TRPC | ETDA สพธอ
www.etda.or.th

PUBLIC DATA AT RISK:
CYBER THREATS TO THE NETWORKED GOVERNMENT

ความเสี่ยงของข้อมูลที่เปิดเผยสู่สาธารณะ
ภัยคุกคามด้านเทคโนโลยีสารสนเทศต่อภาครัฐ

ชื่อเรื่อง **ความเสี่ยงของข้อมูลที่เปิดเผยสู่สาธารณะ: ภัยคุกคามด้านเทคโนโลยีสารสนเทศต่อภาครัฐ**

เขียนโดย บริษัท TRPC

แปลโดย ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต)
สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร

พิมพ์ครั้งที่ 1 กันยายน 2558

พิมพ์จำนวน 1,000 เล่ม

จัดพิมพ์และเผยแพร่โดย

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต) (Thailand Computer Emergency Response Team : ThaiCERT)

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) (สพธอ.) Electronic Transactions Development Agency (Public Organization) (ETDA)

อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี)
ชั้น 21 เลขที่ 33/4 ถนนพระราม 9
แขวงห้วยขวาง เขตห้วยขวาง
กรุงเทพมหานคร 10310

โทรศัพท์ : 0 2123 1212 | โทรสาร : 0 2120 1200

อีเมล : office@thaicert.or.th

เว็บไซต์ไทยเซิร์ต : www.thaicert.or.th
เว็บไซต์ สพธอ. : www.etda.or.th
เว็บไซต์กระทรวงฯ : www.mict.go.th

PUBLIC DATA AT RISK:

CYBER THREATS TO THE NETWORKED GOVERNMENT

ความเสี่ยงของข้อมูลที่เปิดเผยสู่สาธารณะ

ภัยคุกคามด้านเทคโนโลยีสารสนเทศต่อภาครัฐ

http://www.trpc.biz

สารบัญ

บทสรุปผู้บริหาร

"รัฐสามารถเอื้อประโยชน์ให้กับสังคมได้ดีขึ้น ถ้ารัฐสามารถใช้ประโยชน์จากเทคโนโลยีสารสนเทศและการเชื่อมต่อเครือข่ายอินเทอร์เน็ตได้อย่างเหมาะสม อีกทั้งยังเปิดโอกาสให้รัฐสามารถสื่อสารกับประชาชนของตัวเองหรือประชาคมโลก" ตัวอย่างการใช้เทคโนโลยีสารสนเทศที่เอื้อประโยชน์ให้รัฐได้ เช่น การรวบรวมและใช้ประโยชน์จากข้อมูลที่มีมากขึ้น การลดขั้นตอนกระบวนการ การลดการใช้กระดาษ ทั้งนี้เพื่อเพิ่มประสิทธิภาพและประสิทธิผลในการให้บริการภาครัฐต่อประชาชน รวมไปถึงการเพิ่มประสิทธิภาพกระบวนการภายในของภาครัฐเอง

อย่างไรก็ตามการใช้ประโยชน์จากเทคโนโลยีสารสนเทศที่เพิ่มขึ้นก็ทำให้รัฐมีความเสี่ยงกับภัยคุกคามร้ายแรงเพิ่มขึ้น ทั้งต่อความมั่นคงของชาติ โครงสร้างพื้นฐาน ข้อมูล และความสัมพันธ์ระหว่างประเทศ ทั้งนี้การระบุและจัดการภัยคุกคามเหล่านี้เป็นเรื่องสำคัญต่อการสร้างยุทธศาสตร์ที่แข็งแกร่งและยืดหยุ่น (robust and resilient) ในด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศสำหรับการทำงานผ่านเครือข่ายอินเทอร์เน็ต

ในหลายประเทศ รัฐจัดให้มีเจ้าหน้าที่ระดับสูงเข้ามาดูแลงานเทคโนโลยีสารสนเทศ (เทียบเคียบกับ CTO/CIO : Chief Technology Officer/Chief Information Officer ในองค์กรเอกชน) เพื่อที่จะเข้าใจและจัดการเรื่องเทคโนโลยีสารสนเทศ จากการวิจัยพบว่าประเทศที่มีความพร้อมในการจัดการภัยคุกคามด้านเทคโนโลยีสารสนเทศจะจัดการเรื่องนี้แบบองค์รวม โดยมีกิจกรรมตัวอย่าง เช่น

- จัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (CERTs - Computer Emergency Response Teams)
- ให้ความรู้ความเข้าใจกับเจ้าหน้าที่รัฐและประชาชนโดยทั่วไป
- มีกระบวนการจัดซื้อจัดจ้างที่มั่นคงปลอดภัย (เพื่อลดความเสียหายจากภัยคุกคามประเภทมัลแวร์/ไวรัส)

หนังสือฉบับนี้มุ่งให้กรอบการทำงานแก่เจ้าหน้าที่รัฐที่ไม่ได้มีพื้นความรู้ทางด้านเทคโนโลยีสารสนเทศ เช่น เจ้าหน้าที่ด้านประชาสัมพันธ์ เจ้าหน้าที่จากงานจัดซื้อจัดจ้าง ฯลฯ ให้สามารถเข้าใจและอภิปรายประเด็นเหล่านี้ร่วมกันกับเจ้าหน้าที่รัฐที่ทำงานด้านเทคโนโลยีสารสนเทศ ในขณะที่ CTO หรือ CIO สามารถใช้เป็นเครื่องมือขอความสนับสนุนในวงกว้างจากหน่วยงานต่าง ๆ ของรัฐเพื่อหาแนวทางในการจัดการและตอบสนองอย่างเหมาะสมกับภัยคุกคามด้านเทคโนโลยีสารสนเทศต่อรัฐ

ภายในเล่มแบ่งเป็น 5 หัวข้อหลัก เริ่มจาก การใช้งานเทคโนโลยีสารสนเทศภาครัฐ ข้อมูลที่มีการจัดเก็บและบริหารโดยภาครัฐ การใช้จ่ายภาครัฐที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ ภัยคุกคามด้านเทคโนโลยีสารสนเทศที่รัฐกำลังพบในปัจจุบัน โดยมีการเสนอแนวทางที่ภาครัฐสามารถพัฒนานโยบายด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ เพื่อป้องกันภัยภัยคุกคามที่เกิดขึ้นจากการใช้เครือข่ายอินเทอร์เน็ต รวมทั้งรายการตรวจสอบ (Checklist) ที่ช่วยให้สามารถประเมินความพร้อมในการรักษาความมั่นคงปลอดภัยจากภัยคุกคามที่เกิดขึ้นจากการใช้เครือข่ายอินเทอร์เน็ต

บทที่ 1: การพึ่งพาการใช้เทคโนโลยีสารสนเทศของภาครัฐ

- การพัฒนาระบบเทคโนโลยีสารสนเทศเพื่อใช้งานในภาครัฐและบริการออนไลน์ภาครัฐ มีบทบาทสำคัญในเชิงบวกที่สามารถเพิ่มการมีส่วนร่วมกับประชาชน ทั้งนี้ประเทศสหรัฐอเมริกา เกาหลีใต้ และสิงคโปร์ ได้รับการจัดให้เป็นประเทศที่เป็นผู้นำด้านนี้

- ระบบสาธารณูปโภคและระบบการป้องกันประเทศมีการใช้งานผ่านเครือข่ายเทคโนโลยีสารสนเทศมากขึ้น

- ถ้าภาครัฐไม่มีการจัดการในการใช้เทคโนโลยีสารสนเทศอย่างเหมาะสม รัฐและประชาชนอาจจะประสบปัญหาด้านความเป็นส่วนตัว การจารกรรมข้อมูล และการขาดความปลอดภัยในการใช้บริการสาธารณะ

บทที่ 2: ประเภทของข้อมูลที่รัฐจัดเก็บในระบบเทคโนโลยีสารสนเทศ

- ข้อมูลสาธารณะและข้อมูลส่วนตัวปริมาณมากจัดเก็บและให้เข้าถึงได้ผ่านระบบเทคโนโลยีสารสนเทศของภาครัฐ ทั้งนี้ยังพบว่า นอกเหนือจากข้อมูลสาธารณะที่มีการเผยแพร่ผ่านช่องทางบริการออนไลน์ของภาครัฐ ข้อมูลที่อ่อนไหวบางประเภท เช่น เลขประจำตัวประชาชน ข้อมูลภาษี อีเมลที่ใช้ในการสื่อสารภายในรัฐบาล และข้อมูลด้านความมั่นคงปลอดภัยที่เป็นความลับ

- ข้อมูลในแต่ละระดับชั้นความลับ ต้องการความปลอดภัยและการป้องกันที่ต่างกัน ดังนั้นรัฐจึงจำเป็นต้องดำเนินการอย่างเหมาะสมในการจัดเก็บและเข้าถึงข้อมูลเพื่อสร้างความน่าเชื่อถือของข้อมูล

- การโจมตีทางระบบเทคโนโลยีสารสนเทศในหลายปีที่ผ่านมา มุ่งไปที่ข้อมูลที่ภาครัฐจัดเก็บ เช่น ข้อมูลบัตรประจำตัวประชาชน ซึ่งเหตุการณ์ดังกล่าวทำให้ความเชื่อมั่นกับภาครัฐของประชาชนลดลง และภาครัฐเองก็ต้องเสียค่าใช้จ่ายจำนวนมากในการจัดการเรื่องดังกล่าว

บทที่ 3: การใช้จ่ายด้านเทคโนโลยีสารสนเทศภาครัฐ

- ประเทศในแถบอเมริกาเหนือ ยุโรปตะวันตก และออสเตรเลีย ถือเป็นผู้นำในการใช้ทรัพยากรและการใช้จ่ายเพื่อสร้างความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศบนเครือข่ายอินเทอร์เน็ต ประเทศในแถบอ่าวเปอร์เซียและในเอเชียมีการใช้จ่ายในด้านนี้เช่นกัน หลังจากที่พบการโจมตีทางระบบเทคโนโลยีสารสนเทศบนเครือข่ายอินเทอร์เน็ต

- การใช้จ่ายด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศสำหรับบริการออนไลน์ของภาครัฐมักจะเน้นไปที่การตรวจหาและตอบสนองต่อภัยคุกคาม การแก้ไขปัญหาข้อมูลรั่วไหล รวมทั้งการจัดการเว็บไซต์และบริการออนไลน์ภาครัฐ

บทที่ 4: ประเภทของภัยคุกคามด้านเทคโนโลยีสารสนเทศต่อภาครัฐ

- ภัยคุกคามด้านเทคโนโลยีสารสนเทศต่อรัฐมีจำนวนมากและสร้างผลกระทบในหลายระดับ ตัวอย่างภัยคุกคามทางด้านเทคโนโลยีสารสนเทศที่พบได้ทั่วไป ได้แก่ การก่อการร้ายทางเทคโนโลยีสารสนเทศและการคุกคามต่อโครงสร้างพื้นฐานที่สำคัญของรัฐ การจารกรรมข้อมูลที่เป็นความลับหรือข้อมูลที่สำคัญต่ออธิปไตยของประเทศ การโจมตีแบบ Denial of Service ต่อโครงสร้างพื้นฐานสำคัญของรัฐ การจารกรรมทางด้านเทคโนโลยีสารสนเทศต่อรัฐ การโจมตีแบบต่อเนื่องขั้นสูง

- สาเหตุสำคัญที่เพิ่มความเสี่ยง เปิดโอกาสให้มัลแวร์บุกรุกเข้ามาในระบบเทคโนโลยีสารสนเทศของรัฐ และใช้ระบบทำการต่าง ๆ อันไม่พึงประสงฆ์ ได้แก่ การใช้ซอฟต์แวร์ละเมิดลิขสิทธิ์ในหน่วยงานภาครัฐ การขาดการจัดการที่ดี และการจัดซื้อจัดจ้างที่หละหลวม

บทที่ 5: แผนดำเนินการในการสร้างยุทธศาสตร์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของรัฐ

- ยุทธศาสตร์ความมั่นคงด้านเทคโนโลยีสารสนเทศที่ดี ควรมีการจัดการแบบองค์รวม และมีความสามารถในการรับมือกับการโจมตีในแง่มุมต่าง ๆ โดยคำนึงถึงวิธีการทั้งในเรื่องป้องกัน-ตอบสนอง-ลดผลกระทบ

- แผนดำเนินการที่มีประสิทธิผลในการสร้างกลยุทธ์ ควรมีขั้นตอนที่จะ

  - *เพิ่มความตระหนัก* และยกระดับของความเข้าใจในหมู่ประชาชนทั่วไป ด้วยการให้ความรู้แก่เจ้าของธุรกิจ นักเรียน และหน่วยงานของรัฐ ในเรื่องภัยคุกคามที่มีอยู่ รวมทั้งวิธีปกป้องเครือข่ายของตนจากการโจมตี

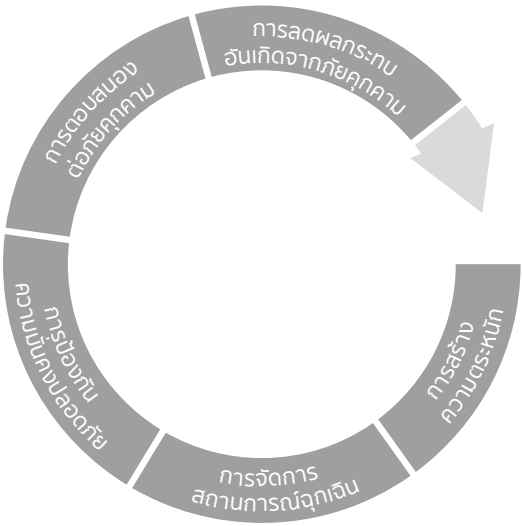
- *สร้างความพร้อม* ด้วยการสร้างศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (CERT) ที่คอยประสานงานเพื่อจัดการภัยคุกคาม รวมถึงแบ่งปันความรู้และทักษะ

- *ป้องกันการโจมตี* ผ่านการสร้างและการดูแลรักษาเครือข่ายคอมพิวเตอร์ให้มีความมั่นคงปลอดภัย รวมไปถึงการจัดซื้อที่มีประสิทธิภาพ

- *ตอบสนองอย่างมีประสิทธิผล* ต่อการโจมตี โดยให้อำนาจแก่ผู้ออกกฎหมาย ผู้มีอำนาจควบคุม ผู้จัดทำนโยบาย โดยมีระเบียบข้อบังคับที่ดี และการใช้เครื่องมือที่สามารถต่อสู้กับการโจมตีทางเทคโนโลยีสารสนเทศ

- *บรรเทาความเสียหาย* เพื่อเรียกคืนความเชื่อมั่นของประชาชนและผู้มีส่วนเกี่ยวข้อง ผ่านการสื่อสารที่มีประสิทธิภาพ กระบวนการรีวิวที่ได้จัดทำไว้ และการสร้างพันธมิตรกับภาคเอกชน รัฐบาลประเทศอื่น และองค์กรระหว่างประเทศ

รูปที่ 1 แผนดำเนินการเพื่อสร้างยุทธศาสตร์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ



บทที่ 1:

การพึ่งพาการใช้เทคโนโลยีสารสนเทศของภาครัฐ

บทที่ 1: การพึ่งพาการใช้เทคโนโลยีสารสนเทศของภาครัฐ

ในปัจจุบัน รัฐต้องรับผิดชอบต่อข้อมูลที่เพิ่มมากขึ้นกว่าในอดีต ข้อมูลที่มีความหลากหลายมีการจัดเก็บในระบบสารสนเทศที่มีการพัฒนาอย่างรวดเร็ว -ระบบที่ภาครัฐใช้ก็ล้าสมัยและอาจเป็นจุดเสี่ยงต่อภัยคุกคามความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

โครงสร้างพื้นฐาน	บริการออนไลน์ภาครัฐ	ระบบสาธารณูปโภคและโครงสร้างพื้นฐานสารสนเทศที่สำคัญ
• การเชื่อมต่อบรอดแบนด์ระดับชาติ (National Broadband Connectivity) • การเพิ่มประสิทธิภาพในการบริหารจัดการ (Management Optimization) • ระบบบริการสาธารณะ (Public Management Systems)	• ระบบชำระภาษีออนไลน์ (e-Taxes) ระบบการออกใบอนุญาต และการชำระค่าปรับ • ระบบการลงคะแนนเสียงเลือกตั้งทางอิเล็กทรอนิกส์ • ระบบประกวดราคาสาธารณะ • ระบบเพื่อให้บริการสาธารณะ • อีเมลสำหรับประชาชน	• ไฟฟ้า • ประปา • โทรคมนาคม • พลังงาน เช่น น้ำมัน LPG NGV • สื่อ เช่น ช่องสัญญาณโทรทัศน์ วิทยุ

ในปี 2556 เฉพาะหน่วยงานรัฐบาลกลางสหรัฐฯ (US Federal Agencies) มีการจัดเก็บข้อมูลราว 1.6 Petabytes และคาดว่าจะเพิ่มเป็น 2.6 Petabytes ก่อนปี 2559[1] โดยสำนักงานความมั่นคงแห่งชาติของสหรัฐอเมริกา (National Security Agency of the USA) กำลังก่อสร้าง Data Center ซึ่งคาดว่าจะเก็บข้อมูลได้ระหว่าง 1 Exabyte - 1 Yottabyte

2 แนวโน้มที่ปรับเปลี่ยนการจัดการเอกสารและข้อมูลสาธารณะในภาครัฐ ในช่วงหลัง ๆ นี้ คือ นโยบาย “รัฐบาลโปร่งใส” (Open Government) และ “การใช้เทคโนโลยี Cloud” (Cloud Initiative) โดยสิ่งที่ตามมากับแนวโน้มเหล่านี้คือระดับความเสี่ยงเรื่องความมั่นคงปลอดภัยที่เพิ่มขึ้นต่อภาครัฐ

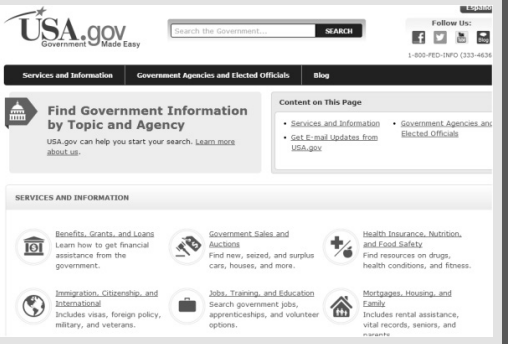
ในทุกระดับชั้นของหน่วยงานรัฐพึ่งพาการใช้งานข้อมูลที่มีคุณภาพมากขึ้น โดยส่งไปยังหน่วยงานต่าง ๆ เพื่อให้บริการที่มีคุณภาพ ทำให้ซอฟต์แวร์กลายเป็นปัจจัยสำคัญที่หน่วยงานรัฐต้องใช้ เพื่อเพิ่มประสิทธิภาพให้กับระบบ กระบวนการและการแลกเปลี่ยนข้อมูล

