ร.ปมท.บ.
เลขรับ 215
วันที่ ๘ ต.ค. ๕๘

งานเลขานุการกรมการ สน.
วันที่ - 8 ต.ค. 2558
เลขรับที่ 20919
เวลา

บันทึกข้อความ

ส่วนราชการ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ส่วนยุทธศาสตร์ฯ โทร. ๕๑๑๐๑

ที่ มท ๐๒๑๐.๕/ ๓๓๖ **วันที่** ๗ ตุลาคม ๒๕๕๘

เรื่อง สรุปผลการสัมมนา "Security Health Check Day : หน่วยงานของท่านพร้อมเข้าสู่ Digital Economy หรือยัง"

เรียน ปลัดกระทรวงมหาดไทย

๑. เรื่องเดิม

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) ได้จัดงานสัมมนา "Security Health Check Day : หน่วยงานของท่านพร้อมเข้าสู่ Digital Economy หรือยัง" เมื่อวันที่ ๖ ตุลาคม ๒๕๕๘ ณ ศูนย์ประชุมเดอะสเปซ ถนนพระราม ๙ กรุงเทพฯ และปลัดกระทรวงมหาดไทยมอบหมายให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเข้าร่วมงานสัมมนาดังกล่าว (เอกสาร ๑)

๒. ข้อเท็จจริง

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารขอรายงานสรุปผลการประชุม ดังนี้

๒.๑ จากข้อมูลสถิติด้านภัยคุกคามไซเบอร์ของไทยปี ๒๕๕๗ ที่รวบรวมโดยศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย หรือไทยเซิร์ต (ThaiCERT) พบการโจมตีด้วยโปรแกรมไม่พึงประสงค์ (Malicious Code) มากที่สุด คิดเป็นสัดส่วนร้อยละ ๔๓.๓ โดยอาศัยการหลอกลวงให้ผู้ใช้งานเรียกใช้งานโปรแกรมก่อนจึงจะสามารถทำการโจมตีได้ เช่น Virus, Trojan หรือ Spyware ต่าง ๆ หรือบางครั้งอาจทำการโจมตีได้ด้วยตนเอง เช่น Worm เป็นต้น การกู้ข้อมูลในทางตรงจะทำได้ยากเนื่องจากผู้โจมตีจะเข้ารหัสลับไว้เพื่อเรียกค่าไถ่จากผู้ใช้งาน แต่สามารถกู้ข้อมูลในทางอ้อมโดยการนำข้อมูลหรือระบบที่สำรองไว้มาดำเนินการ ดังนั้น จึงต้องดำเนินการสำรองข้อมูลอย่างสม่ำเสมอ และทดสอบด้วยว่าสามารถกู้คืนจากข้อมูลที่สำรองไว้ได้จริง เพราะถ้าสำรองไว้แต่กู้คืนไม่ได้ ก็ไม่มีประโยชน์

๒.๒ สภาพปัญหาเกี่ยวกับการเจาะระบบเว็บไซต์ในประเทศไทย มีดังนี้ (๑) เว็บไซต์ส่วนใหญ่อยู่ในส่วนของภาครัฐและภาคการศึกษา (๒) ผู้พัฒนาเว็บไซต์พัฒนาโดยคำนึงถึงแต่ฟังก์ชันการใช้งาน ไม่คำนึงถึงเรื่องความมั่นคงปลอดภัย ส่งผลให้เว็บไซต์ที่พัฒนามีช่องโหว่ ซึ่งช่องโหว่เดียวก็เพียงพอให้เว็บไซต์ถูกควบคุมและใช้เป็นเครื่องมือขอผู้เจาะระบบได้ทันที (๓) ผู้ดูแลเครื่องบริการเว็บไม่มีความตระหนักในการเฝ้าระวังแบบ Realtime บางครั้งใช้เวลาเป็นเดือนหรือเป็นปีกว่าจะรู้ตัวว่าถูกเจาะระบบ ทำให้การแก้ปัญหาเป็นไปได้ช้า และส่วนใหญ่หน่วยงานภายนอกเป็นผู้แจ้งให้เจ้าของระบบเว็บไซต์ทราบว่าเว็บของคุณถูกเจาะระบบแล้ว เนื่องจากผู้ดูแลระบบไม่มีการนำข้อมูลจาก Log มาวิเคราะห์ หากมีการวิเคราะห์ก็จะเห็นความผิดปกติของการทำงานของระบบและดำเนินการตรวจสอบต่อไป (๔) การแก้ปัญหาที่ปลายเหตุทำให้ถูกเจาะระบบซ้ำซาก และบางครั้งถูกใช้เป็นฐานในการโจมตีผู้อื่นต่อไป ซึ่งความผิดจะตกอยู่ที่หน่วยงานเจ้าของเว็บไซต์

