การจัดการความปลอดภัย ปี 2018

ภัยคุกคามที่มีอยู่มากมายหลายชนิด
ทำให้ในปัจจุบันระบบเทคโนโลยีสารสนเทศ
มีความเสี่ยงและแนวโน้มที่จะเผชิญ
ต่อภัยคุกคามในปี 2018 ตั้งแต่ซ่องโหว่
ของระบบ ซอฟต์แวร์เรียกค่าไถ่
และการโจมตีที่เป้าหมายเฉพาะ
สิ่งที่ทั้งองค์กรและผู้ใช้งานทำได้มากที่สุด
คือการลดความเสี่ยงและภัยคุกคาม
ที่อาจจะเกิดขึ้น เพื่อเกิดให้ความปลอดภัย
สูงสุดต่อระบบเทคโนโลยีสารสนเทศ

การมองเห็นภัยคุกคามที่ชัดเจนขึ้นและการรักษาความปลอดภัยแบบหลายชั้น

สำหรับองค์กร

การต่อสู้กับภัยที่มีจำนวนมากขึ้นในทุกวันนี้
และการป้องกันภัยที่ยังมาไม่ถึงนั้น
องค์กรต่างๆ ควรนำโซลูชั่นด้านความปลอดภัย
ที่สามารถมองเห็นภัยคุกคามได้ครอบคลุม
และสามารถปกป้องซ่องโหว่
และการโจมตีในแบบเรียลไทม์
ทั้งยังต้องป้องกันไม่ให้เกิดการบุกรุกใดๆ ในอนาคต
ดังนั้น การมองหาวิธีการรักษาความปลอดภัย
ในระดับองค์กรต้องรองรับการรักษาความปลอดภัย
ทั้งในรูปแบบเดิม และแบบใหม่ได้
เพื่อให้เหมาะกับภัยคุกคามที่มีอยู่อย่างหลากหลาย
สำหรับเทคโนโลยีรักษาความปลอดภัยดังกล่าว มีดังนี้

1. การสแกนแบบเรียลไทม์

การสแกนที่มีการทำงานแบบอัตโนมัติตลอดเวลาจะช่วยให้
สามารถตรวจพบมัลแวร์และเพิ่มประสิทธิภาพการทำงานของ
อุปกรณ์ให้ดียิ่งขึ้นได้

2. การตรวจสอบความน่าเชื่อถือของเว็บไซต์และไฟล์

การตรวจจับมัลแวร์ และการป้องกันผ่านการตรวจสอบความ
น่าเชื่อถือของเว็บไซต์ เทคนิคการต่อต้านสแปม และการควบคุม
แอพพลิเคชั่น ช่วยปกป้องผู้ใช้งานจากการโจมตีด้วยซอฟต์แวร์
เรียกค่าไถ่และการหาประโยชน์ในทางที่ผิดได้

3. การวิเคราะห์พฤติกรรม

ต้องมีการตรวจจับและกีดกันมัลแวร์และเทคนิคต่างๆ จากมิจฉาชีพ
ที่ทันสมัยที่สามารถเอาชนะการรักษาความปลอดภัยแบบเดิมได้

4. แมชชีน เลิร์นนิ่ง (Machine Learning) ที่มีความเที่ยงตรงสูง

คือการทำให้คอมพิวเตอร์มีความสามารถ
ในการเรียนรู้ด้วยตนเอง
เมื่อมีข้อมูลเข้ามา
โดย แมชชีน เลิร์นนิ่ง (Machine Learning)
สามารถทำนายหรือตัดสินใจได้
โดยไม่ต้องใช้คำสั่งโปรแกรมคอยกำกับ
โดยมนุษย์จะเป็นผู้ป้อนข้อมูลเข้าสู่ระบบ
รวมถึงข้อมูลด้านการเรียนรู้ต่อภัยคุกคาม
เพื่อให้คอมพิวเตอร์สามารถตรวจจับภัยคุกคาม
และรักษาความปลอดภัยที่แม่นยำและฉับไวมีที

