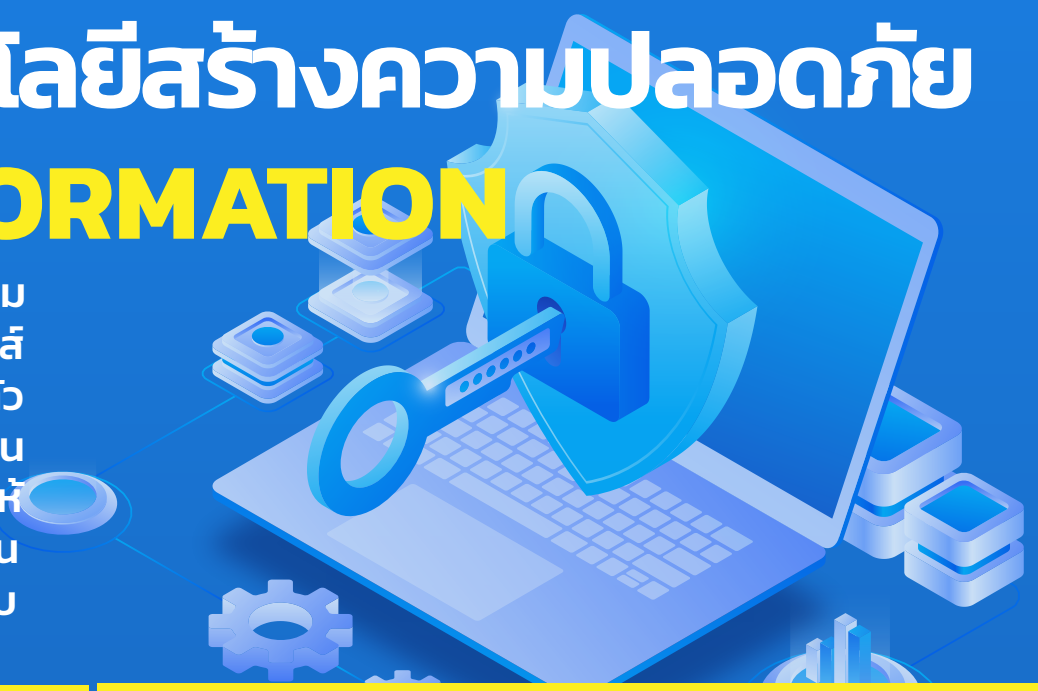
CYBER SECURITY เทคโนโลยีสร้างความปลอดภัย ในยุค DIGITAL TRANSFORMATION



ในยุคที่ Digital Transformation เข้ามามีบทบาท องค์กรควรมีการเตรียมความพร้อมเรื่องความปลอดภัยทางข้อมูล รวมทั้งอุปกรณ์อิเล็กทรอนิกส์และระบบดิจิทัล เนื่องจาก Digital Transformation คือ การปรับตัวให้องค์กรสามารถดำเนินการท่ามกลางความเปลี่ยนแปลงที่เกิดขึ้นอยู่ตลอดเวลาได้อย่างเหมาะสม ซึ่งข้อมูลเป็นสิ่งสำคัญที่ทำให้การขับเคลื่อนองค์กรให้เป็นไปได้อย่างราบรื่น ดังนั้นการป้องกันความเสี่ยงจากการถูกโจมตีทางอินเทอร์เน็ตที่อาจส่งผลกระทบต่อการปฏิบัติงานจึงเป็นสิ่งสำคัญอย่างยิ่งในปัจจุบัน

Cyber Security คืออะไร?