โครงสร้างพื้นฐานรัฐบาลอิเล็กทรอนิกส์

ตั้งแต่ปลายทศวรรษ 1990 ประเทศส่วนใหญ่ได้ประกาศนโยบายรัฐบาลอิเล็กทรอนิกส์หรือได้กำหนดแนวทางสู่การเป็นรัฐบาลอิเล็กทรอนิกส์ ยังผลให้เกิดการพัฒนาอย่างมากต่อการบริหารรัฐกิจในทุกระดับ สำนักงานเศรษฐกิจและกิจการสังคมแห่งสหประชาชาติ[2] (the United Nations Department of Economics) ได้ประกาศหลักการ เบื้องหลังแนวคิดรัฐบาลอิเล็กทรอนิกส์ คือ เพื่อปรับปรุงการทำงานภายในของภาครัฐ โดยลดค่าใช้จ่ายและลดเวลาในการทำธุรกรรม ทำให้การใช้กระบวนการทำงานและการใช้ทรัพยากรมีประสิทธิผล หรืออีกนัยหนึ่งคือ เพื่อส่งเสริมการประสานงานและการเชื่อมต่อระหว่างระบบที่เกี่ยวข้องกันกับผลลัพธ์ของการพัฒนา ในบริบทซึ่งสะท้อนความสำคัญและความเป็นสากลของการพัฒนาเหล่านี้ มีงานวิจัยจำนวนมากที่สำรวจความพร้อมของรัฐบาลอิเล็กทรอนิกส์เพื่อประเมิน

การพัฒนาโครงสร้างพื้นฐานที่เกี่ยวข้อง นอกจากการเชื่อมต่อบรอดแบนด์ การพัฒนาบุคลากร การส่งเสริมการใช้บริการออนไลน์ภาครัฐ รวมถึงตัวชี้วัดอื่น ๆ เช่น การเพิ่มประสิทธิภาพในการบริหาร (Management Optimization) เช่น การเพิ่มประสิทธิภาพระบบและเครือข่าย ระบบบริหารจัดการงบประมาณ การปฏิรูปการบริหารรัฐกิจโดยใช้เทคโนโลยีสารสนเทศ ฯลฯ และระบบที่ให้บริการ เช่น ระบบประกวดราคาทางอิเล็กทรอนิกส์ ระบบชำระภาษีออนไลน์ (e-Taxes) ระบบลงคะแนนเสียงทางอิเล็กทรอนิกส์ ฯลฯ)[3] สหรัฐอเมริกา สิงคโปร์ และเกาหลีใต้ ได้รับการจัดอันดับในเรื่องการพัฒนารัฐบาลอิเล็กทรอนิกส์ในแต่ละปีในลำดับต้น ๆ เสมอ

รูปที่ 2 สหรัฐอเมริกา ประเทศที่เป็นผู้นำ
ในการพัฒนารัฐบาลอิเล็กทรอนิกส์ ปี 2557



- เว็บของรัฐบาลสหรัฐอเมริกา (www.USA.gov) ทำให้ประชาชนเข้าถึงข้อมูลและบริการที่มองหาได้โดยตรง เว็บนี้เชื่อมโยงไปยังหน่วยงานทุกแห่ง รวมทั้งหน่วยงานของแต่ละมลรัฐ หน่วยงานส่วนท้องถิ่น และกลุ่มชาติพันธุ์ต่าง ๆ

- ตั้งแต่ปี 2553 คุณลักษณะที่เป็นการเพิ่มคุณค่า ได้แก่ 1. สามารถเข้าถึงผ่านโทรศัพท์เคลื่อนที่ 2.สามารถแจ้งเตือนเนื้อหาที่ผู้เยี่ยมชมสามารถลงทะเบียนได้ 3. สนทนาสดกับตัวแทนของรัฐ

- รัฐบาลสหรัฐฯ ยังจัดให้มีเว็บไซต์ที่เป็นภาษาสเปน (www.GobiernoUSA.gov) ซึ่งรวบรวมเว็บไซต์ของหน่วยงานภาครัฐทั้งหมดที่เป็นภาษาสเปน เพื่อให้เข้าถึงง่าย

บริการออนไลน์ภาครัฐ

ถ้าการสร้างโครงสร้างพื้นฐานรัฐบาลอิเล็กทรอนิกส์เพื่อปรับปรุงประสิทธิภาพและประสิทธิผลของการให้บริการภาครัฐ เป็นงานด้านหนึ่งของการทำงานภาครัฐที่ต้องเชื่อมโยงกับองค์กรต่าง ๆ (Networked Government) งานอีกด้านหนึ่งที่มีความก้าวหน้าในหลายประเทศ คือ การให้บริการออนไลน์ภาครัฐ หลายประเทศกำลังเปลี่ยนจากการจัดรูปแบบองค์กรแบบกระจายศูนย์ไปสู่รูปแบบการรวมศูนย์โดยให้ทุกภาคส่วนของรัฐบูรณาการเข้าหากัน เพื่อให้ประชาชนสามารถเข้าถึงบริการทั้งหมดที่รัฐให้บริการเป็นจุดเดียว โดยไม่ต้องคำนึงว่าเป็นหน่วยงานใดที่ให้บริการ ในบางประเทศ แนวทางแบบรัฐที่เชื่อมต่อเป็นหนึ่งเดียวนี้ ช่วยสร้างระบบที่โปร่งใส ทำให้เกิดการพัฒนาประสิทธิภาพและประสิทธิผลของรัฐ

ขณะที่รัฐเพิ่มบริการออนไลน์ใหม่ ๆ และให้ประชาชนมีส่วนร่วมมากขึ้น รัฐกลับต้องเผชิญปัญหาเกี่ยวกับการสร้างบริการใหม่ ๆ การรวมบริการ และการเปิดเผยข้อมูลภาครัฐ การที่ต้องเชื่อมโยงระบบที่แตกต่างกันและระบบระหว่างหน่วยงาน ทำให้เจ้าหน้าที่ของรัฐที่รับผิดชอบในการพัฒนาระบบหรือพัฒนาบริการออนไลน์จำเป็นต้องคำนึงถึง 3 ปัจจัยสำคัญ ได้แก่ Open Platforms, Interconnection, Interoperability ซึ่งสิ่งนี้ยิ่งทวีความสำคัญเมื่อภาครัฐถูกกดดันให้เปิดเผยข้อมูลเพื่อความโปร่งใส

Open Platforms, Interconnection, Interoperability เป็นสามประเด็นสำคัญที่เจ้าหน้าที่ของรัฐต้องให้ความสนใจในการพัฒนาระบบ

แนวโน้ม 2 อย่างที่เปลี่ยนวิธีจัดการเอกสารและข้อมูลสาธารณะในภาครัฐเมื่อไม่กี่ปีมานี้คือนโยบาย “รัฐบาลโปร่งใส” (Open Government) และ “การใช้เทคโนโลยี Cloud” (Cloud Initiative) รัฐบาลสหรัฐฯ อ้างว่าโครงการ “รัฐบาลโปร่งใส” ของตนทำให้ “ประชาชนเข้าถึงข้อมูลของหน่วยงานสำคัญกว่า 390,000 ชุดข้อมูล ในหัวข้อต่าง ๆ เช่น ความปลอดภัยของรถยนต์ การเดินทางทางอากาศ คุณภาพอากาศ ความปลอดภัยในสถานที่ทำงาน ความปลอดภัยในการใช้ยา โภชนาการ อาชญากรรม โรคอ้วน การจ้างงาน และสาธารณสุข”[4] รัฐบาลสหรัฐฯ ยังได้ริเริ่มโครงการที่จะบังคับให้หน่วยงานของรัฐย้ายระบบที่มีผลกระทบน้อยถึง

ปานกลางไปสู่ Cloud ภายในปี 2558 ซึ่งการเปลี่ยนแปลงเหล่านี้ส่งผลแง่มุมหนึ่งคือระดับความเสี่ยงด้านความมั่นคงปลอดภัยที่สูงขึ้น

ระบบสาธารณูปโภคและระบบการป้องกันประเทศ

ระบบสาธารณูปโภคต่าง ๆ เช่น ไฟฟ้า ประปา และ โทรคมนาคม (หรือเรียกว่าโครงสร้างพื้นฐานที่สำคัญ) หรือโครงสร้างพื้นฐานสารสนเทศที่สำคัญ (Critical Information Infrastructure - CII) เป็นระบบสำคัญที่เริ่มเชื่อมต่อกันขึ้นเรื่อย ๆ ผ่านเครือข่าย

ระบบสื่อสารโทรคมนาคมและระบบสาธารณูปโภค ก็ต้องพึ่งพาเทคโนโลยีสารสนเทศมากยิ่งขึ้นด้วย เช่น ระบบบริหารจัดการ (Management Software) ซอฟต์แวร์เรียกเก็บเงิน (Billing Software) และโปรแกรมสำเร็จรูป (Package Software) รวมถึงระบบ SCADA (Supervisory Control and Data Acquisition) ซึ่งใช้ควบคุมโรงไฟฟ้าและโรงผลิตสาธารณูปโภคต่าง ๆ แบบ Real time

จากสถานการณ์แบบนี้ได้เพิ่มความกังวลต่อความมั่นคงปลอดภัย รัฐจึงลงทุนในเครือข่ายให้มีความมั่นคงปลอดภัยอย่างเช่น GSI (Government Secure Intranet) และ GCmail (Government Connect Mail) แต่ด้วยความสามารถที่จำกัด ระบบดังกล่าวมักมีการใช้เฉพาะการสื่อสารระหว่างรัฐกับหน่วยงานภายนอกและคู่ค้า[5]

บทที่ 2:

ประเภทของข้อมูลที่รัฐจัดเก็บในระบบเทคโนโลยีสารสนเทศ

บทที่ 2: ประเภทของข้อมูลที่รัฐจัดเก็บในระบบเทคโนโลยีสารสนเทศ

ประเภทของข้อมูลที่รัฐจัดเก็บในระบบเทคโนโลยีสารสนเทศสามารถแบ่งได้เป็น 3 ประเภท ได้แก่

1. ข้อมูลภายใน (Intrinsic Data) – ข้อมูลที่สร้าง รวบรวม จัดเก็บ โดยรัฐ

2. ข้อมูลที่เกี่ยวข้องกับการทำธุรกรรมกับภาครัฐ (Commercial Data) – ข้อมูลที่เกิดจากการทำธุรกรรมและการสื่อสารระหว่างภาครัฐและภาคเอกชน

3. ข้อมูลส่วนบุคคลของภาคประชาชน (Personal Data) – ข้อมูลที่ภาคประชาชนส่งให้รัฐตามกฎระเบียบข้อบังคับหรือเพื่อประโยชน์สาธารณะ

ทั้งนี้วิธีการจัดเก็บข้อมูลสารสนเทศที่มีการประมวลผลและจัดเก็บโดยรัฐ เช่น จัดเก็บโดยจำกัดการเข้าถึงหรือให้เข้าถึงบนเครือข่ายเปิด (Open Network) หรือบน Cloud ขึ้นอยู่กับชั้นความลับของข้อมูล (Information Classification) การเผยแพร่ข้อมูลสารสนเทศของภาครัฐที่ไม่เป็นความลับทั้งบริการที่มีค่าใช้จ่ายและไม่มีค่าใช้จ่าย

ประเภทของข้อมูลที่จัดเก็บบนระบบของรัฐ

เอกสารและข้อมูลสาธารณะ		
ข้อมูลสาธารณะที่อ่อนไหว (Sensitive Information)		
ข้อมูลความมั่นคงของชาติและการป้องกันประเทศ		
ข้อมูลภายใน (Intrinsic Data)	**ข้อมูลที่เกี่ยวข้องกับการทำธุรกรรมกับภาครัฐ (Commercial Data)**	**ข้อมูลส่วนบุคคลของภาคประชาชน (Personal Data)**
ข้อมูลที่สร้าง รวบรวม จัดเก็บ โดยรัฐ	ข้อมูลที่เกิดจากการทำธุรกรรมและการสื่อสารระหว่างภาครัฐและภาคเอกชน	ข้อมูลที่ภาคประชาชนส่งให้รัฐตามกฎระเบียบข้อบังคับหรือเพื่อประโยชน์สาธารณะ

เอกสารและข้อมูลสาธารณะ

รัฐเก็บและควบคุมคลังข้อมูลที่เกี่ยวข้องกับข้อมูลของประชาชนและการทำงานของประเทศ ข้อมูลจำนวนมากซึ่งเดิมเคยเก็บในรูปกระดาษ ได้มีการแปลงเป็นข้อมูลในระบบเทคโนโลยีสารสนเทศ เนื่องจากการผลักดันเรื่องรัฐบาลอิเล็กทรอนิกส์ในช่วงคริสต์ทศวรรษ 1990 และ 2000 ทั้งนี้ ประเภทของข้อมูล ระดับการเข้าถึง และความถูกต้องของข้อมูล มีความแตกต่างกันขึ้นกับแต่ละประเทศ

โดยทั่วไป รัฐพยายามเผยแพร่ข้อมูลมากขึ้นเรื่อย ๆ ให้สาธารณชนโดยไม่คิดค่าใช้จ่าย (หรือคิดน้อยมาก) ข้อมูลดังกล่าวมักจัดให้เป็นของสาธารณะ และมีการเผยแพร่ข้อมูลในรูปแบบเอกสารของรัฐ (Public Record) เช่น ฐานข้อมูลของ

- กฎหมายประเภทต่าง ๆ – เช่น กฎหมายของนิวซีแลนด์ (www.legislation.govt.nz)

- หนังสือและเอกสารในห้องสมุดสาธารณะ – เช่น คณะกรรมการห้องสมุดแห่งชาติของสิงคโปร์ (www.nlb.gov.sg)

- สถิติอาชญากรรม – เช่น ฐานข้อมูลสถิติอาชญากรรมของ FBI สหรัฐอเมริกา (www.fbi.gov/about- us/cjis/ucr/ucr)

- ระบบจัดซื้อจัดจ้างออนไลน์ของรัฐบาล – เช่น ระบบ GeBiz ของสิงคโปร์ (www.gebiz.gov.sg)

หน่วยงานรัฐมีการเชื่อมต่อกันมากขึ้นและสร้างเอกสารจำนวนมาก ทำให้ฐานข้อมูลของภาครัฐตกเป็นเป้าของการจารกรรมข้อมูล ในปี 2555 หน่วยงานรัฐหลายแห่งในยูเครน เบลเยียม โปรตุเกส โรมาเนีย สาธารณรัฐเช็ก และไอร์แลนด์ ตกเป็นเป้าของการโจมตีโดยมัลแวร์ที่ชื่อ 'MiniDuke' ซึ่งโจมตีโดยใช้ช่องโหว่ของเอกสาร PDF[6] ไฟล์เอกสารซึ่ง "ดูเหมือนเอกสารของรัฐบาล" และมี "เนื้อหาที่เขียนไว้อย่างดี" โดยแต่งเรื่องขึ้นมาเป็นข้อมูลสิทธิมนุษยชนและนโยบายต่างประเทศ ได้ฝังมัลแวร์ไว้ ซึ่งจะทำงานเมื่อเปิดเอกสาร ทำนองเดียวกัน การโจมตีที่ญี่ปุ่นทำให้เอกสารกว่า 3,000 รายการรั่วไหลจากหน่วยงานรัฐ ซึ่งเป็นผลมาจากมัลแวร์ที่ติดมากับเอกสาร PDF เช่นกัน[7]

WikiLeaks และ การเปิดโปงของสโนว์เดน

WikiLeaks.org เป็นเว็บไซต์ที่จดทะเบียนโดย Julian Assange ชาวออสเตรเลียในปี 2542 และเริ่มดำเนินการจริงจังในปี 2549 เพื่อเป็น "ระบบที่เปิดเผยเอกสารจำนวนมากที่ติดตามไม่ได้ซึ่งเล็ดลอดออกมาให้สาธารณชนวิเคราะห์" (Uncensorable system for untraceable mass document leaking and public analysis) เอกสารลับของรัฐบาลได้มีการรายงานและเผยแพร่ผ่านความร่วมมือกับสื่อมวลชนหลายแห่ง โดยเฉพาะอย่างยิ่งหนังสือพิมพ์ The Guardian ซึ่งรวมถึงเอกสารที่รัฐถือว่าเป็นการทำลายความมั่งคงของชาติอย่างใหญ่หลวง

เอกสารลับสำคัญชิ้นแรกที่หลุดมาสู่ WikiLeaks นั้นมาจาก Chelsea Manning (ชื่อเดิม Bradley Manning) ทหารแห่งกองทัพบกสหรัฐฯ ที่ประจำการในอิรักในฐานะนักวิเคราะห์ข่าวกรอง เธอถูกตัดสินจำคุก 35 ปีจากความผิด

ในเดือนมิถุนายน 2556 Edward Snowden ผู้เชี่ยวชาญคอมพิวเตอร์ซึ่งเคยทำงานกับสำนักงานข่าวกรองกลาง (CIA) หน่วยข่าวกรองกลาโหม (DIA) และสำนักงานความมั่นคงแห่งชาติ (NSA) ได้ปล่อยเอกสารลับหลายพันชิ้น การเปิดโปงหลักนั้นเป็นเรื่องเกี่ยวกับโครงการสอดแนมระดับโลกโดย NSA ซึ่งรวมถึงการดักฟังโทรศัพท์ การสอดแนมข้อมูลบนอินเทอร์เน็ต และบันทึกตำแหน่งที่อยู่ของประชาชน ผู้กำหนดนโยบายหลายคนเรียกการเปิดโปงนี้ว่าเป็นความปราชัยครั้งใหญ่ที่สุดของงานข่าวกรองนับตั้งแต่สงครามโลกครั้งที่ 2

ข้อมูลสาธารณะที่อ่อนไหว

ข้อมูลสาธารณะจำนวนมากที่รัฐเป็นผู้ดูแลเป็นเรื่องอ่อนไหว (Sensitive Public Data) ข้อมูลนี้อาจได้แก่ ชื่อ วันเกิด หมายเลขโทรศัพท์ หมายเลขประจำตัวผู้เสียภาษี หมายเลขประจำตัวประชาชน หมายเลขหนังสือเดินทาง รายละเอียดสุขภาพ/การแพทย์ ระเบียนคนเข้าเมือง เป็นต้น

ตัวอย่างบริการของรัฐซึ่งบริการจัดการข้อมูลดังกล่าว ได้แก่

1. ทะเบียนราษฎรหรือรายชื่อผู้มีสิทธิเลือกตั้ง – เช่น ทะเบียนบัตรประชาชนและผู้มีสิทธิเลือกตั้งของบังกลาเทศ (www.nidw.gov.bd)