5. การรักษาความปลอดภัยที่อุปกรณ์ปลายทาง

คือการรักษาความปลอดภัยโดยการตรวจหาซ่องโหว่
และความสามารถต่างๆ จากเซ็นเซอร์ที่อุปกรณ์ปลายทาง
เช่น โทรศัพท์มือถือ เครื่องคอมพิวเตอร์ หรือ เซิร์ฟเวอร์ (Server)
ซึ่งจะช่วยตรวจจับกิจกรรมที่มีความเสี่ยงและป้องกันการโจมตี
หรือการเคลื่อนไหวที่ไม่ปลอดภัยภายในเครือข่ายได้

การป้องกันภัยที่ยั่งยืน

สำหรับผู้ใช้งาน

1. เปลี่ยนรหัสผ่านเสมอ

ควรใช้รหัสผ่านที่มีความหลากหลายในรูปแบบและซับซ้อน
สำหรับอุปกรณ์อัจฉริยะ โดยเฉพาะเราเตอร์ (Router)
เพื่อลดโอกาสที่ผู้โจมตีเจาะเข้าอุปกรณ์

2. ตั้งค่าอุปกรณ์ให้มีความปลอดภัย

ควรปรับเปลี่ยนการตั้งค่าต่างๆ ที่ติดมากับอุปกรณ์ เพื่อรักษา
ความเป็นส่วนตัวและควรมีการเข้ารหัสข้อมูลมาใช้ เพื่อป้องกัน
การตรวจสอบและใช้ข้อมูลของผู้ไม่ประสงค์ดี

3. ติดตั้งซอฟต์แวร์อุดช่องโหว่ให้ทันเวลา

ควรปรับปรุงให้เฟิร์มแวร์เป็นรุ่นล่าสุด (หรือเปิดคุณสมบัติปรับปรุง
ซอฟต์แวร์อัตโนมัติ หากมีคุณสมบัตินี้) เพื่อหลีกเลี่ยงช่องโหว่

4. เพิกเฉยต่อกลวิธีโจมตี

ควรคำนึงอยู่เสมอว่าอีเมลที่เราได้รับ และเว็บไซต์ที่เข้าชมบ่อยครั้ง
อาจเป็นสแปม พิชชิง มีมัลแวร์ หรือใช้เป็นเครื่องมือโจมตีระบบได้

องค์กรและผู้ใช้งานจะอยู่ในตำแหน่งที่มีความปลอดภัย
เพิ่มมากขึ้นจากเดิม หากการรักษาความปลอดภัยต่างๆ
สามารถครอบคลุมวิฏจักรของภัยคุกคามทั้งหมด
ด้วยการรักษาความปลอดภัยหลายชั้น
ตั้งแต่อีเมล เกตเวย์เว็บไซต์ ไปจนถึงการใช้งาน
ในอุปกรณ์ปลายทาง และการมีระบบป้องกันภัยที่เชื่อมต่อ
กับคอมพิวเตอร์จะยิ่งทำให้มั่นใจว่าองค์กร
จะได้รับการป้องกันขั้นสูงสุดต่อภัยที่จะเกิดขึ้นใหม่
ในปี 2018 เป็นต้นไป

SAn
Security Awareness news
สาระเสริมสร้างความมั่นคงปลอดภัยด้านสารสนเทศ

SAn ในรูปของ Infographic

อ่านง่าย รู้ไว ไม่เกิน 3คลิก

www.gn.cdd.go.th/san
กลุ่มงานพัฒนาระบบเครือข่าย
ศูนย์สารสนเทศเพื่อการพัฒนาชุมชน
กรมการพัฒนาชุมชน

MALWARE 2018

Malicious Software

หรือที่เรารู้จักกันว่ามัลแวร์ (Malware) เป็นชื่อเรียกโดยรวมของเหล่าโปรแกรมคอมพิวเตอร์ทุกชนิดที่ถูกออกแบบมาเพื่อมุ่งร้ายต่อคอมพิวเตอร์และเครือข่าย ไม่ว่าจะเป็น ไวรัส (Virus), วอร์ม (Worm), โทรจัน (Trojan), สปายแวร์ (Spyware) เป็นต้น ดังนั้นผู้ใช้งานคอมพิวเตอร์ทุกคนควรรู้ลักษณะและพฤติกรรมการทำงานของมัลแวร์ในทุกรูปแบบ รวมถึงการป้องกันตัวเองจากมัลแวร์

