สงครามข้อมูลข่าวสารกับการประยุกต์ใช้

(ตอนจบ)

(Information Warfare and Application)

น.อ.ภาณุฤทธิ์ ยุกตะทัต
รองผู้อำนวยการกองวิชาวิศวกรรมเครื่องกลเรือ ฝ่ายศึกษา โรงเรียนนายเรือ

การที่สงครามข้อมูลข่าวสารเริ่มมีปริมาณมากขึ้น โดยเฉพาะบนเครือข่ายอินเตอร์เน็ตซึ่งเชื่อมโยงข้อมูลทั่วถึงกันทั่วโลก โดยเฉพาะอย่างยิ่งมีการประยุกต์ใช้ไว้รัสคอมพิวเตอรโจมตีเพื่อทำให้เกิดความเสียหายต่อข้อมูลอย่างแพร่หลาย ยิ่งข้อมูลที่มีความสำคัญต่อการบริหารงานขององค์กร กระทรวงกลาโหม โดยกองบัญชาการทหารสูงสุด จึงได้ออกระเบียบ กองบัญชาการทหารสูงสุดว่าด้วย การรักษาความปลอดภัยระบบสารสนเทศ พุทธศักราช ๒๕๔๖ โดยกำหนดมาตรฐานการรักษาความปลอดภัยให้หน่วยงานในกระทรวงกลาโหมปฏิบัติดังนี้

๖.๓ มาตรฐานการรักษาความปลอดภัยข้อมูล

๖.๓.๑ เพื่อให้ข้อมูลมีความปลอดภัยและสามารถใช้ในการประมวลผลได้อย่างมีประสิทธิภาพ จะต้องดำเนินการในด้านการรักษาความปลอดภัยดังนี้

๖.๓.๑.๑ ให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พุทธศักราช ๒๕๔๔พร้อมทั้งปฏิบัติตามระเบียบกองบัญชาการทหารสูงสุดว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศ พุทธศักราช ๒๕๔๖ และระเบียบที่เกี่ยวกับการรักษาความปลอดภัยของเหล่าทัพที่กำหนดไว้

๖.๓.๑.๒ มีการกำหนดสิทธิ์ในการเข้าถึงข้อมูลตามระดับความรับผิดชอบ

๖.๓.๑.๓ การรักษาและป้องกันความลับของข้อมูล

(๑) ต้องไม่เข้าถึงข้อมูลของผู้อื่นโดยไม่ได้รับอนุญาตจากหน่วยเจ้าของข้อมูล

(๒) ห้ามทำการพิมพ์หรือ copy data ที่เป็นความลับ เว้นแต่ได้รับอนุญาตจากหน่วยเจ้าของข้อมูล

๖.๓.๑.๔ ต้องจัดให้มีแผนการสำรองข้อมูล/ การกู้คืนสภาพระบบข้อมูล และทดสอบอย่างน้อยปีละ ๖ ครั้ง โดยสอดคล้องกับระดับความสำคัญของระบบข้อมูลที่มีผลกระทบต่อความมั่นคงของกองทัพ

๖.๓.๒ การรักษาความปลอดภัยฐานข้อมูล

๖.๓.๒.๑ System Administrator ต้องไม่มีสิทธิ์ในการเข้าถึงฐานข้อมูล

๖.๓.๒.๒ Database Administrator ต้องไม่ใช้ Default Username/Default Password และไม่ตั้ง Username/Password ที่ง่ายต่อการคาดเดา

๖.๓.๒.๓ Database Administrator ต้องจัดทำบัญชีรายชื่อผู้มีสิทธิ์เข้าถึงข้อมูลในแต่ละระดับของฐานข้อมูล ดำเนินการตรวจสอบความปลอดภัยของข้อมูล ลักษณะการเข้าถึง และการเรียกใช้ข้อมูลอย่างสม่ำเสมอ

๖.๓.๓ มาตรฐานการรับส่งข้อมูลข่าวสาร (Information-Transfer Standards) เป็นมาตรฐานสำหรับให้บริการการรักษาความปลอดภัยสารสนเทศระหว่างการรับส่งข้อมูลข่าวสารทั้งในระบบและระหว่างระบบซึ่งเป็นส่วนที่สำคัญโดยจะต้องจัดให้มีโครงสร้างพื้นฐานกุญแจสาธารณะ (Public Key Infrastructure :PKI) ตามมาตรฐานที่กระทรวงเทคโนโลยีสารสนเทศและการสื่อสารกำหนดสำหรับ การรักษาความปลอดภัยในการรับส่งข้อมูลข่าวสารที่ต้องกำหนดไว้เป็นมาตรฐาน ได้แก่ มาตรฐาน ระบบ end system (host standards) และมาตรฐานระหว่างเครือข่าย (internetworking standards)

๖.๔ มาตรฐานการรักษาความปลอดภัยระบบเครือข่าย

มาตรฐานการรักษาความปลอดภัยระบบเครือข่ายของกองทัพไทย

๖.๔.๑ ต้องมีการกำหนดนโยบายการบริหารจัดการเครือข่ายที่เข้มงวดและชัดเจนเกี่ยวกับ

๖.๔.๑.๑ บุคคล ให้มีคณะกรรมการความปลอดภัยของข้อมูลและเครือข่ายและมีการกำหนดข้อปฏิบัติของ เจ้าหน้าที่ผู้ใช้ในการใช้งานเครือข่ายและผู้ดูแลเครือข่าย

