ภัยคุกคามทางไซเบอร์ (Cyber Security)

โดย

ฝ่ายวิเคราะห์เทคโนโลยีป้องกันประเทศ
สถาบันเทคโนโลยีป้องกันประเทศ

มีนาคม 59

ภาพ : https://108thinks.blogspot.com

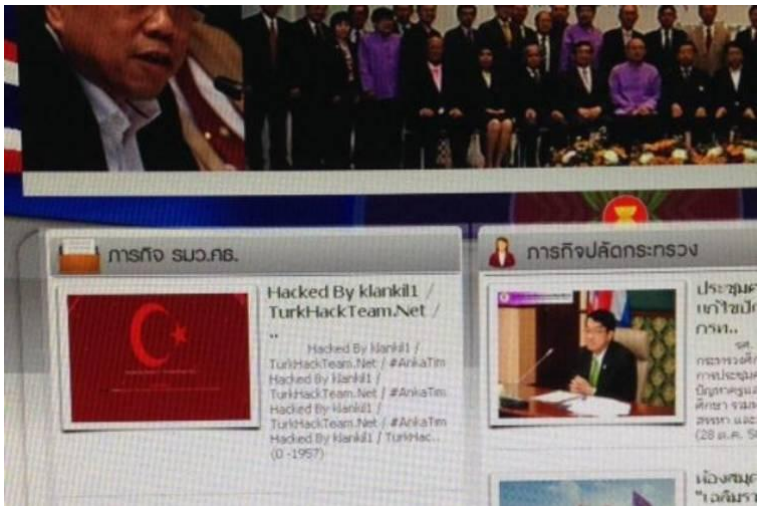
1. บทนำ : การเสริมสร้างความมั่นคงทางเทคโนโลยีสารสนเทศและไซเบอร์ ในการปกป้อง ป้องกัน ภัยคุกคามด้านไซเบอร์ นับว่าเป็นสิ่งที่สำคัญ ตามนโยบายความมั่นคงแห่งชาติ พ.ศ. 2558-2564 ในปัจจุบันภัยคุกคามทางไซเบอร์ได้เพิ่มระดับความรุนแรง และมีความสลับซับซ้อนในการแก้ไขปัญหามากยิ่งขึ้น ส่งผลเสียหายให้กับองค์กรภาครัฐ และเอกชน ไม่ว่าจะเป็นผลเสียในด้านความมั่นคง ธุรกิจการเงิน การธนาคาร และข้อมูลส่วนบุคคล จึงมีความจำเป็นอย่างยิ่งในการกำหนดมาตรการในการป้องกันทั้งเชิงรุก/รับ ต่อภัยคุกคามทาง ไซเบอร์ โดยเฉพาะอย่างยิ่ง หน่วยงานด้านความมั่นคงจำเป็นต้องมีการวางแผน/แนวทาง สำหรับการป้องกันภัยคุกคามทางไซเบอร์ โดยมีการปรับเปลี่ยนมาตรการให้สอดคล้องกับการเปลี่ยนแปลงทางยุทธศาสตร์ เพื่อให้สอดคล้องและทันต่อความทันสมัยของเทคโนโลยีที่มีความล้ำหน้าอย่างรวดเร็วได้อย่างมีประสิทธิภาพ

2. วัตถุประสงค์ : วัตถุประสงค์หลักของการรักษาความมั่นคงปลอดภัยไซเบอร์ คือ การสร้างความมั่นคงปลอดภัยในระบบเครือข่าย (Network) และข้อมูล (Data) การที่จะบรรลุวัตถุประสงค์ดังกล่าว จะต้องใช้ทั้งมาตรการทางเทคโนโลยี มาตรการทางกฎหมาย (Statutory Regulation) รวมถึงการกำกับดูแลตนเอง (Self-regulation) และการกำกับดูแลร่วมกัน (Co-regulation) ของทั้ง 3 ฝ่าย ผู้ที่ได้รับผลกระทบจากการโจมตีทางไซเบอร์ ได้แก่ รัฐ หน่วยงานภาคเอกชน และประชาชน

3. ความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

โลกดิจิทัลในปัจจุบันย่อมก่อให้เกิดภัยคุกคามด้านไซเบอร์ที่ยังคงมีเพิ่มมากขึ้น เนื่องจากการใช้งานผ่านอินเทอร์เน็ต สมาร์ทโฟน และแท็บเล็ต ในการติดต่อสื่อสารระหว่างกันของบุคคล และการติดต่อกันระหว่างหน่วยงานภาครัฐ/เอกชน ทำให้เกิดการเชื่อมโยงแลกเปลี่ยนข้อมูลได้ทุกที่ทุกเวลา ดังนั้นจึงมีช่องโหว่ของโอกาสที่ทำให้เกิดภัยคุกคามทางไซเบอร์ได้ง่ายมากขึ้น ตามข่าวสารที่ปรากฏอยู่เกือบทุกวัน เช่น

- เมื่อ 29 ต.ค. 58 พล.อ.ดาว์พงษ์ รัตนสุวรรณ รัฐมนตรีว่าการกระทรวงศึกษาธิการ (ศธ.) กล่าวถึงกรณีที่เว็บไซต์ของกระทรวงฯ ที่โดนแฮกข้อมูล โดยมีการเปลี่ยนแปลงภาพรัฐมนตรี และข้อมูลภารกิจงานของรัฐมนตรีถูกลบออกพร้อมทั้งได้แสดงข้อความ “Hacked By KlaKil/TurkHack Team Net” (ที่มา : ผู้จัดการออนไลน์)



ภาพ : http://www.dailynews.co.th/education/357457

- เมื่อ 28 ต.ค. 58 ข่าวธนาคารพาณิชย์จำนวน 4 แห่งของไทยได้รับอีเมล์ข่มขู่จากกลุ่มแฮกเกอร์ที่เรียกตนเองว่า “Armada Collective” เพื่อเรียกค่าไถ่เป็นจำนวนเงิน 20 บิตคอยน์ (ประมาณ 2 แสนบาท) เพื่อแลกกับการไม่โจมตีระบบของธนาคาร ซึ่งหากธนาคารไม่ยอมทำตามจะมีการโจมตีและเพิ่มเงินที่เรียกค่าไถ่สูงขึ้น (ที่มา : The Nation)

- การโจรกรรมข้อมูลบัตรเครดิตในเกาหลีใต้ พนักงานของบริษัท “โคเรีย เครดิต” ได้สมคบกับนักเจาะระบบหรือแฮกเกอร์ รวมทั้งพนักงานฝ่ายไอทีและบริษัทคู่สัญญาของบริษัทบัตรเครดิตชั้นนำ แอบขโมยข้อมูลส่วนตัวของผู้ใช้บัตรเครดิตกว่า 80-104 ล้านใบของลูกค้า 20 ล้านราย หรือประมาณ 40 เปอร์เซ็นต์ของชาวเกาหลีใต้ทั้งประเทศด้วยการก็อปปี้ใส่ยูเอสบีแล้วนำไปขายให้กับบริษัทการตลาดนานติดต่อกันถึงกว่าปีครึ่ง

ภาพ : http://www.manager.co.th/Around/View

The Information Security Forum (ISF) เป็นหน่วยงานอิสระ ที่ดำเนินงานเกี่ยวกับโลกไซเบอร์ ได้รายงานเกี่ยวกับแนวโน้มภัยคุกคามความมั่นคงทางสารสนเทศ สำหรับปี 2016 ว่าทิศทางความปลอดภัยทางด้านไซเบอร์ยังเป็นเชิงลบอย่างต่อเนื่อง และได้ข้อสรุปหลัก 3 ประเด็น คือ (1) ไม่มีใครน่าไว้วางใจในไซเบอร์อีกต่อไป (No-one Left to Trust in Cyberspace) (2) ความเชื่อมั่นในระบบการรักษาความมั่นคงปลอดภัยที่ได้มาตรฐานเป็นที่ยอมรับโดยทั่วไปเริ่มเสื่อมถอย (Confidence in Accepted Solution Crumbles) และ (3) ความล้มเหลว

ต่อการรักษาระดับการให้บริการในด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Failure to Deliver the Cyber Resilience Promise)