2. การเข้าเมือง ใบขอวีซ่าและท่องเที่ยว – เช่น ใบขอวีซ่าประเทศจีนสำหรับพลเมืองฮ่องกง

3. ระบบชำระภาษีออนไลน์ เช่น e-Tax Online ของออสเตรเลีย (www.ato.gov.au)

4. การขอใบอนุญาตประกอบธุรกิจ – เช่น ใบอนุญาตออนไลน์สำหรับประกอบธุรกิจในมลรัฐวอชิงตัน (www.bls.dor.wa.gov)

ประเด็นสำคัญประการหนึ่งคือ ข้อมูลรัฐซึ่งดูเหมือนไม่มีความสำคัญ เมื่อนำมาปะติดปะต่อจากฐานข้อมูลต่าง ๆ ก็อาจใช้บ่งชี้หรือระบุตัวบุคคลได้ ตัวอย่างที่พบทั่วไปเป็นข้อมูลที่ส่งผลกระทบต่อบุคคลหรือองค์กร เช่น ข้อมูลผู้เสียภาษี ข้อมูลประกันสังคม เวชระเบียน และข้อมูลทางพันธุกรรม[8] รายการของข้อมูลที่อ่อนไหวอาจรวมถึงข้อมูลที่เกี่ยวข้องกับการสืบสวนอาชญากรรม ข้อมูลทางการเงิน และแผนเตรียมความพร้อมฉุกเฉิน[9] ประเด็นนี้กลายเป็นปัญหาที่เกิดขึ้นจริงในเดือนเมษายน 2557 เมื่อมีการพบช่องโหว่ที่ชื่อ Heartbleed ซึ่งถึงจะไม่สามารถประมาณได้ว่ามีการใช้ช่องโหว่นี้เข้าถึงข้อมูลส่วนบุคคลไปกี่ครั้ง แต่เหตุการณ์ที่เกิดขึ้นเพียงไม่กี่ครั้งก็แสดงความร้ายแรงของสถานการณ์นี้ ตัวอย่างเช่น ในแคนาดา หมายเลขประกันสังคม 900 หมายเลข ถูกขโมยจากสำนักงานสรรพากรในช่วงเวลา 6 ชั่วโมงโดยบุคคลหรือกลุ่มบุคคลที่ใช้ช่องโหว่จาก Heartbleed[10]

ในสิงคโปร์ ประชาชนใช้ระบบที่เรียกว่า SingPass เพื่อเข้าถึงบริการออนไลน์ราว 340 บริการ มีการตรวจพบการเข้าถึงข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตในระบบ SingPass กว่า 1,500 บัญชีในปี 2557 โดยส่วนหนึ่งมีจุดประสงค์เพื่อใบอนุญาตทำงาน (Work Permit) ปลอม [11]

การประมวลผลและจัดเก็บข้อมูลสาธารณะที่อ่อนไหว มีระดับของความมั่นคงปลอดภัยต่างกันไปในแต่ละประเทศหรือแม้กระทั่งภายในประเทศ เช่น รัฐแอลเบอร์ตา ในแคนาดา บังคับให้การเข้าถึงข้อมูลที่อ่อนไหวทั้งหมดต้องได้รับอนุญาตและตรวจสอบตัวตนของผู้ใช้ว่าถูกต้อง[12] ขณะที่มลรัฐนอร์ทแคโรไลนา ในสหรัฐอเมริกา ไม่จำกัดการเข้าถึงข้อมูลที่อ่อนไหวเว้นแต่มีกฎหมายประกาศว่าต้องปกปิด[13]

การสื่อสารผ่านช่องทางอิเล็กทรอนิกส์ การจัดเก็บเอกสาร และข้อมูลอีเมลที่มีการรับส่ง

รัฐบาลสมัยใหม่ได้ปรับปรุงช่องทางสื่อสารไปสู่ช่องทางอิเล็กทรอนิกส์มากขึ้น เช่น การใช้อีเมลหรือการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ ทำให้มีปริมาณข้อมูลในการสื่อสารกันเพิ่มมากขึ้น ซึ่งข้อมูลสื่อสารจำนวนมากของเจ้าหน้าที่ในภาครัฐถือว่าเป็นข้อมูลลับ ถูกจำกัดการเข้าถึง บางครั้งก็มีเนื้อหาน่าอับอาย รัฐยังเป็นเจ้าของเอกสารจำนวนมาก เช่น เอกสารนำเสนอ (Slide Deck) เอกสารแสดงการคำนวณ (Spreadsheet) และเอกสารอื่น ๆ ที่มีข้อมูลภายในที่อ่อนไหว

ข้อมูลที่รัฐบริหารจัดการมีปริมาณที่เพิ่มขึ้นแบบก้าวกระโดด ซึ่งเพิ่มโอกาสเกิดความเสียหาย ถ้าอีเมลส่วนตัวของเจ้าหน้าที่หรือของหน่วยงานภาครัฐถูกเผยแพร่โดยไม่ได้รับอนุญาต เช่น กรณีของ WikiLeaks หรือการเปิดโปง NSA โดย Snowden ผลที่ตามมาคือความเสียหายร้ายแรงต่อหน่วยงานของรัฐที่เกี่ยวข้อง

ความเสี่ยงดังกล่าวยิ่งเพิ่มขึ้น เมื่อองค์กรต่างๆ รวมทั้งหน่วยงานของรัฐ เข้าสู่ยุคของการ “นำอุปกรณ์ส่วนตัวมาทำงาน” (Bring Your Own Device - BYOD) มากขึ้น พร้อม ๆ กับความแพร่หลายของอุปกรณ์ที่ใช้เข้าถึงข้อมูลที่หลากหลาย เช่น โทรศัพท์เคลื่อนที่ แท็บเล็ต และอุปกรณ์อัจฉริยะอื่น ๆ เช่น นาฬิกา และแว่นตา ครั้งหนึ่ง Blackberry เคยเป็นอุปกรณ์สื่อสารที่ใช้กันแพร่หลายที่สุดสำหรับแลกเปลี่ยนข้อมูลที่ห้ามโดยรัฐ ในปี 2555 CESG ของอังกฤษ ได้อนุมัติให้ใช้ iPhone เพื่อรับส่งอีเมลที่มีเนื้อหาอ่อนไหว[14]

ทั้งนี้การเปิดโปงเรื่องที่ NSA พยายามดักฟังโทรศัพท์ของ Angela Markel นายกรัฐมนตรีของเยอรมนี ทำให้มีการออกมาตรฐานความมั่นคงปลอดภัยของโทรศัพท์เคลื่อนที่และแท็บเล็ต เพิ่มมากขึ้น ปัจจุบัน Blackberry ผลิตโทรศัพท์ที่มั่นคงปลอดภัยที่สุด ซึ่งมีการเข้ารหัสลับและจำหน่ายแก่เจ้าหน้าที่ของรัฐเท่านั้น ในโลกที่กำลังพัฒนาโดยเฉพาะในเอเชีย สถานการณ์นี้ยิ่งซับซ้อนไปอีก เมื่อเจ้าหน้าที่ของรัฐจำนวนมากยังใช้อีเมลสาธารณะในการสื่อสารแบบทางการ ตัวอย่างเช่น ที่การประชุมของคณะ

กรรมาธิการเศรษฐกิจและสังคมแห่งสหประชาชาติสำหรับเอเชียและแปซิฟิก (UN-ESCAP) ปี 2555 ในกรุงเทพฯ เจ้าหน้าที่ 20 ประเทศ จาก 33 ประเทศในเอเชีย ระบุที่อยู่อีเมลซึ่งเป็นของ Gmail, Hotmail หรือ Yahoo ในแบบฟอร์มข้อมูลการติดต่อ[15]

เมื่ออีเมลส่วนตัวของเจ้าหน้าที่ในภาครัฐถูกเผยแพร่โดยแหล่งที่ไม่ได้รับอนุญาต เช่น กรณีของ WikiLeaks หรือการเปิดโปง NSA โดย Snowden ผลที่ตามมาคือความเสียหายร้ายแรงต่อหน่วยงานของรัฐที่เกี่ยวข้อง

ความเสี่ยงอีกประการหนึ่งจากสมาร์ตโฟน แท็บเล็ต และอุปกรณ์อื่น ๆ ที่รัฐบาลนำมาใช้คือ เรื่องการดาวน์โหลดแอปพลิเคชัน เช่น Juniper Research ได้เตือนว่า *“การดาวน์โหลดแอปพลิเคชัน จะยิ่งเพิ่มความเสี่ยงต่อเครือข่ายบริษัทและรัฐ เนื่องจากแอปพลิเคชันที่ไม่ได้ดาวน์โหลดจากแหล่งที่น่าเชื่อถือ เช่น Play Store หรือ App Store อาจมีมัลแวร์หรือสปายแวร์แฝงอยู่ซึ่งสามารถขโมยอีเมล SMS ประวัติการโทรศัพท์ รายชื่อลูกค้า และข้อมูลอื่น ๆ ขององค์กร แอปพลิเคชันที่มีมัลแวร์สามารถใช้อุปกรณ์เผยแพร่โทรจันและไวรัสเข้าสู่เครือข่ายองค์กร หรืออาจทำให้ข้อมูลขององค์กรรั่วไหล”*[16]

ภัยคุกคามทางด้านเทคโนโลยีสารสนเทศมุ่งไปที่ข้อมูลความมั่นคงระดับสูงของชาติ

มกราคม 2554 – รัฐบาลแคนาดารายงานว่ามีการโจมตีหน่วยงานของรัฐ ซึ่งรวมถึงสำนักวิจัยและพัฒนากลาโหมของแคนาดา การโจมตีนี้ทำให้กระทรวงการคลังและกรรมาธิการธนารักษ์ ซึ่งเป็นหน่วยงานหลักด้านเศรษฐกิจของแคนาดาต้องระงับการเชื่อมต่ออินเทอร์เน็ต

กันยายน 2555 – ในฟิลิปปินส์ เว็บไซต์ของหน่วยงานหลักด้านพาณิชย์ องค์กรพลเรือน และรัฐบาล ถูกโจมตีในวงกว้าง อันเป็นการตอบโต้ต่อพระราชบัญญัติคอมพิวเตอร์ซึ่งเป็นประเด็นร้อนในขณะนั้น

ตุลาคม 2555 - บริษัท Kaspersky ของรัสเซียค้นพบปฏิบัติการ “Red October” โจมตีคอมพิวเตอร์ทั่วโลกมาตั้งแต่ปี 2550 หรือก่อนหน้า มัลแวร์ที่ใช้โจมตีได้ขโมยข้อมูลจากสถานทูต บริษัทวิจัย ที่ตั้งทางทหาร หน่วยงานด้านพลังงาน โรงไฟฟ้านิวเคลียร์ และโครงสร้างพื้นฐานสำคัญอื่น ๆ

มกราคม 2556 – กลุ่มแฮกเกอร์ “Anonymous” เจาะระบบและแก้ไขเว็บไซต์ของหน่วยงานภาครัฐกว่า 12 แห่ง

เมษายน 2556 – กระทรวงกลาโหมสหรัฐฯ รายงานต่อรัฐสภาว่ากองทัพจีนได้เตรียมการโจมตีทางคอมพิวเตอร์บนเครือข่ายอินเทอร์เน็ตต่อรัฐบาลสหรัฐฯ และผู้รับเหมาของกระทรวงกลาโหม การโจมตีนี้ได้ขโมยข้อมูลเพียงพอที่จะให้เห็นภาพของเครือข่ายกลาโหม การส่งกำลังบำรุง และสมรรถนะทางทหาร ซึ่งอาจใช้เพื่อชิงความได้เปรียบในช่วงวิกฤต ในเดือนกรกฎาคม 2557 แฮกเกอร์ชาวจีนได้เจาะเครือข่ายของสำนักงานบริหารบุคลากรของสหรัฐฯ และขโมยข้อมูลผู้สมัครนับพันรายที่อนุญาตเข้าถึงข้อมูลลับ

ตุลาคม 2556 –กลุ่มแฮกเกอร์ “Anonymous” ได้เจาะระบบเว็บไซต์ของมูลนิธิชุมชน PAP และสภาเมืองอังโมเกียวในสิงคโปร์ เพื่อระบายความไม่พอใจต่อเหตุการณ์ต่าง ๆ ในประเทศ ต่อมาในเดือนเดียวกัน แฮกเกอร์ 2 รายเจาะเข้าเว็บไซต์ของทำเนียบประธานาธิบดีสิงคโปร์ โดยอาศัยช่องโหว่ แล้วแทรกโค้ดอันตรายในเว็บไซต์

ข้อมูลความมั่นคงของชาติ

"คนไม่ดีจะไปที่นั่น ไม่มีละแวกบ้านไหนที่ปลอดภัย เราทุกคนต่างเป็นเพื่อนบ้าน" [ทางออนไลน์][17] James B. Comey คำให้การของผู้อำนวยการ FBI ต่อรัฐสภาที่วอชิงตัน ดี.ซี. ในกรณีการโจมตีทางคอมพิวเตอร์ (14 พฤศจิกายน 2556)

ข้อมูลที่สำคัญที่สุดของรัฐคือข้อมูลที่เกี่ยวกับความมั่นคงของชาติ ซึ่งรวมถึงประเด็นต่าง ๆ ตั้งแต่ข่าวกรองทางทหาร การป้องกันภัยฝ่ายพลเรือน การเตรียมพร้อมรับสถานการณ์ฉุกเฉิน/ภัยพิบัติ ไปจนถึงการปกป้องโครงสร้างพื้นฐานที่สำคัญ และแผนเคลื่อนย้ายกำลังพล

ประเด็นนี้ยิ่งซับซ้อนขึ้นเมื่อมีการใช้ข้อมูลร่วมกัน ระหว่างผู้รับเหมาของกระทรวงกลาโหมและหน่วยงานภายนอกอื่นๆ การโจมตีทางคอมพิวเตอร์หลายครั้งเกิดขึ้นโดยมุ่งเป้าไปที่หน่วยงานภายนอกเพื่อเข้าถึงข้อมูลสำคัญด้านความมั่นคงของชาติ

ปัจจุบันทุกประเทศในเอเชียมีโอกาสถูกโจมตีอย่างมีกลยุทธ์และถูกบุกรุกได้โดยไม่มีข้อยกเว้น ซึ่งสิ่งนี้เป็นความท้าทายต่อการรักษาความมั่นคงปลอดภัยของรัฐ

ภาคเอกชนเองก็ต้องรับมือกับการโจมตีทางคอมพิวเตอร์บนเครือข่ายอินเทอร์เน็ตเช่นกัน ร้านค้าปลีก Target[18] และร้านเคหะภัณฑ์ Home Depot[19] ต่างตกเป็นเหยื่อของการโจมตีทางคอมพิวเตอร์ครั้งใหญ่ คาดว่ามีข้อมูลบัตรเครดิตและบัตรเดบิตรั่วไหลไปราว 100 ล้านบัญชี[20]

ยิ่งระบบเทคโนโลยีสารสนเทศมีความซับซ้อนมากขึ้นเท่าใด โอกาสที่จะเกิดภัยคุกคามต่อระบบเทคโนโลยีสารสนเทศก็จะมีมากขึ้นไปด้วย ทั้งยังจะลดทอนความมั่นคงปลอดภัยในการป้องกันภัยคุกคาม ซึ่งอาจเปิดช่องโหว่ให้อาชญากรคอมพิวเตอร์เข้ามาฉวยประโยชน์ได้ การรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์โดยรัฐ จึงควรมุ่งเน้นที่การป้องกันห่วงโซ่อุปทานทางเทคโนโลยีสารสนเทศ (IT Supply Chain) และ การเพิ่มเรื่องการรักษาความมั่นคงปลอดภัยทางคอมพิวเตอร์ในการจัดซื้อระบบเทคโนโลยีสนเทศของภาครัฐ (เพิ่มการมีส่วนร่วมจากเจ้าหน้าที่รัฐ) โดยรวมเป็นส่วนหนึ่งของมาตรการเพื่อรักษาความมั่นคงปลอดภัย

บทที่ 3:

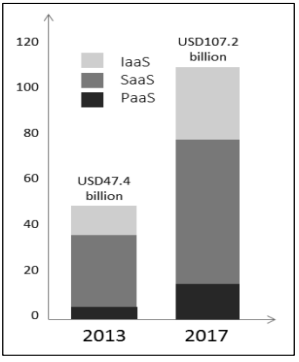
การใช้จ่ายด้านเทคโนโลยีสารสนเทศภาครัฐ

บทที่ 3: การใช้จ่ายด้านเทคโนโลยีสารสนเทศภาครัฐ

จากงานวิจัยของ Gartner หน่วยงานของรัฐบาลทั่วโลกจะใช้จ่ายเงิน 4.495 แสนล้านเหรียญสหรัฐกับโครงการทางด้านเทคโนโลยีสารสนเทศในปี 2556 ซึ่งลดลง 0.1% จากปี 2555[21] ขณะที่การใช้จ่ายด้านเทคโนโลยีสารสนเทศของประเทศสหรัฐอเมริกาได้ชะลอลงในปี 2556 แต่ในช่วงปี 2544 ถึง 2555 ค่าใช้จ่ายด้านเทคโนโลยีสารสนเทศของรัฐบาลสหรัฐฯ ได้เพิ่มจาก 4.6 หมื่นล้านเหรียญสหรัฐ ไปเป็น 8.1 หมื่นล้านเหรียญสหรัฐ ซึ่งเพิ่มเกือบสองเท่าภายในหนึ่งทศวรรษ[22]

ทุกรัฐบาลไม่ใช่จะชะลอการใช้จ่ายด้านเทคโนโลยีสารสนเทศได้ การใช้จ่ายเงินด้านเทคโนโลยีสารสนเทศของภาครัฐในออสเตรเลียคาดว่าจะเติบโต 2.2% ต่อปี จนถึง 1.07 หมื่นล้านเหรียญออสเตรเลียก่อนปี 2550[23] การลงทุนส่วนใหญ่จะเป็นด้านซอฟต์แวร์[24] นิวซีแลนด์คาดว่ารายจ่ายประเภทเดียวกันนี้จะเติบโต 1.4% จนถึงมากกว่า 1.6 พันล้านเหรียญนิวซีแลนด์[25] แนวโน้มของการเติบโตด้านเทคโนโลยีสารสนเทศในภาครัฐเห็นได้จากการใช้จ่ายในเทคโนโลยีอุปกรณ์เคลื่อนที่ การปรับปรุงเทคโนโลยีสารสนเทศให้ทันสมัย และการใช้เทคโนโลยี Cloud[26] คาดว่าทั่วโลกจะมีการใช้จ่ายด้านโครงสร้างพื้นฐานบริการ Cloud สาธารณะถึงเกือบ 1.08 แสนล้านเหรียญก่อนปี 2560[27]