๖.๔.๑.๒ เอกสาร ให้มีการจัดทำคู่มือการตรวจสอบระบบ, อุปกรณ์ประกอบระบบและขั้นตอนการปฏิบัติ, บันทึกการเปลี่ยนแปลงเกี่ยวกับระบบเฉพาะรายการที่สำคัญ, รายงานปัญหาข้อขัดข้องและการแก้ไข

๖.๔.๑.๓ สถานที่

- การรักษาความปลอดภัยพื้นที่ ต้องจัดให้มีมาตรการควบคุมการเข้า – ออก พื้นที่ที่ติดตั้งระบบคอมพิวเตอร์ เครือข่ายสื่อสาร และที่เก็บอะไหล่สำรอง โดยต้องมีการบันทึกเวลาของผู้เข้า-ออก หรือกรณีบุคคลภายนอกมีความจำเป็นต้องเข้าออกพื้นที่ จะต้องจัดเจ้าหน้าที่ติดตามหรือหากคนภายนอก จะต้องทำการ Access อุปกรณ์ใดจะต้องได้รับอนุญาตจากผู้มีสิทธิ์
- เขตหวงห้ามเด็ดขาด Server Room, Network Equipment

๖.๔.๑.๔ อื่น ๆ

- เครือข่ายสื่อสารข้อมูล ใช้ระบบโทรคมนาคมทหารเป็นหลัก
- ข้อกำหนด (Protocol) ที่ใช้ในการรับ-ส่งข้อมูล ต้องมีการควบคุมและการตรวจสอบข้อผิดพลาดตาม Ethernet IEEE 802.3 CSMA/CD (Carrier Sense Multiple Access with Collision Detection)

๖.๔.๒ ต้องแยกระบบเครือข่ายภายในที่สำคัญ (Internal Network) คือ ระบบเครือข่ายสารสนเทศเพื่อการควบคุมบังคับบัญชา (C3I) และระบบเครือข่ายสารสนเทศเพื่อการบริหาร (MIS) ออกจากระบบเครือข่ายที่เชื่อมต่อออกสู่ภายนอก (External Network) และพร้อมที่จะเชื่อมต่อถึงกันผ่านเกทเวย์รักษาความปลอดภัย (Secure Gateway) เมื่อต้องการ

๖.๔.๓ การส่งสารสนเทศที่มีชั้นความลับผ่านระบบเครือข่ายสารสนเทศเพื่อการบริหารที่สามารถเชื่อมต่อถึงระบบเครือข่ายภายนอก จะต้องได้รับอนุมัติจากเจ้าของเรื่องสารสนเทศผู้มีสิทธิ์แและอำนาจในสายงานที่กำหนดชั้นความลับนั้นก่อน เมื่อได้รับอนุมัติแล้ว สารสนเทศกำหนดชั้นความลับจะต้องส่งเข้ารหัส (Encryption) โดยมาตรฐานที่ได้รับการรับรองแล้ว

๖.๔.๔ ต้องมีการควบคุมการอนุญาตให้เข้ามาในระบบ (Access Control)

- Port Protection : การป้องกันการเข้ามาในระบบโดยผ่านช่องทาง หรือ Port
- Automatic call back : การป้องกันการเรียกเข้าในระบบโดยไม่ได้รับอนุญาต
- Differentiated Access Right : การกำหนดระดับสิทธิ์

๖.๔.๕ ต้องมีระบบตรวจสอบความถูกต้องของเครื่องคอมพิวเตอร์ในเครือข่าย (Authentication in Distributed System)

- มีการป้องกันการปลอมแปลงตัว Server
- มีการป้องกันการขโมย หรือแอบดัดแปลงข้อมูลระหว่างติดต่อสื่อสาร
- มีการป้องกันแอบบันทึกข้อมูลการขออนุญาตเข้ามาในระบบ

๖.๔.๖ ต้องมีการป้องกันการรั่วไหลของข้อมูล จากการส่งผ่านระบบเครือข่าย(Traffic Control)

๖.๔.๗ ต้องมีการรักษาความถูกต้องของข้อมูลที่ถูกส่งผ่านระบบเครือข่าย (Data Integrity)

๖.๔.๘ ต้องติดตั้งกำแพงไฟ (Firewall) ในการรักษาความปลอดภัยของระบบเครือข่าย

๖.๔.๙ ให้มีการนำระบบและ/หรืออุปกรณ์ประกอบอื่น ๆ มาติดตั้งเพื่อเสริมระบบการรักษาความปลอดภัยตามเทคโนโลยีใหม่ที่เปลี่ยนแปลงอยู่เสมอ คือ

๖.๔.๙.๑ Intrusion Detection System (IDS)

๖.๔.๙.๒ Viruses, Trojans and Worms Protection

๖.๔.๙.๓ Disaster Prevention and Discovery

๖.๔.๙.๔ Backup or Redundant Network

๖.๔.๙.๕ Redundant Servers

๖.๔.๙.๖ Backup UPS

๖.๕ มาตรฐานการรักษาความปลอดภัยระบบอินเตอร์เน็ต

๖.๕.๑ ไม่อนุญาตให้ผู้ใช้เข้าถึงแฟ้มข้อมูลหรือระบบงานภายในที่มีชั้นความลับโดยผ่านทางระบบอินเตอร์เน็ต

