CYBER SECURITY

SMACK TECH CO.,LTD.

Cyber Security

ความมั่นคงปลอดภัยทางไซเบอร์ ที่ต้องการป้องกันและการรักษาความปลอดภัยของระบบคอมพิวเตอร์ ระบบเครือข่าย และข้อมูลที่เกี่ยวข้อง โดยประกอบไปด้วย ระบบสารสนเทศ (Information System) โปรแกรมประยุกต์ (Application) ข้อมูล (Data) ระบบคอมพิวเตอร์หรือเครื่องมือที่ใช้ในการเข้าระบบเครือข่าย (Mobile Phone, Tablet, TV, IoT) หน่วยบันทึกข้อมูลและอุปกรณ์เครือข่าย (Storage, Network Device) ศูนย์ข้อมูล (Data Center) รวมถึงกระบวนการบริหารจัดการด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับความปลอดภัยของระบบคอมพิวเตอร์โดยเฉพาะระบบเครือข่ายอินเตอร์เน็ต ซึ่งมีจุดประสงค์ คือ เพื่อป้องกันการเข้าถึง การแก้ไข การเปลี่ยนแปลง หรือการทำลายข้อมูลจากบุคคลที่ไม่ได้รับอนุญาต หรือบุคคลที่ต้องการเข้าถึงข้อมูลเพื่อวัตถุประสงค์ที่ไม่เหมาะสม

Cyber Security

Network security

Application security

Data security

Cloud security

Internet of Things Security

ประเภทของการโจมตีด้วยการแฮ็กข้อมูล

มีการโจมตีทางไซเบอร์ประเภทที่เป็นทั้งแบบเปิดเผยและแบบแอบแฝง ซึ่งพบบ่อยที่สุดมีอยู่ 5 ประเภท:

- **มัลแวร์ (Malware)** เป็นช่องโหว่ที่สามารถทะลุการปกป้องเครือข่ายของคุณเช่น สปายแวร์ (spyware) ไวรัสเรียกค่าไถ่ (ransomware) และไวรัสคอมพิวเตอร์ (viruses)
- **ฟิชชิ่ง (Phishing)** – ข้อความเหล่านี้เป็นข้อความที่เป็นอันตราย (โดยส่วนมากที่พบคืออีเมล) ที่มีลิงก์ที่เป็นอันตราย ซึ่งเมื่อได้คลิกเข้าไปแล้ว จะทำการหลอกล่อให้คุณส่งข้อมูลที่ละเอียดอ่อนไปยังเป้าหมาย
- **การปฏิเสธการให้บริการ (Denial of Service (DoS))** – แฮกเกอร์มักทำการโจมตีเพื่อทำให้เครือข่าย หรือระบบของคุณ ที่มีข้อมูลส่วนเกิน จนล้นเครือข่าย และบังคับให้ระบบหยุดทำงาน
- **เทคนิคคนกลาง (Man in the middle (MitM))** – อาชญากรไซเบอร์ที่เข้ามาอยู่ระหว่างการเชื่อมต่อของคุณ ซึ่งมักจะกระทำผ่านเครือข่าย Wi-Fi สาธารณะที่ไม่ปลอดภัย และขโมยข้อมูลที่ละเอียดอ่อนของคุณไป
- **การโจมตีแบบซีโร่เดย์ (Zero-day attack)** – พบได้น้อย แต่มากขึ้นเรื่อย ๆ การโจมตีทั่วไปที่เกิดขึ้นระหว่างรอการประกาศการอัปเดตความปลอดภัย หรือโปรแกรมแก้ไข และการติดตั้งดังกล่าว

การโจมตีทางไซเบอร์เหล่านี้อาจส่งผลกระทบต่อธุรกิจจำนวนมาก เช่น คาเฟ่ที่มีเครือข่าย Wi-Fi ที่ไม่ปลอดภัย หรือร้านค้าออนไลน์ที่เสี่ยงต่อการถูกโจมตีแบบ Zero-day เป็นต้น

Cyber security

1. เข้าใจผิดว่าเป็นเรื่องของฝ่ายไอทีเท่านั้น ไม่เกี่ยวกับฝ่ายอื่น

2. เข้าใจผิดว่าภาครัฐจัดการให้ทั้งหมด

3. เข้าใจผิดว่าเป็นเรื่องของความปลอดภัยของระบบเครือข่าย (Network) อย่างเดียว โดยไม่เกี่ยวข้องกับแอปพลิเคชั่นของผู้ใช้งาน (User Application)

