ความรู้พื้นฐานเกี่ยวกับ Cybersecurity

แบบทดสอบก่อนเรียน
และหลังเรียน

โดย รักชาติ เหมะสิขัณฑกะ

ความหมายและขอบเขตของ Cybersecurity

Cybersecurity คืออะไร

Cybersecurity คือความมั่นคงปลอดภัยทางไซเบอร์ที่ต้องการป้องกันและการรักษาความปลอดภัยของระบบคอมพิวเตอร์ ระบบเครือข่าย และข้อมูลที่เกี่ยวข้อง

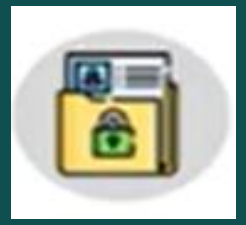
เพื่อป้องกันการเข้าถึง การแก้ไข การเปลี่ยนแปลง หรือการทำลายข้อมูลจากบุคคลที่ไม่ได้รับอนุญาต หรือบุคคลที่ต้องการเข้าถึงข้อมูลเพื่อวัตถุประสงค์ที่ไม่เหมาะสม

ทั้งนี้ หลายองค์กรต่างให้ความสำคัญกับระบบรักษาความปลอดภัยข้อมูลอย่างเท่าเทียมกัน เนื่องจากหากข้อมูลของลูกค้าหรือผู้ใช้บริการถูกโจรกรรมทางอิเล็กทรอนิกส์อาจส่งผลกระทบต่อชื่อเสียงขององค์กรได้

ความสำคัญของ Cybersecurity

1 ความเสี่ยงต่อการถูกโจรกรรมทางไซเบอร์

จากการศึกษาของ University of Maryland พบว่า ระบบคอมพิวเตอร์ทั่วโลกถูกพยายามโจมตีโดยแฮกเกอร์ทุก **39** วินาทีหรือประมาณ **2,244** ครั้งต่อวัน



ดังนั้น องค์กรจึงจำเป็นต้องให้ความสำคัญกับการเก็บข้อมูลโดยเฉพาะข้อมูลส่วนบุคคล ข้อมูลทางการเงิน ทรัพย์สินทางปัญญา และข้อมูลสำคัญระดับประเทศ เป็นต้น เนื่องจากหากขาดมาตรการป้องกันทางไซเบอร์ที่เข้มงวด อาจทำให้แฮกเกอร์เข้าถึงและนำข้อมูลไปใช้ได้โดยง่าย

ความสำคัญของ Cybersecurity

2 การรั่วไหลของข้อมูล

หากองค์กรขาดระบบการป้องกันและรักษาความปลอดภัยข้อมูล ที่มีประสิทธิภาพเพียงพอ อาจทำให้เกิดการั่วไหลของข้อมูลที่สำคัญ ซึ่งอาจถูกเปิดเผยหรือถูกนำไปใช้งานในทางที่ไม่เหมาะสม ส่งผลให้เกิดความเสียหายที่มีขนาดใหญ่ตามมาได้

3 องค์กรสูญเสียชื่อเสียง

เมื่อเกิดเหตุการณ์ณีที่องค์กรไม่สามารถรักษาความปลอดภัยของข้อมูลได้ อาจส่งผลกระทบร้ายแรงต่อองค์กร ซึ่งส่งผลให้ภาพลักษณ์ขององค์กรเสื่อมเสีย และทำให้ยากต่อการกู้คืนความเชื่อมั่นของผู้ใช้บริการให้กลับมามั่นใจในองค์กรเช่นเดิม

อาทิเช่น การสูญเสียค่าใช้จ่ายมหาศาลในการแก้ไขสถานการณ์เฉพาะหน้าและการซื้อข้อมูลที่ถูกขโมยกลับมา หรือแม้กระทั้งชื่อเสียงเกี่ยวกับความปลอดภัยขององค์กรที่ถูกทำลายเป็นต้น