๒.๓ ในการจัดทำข้อกำหนด (Term of Reference : TOR) โครงการจ้างพัฒนาเว็บไซต์สามารถดาวน์โหลดมาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ (Website Security Standard : WSS) จากเว็บไซต์ของ สพธอ. (https://standard.etda.or.th/wp/wp-content/uploads/2014/09/Website-Security-Standard_V6E6.2.pdf) (เอกสาร ๒) มาเป็นแนวทางในการจัดทำ TOR เพื่อการป้องกัน ตรวจสอบ ลดความเสี่ยง หรือสามารถรับมือกับภัยคุกคามที่มีต่อเว็บไซต์ เพื่อสร้างความเชื่อมั่นต่อหน่วยงานได้ ทั้งนี้ การทำให้เว็บไซต์มีความมั่นคงปลอดภัยนั้น ยังจำเป็นต้องอาศัยการบริหารจัดการและการดูแล การดำเนินการตามข้อเสนอแนะมาตรฐานนี้ยังมิได้

/เป็นสิ่งที่...

เป็นสิ่งที่รับรองว่าเว็บไซต์มีความมั่นคงปลอดภัยโดยสิ้นเชิงจากการโจมตี หรือการบุกรุกระบบ หรือขาดความเข้มแข็งในการบริหารจัดการเว็บไซต์ในทางปฏิบัติ หรือมีภัยคุกคามในรูปแบบที่ไม่เคยเกิดขึ้นมาก่อน (Zero Day Attack) หรือถูกโจมตีเพื่อเข้ามาในระบบโดยไม่ได้รับอนุญาตหรือโดยมิชอบ (Unauthorized Access)

๒.๔ ThaiCERT ให้คำแนะนำว่าภัยคุกคามจากการใช้อินเทอร์เน็ตมักเกิดจากพฤติกรรมการใช้งานของของผู้ใช้ (user) หากผู้ใช้งานปลอดภัย ระบบเครือข่ายภายในองค์กรก็จะปลอดภัย เครือข่ายองค์กรอื่น ๆ ที่มาร่วมใช้งานระบบก็ปลอดภัย เกิดเป็นห่วงโซ่แห่งความปลอดภัย แต่หากเกิดปัญหา สามารถขอคำปรึกษาได้ที่สายด่วน ๑๒๑๒ หรืออีเมล office@thaicert.or.th

หลักการเบื้องต้นที่ช่วยให้ใช้อินเทอร์เน็ตได้ปลอดภัยมีดังนี้ (๑) ไม่คลิกลิงก์ หรือเปิดไฟล์อีเมล์ที่น่าสงสัย ถ้าไม่ไว้ใจควรถามจากผู้ส่งโดยตรง (๒) ตั้งนโยบายของระบบปฏิบัติการเพื่อป้องกันปัญหาจากไวรัสคอมพิวเตอร์ (๓) ติดตั้งและปรับปรุง Antivirus รวมทั้งทำการปรับปรุงระบบปฏิบัติการให้ทันสมัยอยู่เสมอ (๔) ทำการสำรองข้อมูลอยู่เสมอ และควรเก็บข้อมูลสำรองในอุปกรณ์ที่ไม่ได้เชื่อมต่อกับคอมพิวเตอร์ หรือระบบเครือข่ายอื่น ๆ (๕) การแชร์ข้อมูลร่วมกันผ่านระบบเครือข่าย ให้ตรวจสอบสิทธิ์เข้าถึงข้อมูล และกำหนดสิทธิ์ให้ผู้ใช้มีสิทธิ์เฉพาะไฟล์ที่จำเป็นเท่านั้น