ลักษณะและพฤติกรรมการทำงานของมัลแวร์ในแต่ละประเภท

Virus

มักจะแฝงตัวมากับโปรแกรมคอมพิวเตอร์หรือไฟล์และสามารถแพร่กระจายไปยังเครื่องอื่นๆ ได้โดยแนบตัวเองไปกับโปรแกรมหรือไฟล์ดังกล่าว แต่ไวรัสจะทำงานก็ต่อเมื่อมีการรันโปรแกรมหรือเปิดไฟล์เท่านั้น

Worm

สามารถแพร่กระจายตัวเองไปยังคอมพิวเตอร์และอุปกรณ์เครื่องอื่นๆ ผ่านทางระบบเครือข่าย เช่น อีเมล หรือระบบแชร์ไฟล์

Trojan

หลอกล่อผู้ใช้ว่าเป็นโปรแกรมที่ปลอดภัย แต่จริงๆแล้วจะทำให้เกิดความเสียหายเมื่อผู้ใช้หลงเชื่อนำไปติดตั้ง โดยที่ผู้ใช้ไม่รู้ตัวว่ามีโปรแกรมอื่นที่อันตรายแฝงตัวมาด้วย

Backdoor

เปิดช่องทางให้ผู้อื่นเข้ามาใช้งานเครื่องคอมพิวเตอร์ของเราโดยไม่รู้ตัว และจะโมยข้อมูลสำคัญต่างๆ ของเหยื่อ

Adware (แอดแวร์)

เป็นโปรแกรมสนับสนุนโฆษณา โดยทางบริษัทต่างๆ จะพยายามโฆษณาสินค้าของตนเองเพื่อที่จะขายสินค้านั้นๆ ตัวอย่างเช่น ถ้าเราลองไปดาวน์โหลดโปรแกรมฟรีตามเว็บไซต์ต่างๆ จะเห็นโฆษณาสินค้าปรากฏขึ้นมาบ่อยๆ ถ้าอยากให้โฆษณานั้นหายไปจะต้องจ่ายค่าลิขสิทธิ์เพื่อไม่ให้มีโฆษณาขึ้นมากวนใจอีก

Spyware

แอบดูพฤติกรรมและบันทึกการใช้งานของผู้ใช้ และอาจขโมยข้อมูลส่วนตัว เช่น บัญชีชื่อผู้ใช้งาน, รหัสผ่าน หรือข้อมูลทางการเงิน เป็นต้น พร้อมทั้งส่งข้อมูลดังกล่าวไปในเครื่องปลายทางที่ได้ระบุเอาไว้อีกด้วย

Ransomware

ทำการเข้ารหัสหรือล็อกไฟล์ ผู้ใช้จะไม่สามารถเปิดไฟล์หรือคอมพิวเตอร์ได้ จากนั้นก็จะส่งข้อความ “เรียกค่าไถ่” เพื่อแลกกับการถอดรหัสเพื่อกู้ข้อมูลคืนมา

อันตรายของ Malware

1. มัลแวร์จะทำลายเครื่องคอมพิวเตอร์ทั้งฮาร์ดแวร์และซอฟต์แวร์ รวมถึงข้อมูลในเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ไปแล้ว
2. มัลแวร์จะพยายามทำให้เครื่องคอมพิวเตอร์ที่ติดมัลแวร์เป็นตัวกระจายมัลแวร์สู่ผู้ใช้รายอื่นด้วยการแอบใช้อีเมล์เพื่อส่งไฟล์ไปยังรายชื่อที่มีอยู่ในอีเมล์ของเรา
3. มัลแวร์พยายามจะล้วงข้อมูลที่เป็นความลับให้กับผู้ไม่ประสงค์ดีด้วยการเปิดช่องโหว่ให้ผู้ไม่ประสงค์ดีเข้ามาสู่ระบบปฏิบัติการได้ หรือไม่ก็แอบส่งข้อมูลต่าง ๆเหล่านี้ผ่านอีเมล์ก็เป็นไปได้
4. มัลแวร์จะก่อความร้ำคาญให้กับผู้ใช้งานอยู่ตลอดเวลา