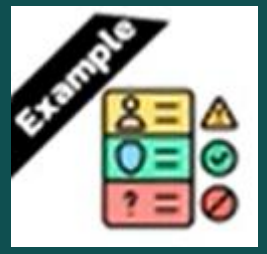
แนวทางปฏิบัติที่ดีด้านความปลอดภัย

(Security Best Practices)

หลักการ Least Privilege

Least Privilege หมายถึง การให้สิทธิ์แก้ผู้ใช้งานหรือระบบต่าง ๆ ควรจำกัดให้เฉพาะสิทธิ์ “จำเป็นต้องใช้” เท่านั่นไม่ควรให้สิทธิ์มากเกิดจำเป็น

การนำหลักนี้ไปใช้สามารถเริ่มได้จากการกำหนด “role-based access” และทบทวนสิทธิ์การเข้าถึงเป็นระยะ อาทิ ทุก ๆ 6 เดือน



พนักงานฝ่ายบัญชีไม่ควรมีสิทธิ์เข้าถึงระบบฐานข้อมูลของฝ่ายไอที การให้สิทธิ์เกิดความจำเป็นอาจเปิดช่องทางให้เกิดการโจมตีได้ หากบัญชีผู้ใช้งานดังกล่าวถูกบุกรุก เป็นต้น

หลักการ Zero Trust

Zero Trust (ZT) คือ แนวคิดที่ถูกออกแบบมาเพื่อลดความไม่แน่นอนในการบังคับใช้การอนุญาตการเข้าถึงระบบและบริการด้านสารสนเทศ โดยใช้การอนุญาตตามคำขอที่แม่นยำในรูปแบบของเครือข่ายที่ถูกมองว่าเป็นอันตราย

Zero Trust Architecture (ZTA) เป็นแผนการด้านความปลอดภัยทางไซเบอร์ขององค์กรที่นำแนวคิด Zero Trust มาใช้ โดยรวมความสัมพันธ์ของแต่ละองค์ประกอบ การวางแผนขั้นตอนการทำงาน และนโยบายด้านการเข้าถึงเข้าด้วยกัน

ดังนั้น องค์กรที่ใช้ Zero Trust จึงมีโครงสร้างเครือข่าย (ทั้งในรูปแบบที่จับต้องได้และแบบเสมือนจริง) และนโยบายการปฏิบัติการที่ถูกนำมาใช้ในองค์กร ซึ่งเป็นผลมาจากการนำแผนโครงสร้าง Zero Trust มาใช้

หลักการพื้นฐานของ Zero Trust

หลักการของ Zero Trust

"**ตรวจสอบทุกอย่าง อย่าเชื่ออะไรทั้งนั้น** ระบบความปลอดภัยรูปแบบเก่า จะมีความเชื่อว่าขอบเขตเครือข่ายที่ปลอดภัยนั้นมีอยู่จริง และอุปกรณ์ใด ๆ ที่อยู่ในขอบเขตนี้ก็ถือว่าเชื่อถือได้"

หลักการ Zero Trust ตระหนักว่า ด้วยความที่มีพนักงานที่ทำงานจากระยะไกล และทำงานแบบไฮบริด การประมวลผลผ่านระบบคลาวด์ และแอปพลิเคชัน "ให้บริการ" ผ่านคลาวด์ จึงทำให้ขอบเขตของเครือข่ายตามแนวคิดเดิมนี้ไม่มีอยู่จริง และไม่ต้องพูดถึงอุปกรณ์เคลื่อนที่ การพิมพ์งานผ่านระบบคลาวด์ และอื่น ๆ อีกมากมาย

ดังนั้น จึงไม่มีอุปกรณ์ใดที่เชื่อถือได้ แม้จะอยู่ในขอบเขตเครือข่ายที่เป็นที่ยอมรับอยู่แล้วก็ตาม โดย**แนวคิด Zero Trust ช่วยลดผลกระทบในกรณีที่ระบบถูกเจาะจากภายในหรือจากอุปกรณ์ที่ถูกบุกรุก**

การตั้งค่าระบบให้ปลอดภัย (System Hardening)