๒.๕ การโจมตีทางไซเบอร์หลายรูปแบบ แม้แต่เด็กที่ไม่มีความรู้ด้านคอมพิวเตอร์ก็สามารถทำได้ง่าย ๆ การตรวจจับและป้องกันก็ทำได้ยาก เพราะการโจมตีมากจากแหล่งที่หลากหลาย และจำแนกการโจมตียากว่าประสงค์ร้ายหรืออยากเข้าใช้งานจริง ๆ เช่น กรณีเว็บไซต์ของหน่วยงานภาครัฐหลายหน่วยงานไม่สามารถใช้งานได้เมื่อปลายเดือนกันยายน ๒๕๕๘ เกิดจากการทำดีดอส DDoS (Distributed Denial-of-Service) ไม่อาจตามได้ว่าใครเป็นคนลงมือเพราะเป็นการกดปุ่ม F5 เพื่อเข้าเรียก (request) หน้าเว็บไซต์นั้นเป็นปริมาณมากจนทำให้เครื่องคอมพิวเตอร์แม่ข่าย (Server) ทำงานหนักเนื่องจากตอบสนอง (Response) ไม่ทัน และล่มในที่สุด เพราะรองรับการเรียกเข้าจากผู้ใช้งานปริมาณมากในเวลาเดียวกันไม่ไหว

วิธีป้องกันไม่ให้ตกเป็นเหยื่อถูกเจาะระบบเว็บไซต์หน่วยงานรัฐ คือ (๑) ควรปิดกั้นการเข้าถึงบริการหรือเว็บไซต์ที่ถูกควบคุมดังกล่าวทันที เพื่อป้องกันไม่ให้ผู้ไม่ประสงค์ดีเข้าถึงข้อมูลหรือกระทำกิจกรรมอันเป็นผลเสียต่อระบบในส่วนอื่น ๆ เพิ่มเติม (๒) รีบตรวจสอบข้อมูล Log จากระบบหรือบริการต่าง ๆ เพื่อยืนยันช่องทางการเข้าโจมตี และประเมินสถานการณ์ผลกระทบที่อาจเกิดขึ้น (๓) ควรปรับปรุงระบบให้เป็นเวอร์ชันล่าสุดเสมอ เพื่อลดความเสี่ยงจากการโจมตีช่องโหว่ของซอฟต์แวร์ที่อาจมีผู้ค้นพบขึ้นได้ (๔) ควรมีการตรวจสอบช่องโหว่ของระบบหรือซอฟต์แวร์ที่ใช้อย่างสม่ำเสมอ และให้รีบแก้ไขปัญหาทันทีที่ได้รับแจ้งเหตุการณ์โจมตีจาก ThaiCERT เพื่อลดผลกระทบจากการที่ข้อมูลในระบบ ซึ่งอาจรวมถึงข้อมูลของผู้ใช้งานถูกขโมยออกไป

๒.๖ โครงการ ThaiCERT Government Monitoring System (ThaiCERT GMS) มี ๒ ส่วน ส่วนที่ ๑ Government Threat Monitoring System ช่วยวิเคราะห์รูปแบบการโจมตีที่เกิดกับระบบไอทีของหน่วยงานภาครัฐ ตั้งเป้าหน่วยงานที่เข้าร่วมโครงการ ๔๐ แห่ง ส่วนที่ ๒ Government Website Protection System ช่วยป้องกันการโจมตีเว็บไซต์ของหน่วยงานภาครัฐ ตั้งเป้าหน่วยงานที่เข้าร่วมโครงการ ๘๐ แห่ง หน่วยงานภาครัฐที่สนใจให้ ThaiCERT เข้าไปช่วยดูแล ติดต่อได้ที่ thaicert-gms@thaicert.or.th หรือโทร ๐ ๒๑๒๓ ๑๒๑๒