ข้อแนะนำในการป้องกันมัลแวร์

- อัพเดทคอมพิวเตอร์และซอฟแวร์ในเครื่องสม่ำเสมอ
- ติดตั้งโปรแกรมป้องกันมัลแวร์ (Anti-malware) บนคอมพิวเตอร์
- ระมัดระวังการใช้งานอุปกรณ์เชื่อมต่อทั้งหลาย เช่น แฟลชไดรฟ์ (USB) เป็นต้น ควรทำการสแกนไวรัสทุกครั้งก่อนใช้งาน
- ไม่คลิกข้อความที่แสดงโฆษณาหรือหน้าต่าง pop-up ปลอม (Adware) บนเว็บไซต์ที่เยี่ยมชม เพราะจะเป็นการเริ่มดาวน์โหลดมัลแวร์ ระต้องเช็คและตรวจสอบก่อนคลิกเสมอ
- ไม่ดาวน์โหลดโปรแกรมจากแหล่งที่ไม่น่าเชื่อถือ เสี่ยงต่อการมีมัลแวร์แฝงอยู่
- หลีกเลี่ยงการเปิดอีเมล รวมถึงไฟล์แนบต้องสงสัยใดๆ ที่ส่งมาจากอีเมลที่เราไม่รู้จัก และต้องตรวจสอบทุกครั้งก่อนดาวน์โหลดหรือเปิดไฟล์ขึ้นมา

มัลแวร์ไร้ไฟล์และมัลแวร์ที่ใช้ไฟล์ขนาดเล็ก

ในช่วงปี 2016 และ 2017 มัลแวร์ไร้ไฟล์และมัลแวร์ที่ใช้ไฟล์ขนาดเล็กมีจำนวนเพิ่มขึ้นอย่างต่อเนื่อง โดยผู้โจมตีอาศัยโอกาสที่องค์กรต่างๆ ที่ขาดความพร้อมในการรับมือกับภัยคุกคามรูปแบบนี้ เนื่องจากความสามารถในการป้องกันการโจมตีที่ยังจำกัด รวมถึงพฤติกรรมของผู้ใช้งานที่มีความซับซ้อน ขาดความระมัดระวังแม้ว่ามัลแวร์ไร้ไฟล์และมัลแวร์ที่ใช้ไฟล์ขนาดเล็กในปัจจุบันยังมีไม่มากนักเมื่อเทียบกับมัลแวร์ที่ใช้เทคนิคแบบเดิม แต่ก็นับว่าเป็นหนึ่งในภัยคุกคามที่สำคัญ ซึ่งจะนำไปสู่การเติบโตอย่างรวดเร็วของมัลแวร์ประเภทนี้ในช่วงปี 2018

มัลแวร์ที่สร้างโดย AI

ในปี 2018 อาจเป็นปีที่เราได้พบกับโฉมหน้าใหม่ของมัลแวร์ที่สร้างขึ้นโดย AI ซึ่งมัลแวร์นี้สามารถเรียนรู้ และหลบเลี่ยงการตรวจจับได้เอง การสร้างด้วย AI ทำให้มัลแวร์เกิดขึ้นได้ในปริมาณมหาศาล โดยอาชญากรไซเบอร์จะรื้อรวมเทคโนโลยี AI เข้ากับวิธีการโจมตีแบบหลายทางเพื่อสแกนตรวจหา และใช้ประโยชน์จากจุดอ่อนในสภาพแวดล้อมของผู้ให้บริการระบบคลาวด์ และอาชญากรไซเบอร์จะสามารถพัฒนาการโจมตีที่ดีที่สุดเท่าที่จะเป็นไปได้ตามลักษณะของจุดอ่อนแต่ละประเภท ซึ่งเดิมทีมัลแวร์เองสามารถใช้โมเดลด้านการเรียนรู้เพื่อหลีกเลี่ยงระบบความปลอดภัยได้อยู่แล้ว ทั้งยังสามารถผลิตสายพันธุ์ไวรัสได้มากกว่าหนึ่งล้านชุดในหนึ่งวัน