System Hardening

การตั้งค่าระบบให้ปลอดภัย (System Hardening) คือ กระบวนการลดจุดอ่อนในระบบ โดยการปิดหรือเอาออกสิ่งที่ไม่จำเป็น ปรับการตั้งค่าที่ปลอดภัยและเพิ่มการควบคุม

ตัวอย่างการตั้งค่าระบบให้ปลอดภัยที่พบบ่อย

การปิดการใช้งาน Service หรือ Port ที่ไม่จำเป็น

การปิด Default Account หรือเปลี่ยนรหัสผ่านค่าเริ่มต้น

การตั้งค่านโยบายรหัสผ่านที่เข้มงวด ต้องมีอักษรพิเศษ ความยาวขั้นต่ำ

การปิด Remote Access ที่ไม่จำเป็น และใช้ VPN แทน

การเปิดใช้ Firewall และ Logging ที่สามารถตรวจสอบย้อนหลังได้

จุดเริ่มต้นที่ดี คือ การใช้งาน Security baseline หรือคำแนะนำการตั้งค่ามาตรฐานจากแหล่งที่เชื่อถือได้ อาทิ CIS Benchmarks หรือแนวทางของ NIST

NIST Cybersecurity Framework

กรอบการทำงานด้านความมั่นคงปลอดภัย ทางไซเบอร์ของ NIST (NIST Cybersecurity Framework)

คือ ชุดแนวทางที่พัฒนาโดย National Institute of Standards and Technology (NIST) ของสหรัฐอเมริกา เพื่อช่วยให้องค์กรสามารถจัดการความเสี่ยงด้านไซเบอร์ได้อย่างมีระบบและมีประสิทธิภาพ โดยเป็นกรอบที่ได้รับการยอมรับอย่างกว้างขวางในระดับสากล

การจัดการ Patch และ Vulnerability

ความสำคัญของการจัดการ Patch

ในโลกของไซเบอร์ ช่องโหว่ (Vulnerability) ของซอฟต์แวร์ถือเป็นจุดอ่อนสำคัญที่อาจถูกภัยคุกคามใช้เป็นช่องทางโจมตีได้ หากระบบใดไม่ได้รับการอัปเดตหรือแก้ไขช่องโหว่ในเวลาที่เหมาะสมก็จะตกเป็นเป้าหมายได้ง่าย

ตัวอย่างช่องโหว่ที่พบบ่อย

ระบบปฏิบัติการ

อาทิ Windows Linux macOS เป็นต้น

ซอฟต์แวร์ทั่วไป

อาทิ เว็บเบราว์เซอร์ (Chrome, Firefox) โปรแกรมจัดการไฟล์ PDF Reader เป็นต้น

ระบบ CMS (Content Management System)

อาทิ WordPress Joomla เป็นต้น

แอปพลิเคชัน

ขององค์กรที่พัฒนาขึ้นมาเอง

อุปกรณ์เครือข่าย

อาทิ Router Firewall ที่มีระบบปฏิบัติการฝังอยู่ (Firmware) เป็นต้น

การจัดการ Patch (Patch Management)

Patch Management คือ กระบวนการบริหารจัดการ
การอัปเดตซอฟต์แวร์หรือระบบปฏิบัติการอย่างเป็นระบบ
โดยมีเป้าหมายเพื่อลดความเสี่ยงจากช่องโหว่ที่ถูกค้นพบใหม่

การจัดการ Patch (Patch Management)

Patch Management คือ กระบวนการบริหารจัดการ
การอัปเดตซอฟต์แวร์หรือระบบปฏิบัติการอย่างเป็นระบบ
โดยมีเป้าหมายเพื่อลดความเสี่ยงจากช่องโหว่ที่ถูกค้นพบใหม่

แนวทางปฏิบัติที่ควรมีในองค์กร

1

การจัดทำบัญชีทรัพยากรระบบทั้งหมด (Asset Inventory)

ต้องรู้ก่อนว่าในองค์กรมีอุปกรณ์หรือซอฟต์แวร์ใดบ้าง อาทิ เครื่องคอมพิวเตอร์ เซิร์ฟเวอร์ ซอฟต์แวร์ที่ติดตั้ง เป็นต้น เพื่อให้สามารถดูแลและอัปเดตได้ครบถ้วน

