Zero Trust Model
เกราะคุ้มกันจากภัยคุกคามไซเบอร์

เผยแพร่เมื่อวันที่ 1 กุมภาพันธ์ 2566

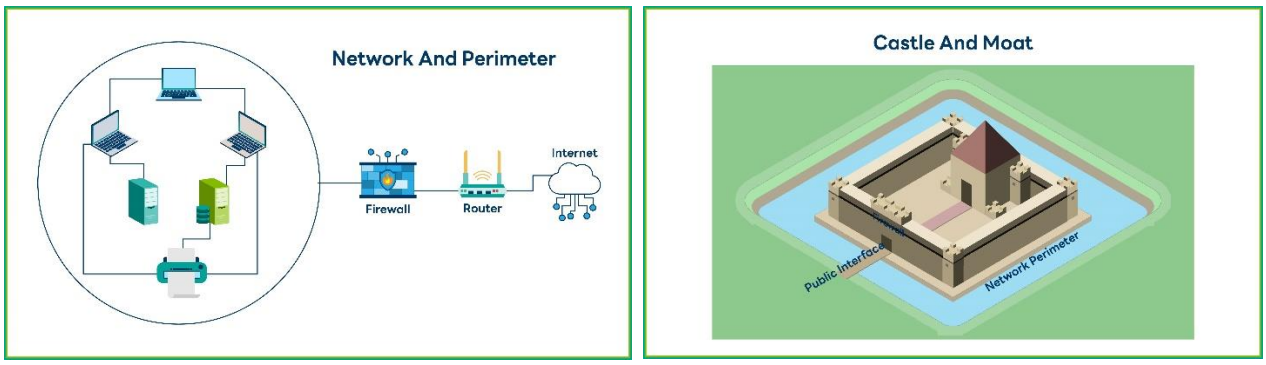
โดย ฝ่ายกำกับและตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ
สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.)

“คนที่ไว้ใจ สุดท้าย...ร้ายที่สุด”

จากข้อมูลในบทความซึ่งเผยแพร่ในเว็บไซต์ CrowdStrike บริษัทเทคโนโลยีความปลอดภัยทางไซเบอร์ของสหรัฐอเมริกา พบว่า มากกว่า 80% ของการโจมตีทางไซเบอร์นั้น เกิดจากสิ่งที่เราไว้ใจแทบทั้งสิ้น ไม่ว่าจะเป็นคน ระบบ หรืออุปกรณ์

อย่างในช่วงสถานการณ์โควิด-19 เมื่อเวลาเราออกนอกบ้าน เราป้องกันอย่างเต็มที่ ทั้งใส่หน้ากากอนามัยตลอดเวลา ฉีดสเปรย์แอลกอฮอล์ แต่เมื่อกลับมาถึงบ้าน การป้องกันก็ลดลง เนื่องจากเราเชื่อใจคนในครอบครัว และนั่นคือสาเหตุหลัก ๆ ที่ทำให้คนติดเชื้อโควิด-19 โดยส่วนใหญ่มาจากคนใกล้ตัวหรือคนที่เราไว้ใจ ที่เราเรียกกันว่า **“การ์ดตก”** นั่นเอง

ในแวดวงความปลอดภัยทางไซเบอร์มีแนวคิดหนึ่งที่พูดถึงเรื่องนี้ เรียกว่า **“แนวคิดปราสาทและคูเมือง (Castle-and-Moat Model)”** ซึ่งเป็นแนวคิดแบบดั้งเดิม หมายถึง การรักษาความปลอดภัยเครือข่ายในลักษณะปราสาทและคูเมือง โดยเปรียบเทียบปราสาทคือเครือข่ายขององค์กร (Network) และคูเมืองคือขอบเขตของเครือข่าย (Network perimeter) สะพานข้ามคูเมืองคือจุดเชื่อมต่อเครือข่าย ดังนั้น บุคคลแปลกหน้าจะไม่สามารถเข้าถึงปราสาทได้ *ดังรูปที่ 1* แต่ถ้าบุคคลใดได้รับความไว้ใจแล้ว จะสามารถข้ามสะพานและอาศัยอยู่ในพื้นที่ปราสาทได้อย่างอิสระ เพราะฉะนั้นการรักษาความปลอดภัยของปราสาท และงบประมาณส่วนใหญ่จะถูกใช้ไปกับสะพานข้ามคูเมือง ซึ่งเปรียบได้กับการที่เราลงทุนอุปกรณ์ Firewall, IDS และ IPS เพื่อป้องกันการโจมตีจากภายนอก



รูปที่ 1 แนวคิด Cybersecurity แบบดั้งเดิม (Castle-and-Moat)