๒.๗ สรุปการบรรยายของ Mr. MohD Zabri Adil Bin Talib, Head of Digital Forensics Department of CyberSecurity Malaysia ได้ดังนี้ ความพร้อมทางด้านการพิสูจน์หลักฐานทางคอมพิวเตอร์ (Computer Forensics) ส่งผลให้ตำรวจทำงานสืบสวนได้ง่ายและรวดเร็วขึ้น ผู้ทำการสืบสวนจะนำอุปกรณ์คอมพิวเตอร์ (เช่น ไฟล์ที่อยู่ในคอมพิวเตอร์ อุปกรณ์อิเล็กทรอนิกส์ โทรศัพท์มือถือ รวมถึงหลักฐานดิจิตอลที่ถูกสร้างจากระบบคอมพิวเตอร์ เป็นต้น) ที่เกี่ยวข้องกับคดีหรือเรื่องที่กำลังสืบสวนมาค้นหาข้อมูล และวิเคราะห์ เพื่อหาเอาพยานหลักฐานสำหรับใช้ในการประกอบการสืบสวนหรือใช้ค้นหาผู้กระทำความผิดออกมา สิ่งที่ได้คือ สามารถบ่งชี้ผู้ต้องสงสัยว่า

/เป็นผู้กระทำผิด...

เป็นผู้กระทำผิด บ่งชี้ผู้สมคบคิดกับผู้กระทำผิด บ่งชี้เว็บไซต์ที่ผู้กระทำผิดเข้าไปใช้ อีเมลที่มีการส่งและรับ ไฟล์ที่ถูกลบทิ้งและไฟล์ที่ซ่อนอยู่ ข้อมูลส่วนบุคคลด้านการเงิน/ที่อยู่ ฯลฯ ความสามารถและความสนใจของบุคคลนั้น ถ้าไม่มีความพร้อมทางด้านการพิสูจน์หลักฐานทางคอมพิวเตอร์ก็จะไม่มีข้อมูลให้ตำรวจวิเคราะห์เพื่อสืบสวนหาผู้กระทำผิด