2

การใช้ระบบจัดการ Patch อัตโนมัติ (Patch Management System)

อาทิ Microsoft WSUS SCCM หรือซอฟต์แวร์ของบริษัทอื่น เป็นต้น ที่ช่วยติดตาม ตรวจสอบ และติดตั้ง Patch แบบรวมศูนย์

3

การตรวจสอบช่องโหว่อย่างต่อเนื่อง (Vulnerability Scanning)

การใช้เครื่องมือ อาทิ Nessus OpenVAS หรือ Qualys เป็นต้น เพื่อค้นหาช่องโหว่ที่ยังไม่ได้รับการแก้ไข และประเมินความเสี่ยงที่อาจเกิดขึ้น

ความสัมพันธ์ระหว่าง Patch และ Vulnerability

ช่องโหว่ (Vulnerability) คือ จุดอ่อนในระบบ

แพตช์ (Patch) คือ "ยาหรือวิธีแก้" ที่ผู้พัฒนาซอฟต์แวร์ปล่อยออกมา
เพื่ออุดช่องโหว่เหล่านั้น

หากไม่มีการจัดการแพตช์อย่างมีประสิทธิภาพ ช่องโหว่ที่ยังไม่ถูกอุด
จะกลายเป็นเป้าหมายของภัยคุกคาม (Threat)
ทำให้เกิด "ความเสี่ยง" (Risk)

กรณีตัวอย่างที่เกิดจากการละเลยการอัปเดต Patch

WannaCry Ransomware ในปี 2017

การแพร่กระจายอย่างรวดเร็วทั่วโลก โดยอาศัยช่องโหว่ของ Windows (EternalBlue) ที่ Microsoft ได้ออกแพตช์แล้วล่วงหน้า 2 เดือน แต่หลายองค์กรยังไม่ได้ทำการอัปเดต ทำให้ถูกโจมตีเป็นวงกว้าง

Equifax Data Breach ในปี 2017

ข้อมูลของประชาชนกว่า 140 ล้านรายถูกขโมย เนื่องจากบริษัทไม่อัปเดตช่องโหว่ใน Apache Struts ซึ่งมีแพตช์ออกมาก่อนแล้ว

ข้อเสนอแนะเพิ่มเติม

1. 
ให้ความรู้แก่พนักงานว่า การกด "ข้ามการอัปเดต" อาจส่งผลร้ายแรงต่อทั้งระบบ

2. 
สร้างนโยบายบังคับให้ติดตั้งอัปเดตในเวลาที่กำหนด

3. 
ตรวจสอบเครื่องมือหรือซอฟต์แวร์เก่าที่เลิกสนับสนุน (End of Support) แล้วให้อัปเกรดหรือถอดถอน

Secure Configuration และ Network Segmentation

Secure Configuration

Secure Configuration คือ การตั้งค่าระบบหรือซอฟต์แวร์อย่างรัดกุมตั้งแต่แรกเริ่ม (Secure by Default)

ตัวอย่างการตั้งค่าระบบ

การใช้การเข้ารหัสข้อมูลระหว่างทาง
อาทิ HTTPS VPN เป็นต้น

การจำกัดการเข้าถึง Control Panel หรือ Admin in Interface

การบันทึกและติดตาม log ทั้งในระบบปฏิบัติการและแอปพลิเคชัน

การไม่ใช้ค่าตั้งต้น
อาทิ admin/admin
123456 เป็นต้น

การใช้ระบบตรวจสอบความผิดปกติ
อาทิ IDS (intrusion Detection System)
เป็นต้น

การแบ่งเครือข่าย (Network Segmentation)