ข้อจำกัดของแนวคิดปราสาทและคูเมือง

แม้จะมีข้อดี แต่แนวคิดนี้ก็มีข้อจำกัดเช่นกัน ถ้าผู้ไม่ประสงค์ดีพบจุดอ่อนที่สามารถข้ามคูเมืองหรือเข้าถึงเครือข่ายภายในได้แล้ว พวกเขาจะสามารถเข้าถึงข้อมูลและระบบในเครือข่ายได้ทั้งหมด นอกจากนี้ รูปแบบของโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศแบบปัจจุบันไม่ได้อยู่รวมกันเป็นศูนย์กลางที่เดียว แต่มีการกระจายข้อมูลไปยังพื้นที่ต่าง ๆ รวมถึงมีการใช้งาน Cloud เพิ่มมากขึ้น ทำให้แนวคิดปราสาทและคูเมืองในการปกป้องภัยคุกคามไซเบอร์จากภายนอกไม่เหมาะสมอีกต่อไป

Zero Trust...ทางแก้ของแนวคิดปราสาทและคูเมือง

Zero Trust Model กำเนิดขึ้นภายใต้แนวคิดที่ว่า **“อย่าไว้ใจสิ่งใด จะมั่นใจต้องตรวจสอบทุกครั้ง: Never Trust, Always Verify”** โดย “การเข้าถึง” ที่มาจากทั้งบุคคล อุปกรณ์ ระบบ หรือจากเครือข่ายภายนอกหรือภายในองค์กรที่จะต้องผ่านการตรวจสอบ และได้รับสิทธิ์เท่าที่จำเป็น (Lease privilege) เท่านั้น ดังนั้น การควบคุมความมั่นคงปลอดภัยไซเบอร์ตามแนวคิด **Zero Trust Architecture** คือ **การออกแบบเพื่อให้มีการปกป้องข้อมูลและบริการเป็นหลักโดยการรับรองความถูกต้องของอุปกรณ์ (เช่น device, infrastructure, application, virtual and cloud component) และผู้ใช้งาน (users) อย่างต่อเนื่อง ไม่ใช่ตรวจสอบแค่เพียงครั้งเดียว** การเข้ารหัสทุกอย่างให้เป็นการเข้าถึงขั้นต่ำเท่าที่จำเป็น และมีการจำกัดระยะเวลาในการเข้าถึง มีการแบ่งส่วนการใช้งานเพื่อจำกัดความเสียหายกรณีมีการละเมิดข้อมูล โดยเฉพาะอย่างยิ่งข้อมูลที่อาจกระทบต่อความมั่นคงปลอดภัยและความเป็นส่วนตัว (Data Security and Privacy)

หลักการตามแนวคิด Zero Trust Architecture

1. แหล่งข้อมูลต่าง ๆ ถือเป็นทรัพย์สินสารสนเทศสำคัญขององค์กรที่ต้องได้รับการปกป้อง
2. ระบบเครือข่ายที่เชื่อมต่อจากทุกแห่งต้องมีความปลอดภัยเสมอ
3. ไม่ใช่การอนุญาตเพียงครั้งเดียวแล้วใช้ได้ทั้งหมด แต่ต้องได้รับอนุญาตให้เข้าใช้งานระบบงาน ข้อมูล หรือทรัพยากรใหม่ทุกครั้ง
4. กำหนดให้เข้าถึง การเข้าใช้ระบบงานและข้อมูลสำคัญ ในลักษณะการยืนยันตัวตนแบบ Dynamic
5. หมั่นตรวจสอบการเข้าถึง การเข้าใช้ระบบงานและข้อมูลสำคัญเป็นไปตามสิทธิการใช้งาน
6. ปรับปรุงมาตรการรักษาความปลอดภัยให้เป็นปัจจุบันอยู่เสมอ

แม้ว่าการนำโมเดลการรักษาความปลอดภัยแบบ Zero Trust มาใช้ อาจทำให้ต้องใช้เวลาและทรัพยากร เพราะเกี่ยวข้องกับการออกแบบสถาปัตยกรรมระบบเครือข่าย (Network architecture) ขององค์กรให้มีความมั่นคงปลอดภัยตั้งแต่แรก หรือที่เรียกว่า Secure by Design แต่ก็คุ้มค่าที่องค์กรควรให้ความสำคัญ

เพราะจะช่วยปกป้องข้อมูลและระบบงานต่างๆ ขององค์กรได้ ทั้งหมดนี้จะเห็นได้ว่า **“การป้องกัน” ไม่ได้เริ่มต้นที่อุปกรณ์ แต่ให้เริ่มที่แนวคิดและการออกแบบกระบวนการ** ท้ายที่สุดไม่ว่าเทคโนโลยี (Technology) จะดีเพียงใด หากกระบวนการ (Process) ไม่ได้รับการออกแบบมาอย่างดี หรือผู้คน (People) ไม่ได้รับการอบรมหรือตระหนักในเรื่องความปลอดภัยทางไซเบอร์ ก็เป็นไปได้ยากที่จะปกป้องค์กรจากภัยคุกคามดังกล่าวได้ ดังนั้น เรื่องของ People Process และ Technology จึงมีความจำเป็นต้องไปด้วยกันเสมอ

ทั้งนี้ ผู้ที่สนใจสามารถศึกษาเพิ่มเติมได้จากเอกสาร NIST SP 800-207 ของสถาบันมาตรฐานและเทคโนโลยีแห่งชาติของสหรัฐฯ (National Institute of Standards and Technology)