๖.๕.๒ ห้าม Download ข้อมูลข่าวสารหรือโปรแกรมรวมถึงการเปิดรับ E-mail ที่ไม่รู้จักเพื่อป้องกันไวรัสโปรแกรมแอบแฝง เช่น ไวรัสคอมพิวเตอร์

๖.๕.๓ ห้าม รับ-ส่ง ข้อมูลทุกประเภทที่มีชั้นความลับผ่านทางระบบอินเตอร์เน็ต ต้องมีการเข้ารหัสลับข้อมูลและผ่านการตรวจสอบลายเซ็นอิเล็กทรอนิกส์ (Digital Signature) ตามมาตรฐานของกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

๖.๕.๔ สำหรับมาตรฐานการรักษาความปลอดภัยเว็บ (Web Security Standard) กำหนดใช้มาตรฐาน The Transport Layer Security (TLS) Protocol, Secure Socket Layer (SSL) และ SMTP Service Extension for Secure SMTP over TLS เป็นต้น

๖.๖ มาตรฐานรหัสผ่าน (Password)

การรักษาความปลอดภัยในหลาย ๆ ด้าน เช่น ข้อมูลระบบงาน ระบบเครือข่าย จำเป็นต้องใช้รหัสผ่าน (Password) เป็นเครื่องมือในการดำเนินการดังนั้นจึงได้กำหนดการบริหารจัดการเกี่ยวกับ รหัสผ่าน (Password) ให้มีการใช้เพื่อเพิ่มความปลอดภัยยิ่งขึ้น จึงกำหนดให้เจ้าหน้าที่ด้าน System Administrator, Database Administrator, Network Administrator และ Application Administrator ปฏิบัติดังนี้

๖.๖.๑ ข้อปฏิบัติการตั้งค่า Password เพื่อการเข้าถึง (access) System, Network, Database และ Application ของผู้ดูแลบริหารจัดการ (Administrator) กำหนดไว้ดังนี้

๖.๖.๑.๑ ต้องกำหนดให้เป็น Single Administrator ต่อ Single Password (ห้าม Share Password)

๖.๖.๑.๒ ต้องตั้งค่า Password ให้มีความยาวไม่น้อยกว่า ๖ ตัวอักษร

๖.๖.๑.๓ ต้องไม่นำ Password เดิมมากลับใช้ซ้ำอีก

๖.๖.๑.๔ ห้าม Save Password เก็บไว้ใน Logon menu

๖.๖.๑.๕ ต้องกำหนดรอบระยะเวลาการเปลี่ยน Password (Set expiration

date) ทุก ๆ ๙๐ วัน (เว้นแต่อุปกรณ์หรือระบบงานที่ไม่สามารถกระทำได้ทางเทคนิค)

๖.๖.๒ ข้อปฏิบัติในการบังคับใช้รหัสผ่าน (password) ที่เกี่ยวข้องกับผู้ใช้ (User)

๖.๖.๒.๑ Network logon Password ต้องจัดให้มีการ Force Password expiration

๖.๖.๒.๒ Application logon Password ให้เป็นไปตามข้อตกลงกับ User

๖.๖.๒.๓ Logon Username/Password session (Authentication) ต้องกำหนดให้มีการ Encryption

๖.๖.๒.๔ การสร้างและส่งมอบ Password ให้กับ User ต้องกำหนดมาตรการให้หน่วยผู้ใช้ (User) เกิดความมั่นใจและปลอดภัย

๖.๖.๒.๕ ในกรณีที่ผู้ใช้ (User) ลืมรหัสผ่าน (Password) ต้องกำหนดให้มีมาตรการการตรวจสอบและยืนยันตัวตนผู้ขอรหัสผ่าน (Password) ใหม่

๖.๖.๒.๖ ต้อง Hidden หรือ Encrypt Password files ของ User

๖.๖.๒.๗ ต้องมีการแจ้งเตือนผู้ใช้ (User) เมื่อผู้ใช้ (User) ใช้รหัสผ่าน (Password) เพื่อพยายามเข้าสู่เครือข่ายหรือระบบงานอย่างไม่เหมาะสมหรือทำการ Disconnect User นั้นออกจากเครือข่ายหรือระบบงานทันที

๖.๖.๒.๘ กำหนดมาตรการตรวจสอบไม่ให้เจ้าหน้าที่ไม่มีสิทธิ์ เช่น เจ้าหน้าที่ ที่ลาออกโยกย้ายและพ้นจากหน้าที่ ไม่ให้เข้าถึงระบบข้อมูลด้วยรหัสผ่าน (Password) เดิม

๖.๖.๓ ข้อปฏิบัติการจัดการเกี่ยวกับ Password เพื่อให้พนักงานสามารถปฏิบัติงานทดแทน กันได้กรณีเหตุฉุกเฉิน หรือต้องให้ปฏิบัติหน้าที่ทดแทนกัน

๖.๖.๓.๑ ต้องมีการบันทึกรหัส (Password) สำหรับการเข้าถึงอุปกรณ์หรือระบบที่สำคัญไว้ในซองปิดผนึก โดยเก็บรักษาไว้ในสถานที่ที่ปลอดภัยจากการพบเห็นหรือถูกไฟไหม้ หรือบันทึกที่อยู่ในรูปของเอกสารอิเล็กทรอนิกส์ที่มีการเข้ารหัส

๖.๖.๓.๒ ต้องสามารถนำเอามาใช้ได้ในกรณีเหตุฉุกเฉิน หรือกรณีที่ต้องปฏิบัติหน้าที่ทดแทนกัน