ตัวอย่างที่กล่าวมา และอีกหลายเหตุการณ์ที่มิได้กล่าวถึง แสดงให้เห็นว่าภัยคุกคามทางไซเบอร์ เป็นภัยคุกคามที่ใหญ่หลวงต่อผลประโยชน์ของชาติเกือบทุกด้าน โดยเฉพาะด้านเศรษฐกิจและด้านความมั่นคงของประเทศ การโจมตีทางไซเบอร์จะเริ่มมีความสลับซับซ้อนมากขึ้นเรื่อย ๆ และมีหลายรูปแบบในการทำลายระบบ ได้แก่ การเจาะระบบข้อมูลคอมพิวเตอร์ (Hacking) การดักรับข้อมูล (Sniffing) การทำลายระบบคอมพิวเตอร์/ข้อมูลคอมพิวเตอร์ (Malicious Software: Malware) การสอดแนมข้อมูลทางคอมพิวเตอร์โดยสปายแวร์ (Spyware) และการรุมสอบถามข้อมูลจนระบบล่ม (Denial of Service Attack : DOS) เป็นต้น

4. นโยบายในการแก้ไขปัญหาภัยคุกคามทางไซเบอร์

ปัจจุบันประเทศไทยถูกจัดว่าเป็นประเทศเป้าหมายของการโจมตีทางไซเบอร์ที่สำคัญประเทศหนึ่งของโลก และมีความเสี่ยงจากการถูกโจมตีทางไซเบอร์เป็นอันดับ 33 จาก 250 ประเทศทั่วโลก เนื่องจากมีผู้นิยมใช้ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ ไม่สามารถทำการอัปเดตซอฟต์แวร์ได้ รวมทั้งยังไม่มีมาตรการดูแลในเรื่องความมั่นคงและปลอดภัยทางไซเบอร์ที่ชัดเจน

รัฐบาลไทยโดย พลเอกประยุทธ์ จันทร์โอชา นายกรัฐมนตรีและหัวหน้าคณะรักษาความสงบแห่งชาติ (คสช.) ได้ตระหนักถึงความสำคัญ จึงมีนโยบายให้บูรณการความมั่นคงปลอดภัยทางไซเบอร์ควบคู่กับการขับเคลื่อนเศรษฐกิจดิจิทัล โดยให้นำแนวความคิด การปฏิบัติการไซเบอร์ และการต่อต้านสงครามไซเบอร์ของศูนย์ไซเบอร์กองทัพบก (Army Cyber Center) ใส่ไว้ในเศรษฐกิจดิจิทัล (Digital Economy) จัดเชื่อมโยงเครือข่ายและขยายผลในระดับชาติ รวมไว้ในโครงสร้างเศรษฐกิจดิจิทัลของรัฐบาลและให้กระทรวงกลาโหมไปดูภาพรวม

ภาพ : http://rittee1834.blogspot.com

เมื่อ 26 ต.ค.58 พล.อ.ประวิตร วงษ์สุวรรณ รองนายกรัฐมนตรีฝ่ายความมั่นคงและรมว.กลาโหม ได้ให้สัมภาษณ์ก่อนเป็นประธานการประชุมสภากลาโหม โดยมี พล.อ.อุดมเดช สีตบุตร รมช.กลาโหม พล.อ.ปรีชา จันทร์โอชา ปลัดกระทรวงกลาโหม ผู้บัญชาการเหล่าทัพ และหน่วยขึ้นตรงของกระทรวงกลาโหม ได้กล่าวไว้เกี่ยวกับเรื่องการตั้งกองสงครามไซเบอร์ ถือเป็นหน่วยงานหนึ่งในกองทัพที่เกี่ยวกับกระทรวงกลาโหมและกองบัญชาการกองทัพไทย เพื่อป้องกันภัยคุกคามทางด้านไซเบอร์ ซึ่งถือว่าเป็นการทำให้เกิดความตื่นตัวของ

กระทรวงกลาโหม และเหล่าทัพ ในการป้องกันภัยคุกคามทางไซเบอร์ นับว่าเป็นงานที่ท้าทายเป็นภัยมืดสำหรับประเทศชาติ

5. ศูนย์เทคโนโลยีทางทหาร-ศูนย์ไซเบอร์กองทัพบก

เพื่อเป็นการตอบสนองนโยบายผู้บังคับบัญชา นับว่าเป็นการแก้ปัญหาอย่างเป็นรูปธรรมของกองทัพบก ที่ตระหนักถึงปัญหา ในด้านการรักษาความมั่นคง/ปลอดภัยด้านไซเบอร์ (Cyber Security) ในการเตรียมความพร้อมรับมือกับภัยคุกคามที่มองไม่เห็นตัวบนโลกไซเบอร์ หรือบนเครือข่ายเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งปัจจุบันนับวันจะทวีความเข้มข้นและมีความรุนแรงเพิ่มขึ้นตามลำดับ

