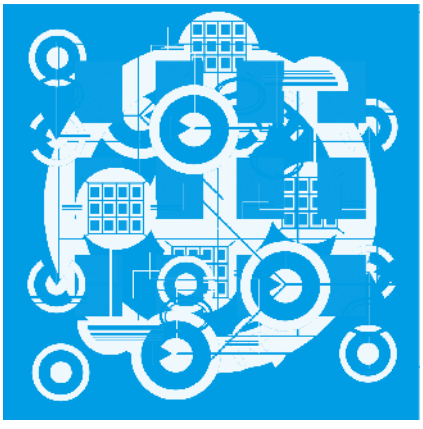
Information Security Awareness เรื่องสำคัญที่ไม่ควรมองข้าม

วิชญ์ศุทธ์ เมาระพงษ์
ที่ปรึกษาโครงการประจำกระทรวง ICT
สังกัดสถาบันวิจัยและให้คำปรึกษาแห่งมหาวิทยาลัยธรรมศาสตร์

เป็นที่ทราบกันดีอยู่แล้วว่าในปัจจุบัน Information Technology หรือ IT เข้ามามีบทบาทอย่างมากต่อการดำเนินกิจกรรมทางธุรกิจ ซึ่งรวมถึงการบริหารจัดการในเรื่องต่างๆ ภายในองค์การ สิ่งหนึ่งที่สำคัญและจำเป็นต้องพูดถึงคือเรื่องของ Information Security (INFOSEC) โดยปกติทั่วไปแล้วเราก็มักนึกถึงเรื่องของไวรัสคอมพิวเตอร์ หรือเรื่องของ Hacker เป็นหลักเพราะเป็นเรื่องที่เราได้ยินได้ฟังอยู่เป็นประจำแทบทุกวัน โดยเฉพาะเวลาไวรัสติดเครื่องคอมพิวเตอร์ของเราก็ต้องหาโปรแกรมกำจัดไวรัสมาทำการ “clean” ไวรัสเหล่านั้น จากนั้นอีกไม่นานก็มีไวรัสตัวใหม่ๆ ออกมาอีกเป็นวัฏจักรไม่มีวันจบสิ้น ขณะเดียวกันพวก Hacker ทั้งมือโปรและพวกมือใหม่ที่ส่วนใหญ่เป็นเยาวชนที่อยากลองวิชา ซึ่งจะเรียก Hacker พวกนี้ว่า “script kiddies” และส่วนใหญ่จะจู่โจมมายังระบบสารสนเทศขององค์การต่างๆ อยู่เป็นประจำ ถ้าโชคร้ายเจอ Hacker ที่มีความรู้ความสามารถสูงเจาะเข้าระบบสารสนเทศของเรา ใน



เบื้องต้นที่พบเห็นกันอยู่บ่อยก็คืออาจมีการเปลี่ยนหน้า web pages หรือถูกลบข้อมูลสำคัญๆ บ้าง แต่ในบางครั้งก็อาจจะใช้เครื่องแม่ข่ายในระบบสารสนเทศขององค์การเราเป็น “ฐานที่มั่น” และใช้แอบอ้างเพื่อจู่โจมไปยังองค์การหรือหน่วยงานอื่น โดยที่เราไม่รู้ตัว เป็นต้น

การแก้ปัญหาในเบื้องต้นก็มักจะมีการติดตั้งโปรแกรม Anti-Virus ติดตั้งอุปกรณ์ Firewall และ อุปกรณ์ IDS (Intrusion Detection System) เพื่อป้องกันและดักจับการบุกรุกเข้าเครือข่ายสารสนเทศขององค์การโดยบุคคลไม่พึงประสงค์ รวมทั้งการติดตั้ง Patch ที่แก้ปัญหา Bug และช่องโหว่ (Vulnerabilities) ต่างๆ ที่อยู่ในระบบปฏิบัติการที่เราใช้อยู่ไม่ว่าจะเป็น Microsoft Windows หรือจำพวก Unix หลังจากนั้นเรามักจะพบว่าองค์การ หรือหน่วยงานส่วนใหญ่ที่มีการลงทุนไปกับด้าน INFOSEC เป็นจำนวนมากนั้น ก็ยังเผชิญกับปัญหาเดิมๆ อยู่ เช่น การติดไวรัส หรือถูก Hacker เจาะระบบสารสนเทศซ้ำอีกหลายต่อหลายครั้งโดยใช้ช่องทางใหม่ๆ ซึ่งเครื่องของเจ้าหน้าที่ที่เป็น User ทั่วไป หรือของผู้บริหารระดับสูง ซึ่งไม่ใช่ผู้ที่มีความรู้ทางด้านเทคนิคนั้น มักมีปัญหาเกิดขึ้นอยู่บ่อยครั้งเหมือนกับว่าสิ่งที่เราได้ดำเนินการไปไม่ว่าจะเป็น Firewall หรือ IDS นั้น แทบจะช่วยอะไรไม่ได้มาก นอกจากนี้พวกเจ้าหน้าที่ System

Administrator ของระบบสารสนเทศต่างๆ ที่องค์การใช้งานอยู่ก็มักจะไม่ค่อยสนใจกับการติดตั้ง Patch หรือ Hotfix ต่างๆ เพื่อปิดช่องโหว่ที่มีบนระบบอีกด้วย จนเป็นเหตุให้ถูก Hack ได้ง่ายขึ้น เรียกว่า **ลงทุนไปมากแต่ก็ยังแก้ปัญหาทางด้าน Information Security ไม่สำเร็จ**