การแบ่งเครือข่าย

การแบ่งเครือข่าย (Network Segmentation) คือ การแยกส่วนระบบเครือข่ายตามหน้าที่

ตัวอย่างความเสี่ยง

การแยกเครือข่ายสำหรับผู้ใช้ทั่วไป
กับเครือข่ายสำหรับระบบควบคุม

การจำกัดการเข้าถึงระหว่าง segment
โดยใช้ firewall หรือ VLAN

หาก segment ใดถูกบุกรุก
จะไม่สามารถลุกลามไปส่วนอื่นได้ง่าย

แนวคิดนี้เปรียบได้กับการแบ่งห้องในบ้าน ถ้าโจรเข้ามาห้องหนึ่ง ก็จะไม่สามารถเข้าทุกห้องได้โดยง่าย

ภัยคุกคามทางไซเบอร์ที่พบบ่อย

- ❑ **DoS / DDoS และ Web-based Attacks**

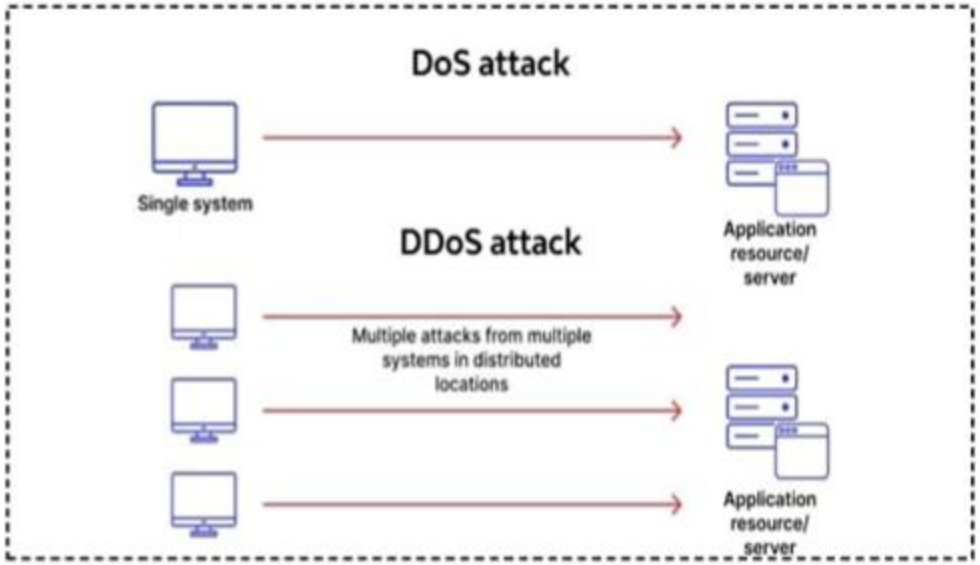
DoS / DDoS และ Web-based Attacks

DoS (Denial of Service)

DoS (Denial of Service) คือ การโจมตีระบบหรือเว็บไซต์โดยการส่งคำขอจำนวนมากอย่างต่อเนื่องจนเกินขีดความสามารถในการประมวลผลของระบบ ส่งผลให้เว็บไซต์ไม่สามารถให้บริการได้ตามปกติ เกิดอาการล่มหรือทำงานล่าช้า ซึ่งสร้างผลกระทบต่อความพร้อมใช้งานของระบบและบริการขององค์กร

DDoS (Distributed Denial of Service)

DDoS (Distributed Denial of Service) คือ รูปแบบการโจมตีที่มีความรุนแรงมากกว่า โดยดำเนินการจากอุปกรณ์หลายเครื่องพร้อมกัน ซึ่งมักเป็นเครื่องที่ติดมัลแวร์และกลายเป็นส่วนหนึ่งของ Botnet ทำให้การป้องกันเป็นไปได้ยากยิ่งขึ้น และอาจส่งผลกระทบต่อความน่าเชื่อถือของเว็บไซต์หรือบริการขององค์กร