สอดคล้องกับคำบรรยายของวิทยากรจาก สพธอ. และ ThaiCERT กรณีหน่วยงานไม่ได้ดูแลระบบเองนั้น เมื่อเกิดภัยคุกคาม หน่วยงานส่วนใหญ่ไม่มีข้อมูลสำหรับวิเคราะห์หาวิธีแก้ไขหรือสืบหาผู้กระทำผิด มีคำแนะนำให้ดำเนินการดังนี้ (๑) จัดทำบัญชีทรัพย์สินเพื่อควบคุมการเพิ่มเติม การเปลี่ยนแปลง และการยกเลิกการใช้งานทรัพย์สินในระบบสารสนเทศ และปรับปรุงให้บัญชีทรัพย์สินมีความถูกต้องและเป็นปัจจุบันอยู่เสมอ รวมทั้งกำหนดค่าระดับความสำคัญให้แก่ทรัพย์สิน กำหนดระดับชั้นความลับให้แก่ข้อมูล เพื่อใช้เป็นข้อมูลตั้งต้นในการประเมินความเสี่ยง/แก้ไขควบคุมความเสี่ยง (๒) จัดทำแผนบริหารความเสี่ยง (Risk Management Plan) และแผนบริหารความต่อเนื่องขององค์กร (Business Continuity Plan) ปรับปรุงข้อมูลผู้ประสานงานหลักให้เป็นปัจจุบันอยู่เสมอ และมีช่องทางประกาศให้หน่วยงานภายนอกทราบข้อมูลที่เป็นปัจจุบัน เพื่อการประสานงานในการแก้ไขปัญหาอย่างทันเวลาและจำกัดความเสียหายที่อาจจะเกิดขึ้น ควรมีการฝึกซ้อมการดำเนินการตามแผนเป็นประจำ เพื่อให้มั่นใจว่าผู้ปฏิบัติสามารถดำเนินการตามขั้นตอนที่เตรียมไว้ได้อย่างมีประสิทธิภาพ (๓) เตรียมความพร้อมของผู้ใช้ระบบสารสนเทศทั่วไปเป็นประจำทุกปี เช่นเดียวกับการซ้อมหนีไฟ เพื่อให้ผู้ใช้คอมพิวเตอร์ในองค์กรตลอดจนผู้บริหารได้ตระหนักรู้ และสร้างประสบการณ์ในการรับมือกับภัยคุกคามอย่างได้ผลในทางปฏิบัติ โดยจำลองสถานการณ์ที่อาจเกิดขึ้นจริง หรือเคยเกิดขึ้นจริงมาแล้ว ตัวอย่างเช่น การส่งอีเมลหลอก (Phishing email) เมื่อผู้เข้ารับการอบรมพบว่าอุปกรณ์คอมพิวเตอร์ของตนติดไวรัสหรือเกิดความเสียหาย ต่อไปก็จะคลิกลิงก์หรือเปิดไฟล์ที่จากอีเมลหลอกน้อยลง ต่อให้มีกระบวนการที่ดีแต่คนไม่ปฏิบัติตามก็ไม่เกิดประโยชน์ ต่อให้มีเทคโนโลยีการป้องกันที่ดี แต่ถ้าคนใช้งานไม่เป็นก็ไม่เกิดประโยชน์ คนเป็นปัจจัยที่ทำให้เกิดปัญหา แต่ก็สามารถใช้คนในการแก้ปัญหาอย่างมีประสิทธิภาพได้ ดังนั้นจึงควรพัฒนาบุคลากรของหน่วยงานให้มีความพร้อมในการแก้ไขปัญหาเมื่อเกิดภัยคุกคาม

๒.๘ สรุปการบรรยายของ Ms. Lim May-Ann, Managing Director, TRCP Pte Ltd, & Executive Director, Asia Cloud Computing Association ได้ดังนี้ แผนดำเนินการในการสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของรัฐ ควรจัดทำในแบบองค์รวม ระบุสถานการณ์สมมติต่าง ๆ เพื่อพัฒนากลยุทธ์การรักษาความมั่นคงปลอดภัยที่แข็งแกร่ง โดยสนับสนุนการใช้กลยุทธแบบ "ก่อน ระหว่าง และหลังเกิดเหตุ" ซึ่งมีแผนดำเนินการ ๕ ขั้น คือ (๑) สร้างความตระหนักและการให้ความรู้แก่สาธารณะ (๒) จัดทำแผนการเตรียมความพร้อมในการจัดการภัยคุกคาม (๓) ป้องกันระบบเครือข่ายจากภัยคุกคาม จัดตั้งแนวทางด้านกฎหมายเพื่อเรียกร้องค่าเสียหายเมื่อถูกโจมตี และพัฒนาแนวปฏิบัติที่ดีและมีมาตรฐานในการปรับปรุง (upgrade and update) ซอฟต์แวร์ให้เป็นปัจจุบัน (๔) ตอบสนองต่อภัยคุกคาม (๕) ลดผลกระทบอันเกิดจากภัยคุกคาม (เอกสาร ๓)

หน่วยงานของรัฐสามารถดำเนินการตรวจสอบ (checklist) ตามรายการตรวจสอบสำหรับแผนความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของรัฐได้ตาม (เอกสาร ๔)

๓. ข้อเสนอ

จึงเรียนมาเพื่อโปรดทราบ

(นายอนุพงศ์ สุขสวนิตย์)
ผู้อำนวยการส่วนอำนวยการ รักษาราชการแทน
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ตป.

(นายณัฐพงศ์ ศิริชนะ)
รองปลัดกระทรวงมหาดไทย ปฏิบัติราชการแทน
ปลัดกระทรวงมหาดไทย