๖.๗ การรักษาความปลอดภัยด้านบุคคล

ให้ถือปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการโดยใช้ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พุทธศักราช ๒๕๑๗ และระเบียบว่าด้วยการรักษาความลับ พุทธศักราช ๒๕๔๔ ประกอบกัน สำหรับการรักษาความปลอดภัยสำหรับผู้ปฏิบัติงาน ชั่วคราวนั้น ให้ดำเนินการ ดังนี้

๖.๗.๑ ผู้ที่มาปฏิบัติงานชั่วคราวหรือผู้ที่เข้ามารับการศึกษา หรือเจ้าหน้าที่เทคนิคของบริษัทที่เกี่ยวข้อง ซึ่งได้ทำการสร้างข้อมูลอิเล็กทรอนิกส์ไว้บนระบบข้อมูลของหน่วยจะต้องทำการลบข้อมูลนั้นทิ้งทั้งหมด เว้นแต่หน่วยงานจะอนุญาตให้เก็บไว้ได้แล้วแต่กรณี

๖.๗.๒ หน่วยจะต้องลบ Username และ Password ของผู้ปฏิบัติงานชั่วคราวทันทีเมื่อครบกำหนดสิ้นสุดการขอใช้งาน

๖.๘ การรักษาความปลอดภัยด้านเอกสาร

ให้ปฏิบัติตามระเบียบที่ออกตามมาตรา ๑๖ แห่งพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พุทธศักราช ๒๕๔๐

๖.๙ การรักษาความปลอดภัยด้านสถานที่

ให้ถือปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการโดยใช้ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พุทธศักราช ๒๕๑๗ และระเบียบว่าด้วยการรักษาความลับ พุทธศักราช ๒๕๔๔ ประกอบกัน

๗. การโจมตีด้วยไวรัส MyDoom

ถ้าเอ่ยชื่อ MyDoom หลายคนคงจะรู้จัก เพราะว่าเจ้า MyDoom นี้ ไม่ใช่อะไรที่ไหน แต่เป็นหนอนคอมพิวเตอร์ ซึ่งโด่งดังมากในช่วงเดือนมกราคม ๒๕๔๗ และมีอัตราการแพร่ระบาดสูงที่สุดในรอบ ๑๒ เดือนหลังการอาละวาดของ Blaster และ SoBig เมื่อปีที่แล้ว ซึ่งเป้าหมายของ MyDoom นั้นคือ เอสซีโอและไมโครซอฟท์ MyDoom (หรือที่รู้จักในชื่ออื่นๆคือ Novarg, Shimgapi, Mimail.R) เป็นหนอนคอมพิวเตอร์ที่ถูกพบครั้งแรกเมื่อวันที่ ๒๗ มกราคม ๒๕๔๗ เป็นหนอนประเภทแมสเมลลิ่ง (Mass Mailing) ที่แฝงตัวมากับไฟล์สกุล .bat, .cmd, .exe, .pif, .scr, หรือ .zip ซึ่งแนบมากับอีเมล์

MyDoom จะสร้างประตูหลัง (Backdoor) ไว้บนระบบ โดยไม่ทำร้ายระบบที่ติดเชื้อ แต่จะทำให้ช่องทางการสื่อสารบนอินเทอร์เน็ตคับคั่งและหยุดทำงาน นักเจาะทำลาย (Cracker) สามารถเข้ามาควบคุมระบบจากระยะไกล หรือเข้าถึงระบบเครือข่ายภายในได้ และทำการส่งคำสั่งเรียกใช้งาน (Request) จากทุก ๆ ระบบที่ติดเชื้อไปยังเว็บไซต์ของบริษัทเอสซีโอ (SCO Group) และยังส่งผลไปยังระบบ และผลิตภัณฑ์ของบริษัท หรือองค์กรอื่นๆทั่วโลกด้วย ในวันที่ ๑ กุมภาพันธ์ ๒๕๔๗ หรือที่เรียกการโจมตีเว็บไซต์ในลักษณะนี้ว่า Denial of Service (DoS) และจะยุติการแพร่ระบาดโดยสิ้นเชิงในวันที่ ๑๒ กุมภาพันธ์ ๒๕๔๗

MyDoom.B สายพันธุ์ที่ ๒ ของ MyDoom มีการปรับแต่งโค้ดภายในใหม่และแนบมากับอีเมล์ พร้อมทั้งมีระบบอีเมล์ภายในตัวเอง ทั่ว ๆ ไปจะสังเกตได้ว่า เป็นอีเมล์ที่เหมือนเป็นข้อความแจ้งเตือนข้อผิดพลาดที่ส่งกลับมาจาก Sendmail นอกจากจะมีการส่งรีเควสต์จากทุกระบบที่ติดเชื้อไปยังเว็บไซต์

ของบริษัทเอสซีโอแล้ว ยังถูกกำหนดให้ส่งรีเควสต์ขยะจากทุกๆระบบที่ติดเชื้อไปยังเว็บไซต์ของบริษัทไมโครซอฟท์ด้วย ในวันที่ ๑ และ ๓ กุมภาพันธ์ ๒๕๔๗ ตามลำดับ รูปแบบการโจมตีเป็นแบบ DOS เช่นกัน