http://www.esansocial.com/site

กองทัพบกได้อนุมัติหลักการให้มีการจัดตั้งศูนย์ไซเบอร์กองทัพบก (Army Cyber Center) ขึ้นเพื่อปฏิบัติงาน โดยมี นายกรัฐมนตรี เป็นประธานคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (National Cyber Security Committee : NCSC) โดยปฏิบัติงานมาตั้งแต่ 1 ตุลาคม 2557 พร้อม ๆ กับเหล่าทัพอื่น กองบัญชาการกองทัพไทย และกระทรวงกลาโหม เพื่อเตรียมการรับมือกับภัยคุกคามด้านไซเบอร์ที่กำลังเผชิญอยู่ในปัจจุบันและมีผลกระทบต่อความมั่นคงของประเทศ รวมถึงผลกระทบด้านความมั่นคง และความปลอดภัยด้านไซเบอร์ ปัจจุบัน พล.ต.ฤทธี อินทราวุธ เป็นผู้อำนวยการศูนย์เทคโนโลยีทางทหาร (มีนาคม 2559) ได้เคยให้สัมภาษณ์ไว้ว่า

“ต่อให้คุณมีกำลังทหารและอาวุธยุทโธปกรณ์ที่ทันสมัยเต็มไปหมด แต่ไม่สามารถควบคุมสั่งการได้ก็เท่านั้น ไม่เห็นภาพการเคลื่อนไหวทางการรบ เพราะถูกแฮกเข้าไปในระบบ โจมตีในเครือข่าย บิดเบือนข้อมูลต่าง ๆ นานาจนกองทัพเสียการควบคุมบังคับบัญชา และพ่ายแพ้”

ภาพ : http://www.dailytech.in.th/army-cyber-center

5.1 วัตถุประสงค์ เพื่อให้มีหน่วยงานรับผิดชอบงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นการเฉพาะโดยตรงตามนโยบายรัฐบาล และมีขีดความสามารถในการปฏิบัติการไซเบอร์เชิงรุกเมื่อจำเป็น รวมถึงการใช้ประโยชน์จากไซเบอร์ในการสนับสนุนการปฏิบัติการข่าวสาร โดยมีสถานะเป็นหน่วยขึ้นตรงกองทัพบก (นขต.ทบ.) และปฏิบัติหน้าที่เป็นฝ่ายกิจการพิเศษ โดยมีภารกิจที่สำคัญ คือ การรักษาความมั่นคงปลอดภัยไซเบอร์ การปฏิบัติการไซเบอร์ การใช้ประโยชน์ไซเบอร์เพื่อสนับสนุนการปฏิบัติการข่าวสาร และการพัฒนาความพร้อมด้าน ไซเบอร์ของกองทัพบก

5.2 การจัดตั้งศูนย์ไซเบอร์กองทัพบก ได้ดำเนินการภายใต้หลักการบริหารงานเชิงกลยุทธ์ 4 ประการ (POLE) คือ

1. การวางแผนงาน (Planning)
2. การจัดองค์กร (Organizing)
3. การนำไปสู่การปฏิบัติ (Leading) และ
4. การประเมินผล (Evaluating)

ศูนย์ไซเบอร์กองทัพบกมีแผนการดำเนินงาน และมีการพัฒนาอย่างต่อเนื่อง โดยให้น้ำหนักไปที่มาตรการเชิงรับ คือการพัฒนาระบบป้องกันเครือข่ายข้อมูลของหน่วยงานในกองทัพ ส่วนเชิงรุกสำหรับประเทศไทยยังต้องมีความชัดเจนเกี่ยวกับเรื่องของกฎหมาย แต่อย่างไรก็ตามได้มีการเตรียมความพร้อมในเรื่องของการพัฒนาบุคลากร เพื่อเตรียมสำหรับภารกิจที่ท้าทายทางด้านไซเบอร์ในอนาคตต่อไป

5.3 กองทัพบกได้กำหนดภารกิจในเรื่องของความมั่นคงของชาติเป็นหลัก โดยให้ความสำคัญและกำหนดระดับภัยคุกคามทางด้านไซเบอร์ไว้ 4 ประการ คือ

5.3.1 ภัยคุกคามที่ส่งผลกระทบต่อความมั่นคงของประเทศ

5.3.2 ภัยคุกคามที่ส่งผลกระทบต่อจังหวัดชายแดนภาคใต้ (จชต.)