รูปที่ 3 การใช้จ่ายด้าน IT Cloud Service ทั่วโลก แยกตามประเภท[28]



เมื่อการใช้จ่ายของภาครัฐสามารถตรวจสอบได้มากขึ้น สังคมก็ให้ความสนใจมากขึ้นว่ามีการใช้จ่ายไปกับทรัพยากรใดบ้าง โดยเฉพาะเมื่องบประมาณเทคโนโลยีสารสนเทศมีมูลค่าหลายพันล้าน การเห็นความสำคัญของความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศนั้นสะท้อนให้เห็นจากงบประมาณที่จัดสรรโดยประเทศที่พัฒนาแล้วเป็นผู้นำในเรื่องนี้ ในปี 2557 กระทรวงกลาโหมสหรัฐฯ

ตั้งงบประมาณสำหรับศูนย์บัญชาการคอมพิวเตอร์มูลค่าถึง 447 ล้านเหรียญ และเพิ่มอีก 792 ล้านเหรียญในการสร้างทีมด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศสำหรับกระทรวงความมั่นคงแห่งมาตุภูมิ (U.S. Department of Homeland Security)[29] รัฐบาลอังกฤษใช้เงิน 650 ล้านปอนด์เพื่อรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศระหว่างปี 2554 ถึง 2558[30] แต่อย่างไรก็ดี เมื่อเปรียบเทียบกับรัฐบาลประเทศอื่น เช่น อินเดีย ตั้งงบประมาณ 7.76 ล้านเหรียญสหรัฐสำหรับการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศในปี 2556[31]

งบประมาณหรือการใช้จ่ายเหล่านี้มีความเข้าใจมากขึ้นว่า บางอย่างต้องเน้นเรื่องปัญหาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ โดยเฉพาะอย่างยิ่งนับตั้งแต่มีการโจมตีที่รัฐอยู่เบื้องหลังหรือรัฐตกเป็นเป้าหมายมากขึ้น[32] ประเทศไทยกำลังตื่นตัวว่าความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศของประเทศอยู่ในระดับ “วิกฤต”[33] ในทำนองเดียวกันการโจมตีทางเทคโนโลยีสารสนเทศต่อที่ตั้งสำคัญในซาอุดิอาระเบียและกาตาร์เมื่อปี 2555/2556 ได้ปลุกให้ภูมิภาคนี้ตื่นตัวกับภัยดังกล่าว สหรัฐอาหรับเอมิเรตส์ ซาอุดิอาระเบีย และประเทศอื่นในภูมิภาคกำลังมุ่งลงทุนอย่างหนักในเรื่องการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ[34]

อย่างไรก็ตาม ความพยายามของรัฐในขณะนี้ที่จะจัดการกับความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศให้ทันการณ์นั้นยังไม่เพียงพอ ตัวอย่างความพยายามของภาครัฐในเรื่องนี้

1. สิงคโปร์ประกาศจัดตั้งหน่วยงานด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศเมื่อเดือนเมษายน 2558 (http://www.channelnewsasia.com/news/singapore/government-to-set-up/1618658.html)

2. เจ้าหน้าที่ของอินโดนีเซียหารือกันในเดือนธันวาคม 2557 เพื่อจัดตั้งองค์กรระดับชาติเพื่อต่อสู้กับการโจมตีทางเทคโนโลยีสารสนเทศ (http://www.futuregov.asia/articles/5924-indonesia-plans-to-set-up- national-cyber-security-agency)

3. ประเทศไทยได้ผ่านความเห็นชอบต่อร่างพระราชบัญญัติรักษาความมั่นคงปลอดภัยไซเบอร์ เมื่อเดือนมกราคม 2558 (http://tech.thaivisa.com/gen-prayut-defends-controversial-new-cyber-laws-thailand/3438/)

4. อินเดียได้เผยแพร่นโยบายความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศฉบับแรกเมื่อเดือนกรกฎาคม 2556 (http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/NationalCyberSecurityPolicyINDIA.pdf)

5. นายกรัฐมนตรีออสเตรเลียประกาศแผนความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศซึ่งเป็นส่วนหนึ่งของแผนกลยุทธ์ความมั่นคงปลอดภัยแห่งชาติเมื่อเดือนมกราคม 2556 (www.abc.net.au/unleashed/4484508.html)

นอกจากการใช้จ่ายที่เฉพาะเจาะจงกับมาตรการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศแล้ว การจัดซื้อจัดจ้างที่คำนึงถึงความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศของรัฐบาลก็เป็นอีกหนึ่งปัจจัยหนึ่งที่มักถูกมองข้ามในการสร้างรัฐบาลที่มีความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ ในการใช้จ่ายด้านเทคโนโลยีสารสนเทศอันประกอบด้วย การจัดซื้อจัดจ้างโครงสร้างพื้นฐานทางเทคโนโลยีสารสนเทศ การสนับสนุนและบริหารด้านเทคโนโลยีสารสนเทศ รวมถึงการบริหารจัดการบริการออนไลน์และเว็บไซต์ มักมีจุดอ่อน เช่น การใช้ซอฟต์แวร์ที่ไม่มีลิขสิทธิ์หรือซื้อมาจากบริษัทที่ไม่น่าเชื่อถือ รวมถึงการใช้งานซอฟต์แวร์ที่ไม่ได้อัปเดตซึ่งเกิดขึ้นเนื่องจากความไม่รู้

ปัญหาที่เกิดขึ้นกับผู้รับผิดชอบด้านการจัดซื้อในเอเชีย คือ คอมพิวเตอร์ที่ติดมัลแวร์มีเพิ่มขึ้นและการขาดประสบการณ์ในการจัดการกับภัยคุกคาม (และ) องค์กรส่วนใหญ่ไม่ระมัดระวังอย่างเพียงพอต่อการโจมตีประเภท Advanced Persistent Threat

กระบวนการจัดซื้อที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศภาครัฐ

ประสิทธิภาพ (Productivity) ความยั่งยืน (Sustainability) และความคุ้มค่า (Cost-Effeciency) เป็นสามองค์ประกอบสำคัญในการจัดซื้อโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ โดยเฉพาะอย่างยิ่งในประเทศที่มีโครงการด้านเทคโนโลยีสารสนเทศจำนวนมาก[35] อย่างไรก็ตาม การเตรียมพร้อมเป็นสิ่งสำคัญต่อการรักษาความมั่นคงปลอดภัย ภายในปี 2563 คาดว่าจะมีการกันงบประมาณด้านเทคโนโลยีสารสนเทศไว้ 75% เพื่อการตรวจหาและตอบสนองต่อภัยคุกคามทางเทคโนโลยีสารสนเทศ ซึ่งเพิ่มขึ้นจากปี 2555 โดยตั้งไว้ไม่ถึง 10%[36] ปัญหา 2 ประการที่เกิดขึ้นกับการจัดซื้อในเอเชีย คือ จำนวนคอมพิวเตอร์ที่ติดมัลแวร์มีเพิ่มขึ้น และการขาดประสบการณ์ในการรับมือกับภัยคุกคาม

ทั้งนี้การสำรวจในระดับนานาชาติโดย ISACA พบว่า ส่วนใหญ่ของผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ ยังไม่เคยรับมือกับการโจมตีประเภทภัยคุกคามต่อเนื่องขั้นสูง (Advanced Persistent Threat - APT) จริง ๆ มีเพียง 21.6% ของผู้ตอบแบบสอบถามที่เคยโดนโจมตีแบบ APT[37] ในขณะที่องค์กรส่วนใหญ่ยังไม่ระมัดระวังอย่างเพียงพอต่อภัยคุกคามแบบ APT ดูได้จาก 81.8% ของผู้ตอบแบบสอบถามไม่เคยปรับปรุงสัญญากับผู้ขายเพื่อจัดหาการป้องกันต่อภัย APT รวมถึงผู้ตอบแบบสอบถามส่วนหนึ่งไม่เคยจัดการฝึกอบรมเพื่อเพิ่มความตระหนักต่อ APT ให้แก่พนักงาน

Cloud กับความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ

หลายประเทศตัดสินใจที่จะหันไปใช้ Cloud เช่น สหรัฐอเมริกา อังกฤษ และออสเตรเลีย ที่ประกาศนโยบาย “Cloud First” โดยผลิตภัณฑ์ที่เกี่ยวข้องกับ Cloud จะได้รับการพิจารณาก่อน เมื่อมีการจัดซื้อผลิตภัณฑ์และบริการด้านเทคโนโลยีสารสนเทศโดยรัฐบาล

Cloud ถือว่าปลอดภัยกว่าระบบเทคโนโลยีสารสนเทศอื่นที่ติดตั้งในองค์กรด้วยเหตุผลหลายประการ:

1. การจัดการข้อมูลส่วนตัวและการเข้าถึง (Identity & Access Management) Cloud สามารถจัดการได้ว่าใครควรเข้าถึงข้อมูลใดบ้าง และสามารถติดตามการเข้าถึงข้อมูลหากระบบความมั่นคงปลอดภัยถูกบุกรุก

2. ความมั่นคงปลอดภัยทางกายภาพ (Physical Security) – Cloud จะช่วยปกป้องและกู้คืนข้อมูลซึ่งบริหารจัดการโดยผู้ให้บริการ Cloud ซึ่งทำได้ดีกว่าบริหารจัดการด้วยตนเอง

3. การบริหารจัดการและการรักษาความมั่นคงปลอดภัยที่ทันสมัย (Up-to-date Security and Maintenance) – ผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยของผู้ให้บริการ Cloud จะดูแลและทำหน้าที่ปรับปรุงความมั่นคงปลอดภัย โดยถือเป็นส่วนหนึ่งของบริการ

การใช้จ่ายด้านเทคโนโลยีสารสนเทศสำหรับการดูแลระบบสารสนเทศของภาครัฐ

ทั่วโลกใช้เงินราว 4 แสนล้านเหรียญสหรัฐไปกับการแก้ไขระบบจากปัญหาข้อมูลถูกขโมย เงินเหล่านี้จะใช้อย่างเป็นประโยชน์มากกว่าถ้านำไปพัฒนาเพื่อเพิ่มผลผลิต ทั้งนี้ค่าใช้จ่ายด้านเทคโนโลยีสารสนเทศเพื่อจัดการมัลแวร์นั้นสูงมากสำหรับภาคเอกชนและภาครัฐ มีการโจมตีกลุ่มธุรกิจขนาดเล็กในอังกฤษเพิ่มขึ้น 10% ในปี 2556 คาดว่าค่าใช้จ่ายนี้จะเพิ่มเป็น 6% ของเงินทุนหมุนเวียนของกิจการ[38] ธุรกิจขนาดเล็กเกือบ 60% ประสบปัญหาการบุกรุกความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับพนักงาน โดยรวมแล้ว การบุกรุกระบบรักษาความมั่นคงปลอดภัยก่อให้เกิดค่าใช้จ่าย 54-100 ล้านเหรียญสหรัฐ ในอังกฤษ คาดว่ามีประชาชนกว่า 800 ล้านคนที่ได้รับผลกระทบจากการขโมยข้อมูลและการจารกรรมทางคอมพิวเตอร์ในปี 2556[39]

การใช้จ่ายด้านเทคโนโลยีสารสนเทศสำหรับการดูแลเว็บไซต์และบริการออนไลน์ภาครัฐ

ไม่ว่าประเทศใด รัฐมักเป็นองค์กรที่มีเว็บไซต์มากที่สุดในการให้บริการประชาชน การอัปเกรด และการหมั่นตรวจสอบหาจุดบกพร่องของการรักษาความมั่นคงปลอดภัยที่มีค่าใช้จ่ายสูงมาก ทางแก้ปัญหาวิธีหนึ่งคือนำเว็บไซต์และบริการทั้งหลายมารวมกันไว้ที่จุดเดียว (Single Portal) ตัวอย่างเช่น รัฐบาลอังกฤษอ้างว่าสามารถประหยัดเงินได้ราว 42 ล้านปอนด์ จากการย้ายเว็บไซต์ต่าง ๆ มาไว้ที่ gov.uk ก่อนเริ่มโครงการนี้ รายงานของ Digital Britain ระบุว่าประเทศอังกฤษมีเว็บไซต์ที่ให้บริการประชาชนราว 4,000 เว็บไซต์[40]

ในอินเดียซึ่งมีเว็บไซต์ของรัฐบาลมากกว่า 303 ล้านไซต์ ซึ่งถูกเจาะระบบเป็นจำนวนมากทุกปี และมีแนวโน้มเพิ่มขึ้นตั้งแต่ปี 2553 การดำเนินการเชิงป้องกันที่รัฐใช้คือมี “การตรวจสอบเว็บไซต์ใหม่ทุกแห่งของรัฐบาลรวมทั้งแอปพลิเคชัน ก่อนที่จะนำขึ้นให้บริการ”[41] การอัปเดตซอฟต์แวร์และการใช้บริการจากผู้ให้บริการที่มีชื่อเสียงจะช่วยบรรเทาปัญหาความมั่นคงปลอดภัย แต่ค่าใช้จ่ายในการจัดการและระดับความรุนแรงของการบุกรุกก็จะยังเพิ่มขึ้นทุกปี

บทที่ 4:

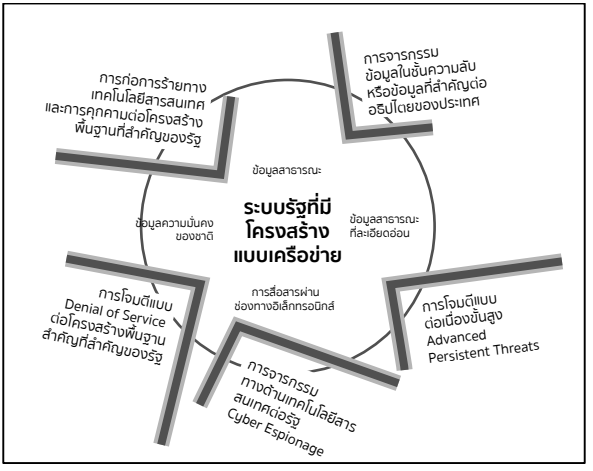
ประเภทของภัยคุกคามทางด้านเทคโนโลยีสารสนเทศต่อภาครัฐ

บทที่ 4: ประเภทของภัยคุกคามด้านเทคโนโลยีสารสนเทศต่อภาครัฐ

ข้อมูลและระบบข้อมูลที่เชื่อมต่อกันนำมาซึ่งภัยคุกคามความมั่นคงปลอดภัยซึ่งนับวันมีแต่จะเพิ่มขึ้น ไม่ว่าจะเป็นโค้ดที่เป็นอันตราย (Malicious Code) มัลแวร์ และซอฟต์แวร์ที่ไม่พึงประสงค์ เช่น ไวรัส โทรจัน โปรแกรมดักการพิมพ์ (Keystroke-Capturing) Authentication Backdoors และสปายแวร์ ที่พบในซอฟต์แวร์ที่มีลิขสิทธิ์ไม่ถูกต้อง เว็บไซต์ หรือเครือข่ายแบบเพียร์-ทู-เพียร์ (P2P)

สำหรับคนส่วนใหญ่ ผลจากการติดมัลแวร์หรือถูกบุกรุก มักจะทำให้คอมพิวเตอร์ทำงานช้าลง มีโฆษณาน่ารำคาญโผล่ขึ้นมา และอาจโดนขโมยข้อมูลส่วนตัว แต่สำหรับรัฐบาลและภาคเอกชน ผลที่ตามมานั้นร้ายแรงกว่ามาก การใช้ซอฟต์แวร์ที่มีลิขสิทธิ์ไม่ถูกต้อง ทำให้หน่วยงานของรัฐตกอยู่ในความเสี่ยงที่จะถูกเจาะระบบ จารกรรมข้อมูล หรือตกเป็นเป้าของการก่อการร้ายทางเทคโนโลยีสารสนเทศ เพราะแฮกเกอร์สามารถใช้มัลแวร์เพื่อควบคุมโครงสร้างพื้นฐานที่สำคัญและข้อมูลที่สำคัญได้

รูปที่ 4 ภัยคุกคามความมั่นคงปลอดภัย
ระบบเทคโนโลยีสารสนเทศของภาครัฐ



การก่อการร้ายด้านเทคโนโลยีสารสนเทศและภัยคุกคามต่อโครงสร้างพื้นฐานที่สำคัญของรัฐ (Cyber Terrorism and Threats to Critical Infrastructure)

การก่อการร้ายทางเทคโนโลยีสารสนเทศ ได้แก่ การโจมตีระบบเทคโนโลยีสารสนเทศโดยมุ่งสร้างความเสียหายต่อโครงสร้างพื้นฐานที่สำคัญ เช่น ระบบป้องกันภัยการบิน ระบบไฟฟ้า ระบบสาธารณูปโภค หรือภาคพลังงาน เช่น โรงไฟฟ้านิวเคลียร์ โรงกลั่นน้ำมันและแก๊ส ฯลฯ นอกจากนี้ยังรวมถึงภัยคุกคามของการโจมตีระบบเทคโนโลยีสารสนเทศที่พุ่งเป้าไปที่ประชาชนส่วนใหญ่ เพื่อสร้างความตื่นตระหนกในวงกว้าง สร้างความสูญเสียทางการเงิน หรือทำลายระบบการรักษาความมั่นคงปลอดภัย

ซอฟต์แวร์และมัลแวร์ที่ใช้ในการก่อการร้ายเริ่มซับซ้อนขึ้นเรื่อย ๆ และรัฐบาลส่วนใหญ่กำลังเตรียมพร้อมรับมือการโจมตีครั้งต่อไปที่จะส่งผลกระทบมากขึ้นเรื่อย ๆ ตัวอย่างเช่น ผู้ให้บริการน้ำประปาในแคลิฟอร์เนียพบว่ากลุ่มแฮกเกอร์สามารถควบคุมระบบน้ำประปาและสามารถสั่งเพิ่มสารเคมีเพื่อบำบัดน้ำ

ในสถานการณ์ทำนองเดียวกันนี้ โปรแกรม Stuxnet ได้รับการออกแบบมาเพื่อโจมตีการทำงานของอุปกรณ์อิเล็กทรอนิกส์ (Electromechanical) ถูกมองว่าเป็นจุดพลิกผันของการโจมตีทางระบบเทคโนโลยีสารสนเทศ โปรแกรมตัวนี้ได้รับการค้นพบเมื่อปี 2553 Kaspersky Labs เรียกมันว่า “ต้นแบบของอาวุธทางระบบเทคโนโลยีสารสนเทศที่ทำงานได้อย่างน่ากลัว ซึ่งจะนำไปสู่การแข่งขันสร้างอาวุธแบบใหม่ในโลก”[42] มีรายงานว่า Stuxnet ทำให้เครื่องแยกยูเรเนียม หนึ่งในห้าของอิหร่านสูญเสียการควบคุม[43]