4. เข้าใจผิดว่ามีพาสเวิร์ดสำหรับการล็อกอินก็ปลอดภัยพอแล้ว

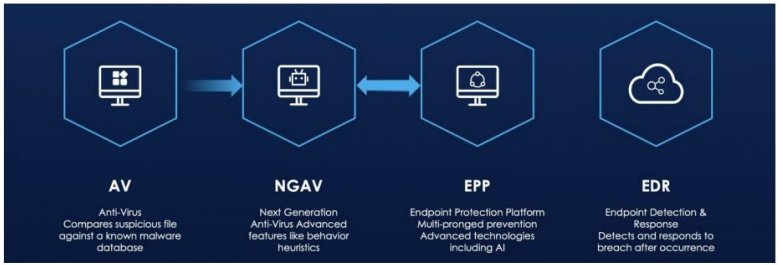
5. เข้าใจผิดว่าเป็นเรื่องของการถูกโจมตีจากแฮ็คเกอร์ภายนอกเท่านั้น

6. เข้าใจผิดว่าเป็นเรื่องไกลตัว ยังไม่ต้องรีบ

7. เข้าใจผิดว่าเป็นการทำโครงการครั้งเดียวแล้วเลิก ไม่ต้องหมั่นซ้อม ไม่พัฒนาต่อเนื่อง

ระบบ Endpoint Detection and Response (EDR)

การพัฒนาระบบ Endpoint Security



1st Generation

Anti-Virus (AV) เป็นระบบที่ช่วยป้องกัน ตรวจหา และกำจัดภัยคุกคาม เช่น ไวรัส ก่อนที่จะเข้ามาโจมตีระบบคอมพิวเตอร์

2nd Generation

Next Generation Anti-Virus (NGAV) เป็นระบบที่พัฒนามาจาก Anti-Virus (AV) โดยจะเพิ่มการวิเคราะห์พฤติกรรมการใช้งานแบบ Artificial Intelligence (AI) และ Machine Learning (ML) เข้ามา เพื่อช่วยในการตรวจจับภัยคุกคามให้มีประสิทธิภาพมากขึ้น

3rd Generation

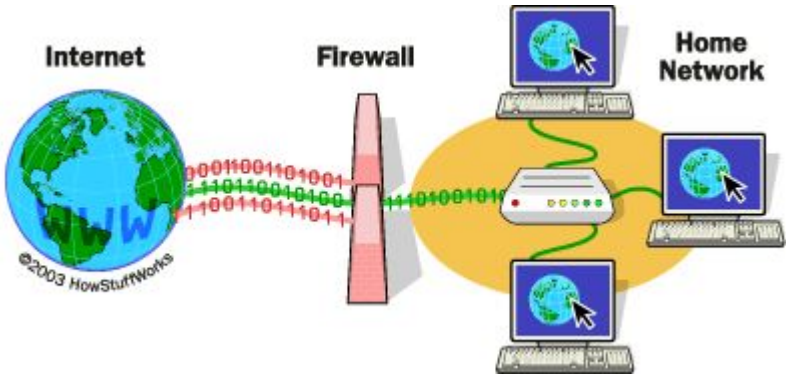
Endpoint Protection Platform (EPP) เป็นระบบที่พัฒนามาจาก Next Generation Anti-Virus (NGAV) โดยเพิ่มความสามารถในการป้องกันการโจมตีเพิ่มขึ้นมา

4th Generation

Endpoint Detection & Response (EDR) เป็นระบบที่พัฒนามาจาก Endpoint Protection Platform (EPP) และเป็นระบบที่ใหม่ที่สุดและมีประสิทธิภาพมากที่สุดในตอนนี้ สามารถตรวจจับการโจมตี ป้องกันการโจมตี และสามารถตอบสนองต่อการโจมตีได้ เช่น เมื่อสามารถตรวจจับการโจมตีได้ ระบบจะทำการป้องกันการโจมตีที่เกิดขึ้น และแยกอุปกรณ์พร้อมตัดขาดออกจากระบบเครือข่าย (Network) เพื่อป้องกันการแพร่ระบาดไปยังอุปกรณ์เครื่องอื่น

Firewall

คืออุปกรณ์ป้องกันการบุกรุก รักษาความปลอดภัยของเครือข่ายคอมพิวเตอร์ ทำหน้าที่ตรวจสอบข้อมูลที่ผ่านเข้า-ออกการเข้าถึงข้อมูลจากภายนอก จนถึงการเข้าถึงเครือข่ายภายใน เช่น เครือข่ายภายในองค์กรหรือคอมพิวเตอร์ส่วนตัวผ่านการกำหนดนโยบาย เพื่อป้องกันว่าข้อมูลที่จะส่งผ่านนั้นมีจะความปลอดภัยในระดับหนึ่ง แต่ก็ขึ้นกับการตัดสินใจของผู้ใช้งานเองด้วย ถ้าหากข้อมูลไม่ปลอดภัยได้แต่รับการอนุญาตจากผู้ใช้งาน Firewall ก็จะอนุญาตให้ผ่านเข้าไปได้



Thank you