5.3.3 ภัยคุกคามที่ส่งผลกระทบต่อสถาบันฯ

5.3.4 ภัยคุกคามที่ส่งผลกระทบต่อภาพลักษณ์ของกองทัพ

นอกเหนือจากภารกิจทั้ง 4 ประการที่กล่าวมา ศูนย์ไซเบอร์กองทัพบกยังได้รณรงค์ปลูกฝังให้ความรู้แก่กำลังพลและประชาชนให้เกิดความตระหนักในเรื่องของการใช้เครื่องมือสื่อสารอย่างฉลาดปลอดภัย ไม่ตกเป็นเหยื่อ/เป็นพาหะในการแพร่กระจายความผิดโดยรู้เท่าไม่ถึงการณ์ด้วย

ภาพ : http://www.weloverta.org

6.แนวทางในการป้องกันภัยคุกคามทางด้านไซเบอร์ในขั้นต้น

- คงไม่มีซอฟต์แวร์ชนิดไหนที่สามารถป้องกันภัยคุกคามทางไซเบอร์ได้ร้อยเปอร์เซ็นต์ เพียงแต่เป็นการป้องกันการโจมตีทางไซเบอร์ให้น้อยที่สุดเท่าที่จะดำเนินการได้เท่านั้น ทั้งนี้ต้องรีบเร่งในการผลิตบุคลากรหรือผู้เชี่ยวชาญทางด้านความมั่นคงทางไซเบอร์ให้เพิ่มมากขึ้นอย่างต่อเนื่อง อีกทั้งหน่วยงานยังมีความจำเป็นสำหรับการพัฒนาทักษะการรักษาความปลอดภัยทางไซเบอร์ให้กับบุคลากร ซึ่งการพัฒนาดังกล่าวจะมีส่วนช่วยให้มีการโจมตีทางไซเบอร์ลดน้อยลง
- หน่วยงานจะต้องมีการสำรวจช่องโหว่ ข้อบกพร่อง หรือสิ่งที่เปลี่ยนแปลงต่าง ๆ ของหน่วยงานอยู่อย่างต่อเนื่องสม่ำเสมอ ซึ่งหากตรวจพบให้รีบดำเนินการแก้ไขโดยด่วนจากปัญหาที่เกิดจากไซเบอร์
- หน่วยงานควรให้ความสำคัญกับปัญหาภัยคุกคามทางด้านไซเบอร์ดังกล่าว และจัดสรรงบประมาณอย่างเหมาะสมต่อการพัฒนาป้องกัน

ภัยคุกคามทางด้านไซเบอร์กำลังเป็นภัยร้ายที่ไม่สามารถจับต้องได้ แต่มีประสิทธิภาพในการทำลายมากเสียยิ่งกว่าการใช้อาวุธยุทโธปกรณ์ทางทหาร ซึ่งสามารถนำมาประยุกต์ที่จะใช้ในเกิดการปฏิบัติการทางด้านการทหารก็ย่อมสามารถทำได้ เช่น ในการโฆษณาชวนเชื่อ สร้างความบิดเบือนทำให้เกิดการเข้าใจผิด ชี้นำ หรือควบคุมอาวุธยุทโธปกรณ์ทางทหารของฝ่ายข้าศึก สร้างความปั่นป่วนในฝ่ายเดียวกันทำให้เกิดการโจมตีฝ่ายเดียวกัน สิ่งที่กล่าวมานับว่าเป็นการเปลี่ยนสนามรบที่กำลังจะเกิดขึ้นในอนาคต สามารถสร้างความเสียหายต่อหน่วยงานและประเทศชาติได้อย่างมาก

เอกสารอ้างอิง

1. นโยบายความมั่นคงแห่งชาติ พ.ศ.2558-2564. สำนักงานสภาความมั่นคงแห่งชาติ.
2. พันเอก ดร.เศรษฐพงค์ มะลิสุวรรณ, “อาชญากรรมไซเบอร์ (Cyber Crime) ภัยคุกคามของเศรษฐกิจรูปแบบใหม่,” [Online].http://it24hrs.com [9 พฤศจิกายน 2558]
3. http://thainetizen.org/2015/10/nation-cybersecurity
4. http://www.manager.co.th/Around
5. http://rittee1834.blogspot.com
6. http://www.mtc.rta.mi.th
7. http://www.sran.net/en/blog/show/1