การจารกรรมข้อมูลที่เป็นความลับหรือข้อมูลที่สำคัญต่ออธิปไตยของประเทศ (Theft of Confidential or Sovereign Data)

วัตถุประสงค์ของการโจมตีทางเทคโนโลยีสารสนเทศส่วนใหญ่ คือ เพื่อล้วงข้อมูลลับ ขโมยความลับทางการค้า หรือหาทางชิงความได้เปรียบเหนือบริษัทคู่แข่ง องค์กรหรือรัฐบาลอื่น หลายปีที่ผ่านมามีเหตุการณ์การจารกรรมข้อมูลเพิ่มขึ้นอย่างมาก องค์กรจำนวนน้อยที่สามารถป้องกันตัวได้แบบครอบคลุม[44] ตัวอย่างที่สุ่มมาศึกษาจากคดีดังในช่วงปี 2554-2557 แสดงให้เห็นว่าการถูกเจาะระบบโดยแฮกเกอร์แผ่วงกว้างออกไปเพียงใด เหยื่อมีทั้งร้านค้าปลีก (Zappos ของ Amazon) บริษัทการตลาด (Epsilon) เกมออนไลน์ (Sony) ธนาคาร (Citigroup) หน่วยงานภาครัฐต่าง ๆ (กระทรวงกลาโหมของสหรัฐฯ, รัฐบาลแคนาดา) ผู้รับเหมาของกองทัพ (Lockheed Martin) เว็บไซต์เครือข่ายสังคม (RockYou) ผู้ให้บริการ Cloud (Gmail ของ Google) และแม้กระทั่งบริษัทด้านความมั่นคงปลอดภัย (RSA ของ EMC, Stratfor, Symantec) กรณีที่เกิดขึ้นเมื่อเร็ว ๆ นี้อีเมลประสงค์ร้ายฉบับหนึ่งถูกส่งไปถึงเจ้าหน้าที่กรมสรรพากรของเซาท์แคโรไลนา จนนำไปสู่การขโมยหมายเลขประกันสังคม 1.9 ล้านหมายเลข ข้อมูลการคืนภาษี 3.8 ล้านรายการ และรายละเอียดบัญชีธนาคาร 3.3 บัญชีทั่วมลรัฐ[45]

การโจมตี eBay ซึ่งเป็นบริษัทยักษ์ใหญ่ด้านพาณิชย์อิเล็กทรอนิกส์ในปี 2557 ส่งผลให้ข้อมูล เช่น ที่อยู่อีเมล รหัสผ่านที่เข้ารหัสไว้ วันเกิด และที่อยู่ทางไปรษณีย์ถูกขโมย จนทาง eBay ต้องขอให้ผู้ใช้ 145 ล้านรายของตนเปลี่ยนรหัสผ่านหลังถูกโจมตี[46] เดือนกันยายนปีเดียวกัน ร้านเคหะภัณฑ์ Home Depot รายงานว่าระบบชำระเงินของบริษัทถูกโจมตี ทำให้บัตรเครดิตและบัตรเดบิตของลูกค้ากว่า 56 ล้านใบต้องตกอยู่ในความเสี่ยง

จำนวนครั้งและชนิดของการบุกรุกระบบรักษาความมั่นคงปลอดภัยส่งผลต่อธุรกิจทุกประเภท ในปี 2555 บริษัทขนาดกลางและเล็กต่างประสบปัญหาซึ่งเดิมจะพบแต่ในบริษัทใหญ่ๆ เท่านั้น เช่น 87% ของธุรกิจขนาดเล็กในอังกฤษถูกเจาะระบบในปี 2555[47]

การโจมตีแบบ Denial of Service ต่อโครงสร้างพื้นฐานสำคัญของรัฐ (Denial of Service Attacks on Key Government Infrastructure)

การโจมตีแบบ Denial of Service (DoS) คือ การทำให้บริการหรือเซิร์ฟเวอร์ไม่สามารถเข้าถึงได้ การขโมยข้อมูลเพื่อใช้เข้าสู่ระบบคอมพิวเตอร์ต่าง ๆ หรือการเจาะระบบเครือข่ายนั้น เป็นขั้นแรกของการโจมตีแบบ DoS จากนั้นก็ใช้คอมพิวเตอร์ที่เข้าถึงแล้วเป็นฐานในการโจมตีเว็บไซต์เป้าหมาย โดยทำการร้องขอเข้าเว็บไซต์เป็นจำนวนมาก จนกระทั่งระบบล่มหรือทำให้ผู้ใช้คนอื่นไม่สามารถเข้าเว็บไซต์นั้น

วิธีนี้สามารถทำเป็นแบบอัตโนมัติ และขยายไปสู่การโจมตีแบบกระจายกำลัง (Distributed DoS หรือ DDoS) โดยใช้ซอฟต์แวร์ที่เรียกว่า “Botnets” เพื่อควบคุมคอมพิวเตอร์จำนวนมากในคราวเดียว ซึ่งการควบคุมคอมพิวเตอร์จำนวนมากเหล่านั้น Botnets ไม่จำเป็นต้องอาศัยทักษะขั้นสูงทางเทคโนโลยีสารสนเทศ โดยสามารถหาซื้อได้ในราคา 100 ถึง 200 เหรียญสหรัฐต่อคอมพิวเตอร์ที่ถูกควบคุมโดย Botnets 1,000 เครื่อง การโจมตีแบบ DoS ได้รับความนิยมสูง โดยมีระบบเทคโนโลยีสารสนเทศของรัฐบาลและสถาบันการเงินเป็นเป้าหมายยอดนิยม การศึกษาชิ้นหนึ่งรายงานว่าแค่ปี 2556 ปีเดียว DoS เพิ่มสูงขึ้น 8 เท่าเมื่อเทียบกับปีก่อนหน้า[48]

การโจมตีเหล่านี้เป็นโฉมหน้าใหม่ของการจู่โจมที่เปิดฉากขึ้นที่เอสโตเนีย ในปี 2550 และที่จอร์เจีย ในปี2551 การโจมตีเอสโตเนียเมื่อเดือนเมษายน 2550 ทำให้เว็บไซต์ของรัฐสภาล่ม บริการของรัฐและธนาคารหยุดชะงัก เครือข่ายต้องออฟไลน์ การทำงานของรัฐบาลและสื่อมวลชนถูกขัดขวางเพราะการโจมตีแบบ DoS หลายระลอก[49] สำหรับประเทศซึ่งธุรกรรมทางการเงิน 90% ทำผ่านอินเทอร์เน็ต และการยื่นภาษี 70% ทำด้วยระบบอิเล็กทรอนิกส์นั้น ผลกระทบที่เกิดขึ้นทำให้ประเทศอยู่ในสภาพง่อยเปลี้ย อีกตัวอย่างหนึ่งคือการโจมตีกลับแบบ DoS ซึ่งทำให้เกิดความตึงเครียดระหว่างฟิลิปปินส์กับไต้หวัน เมื่อต้นปี 2556 จากเหตุการณ์ยิงชาวประมงไต้หวัน ทำให้ “นักเคลื่อนไหวแฮกเกอร์” ชาวไต้หวัน ระดมโจมตีแบบ DoS ใส่เว็บไซต์ของรัฐบาลฟิลิปปินส์และสร้างความเสียหายทางเศรษฐกิจโดยตรง[50]

ท่ามกลางการขยายตัวของภัยคุกคามจากการโจมตีแบบ DoS นั้น แอปพลิเคชันที่ใช้เทคโนโลยีอัจฉริยะมีความก้าวหน้าไปมาก และการถือกำเนิดของ “Internet of Things” ทำให้มีอุปกรณ์อัจฉริยะต่าง ๆ ที่มี IP เพิ่มมากขึ้น ซึ่งอาจกลายเป็น Botnet หรือเป็นแพลตฟอร์มใหม่สำหรับการระดมกำลังโจมตี[51] ภัยคุกคามใหม่นี้คือการหาช่องทางการโจมตีเพื่อเข้าควบคุมระบบประมวลผลของอุปกรณ์เหล่านี้ได้ด้วยตัวเอง[52]

ปัจจุบัน ระบบที่น่าเป็นห่วงอย่างยิ่งในการถูกโจมตี คือ ระบบ SCADA (Supervisory Control and Data Acquisition) ซึ่งรัฐนิยมใช้ควบคุมอุปกรณ์ของโรงงานสาธารณูปโภคและโครงสร้างพื้นฐาน ตัวอย่างเช่น ระบบ SCADA ในควีนสแลนด์ ออสเตรเลีย ถูกเจาะระบบ ส่งผลให้ “น้ำเสียจากท่อไหลท่วมสวนสาธารณะและลงคลองกั้นน้ำ”[53]

แผนแม่บทและกฎหมายการรักษาความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศในเอเชีย

หลายประเทศในเอเชียมีแผนการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศหรือมีกฎหมายที่เกี่ยวข้องอยู่แล้ว โดยมีบางส่วนอยู่ระหว่างกระบวนการพิจารณา ดังนี้

อินโดนีเซีย กำลังจัดตั้งหน่วยงานเพื่อต่อสู้กับการโจมตีทางเทคโนโลยีสารสนเทศ ตามคำแนะนำของรัฐมนตรีกระทรวงคมนาคมและสารสนเทศกับรัฐมนตรีกระทรวงความร่วมมือทางการเมือง กฎหมายและกิจการความมั่นคงเมื่อเดือนมกราคม 2558 กฎหมายที่เกี่ยวข้อง ได้แก่ พ.ร.บ. ข้อมูลและธุรกรรมอิเล็กทรอนิกส์[54]

มาเลเซีย มีนโยบายความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ซึ่งเป็นรูปร่างเมื่อปี 2548 โดยประสานงานผ่านกระทรวงวิทยาศาสตร์ เทคโนโลยีและนวัตกรรม (MOSTI) องค์กร Cyber Security Malaysia เปิดตัวเมื่อเดือนสิงหาคม 2550 GCERT MAMPU ก่อตั้งในปี 2544 โดยกรอบนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของรัฐบาล เพื่อรับประกันความต่อเนื่องของการจัดการเทคโนโลยีสารสนเทศและการสื่อสาร และ

เกี่ยวข้องกับหน่วยงาน CERT อีก 55 หน่วยงาน กฎหมายที่เกี่ยวข้อง ได้แก่ พ.ร.บ. การสื่อสารและมัลติมีเดีย 2541 พ.ร.บ. การคุ้มครองข้อมูลส่วนบุคคล 2553 พ.ร.บ. อาชญากรรมคอมพิวเตอร์ 2540[55]

เมียนมา ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ของเมียนมา (MMCERT) และสมาพันธ์คอมพิวเตอร์เมียนมา (MCF) กำลังทำงานร่วมกันเพื่อปฏิรูปหน่วยงาน CERT ของประเทศเพื่อปรับปรุงความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ สภาไอซีทีสหรัฐฯ-เมียนมา จัดตั้งขึ้นด้วยร่วมมือกับ USAID และกำลังจัดทำแผนแห่งชาติ[56]

ฟิลิปปินส์ สำนักงานความมั่นคงทางเทคโนโลยีสารสนเทศแห่งชาติดูแลการดำเนินงานตามแผนความมั่นคงด้านเทคโนโลยีสารสนเทศปี 2551 กฎหมายที่เกี่ยวข้อง ได้แก่ พ.ร.บ. ป้องกันอาชญากรรมคอมพิวเตอร์ปี 2555 (RA 10175 - ยกเลิกจนกว่าจะมีการเปลี่ยนแปลง) พ.ร.บ. ความเป็นส่วนตัวของข้อมูลปี 2555 (RA 10173) พ.ร.บ. พาณิชย์อิเล็กทรอนิกส์ปี 2543 (RA 8792)[57]

สิงคโปร์ มีแผนแม่บทด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่ยาวนาน ได้แก่ Infocomm Security Masterplan I (2548-2550), II (2551-2555), National Cyber Security Masterplan 2561 (NCSM2018) กฎหมายที่เกี่ยวข้อง ได้แก่ พ.ร.บ. การใช้งานคอมพิวเตอร์โดยมิชอบและความมั่นคงทางทางเทคโนโลยีสารสนเทศ พ.ร.บ. ธุรกรรมอิเล็กทรอนิกส์ พ.ร.บ. การคุ้มครองข้อมูลส่วนบุคคล ความมั่นคงปลอดภัยทางคอมพิวเตอร์บนโลกไซเบอร์มีการประสานงานโดยสำนักเลขาธิการประสานงานความมั่นคงแห่งชาติ ภายใต้สำนักนายกรัฐมนตรี[58]

ไทย เนื่องจากสถานการณ์ทางการเมืองที่ผันผวนของประเทศไทย การทบทวน พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จึงชะงักงัน กฎหมายที่เกี่ยวข้อง ได้แก่ พ.ร.บ. คุ้มครองผู้บริโภค 2545 ประมวลกฎหมายอาญามาตรา 269/1-7 พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์

2544 ประมวลกฎหมายแพ่งและพาณิชย์ พ.ร.บ. การประกอบธุรกิจข้อมูลเครดิต และ พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล (ร่าง)

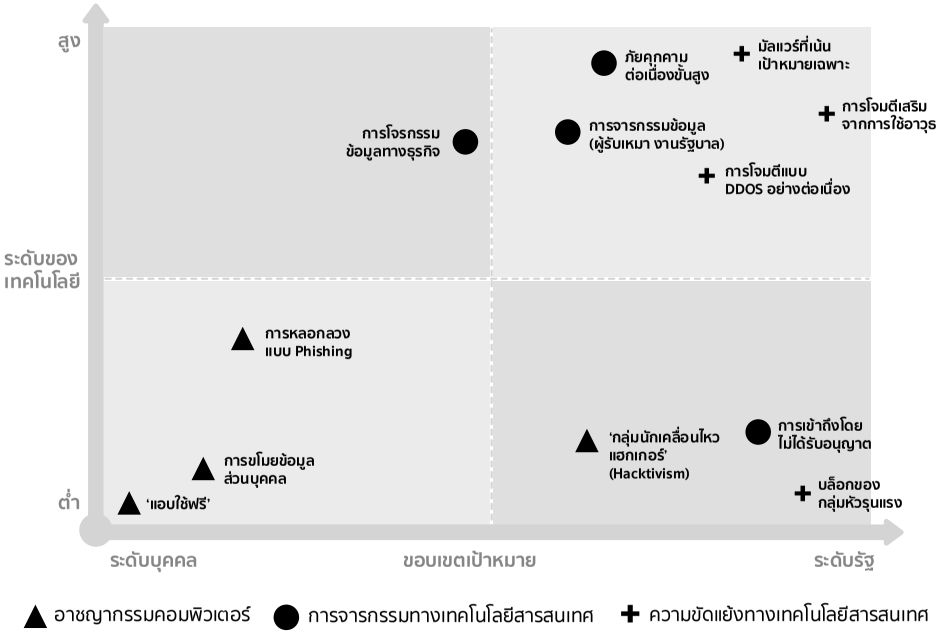
เวียดนาม ปัจจุบันกำลังจัดตั้งศูนย์เทคโนโลยีเครือข่ายแห่งชาติ และมีกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ 3 ฉบับ คือ กฎหมายด้านโทรคมนาคม ด้านเทคโนโลยีสารสนเทศ และด้านธุรกรรมอิเล็กทรอนิกส์

การจารกรรมทางด้านเทคโนโลยีสารสนเทศต่อรัฐ (Cyber Espionage)

การจารกรรมทางเทคโนโลยีสารสนเทศ คือ การขโมยความลับที่เก็บในรูปแบบดิจิทัล ซึ่งอาจอยู่บนคอมพิวเตอร์หรือในเครือข่าย[59] การโจมตีเพื่อจารกรรมมีทั้งใช้วิธีที่อาศัยเทคโนโลยีง่าย ๆ และใช้เทคโนโลยีที่ซับซ้อน ตั้งแต่การขโมยข้อมูลส่วนบุคคลไปจนถึงความลับของประเทศ ในปี 2556 บริษัทด้านความมั่นคงปลอดภัยในแคลิฟอร์เนียให้ข้อมูลที่เปิดเผยได้ว่ามีแฮกเกอร์ชาวจีน เริ่มโจมตีองค์กร 141 แห่ง ในอุตสาหกรรม 20 ชนิดทางเทคโนโลยีสารสนเทศ เป้าหมายมีทั้งหน่วยงานของรัฐบาลและบริษัทเอกชน ตั้งแต่กระทรวงกลาโหมไปจนถึงสำนักข่าว New York Times เหตุการณ์นี้ทำให้สหรัฐฯ ฟ้องดำเนินคดีแฮกเกอร์ชาวจีน 5 คน ซึ่งเชื่อว่าอยู่เบื้องหลังการขโมยความลับทางการค้า

อีกตัวอย่างหนึ่งของการจารกรรมทางเทคโนโลยีสารสนเทศในฟินแลนด์ มีรายงานว่ารัฐบาลตกเป็นเหยื่อของการจารกรรมทางเทคโนโลยีสารสนเทศมานาน โดยลักลอบเข้าถึงเอกสารนโยบายต่างประเทศ เอกสารเหล่านี้เชื่อกันว่าทำให้ฟินแลนด์พลาดท่าในการเจรจาระหว่างประเทศ[60]

รูปที่ 5 ภัยคุกคามต่อความมั่นคงปลอดภัย
ทางเทคโนโลยีสารสนเทศและการจารกรรมต่อบุคคลหรือรัฐ



ตัวอย่าง

1. การใช้ WiFi โดยไม่ได้รับอนุญาต
2. บัญชี Facebook โดนแฮก
3. เว็บไซต์ DBS ปลอม 'DBSonline.com' (2547)
4. กลุ่ม Anonymous แก้ไข เว็บไซต์ของ MPAA และกระทรวงกลาโหม (2555)
5. Wikileaks
6. การโจรกรรมข้อมูล Google ประเทศจีน (2553) 'Google Aurora'
7. ความพยายามขโมยเทคโนโลยีของ Lockheed Martin (2554)
8. ปฏิบัติการ 'Titan Rain' (2546-2551), ไวรัส 'Flame' (2552-2555)
9. นิตยสาร 'Inspire'
10. การโจมตีเอสโตเนีย (2550)
11. 'Stuxnet' (2553)
12. วิกฤตการณ์ระหว่าง รัสเซีย-จอร์เจีย (2551)

Advanced Persistent Threats

Advanced Persistent Threats (APT) เป็นภัยคุกคามประเภทใหม่ ที่มักมุ่งเน้นการโจรกรรมทรัพย์สินทางปัญญา ซึ่งมีเป้าหมายแน่ชัด มีความต่อเนื่อง รู้จักหลบซ่อน และใช้เทคนิคขั้นสูง[61]