MyDoom.B ถูกโปรแกรมมาให้ขัดขวางการเข้าถึงเว็บไซต์ของบริษัทแอนตี้ไวรัสต่าง ๆ เช่น บริษัท F-Secure และบริษัท Symantec รวมถึงเว็บไซต์สำหรับปรับปรุงระบบรักษาความปลอดภัยของไมโครซอฟท์ (วิธีแก้ไขคือ ต้องลบไฟล์บางไฟล์ออกก่อน จึงจะสามารถเข้าเว็บไซต์ดังกล่าวและอัพเดทโปรแกรมแอนตี้ไวรัสได้ โดยให้ไปอัพเดทโดยตรงที่ http://information.microsoft.com)

ถัดจากนั้นมา เมื่อวันที่ ๙ กุมภาพันธ์ ๒๕๔๗ Doomjuice หนอนคอมพิวเตอร์อีกตัวก็ได้ออกมาปฏิบัติ การร่วมกับตัวเก่า ๆ โดยมุ่งไปยังเครื่องที่ติดเชื่อ MyDoom.A และ MyDoom.B ถล่มซ้ำเว็บไซต์ Microsoft.com ด้วยข้อมูลขยะ หรือ DDos Attack (Distributed Denial of Service) ด้วยวิธีการก็อปปี้ตัวมันเองส่งไปยังเครื่องที่ติดเชื้อ โดยไม่ผ่านระบบอีเมล์ ซึ่งลักษณะการแพร่ระบาดนั้นจะมีการแพร่ระหว่างเครื่องที่ติดเชื้อโดยตรง ซึ่งจะแตกต่างจาก MyDoom ตัวอื่น แต่ทางบริษัทแอนตี้ไวรัสบางแห่งและบริษัทไมโครซอฟท์ยืนยันว่า Doomjuice เป็นสายพันธุ์หนึ่งของ MyDoom และเรียกมันว่า “MyDoom.C”

หลังจาก Doomjuice ออกมาได้ ๒ วัน ก็มี Doomjuice.B ซึ่งมีลักษณะคล้ายกัน คือ เป็นหนอนคอมพิวเตอร์ที่แพร่ระบาดในขอบเขตที่จำกัดเฉพาะเครื่องหรือระบบคอมพิวเตอร์ ที่ติดเชื้อ MyDoom อยู่แล้วเท่านั้น โดยจะก๊อปปี้ตัวเองไปยังเครื่องเป้าหมายโดยตรงภายใต้ชื่อไฟล์ “regedit.exe” และก็อปปี้ตัวเองไปไว้ในรีจีสทรีของระบบวินโดวส์ด้วย มันจะทำงานทุกครั้งที่เปิดเครื่อง และจะหยุดการทำงานในวันที่ ๑๒ กุมภาพันธ์ ๒๕๔๗ เหมือนตัวก่อน ๆ

สำหรับระบบปฏิบัติการที่มีผลกับ MyDoom ได้แก่ Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003 และ Windows XP ส่วนระบบที่ไม่ได้รับผลกระทบได้แก่ DOS, Linux, Macintosh, OS/2, UNIX และWindows 3.x ตามข้อมูลจากบริษัท Symantec

วิธีป้องกันเบื้องต้น คือ ไม่เปิดอีเมล์ที่ส่งมาจากคนซึ่งไม่รู้จัก หรือรู้จักแต่ไม่มีนิสัยชอบส่งอีเมล์ให้ลบทิ้งสถานเดียว และอัพเดท โปรแกรมแอนตี้ไวรัสอย่างสม่ำเสมอ วิธีแก้ไขเพิ่มเติมสามารถหาดูได้จากเว็บไซต์ของบริษัทผู้พัฒนาแอนตี้ไวรัส เช่น บริษัทซิมแมนเทค (www.symantec.com), บริษัทแมคอะฟี (www.mcafee.com), บริษัทโซฟอส (www.sophos.com), บริษัท เทรนด์ไมโคร (www.trend micro.com) และบริษัทแพนด้า (www.pandasoftware.com) เป็นต้น