Cyber Security คือ เทคโนโลยีที่ช่วยปกป้องเครือข่าย อุปกรณ์ โปรแกรม ตลอดจนข้อมูลจากการถูกโจมตีจากบุคคลที่ไม่ได้รับอนุญาต ซึ่งถือเป็นสิ่งสำคัญสำหรับองค์กรต่าง ๆ ในการก้าวเข้าสู่ Digital Transformation

ความสำคัญของ Cyber Security

เนื่องจากการดำเนินงานในปัจจุบันนั้นมีการนำเทคโนโลยีเข้ามาใช้งานมากขึ้น ตั้งแต่สมาร์ทโฟน คอมพิวเตอร์ แท็บเล็ต ไปจนถึงการจัดเก็บข้อมูลบุคลากรในระบบคลาวด์ ดังนั้น การกำหนดวิธีการปกป้องข้อมูลจึงมีความสำคัญมาก เนื่องจากการโจมตีทางไซเบอร์มีการพัฒนาอย่างต่อเนื่องและมีความซับซ้อนมากขึ้น

ภัยคุกคาม คืออะไร?

ภัยคุกคาม (Threat) หมายถึง สิ่งที่อาจจะก่อให้เกิดความเสียหายต่อคุณสมบัติของข้อมูลด้านใดด้านหนึ่ง การกระทำที่อาจก่อให้เกิดความเสียหายนี เราจะเรียกว่าการโจมตี (Attack) ส่วนผู้ที่ทำให้เกิดเหตุการณ์ดังกล่าว เรียกว่า ผู้โจมตี (Attacker) หรือเรียกว่า แฮคเกอร์ (Hacker) ภัยคุกคามที่จะสร้างปัญหาให้กับองค์กรในปัจจุบันนั้นมีอยู่หลายประเภทด้วยกัน ยกตัวอย่าง เช่น

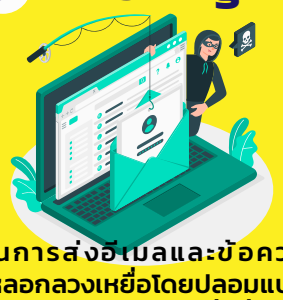
1. Malware

เป็นซอฟต์แวร์ที่สร้างขึ้นเพื่อโจมตีทางไซเบอร์ สามารถแพร่กระจายตัวเองจนสร้างความเสียหายให้กับระบบคอมพิวเตอร์ได้

2. Ransomware

เป็น Malware ประเภทหนึ่งที่ล็อกไฟล์ระบบคอมพิวเตอร์ของผู้เสียหายผ่านการเข้ารหัส เพื่อเรียกร้องเงินค่าไถ่จำนวนมากแลกกับการถอดรหัสและปลดล็อกไฟล์เหล่านั้น

3. Phishing



เป็นการส่งอีเมลและข้อความไปหลอกลวงเหยื่อโดยปลอมแปลงเป็นองค์กรหรือเว็บไซต์ที่มีชื่อเสียง โดยมีเจตนาที่จะขโมยข้อมูลส่วนบุคคลที่ละเอียดอ่อน เช่น ข้อมูลบัตรเครดิต หรือข้อมูลแอปพลิเคชันสำคัญต่าง ๆ เป็นต้น

4. APTs
(Advanced Persistent Threats)

เป็นการโจมตีทางไซเบอร์แบบกำหนดเป้าหมายระยะยาวกับองค์กรโดยผู้โจมตีจะแทรกซึมเข้าไปในเครือข่ายและหลบหลีกการตรวจจับ มักมีเป้าหมายเพื่อขโมยเงินหรือข้อมูลลูกค้า รวมทั้งการทำลายหรือขัดขวางระบบการทำงานขององค์กร

5. Code Injection

เป็นการส่งรหัสที่เป็นอันตรายไปยังระบบคอมพิวเตอร์และทำให้ระบบประมวลผลเรียกใช้รหัสนั้น จากนั้นจะใช้การแทรกโค้ดเพื่อเข้าควบคุมระบบต่าง ๆ เช่น เว็บเซิร์ฟเวอร์ หรือฐานข้อมูล และดำเนินการตามเป้าหมายที่ผู้โจมตีต้องการ