จากการสำรวจโดย ISACA ซึ่งเป็นองค์กรเอ็นจีโอด้านการกำกับดูแลไอทีพบว่า 67.6% ของผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยที่ตอบแบบสอบถาม คุ้นเคยว่า APT คืออะไรและมองว่าเป็นภัยคุกคามร้ายแรงต่อความมั่นคงของชาติและเศรษฐกิจ แต่อีก 53.4% เชื่อว่า APT ไม่ต่างอะไรจากภัยคุกคามเดิม ๆ[62] โปรแกรมสอดแนมตระกูล NetTraveler ที่เป็นอันตรายได้เริ่มทำงานตั้งแต่ปี 2547 แต่ไม่ค่อยแสดงพฤติกรรมไม่พึงประสงค์ จนกระทั่งปี 2553-2556 NetTraveler ถูกใช้โดยแฮกเกอร์ เพื่อเจาะระบบคอมพิวเตอร์สำคัญ ๆ กว่า 350 เครื่องใน 40 ประเทศ ในปี 2553 Google รายงานว่าทางบริษัทเองรวมทั้งบริษัทอื่น ๆ หลายสิบแห่งตกเป็นเหยื่อของการโจมตีแบบ APT ซึ่งมีที่มาจากประเทศจีน และนำไปสู่การจารกรรมทรัพย์สินทางปัญญาจาก Google

มัลแวร์

มัลแวร์ (Malware) คือ ซอฟต์แวร์ที่เจตนาสร้างความเสียหายต่อคอมพิวเตอร์หรือทำให้ระบบคอมพิวเตอร์ใช้งานไม่ได้ มักพบในซอฟต์แวร์ที่มีลิขสิทธิ์ไม่ถูกต้อง โปรแกรมเหล่านี้สร้างโอกาสให้แฮกเกอร์ด้วยการฝังโปรแกรมอันตรายลงในคอมพิวเตอร์เพื่อขโมยข้อมูลหรือบางครั้งเพื่อควบคุมคอมพิวเตอร์ประเภทของมัลแวร์ ได้แก่

• สปายแวร์ (Spyware) คือ ซอฟต์แวร์ที่ติดตั้งตัวเองลงในคอมพิวเตอร์และแอบรวบรวมข้อมูลเกี่ยวกับการใช้อินเทอร์เน็ต รหัสผ่าน ฯลฯ เช่น สปายแวร์ iBryte สามารถติดตามพฤติกรรมการท่องเว็บ รวบรวมข้อมูลส่วนบุคคล แล้วส่งกลับไปให้ผู้โจมตี

• Tracking Cookies คือ ไฟล์ข้อมูลที่เว็บเบราว์เซอร์เก็บในคอมพิวเตอร์ของผู้ใช้ ซึ่งถูกใช้เพื่อติดตามกิจกรรมทางออนไลน์ของผู้ใช้

• แอดแวร์ (Adware) คือ แพ็กเกจซอฟต์แวรซึ่งแสดงโฆษณาอัตโนมัติเพื่อสร้างรายได้ให้เจ้าของแอดแวร์

• โทรจัน (Trojan) คือ โปรแกรมหรือข้อมูลที่ดูเหมือนไม่มีอันตราย แต่ซ่อนโค้ดโปรแกรมที่มุ่งร้ายหรือเป็นอันตรายอยู่ข้างใน

• ไวรัส (Virus) คือ โปรแกรมซอฟต์แวร์ที่สามารถจำลองตัวเองและมักก่อให้เกิดความเสียหายกับไฟล์หรือโปรแกรมอื่นบนเครื่องคอมพิวเตอร์

• คีย์ล็อกเกอร์ (Keylogger) คือ โปรแกรมซึ่งบันทึกการกดแป้นพิมพ์บนคอมพิวเตอร์ ข้อมูลที่บันทึกนี้อาจมีรหัสผ่าน ซึ่งเก็บไว้เพื่อให้แฮกเกอร์ในภายหลัง โปรแกรมดังกล่าวนี้ไม่ต้องอาศัยความรู้พิเศษแต่อย่างใด

สามารถหาซื้อได้ในราคา 25 เหรียญสหรัฐ และสามารถใส่ในซอฟต์แวร์ที่ไม่มีใบอนุญาตการใช้งาน

ปัจจุบันการสร้างมัลแวร์มาถึงจุดสูงสุดของอุตสาหกรรม โดยมีมัลแวร์ที่สร้างใหม่ ราว 250,000 ตัว และแพร่กระจายในเว็บไซต์ 30,000 แห่งในแต่ละวัน รัฐบาลสหรัฐฯ จัดอันดับให้ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศอยู่เหนือการโจมตีโดยผู้ก่อการร้าย โดยเพิ่มความระแวดระวังต่อภัยคุกคามด้านเทคโนโลยีสารสนเทศที่เตรียมการและประสานงานกันเป็นอย่างดี

บทที่ 5:

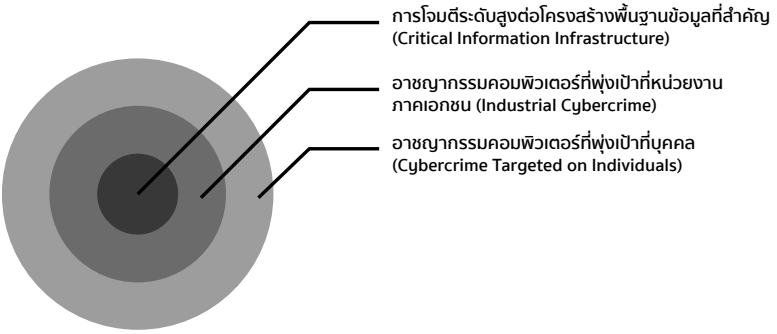
แผนดำเนินการในการสร้างยุทธศาสตร์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของรัฐ

บทที่ 5: แผนดำเนินการในการสร้างยุทธศาสตร์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของรัฐ

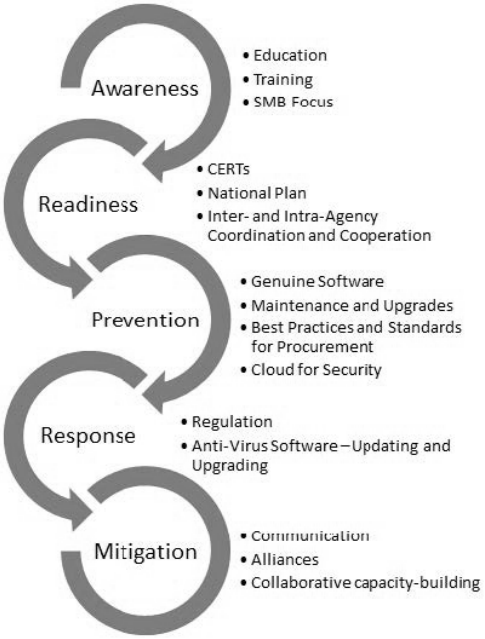
ทุกสังคมและทุกรัฐต่างเสี่ยงต่อการถูกโจมตีผ่านทางเครือข่ายอินเทอร์เน็ตมากขึ้น เนื่องจากเครือข่ายที่เชื่อมต่อกันมีมากขึ้น การมี 'Internet of Things' เช่น คอมพิวเตอร์ ตัวเชื่อมต่อ (sensor) รวมทั้ง ข้อมูลปริมาณมากที่ส่งผ่านอุปกรณ์ที่เชื่อมต่อดังกล่าว

นักวิเคราะห์ได้ประเมินจุดอ่อนด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศไว้ใน 3 ระดับ ดังนี้ (1) การโจมตีระดับสูงต่อโครงสร้างพื้นฐานข้อมูลที่สำคัญ (Critical Information Infrastructure) ซึ่งอาจทำให้กิจการบางส่วนของประเทศหยุดชะงักและมักเกิดขึ้นโดยผู้ก่อการร้ายหรือการทำสงครามทางเทคโนโลยีสารสนเทศที่มีจุดประสงค์ทางการเมือง (2) อาชญากรรมทางคอมพิวเตอร์ที่เริ่มตั้งแต่การจารกรรมข้อมูลในระดับภาคอุตสาหกรรมไปจนถึงการขโมยและการฉ้อโกงทางการค้า (3) การโจมตีที่พุ่งเป้าที่บุคคล เช่น การฉ้อโกงทรัพย์และการขโมยข้อมูลตัวตน

รูปที่ 6 เป้าหมายของภัยคุกคามทางเทคโนโลยีสารสนเทศ



รูปที่ 7 องค์ประกอบของนโยบายความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ

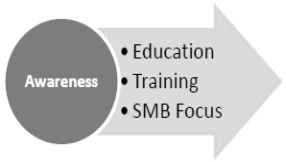


ทั้งนี้ทางออกและกระบวนการตอบสนองต่อภัยคุกคามด้านเทคโนโลยีสารสนเทศที่ดีควรจัดทำในแบบองค์รวม ระบุสถานการณ์สมมติต่าง ๆ เพื่อพัฒนากลยุทธ์การรักษาความมั่นคงปลอดภัยที่แข็งแกร่ง ซึ่งมีแผนดำเนินการ 5 ขั้นเพื่อเสริมสร้างความพร้อม การเฝ้าระวัง การตอบสนอง และการกู้คืนเพื่อกลับสู่สถานการณ์เดิมเมื่อต้องเผชิญกับภัยคุกคามและการโจมตีที่หลีกเลี่ยงไม่ได้ โดยสนับสนุนการใช้กลยุทธ์แบบ “ก่อน ระหว่าง และหลังเกิดเหตุ” เนื่องจากเป็นเรื่องสำคัญสำหรับหน่วยงานของรัฐในทุกระดับ ตั้งแต่การจัดซื้อเทคโนโลยีสารสนเทศ การดูแลและอัปเกรดซอฟต์แวร์ ไปจนถึงศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (CERT) ฯลฯ เพื่อให้เกิดความตระหนักรู้และตั้งมั่นที่จะปกป้องโครงสร้างพื้นฐานและประชาชนจากภัยคุกคามที่อันตรายที่สุดอย่างหนึ่งในโลกยุคใหม่

หนังสือฉบับนี้หวังจะให้คำแนะนำเกี่ยวกับประเด็นต่าง ๆ ได้แก่ การระบุช่องโหว่ว่ามีอะไรบ้างและการกำหนดระดับของความเสี่ยง ยิ่งมีนัยสำคัญมากแปลว่ายิ่งมีโอกาสตกเป็นเป้าได้มาก (ความเสี่ยงประเภทที่ 1) แต่ไม่จำเป็นว่าจะต้องจะถูกโจมตีได้ง่ายขึ้น (ความเสี่ยงประเภทที่ 2) ระดับความสำคัญของเป้าหมายยิ่งน้อยก็อาจถูกโจมตีได้มากที่สุด เนื่องจากถูกโจมตีได้ง่าย การวางกลยุทธ์ต้องคำนึงถึงอาชญากรรมคอมพิวเตอร์ประเภท

ต่าง ๆ ที่กระทำโดยองค์กรอาชญากรรมที่ต่างกัน การจารกรรมทางเทคโนโลยีสารสนเทศในภาคอุตสาหกรรมมีความเร่งด่วนและมีวิธีการที่เฉพาะตัว ผู้ก่อการร้ายและรัฐบาลจะมุ่งไปที่เป้าหมายที่มีมูลค่าสูง เช่น โครงสร้างพื้นฐาน หรือหน่วยงานที่มีความสำคัญต่อสาธารณะมาก เช่น บริการออนไลน์ภาครัฐ ในขณะที่เป้าหมายซึ่งเป็นโครงสร้างพื้นฐานที่สำคัญเป็นจุดหลักที่ต้องให้การรักษาความมั่นคงปลอดภัยในระดับชาติ

การสร้างความตระหนักและการให้ความรู้แก่สาธารณะ



ความรับผิดชอบในการรักษาความมั่นคงปลอดภัยของอินเทอร์เน็ตและเครือข่ายเป็นหน้าที่ของทุกภาคส่วนในสังคม ทั้งนี้ผู้ใช้เทคโนโลยีสารสนเทศทุกคนมีส่วนในการป้องกันภัยคุกคามและการโจมตีทางเทคโนโลยีสารสนเทศ รวมไปถึงการโจมตีเครือข่ายและอุปกรณ์ต่าง ๆ กระบวนการป้องกัน ควรเข้มแข็งพอที่จะต่อสู้กับภัยคุกคามและการโจมตีทางไซเบอร์ ด้วยความร่วมมือระหว่างภาครัฐ ผู้บริโภค ธุรกิจขนาดกลางและย่อม (SMB) ธุรกิจขนาดใหญ่ ผู้รับเหมา ผู้ค้าระบบรักษาความมั่นคงปลอดภัย อุตสาหกรรมเทคโนโลยีสารสนเทศ และชุมชนนักวิจัยความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ จะทำให้เครือข่ายและเครื่องมือต่าง ๆ เกิดความมั่นคงปลอดภัยเพียงพอที่จะรับมือภัยคุกคามได้

ในขณะที่อาชญากรรมคอมพิวเตอร์ที่เกิดขึ้นจากการใช้เทคโนโลยีสารสนเทศช่องโหว่ขององค์กร ระบบเทคโนโลยีสารสนเทศที่ใช้ และความผิดพลาดของบุคลากร ได้แก่ แนวปฏิบัติในการใช้อินเทอร์เน็ต การจัดซื้อจัดจ้างเทคโนโลยีสารสนเทศ การนำอุปกรณ์ส่วนตัวมาใช้ในที่ทำงาน และการกำหนดคุณลักษณะเทคโนโลยีสารสนเทศ ทั้งนี้การแก้ปัญหา/กรอบการทำงานของการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศที่ไม่ได้ครอบคลุมประเด็นเหล่านี้ ทำให้การลดความเสี่ยงต่ออาชญากรรมทางคอมพิวเตอร์เป็นไปได้ยาก

รัฐจึงควรเริ่มดำเนินการและให้ทุนสนับสนุนโครงการที่จะเพิ่มความตระหนักให้กับผู้มีส่วนได้ส่วนเสียในด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ ด้านแนวปฏิบัติด้านเทคโนโลยีสารสนเทศ และด้านการบริหารความเสี่ยง โดยเฉพาะอย่างยิ่งภายในหน่วยงานของรัฐ ทั้งในระดับประเทศและระดับท้องถิ่น การยกระดับความตระหนักนี้ควรเน้นเป็นพิเศษที่การใช้ผลิตภัณฑ์ซอฟต์แวร์และแอปพลิเคชันที่ถูกกฎหมาย เป็นของแท้ และทันสมัย รวมทั้งแนวปฏิบัติในการใช้อินเทอร์เน็ตที่มั่นคงปลอดภัย และการใช้ซอฟต์แวร์แอนติไวรัสที่เสริมการป้องกันมัลแวร์ โดยเฉพาะ

อย่างยิ่งในธุรกิจขนาดกลางและย่อม ซึ่งอาจตกเป็นเหยื่อของอาชญากรรมทางเทคโนโลยีสารสนเทศได้ง่ายเนื่องจากขาดความใส่ใจต่อความมั่นคงปลอดภัยทางไซเบอร์และมีระบบเทคโนโลยีสารสนเทศที่ไม่มั่นคงปลอดภัย

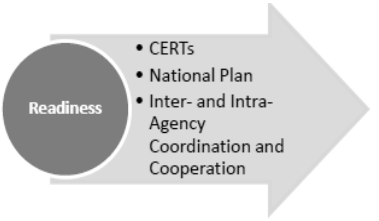
เจ้าหน้าที่ฝ่ายจัดซื้อที่ดูแลการจัดซื้ออุปกรณ์และระบบเทคโนโลยีสารสนเทศของรัฐและผู้รับเหมาของหน่วยงานรัฐ ควรปฏิบัติตามกฎระเบียบและการตรวจสอบอย่างเคร่งครัดตามมาตรฐานของความมั่นคงปลอดภัย ซึ่งจะลดผลกระทบจากมัลแวร์และภัยคุกคามอื่น ๆ ที่จะเข้ามาทางห่วงโซ่อุปทาน (Supply Chain) เทคโนโลยีสารสนเทศและทำให้เครือข่ายของรัฐและข้อมูลสาธารณะตกอยู่ในอันตราย ดังนั้นจึงควรมีการกำหนดแนวทางปฏิบัติที่ดีในการจัดซื้อ การดูแลรักษาและอัปเกรดซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้อง และมีการตรวจสอบเป็นระยะเพื่อลดความเสี่ยงที่เกิดขึ้นจากการจัดซื้อระบบเทคโนโลยีสารสนเทศที่ไม่มีลิขสิทธิ์

โรงเรียนและมหาวิทยาลัยควรพัฒนาหลักสูตรที่เพิ่มเนื้อหาในเรื่องการใช้เทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยทางระบบเทคโนโลยีสารสนเทศ ซึ่งเป็นขั้นตอนสำคัญในการให้ความรู้แก่เด็กวัยเรียนและวัยรุ่นให้รู้จักใช้เทคโนโลยีสารสนเทศอย่างรับผิดชอบและมั่นคงปลอดภัย พร้อมกันนี้ ผู้มีหน้าที่ปฏิบัติงานระบบเทคโนโลยีสารสนเทศทั้งภาครัฐและภาคเอกชนควรได้รับการฝึกอบรมระดับผู้เชี่ยวชาญเพื่อบริหารจัดการความเสี่ยงที่เกี่ยวข้องกับงานที่รับผิดชอบ เช่น ยุทธศาสตร์ความมั่นคงปลอดภัยทางไซเบอร์ของออสเตรียปี 2556 ได้รวม “Human Sensor Program” ซึ่งจัดอบรมแก่ผู้ดูแลระบบเทคโนโลยีสารสนเทศให้สังเกตสิ่งที่เกิดขึ้นเพื่อตรวจหาความผิดปกติในระบบเทคโนโลยีสารสนเทศและรายงานต่อเจ้าหน้าที่ความมั่นคงปลอดภัย