๘. ระบบเครือข่ายของโรงเรียนนายเรือโดนโจมตี

ในปัจจุบันอาจจะมีผู้อ่านหลายท่านที่ยังไม่เคยทราบเลยว่า ระบบเครือข่ายของโรงเรียนนายเรือก็เคยถูกโจมตีโดยสงครามข้อมูลข่าวสารเช่นกัน เริ่มแรกในการจัดตั้งระบบเครือข่ายของโรงเรียนนายเรือมุ่งเน้นที่จะให้ข้าราชการทุกคน นักเรียนนายเรือทุกนาย มีสิทธิ์ในการงานระบบเครือข่ายได้อย่างทั่วถึงตามนโยบายของฝ่ายศึกษาและโรงเรียนนายเรือ อย่างไรก็ตามการที่ผู้ใช้ (User) ทุกคนในโรงเรียนนายเรือสามารถเข้าใช้งานระบบเครือข่ายได้โดยง่าย จะทำให้ผู้ไม่หวังดีสามารถจู่โจมระบบเครือข่ายได้โดยง่ายเช่นกัน ซึ่งจากสถิติการถูกจู่โจม ระบบเครือข่ายของโรงเรียนนายเรือเริ่มจะถูกจู่โจมมากขึ้นนับตั้งแต่ขยายการต่อเชื่อมออกสู่ระบบเครือข่ายอินเตอร์เน็ตเป็น 1 Mbps. ต่อมาภายหลังศูนย์คอมพิวเตอร์ได้พยายามเพิ่มระบบการรักษาความปลอดภัยในรูปแบบต่าง ๆ ให้กับระบบเครือข่ายของโรงเรียนนายเรือจนคาดว่าจะปลอดภัย หากได้รับความร่วมมือจากผู้ใช้ทุกคน นับตั้งแต่เดือน พฤศจิกายน ๒๕๔๖ ระบบเครือข่ายของโรงเรียนนายเรือถูกโจมตีอย่างไม่หยุดยั้ง ไม่ว่าจะเป็นจากบุคคลภายนอกที่เจ้าหน้าที่ตรวจพบว่าพยายามที่จะเข้ามาใช้ทางออกอินเตอร์เน็ตของโรงเรียนนายเรือโดยที่ไม่มีสิทธิ์ หรือพยายามที่จะเข้ามาดูข้อมูลภายในโรงเรียน นอกจากนั้นบุคลากรที่ใช้ระบบเครือข่ายของโรงเรียนนายเรือยังขาดความเอาใจใส่ที่จะช่วยกันดูแลระบบเครือข่าย ที่เห็นได้อย่างเด่นชัดคือการที่ศูนย์คอมพิวเตอร์ได้ออกประกาศเตือนเรื่องเกี่ยวกับไวรัสคอมพิวเตอร์ไปแล้วหลายครั้งแต่ก็ไม่ได้รับความร่วมมือ การออกประกาศเตือนไม่ใช่ว่าจะต้องเตือนกันตลอดเวลาว่าขณะนี้มีไวรัสอะไร คุกคามอย่างไร แต่ทำเพื่อเตือนให้ข้าราชการทุกนายมีจิตสำนึกที่จะช่วยกันสอดส่อง ดูแล และแจ้งข่าวสารที่สำคัญ ให้กับผู้รับผิดชอบทราบ เคยมีบ้างไหมที่เจ้าหน้าที่ศูนย์คอมพิวเตอร์ได้รับแจ้งจาก ข้าราชการโรงเรียนนายเรือ ว่าพบเห็นผู้ใดนำเกมคอมพิวเตอร์ซึ่งติดเชื้อไวรัสมาแพร่ในระบบ จะมีก็แต่เพียงเสียงร้องว่าใช้งานอินเตอร์เน็ตไม่ได้ ซึ่งก็หมายความว่า **สายเกินไป** จะต้องใช้เวลาในการ แก้ไขกันอีกระยะหนึ่ง ไวรัสบางตัวที่ทำความเสียหายให้กับเครื่องแม่ข่ายเกือบจะทั่วโลกก็มีข่าวคราวทางหน้าหนังสือพิมพ์ เคยมีผู้ใดสนใจบ้างไหม หรือเพียงแต่ว่า รับทราบข่าวเหล่านั้น แล้วก็ทึกทักเอาเองว่า ตนเองคงไม่สามารถช่วยอะไรได้เพราะไม่รู้เรื่องบ้าง เพราะไม่มีความรู้บ้าง ผู้เขียนมั่นใจว่าข้าราชการทุกคนล้วนมีความรู้ ความสามารถ ที่เหนือกว่าคนทั่วๆ ไปในประเทศไทยอีกหลายล้านคน คงไม่ต้องบอกว่าจะช่วยกันดูแลระบบเครือข่ายของโรงเรียนนายเรือให้สามารถใช้งานได้อย่างปลอดภัยไปอีกนานได้อย่างไร

ผู้เขียนขอยกตัวอย่างที่ระบบเครือข่ายของโรงเรียนนายเรือถูกโจมตีโดยหนอนและไวรัสอินเตอร์เน็ต ในราวกลางเดือนสิงหาคม ๒๕๔๖ ระบบเครือข่ายถูกโจมตีโดยหนอนอินเตอร์เน็ต W32.Nachi worm ทำให้ระบบเครือข่ายบางจุดใช้งานไม่ได้ เจ้าหน้าที่ศูนย์คอมพิวเตอร์ต้องใช้เวลาในการแก้ไขเกือบ ๒ สัปดาห์ ต่อมาในราวปลายเดือนมกราคม ๒๕๔๗ ไวรัส MyDoom ได้เข้ามาโจมตีระบบเครือข่ายของโรงเรียนนายเรืออีกครั้งทำให้เจ้าหน้าที่ศูนย์คอมพิวเตอร์ต้องใช้เวลาทั้งหมดที่มีในการกำจัดซึ่งก็เหมือนเดิมเดินหาเครื่องคอมพิวเตอร์ที่ติดเชื้อไวรัสนี้จนเกือบทั่วโรงเรียน และทำให้ระบบ

เครือข่ายบางจุดใช้งานไม่ได้อีกเกือบ ๒ สัปดาห์เช่นเดียวกัน ต่อจากนั้นอีกไม่นานไวรัส Sasser ก็เข้ามามีบทบาทสำคัญในการโจมตีเครื่องคอมพิวเตอร์แม่ข่ายของระบบเครือข่ายทั่วโลก ซึ่งสร้างความเสียหายไปไม่น้อย และก็ส่งผลกระทบต่อระบบเครือข่ายของโรงเรียนนายเรือเช่นเดียวกัน ผู้เขียนได้ตั้งข้อสังเกตไว้อย่างหนึ่งว่าการระบาดของไวรัสและหนอนคอมพิวเตอร์ในระบบเครือข่ายของโรงเรียนนายเรือ ล้วนเกิดจากเครื่องคอมพิวเตอร์ภายในโรงเรียนนายเรือทั้งสิ้น ไม่ว่าจะเป็นการนำเครื่องคอมพิวเตอร์ที่ติดเชื้อไวรัสเข้ามาต่อเชื่อมเข้ากับระบบเครือข่าย หรือการเปิดจดหมายอิเล็กทรอนิกส์ ไฟล์ที่แนบมากับจดหมาย อิเล็กทรอนิกส์ ซึ่งมีเชื้อไวรัสอยู่ โดยรู้เท่าไม่ถึงการณ์ หรือโดยความไม่ใส่ใจในเรื่องเหล่านี้ของผู้ใช้เอง จึงทำให้ระบบเครือข่ายของโรงเรียนนายเรือล้มในที่สุด