การแก้ปัญหาด้านระบบการรักษาความปลอดภัยคอมพิวเตอร์นั้นต้องมีการทำอย่างเป็นระบบและมีความต่อเนื่อง องค์การต่างๆ จึงพยายามที่จะพัฒนา **"Security Policy"** หรือ **"นโยบายในการใช้งานระบบคอมพิวเตอร์ให้ปลอดภัย"** ซึ่งจะต้องประกอบไปด้วย**นโยบาย (Policy) มาตรฐาน (Standard) ระเบียบปฏิบัติ (Procedure)** และ**แนวทางในการดำเนินการ (Guideline)** ซึ่งทั้ง 4 หัวข้อนี้มีความหมายที่แตกต่างกัน กล่าวคือ **Policy ก็คือนโยบายในภาพรวมที่กระชับและได้ใจความ** เรียกว่า "Goal" หรือเป้าหมายที่เราต้องการบรรลุ ขณะที่ **Standard จะพูดถึงมาตรฐานที่ต้องบังคับในการปฏิบัติจริง** เช่น การกำหนดรหัสผ่านต้องใช้เป็นตัวอักษรผสมกับตัวเลขและมีความยาวไม่ต่ำกว่า 8 อักขระ เป็นต้น ส่วน **Procedure ก็หมายถึงรายละเอียดปลีกย่อยเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่ง Standard ที่ได้วางไว้สำหรับ Guideline เป็นแนวทางในการปฏิบัติที่ไม่ได้บังคับ แต่จะเป็นการแนะนำเพื่อให้เจ้าหน้าที่ผู้ปฏิบัติสามารถบรรลุเป้าหมายได้ง่ายยิ่งขึ้น**

หลายองค์การมีการลงทุนในเรื่อง "Security Policy" โดยว่าจ้างองค์การที่ปรึกษาผู้เชี่ยวชาญด้านระบบรักษาความปลอดภัยมาให้คำแนะนำและจัดทำเป็น Security Policy ออกมาใช้ในองค์การ รวมทั้งมีการทำ Security Assessment หรือ Penetration test กับระบบสารสนเทศที่ใช้งานอยู่และยังลงทุนกับ Firewall และ IDS อีกเป็นเม็ดเงินจำนวนมาก แต่ผลลัพธ์ที่ได้หลังจากทำการ Implement ในเรื่องดังกล่าวผ่านไปราว 2-3 เดือนก็พบว่าสิ่งที่เกิดขึ้นนั้นไม่เป็นไปตามที่ได้วางแผนไว้ โดยปัญหาใหญ่ก็คือ การขาดความร่วมมือจากเจ้าหน้าที่และผู้บริหารขององค์การ ที่ส่วนใหญ่ยังไม่เข้าใจเรื่อง "Information Security" ดีพอและยังคิดว่าหน้าที่ในการจัดการเรื่องระบบรักษาความปลอดภัยให้กับคอมพิวเตอร์และเครื่องแม่ข่าย รวมไปถึงระบบสารสนเทศนั้นเป็นหน้าที่ของฝ่าย IT เท่านั้น

จะเห็นว่าเมื่อขาดความร่วมมือจากเจ้าหน้าที่ระดับผู้ใช้ ผู้ปฏิบัติงานจนถึงระดับผู้บริหารขององค์การ จึงเป็นเรื่องยากที่จะทำให้องค์การมีความปลอดภัยทางสารสนเทศในระดับที่น่าพอใจ Security Policies ที่พัฒนาขึ้นมาอย่างรอบคอบและสมบูรณ์แบบก็อาจเป็นเพียงแค่เนื้อความบนกระดาษที่ไม่มีใครนำไปประพฤติปฏิบัติ แม้กระทั่งเจ้าหน้าที่ System Administrator เองเพราะทุกคนเห็นเป็นเรื่องไกลตัว หรือคิดว่าไม่ใช่หน้าที่รับผิดชอบของตน

ดังนั้น เรื่อง "Security Awareness" จึงเป็นสิ่งสำคัญที่องค์การต้องให้ความสนใจเป็นอย่างยิ่งไม่ว่าจะทำการติดตั้ง Firewall IDS หรือ Antivirus Program ไปแล้ว หรือยังไม่ได้ติดตั้งและไม่ว่าจะมี Security Policy แล้ว หรือยังไม่ได้เริ่มเขียนขึ้นมาใช้งานเลยก็ล้วนแต่ต้องสนใจใน "Security Awareness" เช่นกัน

"Security Awareness" จะเน้นไปที่ "ตัวบุคคล" ที่มีส่วนเกี่ยวข้องเป็นหลัก เพราะถ้าปราศจากความร่วมมือและความเข้าใจของทุกคนในองค์การแล้ว เรื่องความปลอดภัยคอมพิวเตอร์ที่ดีในระดับที่น่าพอใจนั้นก็จะไม่สามารถเกิดขึ้นได้ เพราะไม่ว่าเราจะลงทุนกับ Firewall, IDS, VPN, Content Security, Anti-Virus Solution ทั้ง Hardware และ Software ไปมากมายเท่าใดก็ตาม เราก็ต้องมีการจัดฝึกอบรมเจ้าหน้าที่ในเรื่อง Information security เพราะเจ้าหน้าที่ขององค์การต้องใช้คอมพิวเตอร์กันแทบทุกคน ไม่ว่าจะเป็น User ทั่วไป System Administrator ผู้บริหารระดับกลาง รวมทั้งผู้บริหารระดับสูง แม้กระทั่งตัวเราเองที่เป็น "Security Manager" หรือ "Security Admin" ให้ทุกคนทราบและตระหนักว่าเรื่องการรักษาความปลอดภัยระบบคอมพิวเตอร์นั้นเป็นความรับผิดชอบของทุกคน ไม่ใช่แต่เพียงแผนกคอมพิวเตอร์เท่านั้น

อ่านต่อฉบับหน้า