นคงปลอดภัย เช่น Antivirus, Intrusion Detection System(IDS) เป็นต้น ที่มีคุณลักษณะการทำงานแบบ heuristics [7]
- ควรเปิดการใช้งานคุณลักษณะด้านความมั่นคงปลอดภัยในระบบปฏิบัติการบางชนิดที่มี เช่น SELinux ใน Linux Kernel, Security Level ใน FreeBSD Kernel เป็นต้น
- หมั่นตรวจสอบความผิดปกติของระบบเครือข่าย หรือคอมพิวเตอร์
- ผู้ใช้งานทั่วไปควรทำการสำรองข้อมูลที่สำคัญอย่างสม่ำเสมอ
- องค์กรควรมีนโยบายแผนการกู้ระบบให้ทำงานได้อย่างต่อเนื่อง (Business Continue Plan) ซึ่งนโยบายนี้อาจจะประกอบด้วย การสร้างทีมงานตอบสนองต่อเหตุการณ์การบุกรุก (Computer Security Incident Response Team, CSIRT) ระบบสำรองข้อมูล ระบบกู้คืนข้อมูล เป็นต้น
- ติดตามข่าวสารช่องโหว่อย่างต่อเนื่องและสม่ำเสมอจากแหล่งข้อมูล [1]

สรุป

ความเสี่ยงจากช่องโหว่ชนิด Zero Day ถือเป็นสิ่งท้าทายใหม่ต่อการเสริมสร้างความมั่นคงปลอดภัยของระบบสารสนเทศ ความเสี่ยงนี้มีผลกระทบกับทุกระดับไม่ว่าจะเป็นผู้ใช้งาน ผู้ดูแลระบบ รวมทั้งผู้พัฒนาผลิตภัณฑ์ นอกเหนือจากการสร้างความมั่นคงปลอดภัยพื้นฐาน(เช่น การติดตั้งไฟร์วอลล์ การอัพเดตซอฟต์แวร์ใหม่ล่าสุดเสมอ การติดตั้งโปรแกรม Antivirus หรือการติดตั้งโปรแกรม IDS เป็นต้น) การรับรู้ข่าวสารทุกด้านของระบบความมั่นคงปลอดภัยถือว่าเป็นสิ่งที่สำคัญมาก ยิ่งได้รับข้อมูลได้เร็วเท่าไร และแก้ไขได้รวดเร็วเท่าไรก็จะทำให้ลดผลกระทบจากความเสี่ยงชนิดนี้ได้ และหากได้รับผลกระทบจากความเสี่ยงนี้แล้ว การตอบสนองต่อเหตุการณ์การบุกรุกให้รวดเร็วที่สุดถือว่าเป็นสิ่งที่สำคัญเช่นเดียวกัน ซึ่งในอนาคตมีแนวโน้มที่ช่องโหว่ชนิดนี้จะเพิ่มมากขึ้น และก่อความเสียหายให้ระบบเครือข่าย และคอมพิวเตอร์ได้อย่างมาก

เอกสารเพิ่มเติม

[1] เว็บไซต์รวบรวมข่าวสารช่องโหว่
BugTraq Mailling List: SecurityFocus
http://www.securityfocus.com/archive/1

Vulnerability Database: SecurityFocus
http://www.securityfocus.com/vulnerabilities

Advisory Database : Packet Strom
http://packetstormsecurity.nl/alladvisories/advisories/

CERT/CC Vulnerability Note Database
http://www.kb.cert.org/vuls

ThaiCERT Advisory
http://www.thaicert.org/advisory/cert.php

Secunia monitors vulnerabilities
http://secunia.com/

Microsoft Security Bulletin
http://www.microsoft.com/athome/security/update/bulletins/default.mspx

Red Hat Errata
http://rhn.redhat.com/errata/

Debian Security Advisory
http://www.debian.org/security/

FreeBSD Security Advisory
http://www.freebsd.org/security/

Security Advisory By Distro: LinuxSecurity
http://www.linuxsecurity.com/content/view/101887/154/

[2] มาตราฐานการกำหนดชื่อช่องโหว่ด้วย CVE (Common Vulnerabilities and Exposures)
http://www.thaicert.org/paper/basic/cve.php

[3] Wikipedia, Zero Day
http://en.wikipedia.org/wiki/Zero_day

[4] CVE-2005-1790
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CAN-2005-1790

[5] Microsoft Internet Explorer JavaScript "windows()" Code Execution Vulnerability
http://www.thaicert.org/advisory/alert/msiejs.php

[6] Wikipedia, Heuristic (computer science)
http://en.wikipedia.org/wiki/Heuristic_%28computer_science%29