ถึงเวลาที่โรงเรียนนายเรือจะให้ความสำคัญในเรื่องของสงครามข้อมูลข่าวสารแล้วหรือยัง ???

หากพิจารณาจากมาตรการการรักษาความปลอดภัยระบบสารสนเทศของกระทรวงกลาโหมแล้ว ยังเห็นได้ว่าโรงเรียนนายเรือซึ่งเป็นหน่วยขึ้นตรงของกองทัพเรือ ยังให้ความสำคัญในเรื่องต่าง ๆ น้อยกว่าที่ควร โดยเฉพาะอย่างยิ่งเมื่อมองปัญหาในเรื่องของสงครามข้อมูลข่าวสารที่กำลังเติบโตอย่างรวดเร็วในยุคปัจจุบัน สิ่งที่เห็นอย่างเด่นชัดคือ ไม่มีการจัดตั้งหน่วยงานขึ้นมาดูแลระบบ เครือข่ายโดยเฉพาะ ทั้ง ๆ ที่เรื่องนี้มีการหารือกันทุกปี และผู้บริหารส่วนใหญ่จะเห็นชอบในหลักการ แต่ก็ยังไม่มีการดำเนินการให้เป็นรูปธรรม ผู้เขียนเป็นส่วนหนึ่งในคณะทำงานปรับปรุงโครงสร้างการจัดหน่วยของฝ่ายศึกษา ได้เสนอแนวทางการแก้ปัญหาในหลายรูปแบบ ซึ่งรวมถึงการจัดตั้งศูนย์คอมพิวเตอร์และกำหนดอัตราให้มีผู้รับผิดชอบ ดูแลโดยตรง โดยไม่มีการเพิ่มอัตราแต่อย่างใด การดำเนินการก็ยังคงต้องทำในลักษณะเดิม คือลงคำสั่งแต่งตั้ง ครู อาจารย์ในกองวิชาต่าง ๆ (มักจะเป็น กองวิชาวิศวกรรมศาสตร์ และ กองวิชาวิศวกรรม เครื่องกลเรือ) ผู้ใดที่โรงเรียนแต่งตั้งให้ดูแลระบบเครือข่าย ก็ต้องทำงานมากกว่าครู อาจารย์ท่านอื่นเป็น ๒ เท่า ต้องศึกษาหาความรู้ในเรื่องของระบบเครือข่ายคอมพิวเตอร์ด้วยตัวเอง ต้องทำงานด้วยวิธีการลองผิด – ลองถูก มาตลอด ทั้งนี้เนื่องจาก ครู – อาจารย์เหล่านี้ไม่มีผู้ใดจบการศึกษาทางด้านเทคโนโลยีสารสนเทศโดยตรง (เท่าที่ผู้เขียนทราบส่วนใหญ่จะจบวิศวกรรมศาสตร์มหาบัณฑิตมาจากสถาบันต่างๆ) จากการปฏิบัติงานในอดีต ๒ – ๓ ปีที่ผ่านมา การที่ระบบเครือข่ายของโรงเรียนนายเรืออยู่มาได้จนถึงทุกวันนี้จะต้องมีผู้ที่เสียสละมาทำหน้าที่ Network Administrator คอยตรวจสอบ Firewall ที่ขวนขวายไปซื้อหามาติดตั้งด้วยตัวเอง เพื่อติดตามความผิดปกติ และจัดการแก้ไขปัญหาระบบเครือข่าย โดยใช้เวลาในช่วงกลางคืน บางครั้งอาจจะถึงเที่ยงคืน ตีหนึ่ง พอเช้าของวันใหม่ก็ต้องมาทำหน้าที่เป็นครูที่ดีสอน ลูกศิษย์นักเรียนนายเรือให้มีความรู้เพียงพอที่จะจบออกไปเป็นนายทหารเรือที่ดีในขณะที่มีหลายหน่วยงาน ในกองทัพเรือซึ่งมีแผนกกรรมวิธีข้อมูลฯ เป็นหน่วยงานที่คอยดูแลด้านระบบเทคโนโลยีสารสนเทศของหน่วยโดยตรง