มัลแวร์เรียกค่าไถ่

มัลแวร์เรียกค่าไถ่มีการเติบโตมากขึ้นถึง 35 เท่าในปีที่ผ่านมา ซึ่งเป้าหมายต่อไปสำหรับมัลแวร์เหล่านี้ คือผู้ให้บริการระบบคลาวด์และบริการเชิงพาณิชย์อื่นๆ เนื่องจากผู้ให้บริการระบบคลาวด์มักมีการเชื่อมต่อกับเครือข่ายต่างๆ ที่ซับซ้อน จึงเป็นจุดอ่อนที่สามารถทำให้ธุรกิจ หน่วยงานภาครัฐ และโครงสร้างพื้นฐานที่สำคัญ เกิดปัญหาด้านการให้บริการ ซึ่งผลกระทบจากการโจมตีดังกล่าวอาจสร้างรายได้มหาศาลให้แก่องค์กรอาชญากรรม และทำให้บริการของบองค์กรต่างๆ นับร้อยนับพันแห่งหยุดชะงักลง หรืออาจขัดขวางการใช้บริการของผู้บริโภคนับล้านคนได้นั่นเอง โดยกลุ่มเป้าหมายของมัลแวร์เรียกค่าไถ่ ยังเป็นกลุ่มอุตสาหกรรมที่มีแนวโน้มยอมจ่ายค่าไถ่ข้อมูลมากกว่า ไม่ว่าจะเป็นบริการด้านสุขภาพ, โครงสร้างพื้นฐานที่สำคัญ, ไปจนถึงกลุ่มธุรกิจขนาดเล็ก เนื่องจากความอ่อนไหวของข้อมูลที่เกี่ยวข้อง รวมทั้งมูลค่าของข้อมูลประวัติผู้ป่วยที่สามารถนำไปขายต่อได้มูลค่ามหาศาล

Ransomware รูปแบบใหม่

การเรียกค่าไถ่จาก Ransomware แบบเดิมๆ จะเริ่มลดลง เนื่องจากโซลูชันสำหรับป้องกัน Ransomware มีให้เลือกมากขึ้น ผู้ใช้มีความตระหนัก และหลายองค์กรเริ่มวางกลยุทธ์สำหรับรับมือกับการโจมตี ส่งผลให้แฮกเกอร์เริ่มปรับเปลี่ยนเป้าหมายไปยังกลุ่มอื่น เช่น ผู้ใช้ทั่วไปที่มีฐานะ และอุปกรณ์ Internet of Things แทน อย่างไรก็ตาม Ransomware กลับมีเทคนิคในการโจมตีเพื่อเรียกค่าไถ่มากขึ้น แทนที่จะเข้ารหัสหรือล็อกการเข้าไฟล์เพียงอย่างเดียว ยังมีการเพิ่มการทำลายข้อมูลและการขัดขวางธุรกิจเข้าไปด้วย เพื่อกดดันให้เหยื่อต้องจ่ายค่าไถ่แลกกับการไม่ต้องผจญกับวิกฤตทางธุรกิจ

ESET Endpoint

โปรแกรมป้องกันไวรัส ESET Endpoint เวอร์ชั่น 6 สำหรับการติดตั้งให้กับคอมพิวเตอร์ส่วนกลางและส่วนภูมิภาค ของกรมการพัฒนาชุมชน ทุกเครื่อง

แจ้งปัญหาการติดตั้ง

โปรแกรมป้องกันไวรัส ESET Endpoint เวอร์ชั่น 6 ได้ที่กลุ่มงานสารสนเทศการพัฒนาชุมชน สำนักงานพัฒนาชุมชนทุกจังหวัด หรือกลุ่มงานพัฒนาระบบเครือข่าย 0 2141 6252, 0 2141 6281

ดาวน์โหลดคู่มือ

การติดตั้งและใช้งานโปรแกรมป้องกันไวรัส ESET Endpoint เวอร์ชั่น 6 ได้ที่ www.gn.cdd.go.th