7 ประเภท Cyber Security

ปัจจุบันทคโนโลยี Cyber Security ได้มีการพัฒนาขึ้นมาหลายประเภทด้วยกัน ดังนี้

Network Security
ความปลอดภัยของเครือข่าย

เป็นการป้องกันเครือข่ายถูกบุกรุกและโจมตี Internal Networks โดยไม่ได้รับอนุญาต โดย Network Security ช่วยให้ Internal Networks มีความปลอดภัย และป้องกันการเข้าถึงโครงสร้างพื้นฐานภายใน

Application Security
ความปลอดภัยของแอปพลิเคชัน

เป็นการรักษาความปลอดภัยที่ใช้ซอฟต์แวร์และฮาร์ดแวร์เพื่อจัดการกับภัยคุกคามภายนอกที่อาจเกิดขึ้นในขั้นตอนการพัฒนาแอปพลิเคชัน และแอปพลิเคชันจำเป็นต้องมีการอัปเดตและทดสอบอย่างต่อเนื่อง เพื่อป้องกันจากการถูกโจมตีจากบุคคลอื่น การรักษาความปลอดภัยเกี่ยวกับระบบซอฟต์แวร์และอุปกรณ์ต่าง ๆ ต้องใช้ผู้เชี่ยวชาญและมีประสบการณ์เข้ามาช่วยตรวจสอบว่าระบบแอปพลิเคชันมีความปลอดภัยแค่ไหน

Cloud Security
ความปลอดภัยบนคลาวด์

เป็นการป้องกันเครือข่ายถูกบุกรุกและโจมตี Internal Networks โดยไม่ได้รับอนุญาต ซึ่ง Network Security ช่วยให้ Internal Networks มีความปลอดภัย และป้องกันการเข้าถึงโครงสร้างพื้นฐานภายใน

Machine Learning

เทคโนโลยี Machine Learning คือ การวิเคราะห์และเปรียบเทียบเชิงบริบท โดยอ้างอิงจากการเรียนรู้ของเครื่องจักร เพื่อช่วยระบุพฤติกรรมทางไซเบอร์ที่ผิดปกติหรือน่าสงสัย พร้อมจัดลำดับความสำคัญของการแจ้งเตือน จึงช่วยให้ทีมงานรักษาความปลอดภัยด้านไอทีทำงานได้ง่ายและมีประสิทธิภาพมากขึ้น

Data Security
ความปลอดภัยของข้อมูล

ข้อมูลคือสิ่งสำคัญที่จะช่วยให้การทำ Digital Transformation เดินหน้าอย่างมีประสิทธิภาพ เพราะข้อมูลเป็นตัวบ่งบอกความเปลี่ยนแปลงของสิ่งต่าง ๆ ทั้งอดีต ปัจจุบัน และสามารถนำมาคาดการณ์ความเป็นไปในอนาคตได้ ดังนั้น การป้องกันความปลอดภัยของข้อมูลจะต้องให้สิทธิในการเข้าถึงได้เฉพาะผู้ที่มีสิทธิเท่านั้น และป้องกันไม่ให้บุคคลที่สามเข้าถึงข้อมูลโดยที่ไม่ได้รับอนุญาต

File Security
ความปลอดภัยของไฟล์

เป็นเทคโนโลยีการรักษาความปลอดภัยของไฟล์ สามารถระบุกิจกรรมของไฟล์ที่น่าสงสัยได้โดยอัตโนมัติ เช่น ไฟล์ที่แสดงถึงความพยายามในการขโมยข้อมูล การโจมตีของ Ransomware หรือแม้แต่ความผิดพลาดของผู้ใช้ที่ลบไฟล์โดยไม่ได้ตั้งใจหรือคัดลอกไฟล์ไปยังตำแหน่งที่ไม่ปลอดภัย

ที่มา : https://blog.peakaccount.com/blog/cyber-security

จัดทำโดย : กลุ่มพัฒนาระบบบริหาร

การจัดการความรู้ KNOWLEDGE MANAGEMENT