จริงอยู่ในปัจจุบันได้เริ่มมีการจัดตั้งระบบฐานข้อมูลด้านกำลังพล และระบบฐานข้อมูลด้านวัสดุคงคลังไว้บ้างแล้ว แต่ศูนย์คอมพิวเตอร์ยังจำกัดการใช้งานให้อยู่ในวงแคบ เฉพาะผู้ที่เกี่ยวข้องโดยตรง ทั้งนี้เนื่องจากเท่าที่สังเกต ยังเห็นว่าข้าราชการในโรงเรียนนายเรือให้ความสำคัญในเรื่องของระบบเทคโนโลยีสารสนเทศน้อยเกินไป เนื่องจากอาจจะยังเข้าใจคลาดเคลื่อนอยู่ว่าระบบสารสนเทศคือเครื่องคอมพิวเตอร์ ระบบสารสนเทศคือการใช้อินเตอร์เน็ต หรือระบบสารสนเทศคือความสามารถในการใช้เครื่องพิมพ์เลเซอร์ร่วมกันได้ ความเข้าใจเหล่านี้ไม่ใช้เรื่องที่ผิดเสียทีเดียว แต่ยังเข้าใจไม่ครบวงจร การใช้อินเตอร์เน็ตในปัจจุบันนับว่าเริ่มที่จะมีอันตรายมากขึ้นในทุกด้าน เริ่มตั้งแต่ข้อมูลที่มีอยู่ในระบบเครือข่ายซึ่งอาจจะไม่ใช่ข้อเท็จจริงทั้งหมด มีสื่อต่างๆ ที่ไม่เหมาะสมกับสถาบันการศึกษาเป็นจำนวนมาก จนกระทั่งการแพร่กระจายของไวรัสคอมพิวเตอร์เมื่อเปิด E-mail หรือเปิด Attachment File ต่าง ๆ ถึงแม้ว่าขณะนี้ศูนย์คอมพิวเตอร์ได้จัดตั้งกำแพงไฟ (Firewall) ไว้สำหรับป้องกันสิ่งเหล่านี้ไว้บ้างแล้ว หากแต่สิ่งที่เกิดขึ้นใหม่ ๆ ก็ใช่ว่าบุคคลเพียง ๒ – ๓ คน จะทราบความเคลื่อนไหวตลอดเวลา โดยเฉพาะอย่างยิ่งในกรณีที่เจ้าหน้าที่ศูนย์คอมพิวเตอร์ฯ ต้องทำหน้าที่หลักในการเป็นอาจารย์สอนนักเรียนนายเรือ จึงทำให้มีโอกาสพลาดพลั้งต่อปัจจัยจากภายนอกได้ง่าย

นับตั้งแต่เดือนสิงหาคม ๒๕๔๖ เป็นต้นมา เจ้าหน้าที่ศูนย์คอมพิวเตอร์ได้ตระเวนเดินไปทั่วทั้งโรงเรียน เพื่อหาเครื่องคอมพิวเตอร์ซึ่งติดไวรัสดังกล่าวและกำจัดไวรัสไม่ให้แพร่เข้ามายังระบบเครือข่าย และข้อเท็จจริงที่พบก็คือส่วนใหญ่การที่ระบบเครือข่ายของโรงเรียนนายเรือติดไวรัส มักจะมาจากการนำเชื้อไวรัส จากภายนอกเข้ามาติดภายในระบบเครือข่ายโดยตรง ไม่ว่าจะอยู่ในรูปแบบของเกมคอมพิวเตอร์ที่มีเชื้อไวรัส หรือสำเนาไฟล์งานที่ทำมาจากที่อื่นและติดเชื้อไวรัสเข้าเผยแพร่ภายในระบบเครือข่ายของโรงเรียนนายเรือ การที่เจ้าหน้าที่ศูนย์คอมพิวเตอร์ทั้งหมดจะต้องมีภารกิจในการเป็นคณะทำงาน หรือคณะอนุกรรมการต่าง ๆ ในการสอบคัดเลือกบุคคลพลเรือนเข้าเป็นนักเรียนเตรียมทหารในส่วนของกองทัพเรือ ทำให้ไม่มีเวลาดูแลระบบเครือข่ายดังเดิม ซึ่งประจวบเหมาะกับการติดเชื้อไวรัสในระบบเครือข่าย ที่คาดว่าอาจจะมาจากเครื่องคอมพิวเตอร์เพียงไม่กี่เครื่องภายในโรงเรียนนายเรือเอง แต่ก็ทำให้ขอบเขตของความเสียหายขยายตัวไปทั่วทั้งโรงเรียน จนกระทั่งไม่สามารถใช้งานได้ในที่สุด ผลลัพธ์ ที่ได้ก็คือ นักเรียนนายเรือไม่สามารถเข้าไปค้นคว้าหาข้อมูลเพิ่มเติมผ่านทางเครือข่ายอินเตอร์เน็ตได้ นักเรียนนายเรือไม่สามารถเข้าไปดูบทเรียนในเครือข่ายอินทราเน็ตที่อาจารย์จัดทำไว้ให้ได้ ไม่สามารถส่งงานมอบผ่านระบบเครือข่ายของโรงเรียนนายเรือได้ ผู้ใช้งานระบบอินทราเน็ตภายในโรงเรียนนายเรือไม่สามารถส่งข้อมูล ข่าวสารถึงกันและกันได้เช่นเดิม และยิ่งไปกว่านั้นในสถานการณ์เช่นนี้ กองทัพเรือยังคงต้องจ่ายค่าใช้บริการอินเตอร์เน็ตให้กับบริษัทผู้ให้บริการอีกเดือนละหลายหมื่นบาท สิ่งเหล่านี้คงตอบคำถามที่ว่าถึงเวลาแล้วหรือยังที่โรงเรียนนายเรือจะให้ความสำคัญในเรื่องของการทำสงครามข้อมูลข่าวสารในโลกยุคไซเบอร์ในปัจจุบัน ?????