คำแนะนำ

- จัดให้มีโครงการใช้เทคโนโลยีสารสนเทศอย่างมั่นคงปลอดภัย (Cyber Wellness Program) สำหรับประชาชน กลุ่มธุรกิจขนาดใหญ่ กลาง และเล็ก
- จัดฝึกอบรมเรื่องการใช้เทคโนโลยีสารสนเทศอย่างมั่นคงปลอดภัย รวมทั้งการใช้เครื่องมือแอนติไวรัส ให้หน่วยงานของรัฐเป็นประจำ
- มีแนวปฏิบัติที่เคร่งครัดในการตรวจสอบผู้จำหน่ายอุปกรณ์และระบบเทคโนโลยีสารสนเทศเพื่อให้มั่นใจว่าระบบการจัดซื้อมีความน่าเชื่อถือและมั่นคงปลอดภัย เพื่อจะได้ซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องและอัปเดตให้ทันสมัยตลอดเวลา
- ปรับปรุงโครงการสร้างความตระหนักในเรื่องความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและจัดฝึกอบรมอย่างสม่ำเสมอ
- ปรับปรุงและบรรจุในหลักสูตรระดับโรงเรียนและมหาวิทยาลัย เพื่อให้ความรู้พื้นฐานในเรื่องการใช้เทคโนโลยีสารสนเทศและบริการออนไลน์

แผนการเตรียมความพร้อมในการจัดการภัยคุกคาม



การเตรียมความพร้อมเป็นเรื่องสำคัญที่หน่วยงานของรัฐต้องร่วมมืออย่างใกล้ชิดและแลกเปลี่ยนข้อมูลในระดับประเทศ ระดับภูมิภาค และระดับนานาชาติ กระทรวงและผู้มีหน้าที่ควบคุมกฎระเบียบ จำเป็นต้องมีส่วนร่วมในกระบวนการวางแผนกลยุทธ์ทางเทคโนโลยีสารสนเทศระดับชาติ เช่น ในมอริเชียส กระทรวงสารสนเทศและการสื่อสารโดยการสนับสนุนจากธนาคารเพื่อการพัฒนาแอฟริกาได้พัฒนาแนวทางแบบองค์รวมที่เป็นแผนยุทธศาสตร์แห่งชาติด้านความมั่นคงทางเทคโนโลยีสารสนเทศสำหรับปี 2550-2554 และมีการปรับปรุงสำหรับปี 2554-2557[63] จากนั้นมีการจัดตั้งหน่วยปราบอาชญากรรมคอมพิวเตอร์ของตำรวจในปี 2543 และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (CERT) ในปี 2551 แผนที่จัดทำขึ้นระบุชัดเจนว่าต้องเสริมความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศด้านใดบ้าง ซึ่งถือเป็นก้าวแรกของการลดความเสี่ยง นอกจากนี้ได้มีการวางโครงสร้างกลไกความร่วมมือที่จำเป็นระหว่างหน่วยงานต่าง ๆ

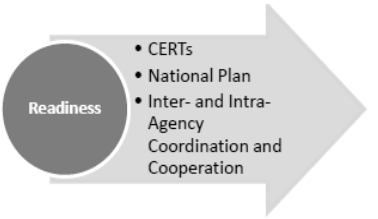
การจัดตั้ง CERT เป็นก้าวสำคัญอีกก้าวหนึ่ง และเป็นแนวปฏิบัติที่ดีต่อมาสำหรับหลายประเทศ สิ่งสำคัญคือทีมเหล่านี้ต้องบูรณาการความรู้และความชำนาญจากหน่วยงานต่าง ๆ ของรัฐ หัวใจสำคัญคือการแบ่งปันข้อมูล/ข่าวกรองอย่างมีประสิทธิผลและร่วมมือกันโดยใช้ความสามารถที่แต่ละหน่วยมีในการตอบสนองเหตุการณ์อย่างสอดคล้องกัน เช่น US-CERT เป็นทีมปฏิบัติการตลอด 24 ชั่วโมงของกระทรวงความมั่นคงแห่งมาตุภูมิ[64] ในแอฟริกาตะวันออกมีการจัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ในปี 2551 ขององค์กรประชาคมแอฟริกาตะวันออก (EACO) ซึ่งประเทศสมาชิก ได้แก่ บุรุนดี เคนยา รวันดา แทนซาเนีย และยูกันดา โดยมีภารกิจคือการจัดตั้ง CERT แห่งชาติในประเทศสมาชิกแต่ละประเทศ

ผู้เชี่ยวชาญปัญหาอาชญากรรมคอมพิวเตอร์ระดับชาติควรกระจายอยู่ตามกระทรวงและหน่วยงานต่าง ๆ ที่ทำหน้าที่บังคับใช้กฎหมาย ตลอดจนในภาคเอกชน บริษัทด้านความมั่นคงปลอดภัย และบริษัทโทรคมนาคม ดังนั้นจึงเป็นสิ่งสำคัญที่แผนกลยุทธ์ระดับชาติต้องปรับวิธีแบ่งปันข้อมูลให้มีประสิทธิภาพสูงสุด รวมทั้งทำให้การตอบสนองต่อข่าวกรองด้านภัยคุกคามด้านเทคโนโลยีสารสนเทศทันเหตุการณ์

คำแนะนำ

- มีแผนแห่งชาติเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อให้ทุกฝ่ายที่เกี่ยวข้องในภาครัฐมีแนวทางในการดำเนินงานที่ตรงกัน
- มีหน่วยงานที่รับผิดชอบในการประสานความพร้อมด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและมีระเบียบขั้นตอนในการป้องกันภัย
- มีหน่วยงานเดียวที่รับผิดชอบในการประสานงานเพื่อการตอบสนองภัยคุกคามไซเบอร์เมื่อเกิดการโจมตีระดับรัฐ
- จัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (CERT)
- สร้างหรือร่วมเป็นพันธมิตรกับเครือข่าย CERT เพื่อแบ่งปันข้อมูล/ข่าวกรอง ฝึกการระดมกำลังและเผชิญเหตุการณ์จำลองการโจมตี
- ติดต่อและเชื่อมโยงผู้ให้บริการโครงสร้างพื้นฐานที่สำคัญ (สาธารณูปโภค เช่น พลังงาน น้ำ เครือข่าย) เข้าด้วยกัน เพื่อสร้างความสัมพันธ์ที่ราบรื่นและการตอบสนองที่ฉับไวระหว่างถูกโจมตี

การป้องกันระบบเครือข่ายจากภัยคุกคาม



เราสามารถป้องกันการโจมตีทางเทคโนโลยีสารสนเทศได้ด้วยการปฏิบัติตามแนวปฏิบัติที่ดี เช่น การติดตั้ง Firewall การใส่ใจกับการปรับปรุงเรื่องความมั่นคงปลอดภัยให้ทันสมัย ตรวจสอบการติดตั้งซอฟต์แวร์ของผู้ใช้ในองค์กร ใช้เครื่องมือตรวจจับมัลแวร์ที่ทันสมัย และยึดมั่นในหลักปฏิบัติและนโยบายด้านความมั่นคงปลอดภัย เช่น เปิดใช้งานเฉพาะแอปพลิเคชันในบัญชีรายชื่อซอฟต์แวร์ที่มั่นคงปลอดภัย และเปิดใช้แอปพลิเคชันด้านความมั่นคงปลอดภัยของเว็บเบราว์เซอร์ก็เป็นอีกส่วนหนึ่งที่สามารถช่วยป้องกันภัยคุกคามด้านเทคโนโลยีสารสนเทศได้ แต่วิธีป้องกันที่ดีที่สุดคือใช้แต่ซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องและเป็นชุดที่เป็นปัจจุบันที่สุด ซึ่งหมายความว่าการจัดซื้อคอมพิวเตอร์และซอฟต์แวร์ต้องมาจากแหล่งที่น่าเชื่อถือ ใช้ซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องและทำตามขั้นตอนการลงทะเบียนเปิดใช้งานเพื่อรับประโยชน์จากบริการช่วยเหลือได้

การจัดซื้อที่ไม่มีคุณภาพอาจนำมาซึ่งมัลแวร์ที่ไม่พึงประสงค์หรือซอฟต์แวร์ที่ล้าสมัยเข้าสู่ระบบได้ ซึ่งเป็นการกระทำผิดต่อระบบการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศของหน่วยงาน สำหรับภาครัฐ ซอฟต์แวร์ที่ฝ่าฝืนลิขสิทธิ์และซอฟต์แวร์ที่ไม่พึงประสงค์อาจมาจากผู้จัดจำหน่ายโดยไม่รู้ตัว อาจจะทำให้เครือข่ายเว็บไซต์หรือคอมพิวเตอร์ใช้การหรือให้บริการไม่ได้ หรือเลวร้ายไปกว่านั้น วิธีหนึ่งในการรับมือคือ จัดให้มีมาตรฐานขั้นต่ำของความมั่นคงปลอดภัยที่ผู้ค้าหรือหน่วยงานธุรกิจที่ขายสินค้าให้กับหน่วยงานของรัฐต้องปฏิบัติตาม รัฐบาลอังกฤษได้จัดทำมาตรฐานความปลอดภัย “cyber kite mark” ตามใบรับรอง ISO27001:2005 ซึ่งคู่ค้าจำเป็นต้องมีเพื่อใช้ในการประมูลงานของรัฐ ยุทธศาสตร์ความมั่นคงปลอดภัยด้านคอมพิวเตอร์แห่งชาติของอินเดียสนับสนุนให้ใช้ผลิตภัณฑ์ทางเทคโนโลยีสารสนเทศที่ถูกต้องและผ่านการรับรอง รวมทั้งกำหนดให้มีการพัฒนาแอปพลิเคชันและซอฟต์แวร์ที่มั่นคงปลอดภัยตามแนวทางปฏิบัติที่ดีระดับสากล

ข้อมูลจาก BSA ระบุว่าการใช้ซอฟต์แวร์ที่มีลิขสิทธิ์ไม่ถูกต้อง เพิ่มโอกาสให้ผู้ใช้ต้องเจอกับปัญหามัลแวร์มากถึงหนึ่งในสามโดยเฉลี่ย และเมื่อนำอัตราการใช้ซอฟต์แวร์ที่มีลิขสิทธิ์ไม่ถูกต้องมาคำนวนร่วมด้วยแล้ว ปรากฏว่า หน่วยงานภาครัฐมีโอกาสพบมัลแวร์จากการติดตั้งซอฟต์แวร์ในคอมพิวเตอร์ 1 เครื่องจากทุก ๆ 9 เครื่อง อย่างไรก็ดี การจัดการกับปัญหานี้สามารถทำได้ด้วยขั้นตอนง่าย ๆ แต่เข้มงวด การวิจัยพบว่ามีพีซี 5% เท่านั้นที่ใช้ Windows รุ่นปัจจุบัน ผู้ใช้อย่างน้อย 40% ไม่อัปเดตระบบของตนอย่างสม่ำเสมอแม้จะได้รับคำเตือนก็ตาม และมี 25% ที่ข้ามขั้นตอนการอัปเดตซอฟต์แวร์อื่น ๆ ด้วย ในหน่วยงานของรัฐมีรายงานว่า 10% ของผู้จัดการและผู้บริหารด้านเทคโนโลยีสารสนเทศปิดการอัปเดตอัตโนมัติ มีราว 33% ที่ไม่ตรวจสอบเครื่องของผู้ใช้เพื่อหาซอฟต์แวร์ที่ผู้ใช้ติดตั้งเอง

การใช้ซอฟต์แวร์ที่ถูกต้องตามลิขสิทธิ์นั้นมีประโยชน์ต่อเศรษฐกิจอย่างมาก การใช้ซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องเพิ่มขึ้น 1% ในเอเชียแปซิฟิก จะเพิ่มมูลค่าทางเศรษฐกิจ 1.87 หมื่นล้านเหรียญในภูมิภาค เมื่อเทียบกับการใช้ซอฟต์แวร์ที่มีลิขสิทธิ์ไม่ถูกต้องที่มีมูลค่า 6 พันล้านเหรียญ ซึ่งความแตกต่าง 1.27 หมื่นล้านเหรียญนี้มีนัยสำคัญยิ่ง และการใช้ซอฟต์แวร์ที่มีลิขสิทธิ์การใช้งานถูกต้องเพิ่มขึ้น 1% จะเพิ่มมูลค่าเศรษฐกิจโลกได้ราว 7.3 หมื่นล้านเหรียญ เมื่อเทียบกับมูลค่าการใช้ซอฟต์แวร์ที่มีลิขสิทธิ์ไม่ถูกต้อง 2 หมื่นล้านเหรียญ คิดเป็นความแตกต่างมากถึง 5.3 หมื่นล้านเหรียญ

คำแนะนำ:

- มีนโยบายการจัดซื้อ (เช่น รายการผลิตภัณฑ์ที่มั่นคงปลอดภัย) สำหรับซอฟต์แวร์ และมีการป้องกันมัลแวร์สำหรับการจัดซื้อของภาครัฐ
- พัฒนาแนวปฏิบัติที่ดีในการจัดซื้อสำหรับภาคเอกชน ผู้ให้บริการอินเทอร์เน็ต กลุ่มธุรกิจขนาดใหญ่ กลาง และเล็ก
- พัฒนา จัดทำ และบังคับใช้มาตรฐานความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศสำหรับผู้จัดจำหน่ายผลิตภัณฑ์ทางเทคโนโลยีสารสนเทศให้ภาครัฐ รวมทั้งโครงการสำคัญระดับชาติ
- พิจารณาการใช้งานบน Cloud ที่ระดับความมั่นคงปลอดภัยสูง

การตอบสนองต่อภัยคุกคาม

แม้จะมีการป้องกันอย่างดีเพียงใด ก็ยังคงพบช่องโหว่ให้ถูกใช้โจมตี CERT เป็นกองกำลังแนวหน้า ที่สามารถตอบสนองและปกป้องเครือข่ายและโครงสร้างพื้นฐานเพื่อป้องกันความเสียหาย และเพื่อให้การตอบสนองผู้ทำหน้าที่ป้องกันทั้งหลายมีประสิทธิภาพมากขึ้น CERT และหน่วยงานที่เกี่ยวข้องจึงควรซ้อมรับมือภัยคุกคามเป็นประจำ โดยมีการฝึกร่วมและจำลองเหตุการณ์เพื่อทดสอบความสามารถในการรับมือภัยคุกคามระดับโลกในปัจจุบัน

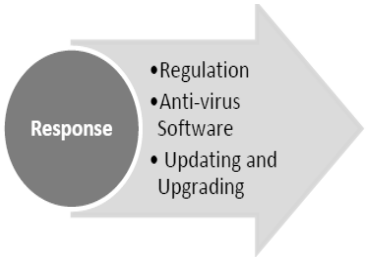
การดำเนินการทั้งหลายเพื่อให้สอดคล้องกัน รัฐควรมีแนวนโยบายทางกฎหมายเพื่อให้รัฐและผู้มีบทบาททั้งหลายสามารถดำเนินคดีและเรียกร้องการชดเชยจากการโจมตีความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ กฎระเบียบควรสมดุลระหว่างการจูงใจกับการบังคับเพื่อให้หน่วยงานสามารถรับมือต่อการโจมตีและภัยคุกคามเมื่อเกิดขึ้น

สุดท้าย ควรติดตั้ง ใช้งาน และอัปเดตซอฟต์แวร์ที่สามารถจัดการมัลแวร์และภัยคุกคามอื่น ๆ เช่น ยุทธศาสตร์ความมั่นคงปลอดภัยไซเบอร์ของรัฐบาลอังกฤษระบุว่าภัยคุกคามทั่วไปทางเทคโนโลยีสารสนเทศสามารถป้องกันได้ด้วย ‘แนวปฏิบัติการใช้งานเทคโนโลยีสารสนเทศอย่างมั่นคงปลอดภัย’ (cyber hygiene) โดยคาดว่า 80% ของการโจมตีที่ทำสำเร็จสามารถป้องกันได้ด้วยแนวปฏิบัติที่ดีแบบง่าย ๆ เช่น หมั่นอัปเดตซอฟต์แวร์แอนติไวรัส

คำแนะนำ:

- จัดตั้งแนวทางด้านกฎหมายทั้งระดับประเทศ ระดับภูมิภาค และระดับสากลเพื่อเรียกร้องค่าเสียหายเมื่อถูกโจมตี
- พัฒนาแนวทางปฏิบัติที่ดี และมีมาตรฐานในการอัปเกรดและอัปเดตซอฟต์แวร์ที่ใช้ในภาครัฐ ทั้งนี้ควรมีกำหนดแล้วเสร็จและสามารถใช้ได้จริงภายในระยะเวลาที่กำหนด

การลดผลกระทบอันเกิดจากภัยคุกคาม



ผลกระทบทางเศรษฐกิจและสังคมจากการโจมตีทางเทคโนโลยีสารสนเทศที่ทำสำเร็จนั้นอาจร้ายแรงมาก ในกรณีดังกล่าว มาตรการที่เด็ดขาดเป็นสิ่งสำคัญเพื่อฟื้นฟูความมั่นใจและสร้างโครงสร้างพื้นฐานที่มั่นคงปลอดภัยอีกครั้ง เช่นเดียวกับการบรรเทาความเสียหายในระยะกลางและระยะยาว เช่น การโจมตีสายการบินแห่งชาติอาจทำลายความเชื่อมั่นของสาธารณชนจนไม่กล้าใช้บริการเป็นเวลาหลายปี ซึ่งจะทำให้อุตสาหกรรมนี้เสียหายหนัก การจัดการสถานการณ์วิกฤตที่ได้ผลและยุทธศาสตร์การสื่อสารในยามวิกฤต ต้องเน้นเรื่องการสร้างความเชื่อมั่น และการมีมาตรการชดเชยที่ชัดเจน เป็นสองปัจจัยสำคัญของการจัดการดังกล่าว

รัฐบาลควรมีและปฏิบัติตามกระบวนการสำหรับการสืบสวน การประเมิน และการให้คำปรึกษา เพื่อตรวจหาจุดอ่อนของระบบ และเพื่อฟื้นฟูความเชื่อมั่นควรรับฟังความเห็นทั้งจากสาธารณชนและพันธมิตร เพื่อพิจารณาว่ากระบวนการปฏิบัติที่มีเพียงพอหรือไม่ เพื่อจะได้ปรับปรุงการรับมือภัยคุกคามและการโจมตีโดยรวม

จากลักษณะของภัยคุกคามและการโจมตีในระดับโลก การเป็นพันธมิตรกับรัฐบาลอื่นและองค์กรระหว่างประเทศนั้นคือช่องทางที่สำคัญในการแบ่งปันข้อมูลและสร้างแนวร่วมเพื่อต่อสู้กับสิ่งที่จะเกิดในอนาคต เวทีสนทนา เช่น Japan-US Cyber Dialogue เป็นกิจกรรมที่สำคัญเพื่อแบ่งปันแนวปฏิบัติ กรณีศึกษา และแนวทางที่เป็นประโยชน์จากการแลกเปลี่ยนประสบการณ์และความเชี่ยวชาญ

คำแนะนำ:

- จัดตั้งทีมดิจิทัลฟอเรนสิกส์ ซึ่งจะทำงานร่วมกับ CERT ภาคเอกชน และตำรวจ เพื่อสืบสวนการโจมตี
- พัฒนาหรือเข้าร่วมกับเครือข่ายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของรัฐอื่นหรือองค์กรระหว่างประเทศอื่น เพื่อแลกเปลี่ยนข้อมูล ข่าวกรอง และสร้างแนวร่วม

รายการตรวจสอบสำหรับแผนความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของรัฐ

รัฐบาลควรพิจารณาเรื่องดังต่อไปนี้ เมื่อสร้างแผนความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของภาครัฐ

1. การสร้างความตระหนักและการให้ความรู้แก่สาธารณะ

1.1. เตรียมโปรแกรมสร้างความตระหนัก สำหรับประชาชน กลุ่มธุรกิจขนาดใหญ่ กลาง และเล็ก

1.2. จัดฝึกอบรมอย่างสม่ำเสมอในเรื่องการใช้เทคโนโลยีสารสนเทศแก่เจ้าหน้าที่รัฐ และการบังคับใช้ ซอฟต์แวร์ที่อัปเกรดและมาจากแหล่งที่น่าเชื่อถือ แนวทางการใช้อินเทอร์เน็ตอย่างมั่นคงปลอดภัย และการใช้แอนติไวรัสเพื่อป้องกันมัลแวร์

1.3. มีแนวปฏิบัติที่เคร่งครัดในการตรวจสอบผู้จำหน่ายอุปกรณ์และระบบเทคโนโลยีสารสนเทศ เพื่อให้เป็นไปตามมาตรฐานความมั่นคงปลอดภัยด้านต่าง ๆ เช่น ความมั่นคงปลอดภัยของข้อมูลสาธารณะ และความมั่นคงของชาติ

1.4. ปรับปรุงหลักสูตรการสร้างความตระหนักในเรื่องความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศและจัดฝึกอบรมอย่างสม่ำเสมอ

1.5. ปรับปรุงและบรรจุหลักสูตรสร้างความตระหนักในหลักสูตรระดับโรงเรียนและมหาวิทยาลัย เพื่อเป็นความรู้พื้นฐานในเรื่องการใช้อินเทอร์เน็ตและคอมพิวเตอร์อย่างมั่นคงปลอดภัย

2. การเตรียมความพร้อมในการจัดการภัยคุกคามยามวิกฤต

2.1. มีแผนเรื่องความมั่นคงปลอดภัยทางทางเทคโนโลยีสารสนเทศ ให้ทุกฝ่ายที่เกี่ยวข้อง (ไอซีที กฎหมาย ตำรวจ วิทยาศาสตร์และเทคโนโลยีอุตสาหกรรม) มีแนวทางที่ตรงกัน

2.2. มีหน่วยงานที่รับผิดชอบในการประสานเพื่อเตรียมความพร้อมด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการป้องกัน

2.3. มีหน่วยงานเดียวที่รับผิดชอบในการประสานงานเพื่อจัดการภัยคุกคามเมื่อเกิดการโจมตีระดับรัฐ

2.4. จัดตั้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ (CERT)

2.5. สร้างหรือร่วมเป็นพันธมิตรกับเครือข่าย CERT เพื่อแบ่งปันข้อมูล/ข่าวกรอง และการซ้อมรับมือภัยคุกคาม

2.6. ระบุและติดต่อผู้ให้บริการโครงสร้างพื้นฐานที่สำคัญ (สาธารณูปโภค เช่น พลังงาน น้ำ เครือข่าย) เพื่อสร้างเครือข่ายประสานงานและตอบสนองที่ฉับไวเมื่อถูกโจมตี

3. การป้องกันภัยคุกคาม

3.1. มีนโยบายด้านความมั่นคงปลอดภัยสำหรับการจัดซื้อ เมื่อจัดซื้อซอฟต์แวร์ของแท้ ได้รับการอัปเดต และจัดซื้อแอนติไวรัสที่น่าเชื่อถือเพื่อป้องกันมัลแวร์

3.2. พัฒนาแนวปฏิบัติที่ดีในการจัดซื้อสำหรับภาคเอกชน ผู้ให้บริการอินเทอร์เน็ต กลุ่มธุรกิจขนาดใหญ่ กลาง และเล็ก

3.3.พัฒนา จัดทำ และบังคับใช้มาตรฐานความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศสำหรับผู้จัดจำหน่ายผลิตภัณฑ์ทางเทคโนโลยีสารสนเทศให้ภาครัฐ รวมทั้งโครงการสำคัญระดับชาติ

3.4.พิจารณาการใช้งานบน Cloud เพื่อความมั่นคงปลอดภัย

4. การตอบสนองต่อภัยคุกคาม

4.1. จัดตั้งแนวทางด้านกฎหมายทั้งระดับประเทศ ระดับภูมิภาค และระดับสากลเพื่อเรียกร้องการชดเชยหลังการโจมตี

4.2. พัฒนาแนวทางปฏิบัติที่ดี มีการกำหนดระยะเวลาและมาตรฐานในการอัปเกรดและอัปเดตซอฟต์แวร์ที่ใช้ในภาครัฐเป็นประจำ

5. การลดผลกระทบอันเกิดจากภัยคุกคาม

5.1. จัดตั้งทีมดิจิทัลฟอเรนสิกส์ ซึ่งจะทำงานร่วมกับ CERT ภาคเอกชน และตำรวจ เพื่อสืบสวนการโจมตี

5.2. พัฒนาหรือเข้าร่วมกับเครือข่ายความมั่นคงด้านเทคโนโลยีสารสนเทศของรัฐอื่นหรือองค์กรระหว่างประเทศอื่น เพื่อแลกเปลี่ยนข้อมูล ข่าวกรอง และสร้างแนวร่วม

บทสรุป

แม้การโจมตีความมั่นคงปลอดภัยทางคอมพิวเตอร์จะรุนแรงและอาจสร้างความเสียหายร้ายแรงต่อรัฐและต่อโครงสร้างพื้นฐานที่สำคัญ แต่ทรัพยากรที่ประเทศใช้เพื่อสร้างความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศยังถูกกว่าค่าใช้จ่ายด้านการทหารหรือการป้องกันภัยแบบเดิมมากนัก ความลังเลที่จะเพิ่มค่าใช้จ่ายและทุ่มเททรัพยากรในด้านนี้จะส่งผลเสียต่อความมั่นคงของประเทศ และเป็นที่มาของจุดอ่อนในยุทธศาสตร์การป้องกันในภาพรวม บวกกับข้อเท็จจริงที่ว่าการฟื้นตัวจากการโจมตีทางคอมพิวเตอร์มีค่าใช้จ่ายสูงกว่าการวางมาตรการที่ถูกต้องเพื่อป้องกันไม่ให้เกิดขึ้นตั้งแต่แรก ยิ่งไปกว่านั้น เรายังไม่ได้พิจารณาถึงผลกระทบที่วัดปริมาณไม่ได้ เช่น การสูญเสียความเชื่อมั่นต่อรัฐบาล และผลกระทบต่อสังคมและอุตสาหกรรมในระยะยาว

แม้แต่ในประเทศที่จัดสรรทรัพยากรจำนวนมากขึ้นเพื่อความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ ความมุ่งมั่นดังกล่าวยังเป็นแค่เศษเสี้ยวของค่าใช้จ่ายพื้นฐานทางทหาร เมื่ออินเทอร์เน็ตและการเชื่อมต่อเครือข่าย กลายเป็นสื่อหลักในการทำงานของรัฐและช่องทางในการเชื่อมต่อกับภาคอุตสาหกรรมและสังคม จึงจำเป็นอย่างยิ่งที่นโยบายและมาตรการต้องมาบรรจบกันในโลกของความเป็นจริง

ปัจจุบันชาติอุตสาหกรรมในโลกตะวันตกได้นำหน้าในเรื่องยุทธศาสตร์ความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ซึ่งเพิ่งจะให้ความสำคัญเมื่อ 2-3 ปีที่แล้ว[65] และเนื่องจากลักษณะเฉพาะของภัยคุกคาม รัฐบาลของชาติในเอเชียจึงไม่สามารถใช้ทางแก้ปัญหาแบบเดียวกับโลกตะวันตก

การรับมือและลดความเสียหายจากภัยคุกคามด้านเทคโนโลยีสารสนเทศต่อรัฐถือเป็นวาระเร่งด่วน และต้องใช้แนวทางของนโยบายความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศแบบองค์รวมในภาครัฐทั้งหมดเพื่อสร้างศักยภาพ หวังว่าด้วยข้อมูลพื้นฐานที่หนังสือฉบับนี้มีให้เจ้าหน้าที่ของรัฐจากทุกส่วนที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศจะมีความเข้าใจที่ตรงกันถึงภัยคุกคามที่รัฐบาลต้องเผชิญ ทั้งยังให้แผน

ดำเนินการด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ รวมทั้งรายการตรวจสอบ (Checklist) ซึ่งเจ้าหน้าที่ของรัฐสามารถใช้ประเมินความมั่นคงปลอดภัยในองค์กรของตน เพื่อระบุได้ว่าความเสี่ยงด้านใดบ้างที่ต้องจัดการและต้องการทรัพยากรเพิ่มเติม

รายการอ้างอิง

1 www.dc.tw.ubm-us.com/i/149381/1

2 United Nations E-Government Survey 2012, “E-Government for the People”, unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf

3 WASEDA – IAC 10th International E-Government Ranking 2014

4 www.whitehouse.gov/sites/default/files/us_national_action_plan_final_2.pdf

5 www.egress.com/local-central-government/

6 http://bit.ly/1ovVd96

7 http://japandailypress.com/malware-identified-in-hacking-incident-over-government-documents-0420850

8 http://www.alrc.gov.au/publications/6.%20The%20Privacy%20Act%3A%20Some%20Important%20Definitions/sensitive-information

9 http://www.secureit.com/resources/WP_Data_Class_and_Protect.pdf

10 http://globalnews.ca/news/1269168/900-sin-numbers-stolen-due-to-heartbleed-bug-canada-revenue-agency

[11] www.straitstimes.com/news/singapore/more-singapore-stories/story/three-breached-singpass-accounts-used-apply-fraudulent-w

[12] www.rimp.gov.ab.ca/publications/pdf/infosecurityclassification.pdf

[13] www.records.ncdcr.gov/erecords/faq.html

[14] www.computerweekly.com/news/2240170360/Departments-given-go-ahead-to-use-iPhones-for-sensitive-data

[15] www.thejakartaglobe.com/international/across-asia-officials-e-mails-may-be-vulnerable/

[16] www.computerweekly.com/news/2240170360/Departments-given-go-ahead-to-use-iPhones-for-sensitive-data

[17] www.rt.com/usa/fbi-cyber-attack-threat-739/

[18] http://www.reuters.com/article/2013/12/19/us-target-breach-idUSBRE9BH1GX20131219

[19] http://www.ft.com/intl/cms/s/0/7f9a2b26-3f74-11e4-984b-00144feabdc0.html#axzz3E2b6V9lG

[20] http://www.reuters.com/article/2014/09/18/us-home-depot-dataprotection-idUSKBN0HD2J420140918

[21] www.computerweekly.com/news/2240186339/Worldwide-government-IT-spending-to-remain-flat-in-2013-says-Gartner

22 www.oversight.house.gov/release/video-why-the-waste-in-it-spending/

23 www.itnews.com.au/News/347092,govt-it-spending-to-outrank-world-average.aspx

24 http://www.computerweekly.com/news/2240186339/Worldwide-government-IT-spending-to-remain-flat-in-2013-says-Gartner

25 http://cio.co.nz/cio.nsf/news/new-zealand-bucks-flat-government-it-spending-trend

26 http://www.bloomberg.com/news/2013-06-18/gartner-revises-2013-government-it-spending-outlook-to-0-1-drop.html

27 http://www.idc.com/getdoc.jsp?containerId=prUS24298013

28 http://www.idc.com/getdoc.jsp?containerId=prUS24298013

29 http://www.informationweek.com/government/cyber-security/budget-bill-boosts-cyber-security-spending/d/d-id/1113494

30 http://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf

31 http://thediplomat.com/2014/06/india-scrambles-on-cyber-security/

32 http://www.govtech.com/security/Seven-Cyber-security-Predictions-for-2013.html

[33] http://www.zdnet.com/th/thailand-cyber-security-state-in-crisis-7000008126/

[34] http://www.defensenews.com/article/20140224/DEFREG04/302240015/UAE-Double-Security-Budget-Focus-Cyber

[35] http://ovum.com/2012/02/28/the-shape-of-uk-public-sector-procurement-in-2012/

[36] http://gcn.com/blogs/pulse/2013/06/gartner-mobile-big-data-advanced-targeted-attacks-shape-threat-landscape.aspx?admgarea=TC_SecCybersSec

[37] http://www.futuregov.asia/articles/2013/may/02/global-study-shows-low-understanding-new-security-/

[38] http://www.guardian.co.uk/media-network/media-network-blog/2013/jun/06/cost-security-breach-business

[39] http://www.telegraph.co.uk/technology/internet-security/10886640/Cyber-crime-costs-global-economy-445-bn-annually.html

[40] http://www.v3.co.uk/v3-uk/news/2272215/government-touts-gbp10bn-savings-as-it-spending-streamlined

[41] http://articles.timesofindia.indiatimes.com/2013-05-07/security/39089484_1_government-websites-cyber-security-nic

[42] www.kaspersky.com/news?id=207576183

[43] www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?pagewanted=all&_r=0

[44] www.americanbar.org/publications/law_practice_today_home/law_practice_today_archive/march12/network-risk-insurance-privacy-security-exposures-and-solutions-for-law-firms.html

[45] http://investigations.nbcnews.com/_news/2012/11/20/15313720-one-email-exposes-millions-of-people-to-data-theft-in-south-carolina-cyberattack

[46] http://bgr.com/2014/05/27/ebay-hack-145-million-accounts-compromised/

[47] http://data.gov.uk/dataset/information-security-breaches-survey

[48] http://www.zdnet.com/ddos-attacks-rise-as-companies-fail-to-address-dns-security-7000025712/

[49] http://en.wikipedia.org/wiki/2007_cyberattacks_on_Estonia

[50] http://www.rappler.com/nation/29045-hackers-deface-philippine-government-sites-taiwan

[51] http://gcn.com/blogs/cybereye/2013/05/how-hackers-turn-internet-of-things-into-weapon.aspx

[52] http://www.nytimes.com/2013/05/13/us/cyberattacks-on-rise-against-us-corporations.html?pagewanted=all&_r=0

[53] http://www.theaustralian.com.au/australian-it/it-business/hackers-tap-into-local-essential-services/story-e6frganx-1226444141880

[54] http://www.thejakartapost.com/news/2015/01/07/govt-set-national-cyber-agency.html#sthash.f9OifJ51.dpuf

[55] http://nitc.kkmm.gov.my/index.php/national-ict-policies/national-cyber-security-policy-ncsp and http://asia.marsh.com/Portals/59/Documents/Cybercrime%20in%20Asia%20A%20Changing%20Regulatory%20Environment.pdf

[56] http://elevenmyanmar.com/index.php?option=com_content&view=article&id=3539:myanmar-to-reform-national-cyber-security-team&catid=44&Itemid=384 and http://photos.state.gov/libraries/burma/895/pdf/20141219USMyanmarICTCouncil.pdf

[57] https://www.itu.int/ITU-D/asp/CMS/Events/2010/NGN-Philippines/S5-Philippines_cybersecurity.pdf

[58] http://www.ida.gov.sg/Collaboration-and-Initiatives/Initiatives/Store/National-Cyber-Security-Masterplan-2018

[59] http://lexicon.ft.com/Term?term=cyber-espionage

[60] http://online.wsj.com/articles/finland-victim-of-long-term-cyberespionage-1404309676

[61] http://www.zdnet.com/microsoft-us-government-is-an-advanced-persistent-threat-7000024019/

62 http://www.futuregov.asia/articles/2013/may/02/gloal-study-shows-low-understanding-new-security-/

63 www.gov.mu/portal/goc/telecomit/file/ICTplan.pdf

64 www.us-cert.gov/

65 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

TRPC เป็นบริษัทที่ปรึกษาและวิจัยซึ่งมีประสบการณ์กว่า 25 ปีในอุตสาหกรรมโทรคมนาคม เทคโนโลยีสารสนเทศและการสื่อสารในเอเชียแปซิฟิก ซึ่งให้บริการคำปรึกษาเฉพาะด้าน การวิจัยและบริการฝึกอบรม โดยเน้นประเด็นด้านกฎระเบียบและกลยุทธ์ทางธุรกิจ มีเครือข่ายผู้เชี่ยวชาญและมืออาชีพทางอุตสาหกรรมที่ครอบคลุมทั่วภูมิภาค

งานวิจัยของ TRPC เน้นเรื่องเศรษฐกิจของโทรคมนาคมและเทคโนโลยีสารสนเทศและประเด็นเกี่ยวกับนโยบายและกฎระเบียบที่เกี่ยวข้องกับการพัฒนาโครงสร้างพื้นฐานข้อมูลระดับชาติ โดยมุ่งที่ภูมิภาคเอเชียตะวันออกเฉียงใต้และเอเชียตะวันออก ทั้งประเทศที่โครงสร้างพื้นฐานด้านไอซีทีพัฒนาไปมากแล้ว เช่น เกาหลีใต้ ญี่ปุ่น ฮ่องกง และประเทศที่โตเร็วและอุตสาหกรรมไอซีทีกำลังมาแรง เช่น อินโดนีเซีย เวียดนาม

http://www.trpc.biz

TRPC ขอขอบคุณบริษัท Microsoft ที่สนับสนุนการวิจัยที่จำเป็นต่อการศึกษานี้ อย่างไรก็ดี TRPC ยังคงรับผิดชอบแต่ผู้เดียวต่อความถูกต้องของข้อมูลและความเห็นที่แสดงในรายงานนี้ ซึ่งไม่ได้เป็นตัวแทนความเห็นของ Microsoft

PUBLIC DATA AT RISK:
CYBER THREATS TO THE NETWORKED GOVERNMENT
ความเสี่ยงของข้อมูลที่เปิดเผยสู่สาธารณะ
ภัยคุกคามด้านเทคโนโลยีสารสนเทศต่อภาครัฐ

บทความโดย
บริษัท TRPC

แปล จัดพิมพ์ และเผยแพร่โดย
ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต)

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน)
อาคารเดอะ ไนน์ ทาวเวอร์ แกรนด์ พระรามเก้า (อาคารบี)
ชั้น 21 เลขที่ 33/4 ถนนพระราม 9 แขวงห้วยขวาง เขตห้วยขวาง
กรุงเทพมหานคร 10310

เว็บไซต์ไทยเซิร์ต www.thaicert.or.th
เว็บไซต์สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (องค์การมหาชน) www.etda.or.th
เว็บไซต์กระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร www.mict.go.th

ISBN 978-616-7956-08-4