Web-based Attacks

Web-based Attacks คือ การโจมตีผ่านช่องโหว่ของเว็บไซต์ อาทิ

SQL Injection เป็นเทคนิคการโจมตีที่อาศัยการส่งคำสั่ง SQL ผ่านทางเว็บแอปพลิเคชันไปยังระบบฐานข้อมูล โดยใช้ประโยชน์จากช่องโหว่ในการตรวจสอบข้อมูลที่ผู้ใช้กรอก (Input Validation) ซึ่งมีข้อจำกัดหรือขาดความเข้มงวด โดยนักพัฒนามักนำข้อมูลที่ผู้ใช้กรอกไปใช้เป็นส่วนหนึ่งของคำสั่ง SQL เพื่อส่งต่อไปยังฐานข้อมูล

ผู้เจาะระบบ (Hacker) จึงแทรกคำสั่ง SQL อันตรายลงในข้อมูลที่กรอก เพื่อให้ระบบประมวลผลคำสั่งเหล่านั้นร่วมกับคำสั่ง SQL ปกติ ส่งผลให้ผู้เจาะระบบสามารถเข้าถึง ดัดแปลง หรือลบข้อมูลในระบบฐานข้อมูลได้ตามที่ต้องการ

ตัวอย่างที่พบได้บ่อย คือการใช้ข้อความ อาทิ "OR 1=1" เพื่อหลอกให้ระบบข้ามขั้นตอนการตรวจสอบสิทธิ์และเข้าสู่ระบบโดยไม่ต้องใช้ข้อมูลยืนยันตัวตนที่ถูกต้อง

ภัยคุกคามทางไซเบอร์ที่พบบ่อย

- ❑ **Malware** : Virus Worm Trojan Ransomware
- ❑ **Phishing** และ **Social Engineering**
- ❑ **Insider Threats** และ **Human Error**

มัลแวร์ (Malicious Software) : Virus Worm Trojan Ransomware

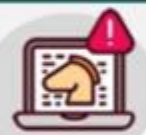
มัลแวร์ (Malicious Software)

มัลแวร์ (Malicious Software) คือ ซอฟต์แวร์ที่ได้รับการออกแบบมาเพื่อแทรกแซง ทำลาย หรือขโมยข้อมูลจากระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาต โดยสามารถแบ่งออกได้เป็นหลายประเภท ซึ่งแต่ละประเภทมีพฤติกรรมที่แตกต่างกัน

ตัวอย่างมัลแวร์

ไวรัส (Virus) คือ โปรแกรมที่แทรกตัวเองเข้าไปในไฟล์หรือโปรแกรมอื่น ๆ เมื่อมีการเปิดใช้งาน ไวรัสจะกระจายไปยังไฟล์อื่น ๆ ภายในระบบและมักทำลายไฟล์หรือทำให้ระบบทำงานผิดปกติ

เวิร์ม (Worm) คือ มัลแวร์ที่สามารถแพร่กระจายได้เองผ่านเครือข่ายโดยไม่ต้องแทรกตัวกับไฟล์หรือโปรแกรม เมื่อเข้าสู่ระบบหนึ่งแล้วจะพยายามแพร่ไปยังระบบอื่น ๆ อย่างรวดเร็ว



โทรจัน (Trojan Horse) คือ มัลแวร์ที่ซ่อนตัวอยู่ในโปรแกรมที่ดูเหมือนไม่มีอันตราย เช่น เกมหรือซอฟต์แวร์ฟรี เมื่อผู้ใช้ติดตั้งโปรแกรมดังกล่าวจะเปิดช่องทางให้ผู้ไม่ประสงค์ดีสามารถเข้าควบคุมเครื่องคอมพิวเตอร์ได้

แรนซัมแวร์ (Ransomware) คือซอฟต์แวร์ที่ทำการล็อกไฟล์หรือระบบทั้งหมดของเหยื่อ และเรียกร้องค่าไถ่เพื่อปลดล็อกข้อมูลดังกล่าว มักพบได้บ่อยในองค์กร โดยเฉพาะกลุ่มที่ขาดระบบสำรองข้อมูลที่เพียงพอ

From: Kasikorn Bank Internet Banking <ib3@monitoremail.co.cc>
Date: November 13, 2011 4:36:44 PM GMT+07:00
To: undisclosed-recipients:;
Subject: Your Account Validation is Required!

Example

Message ID : 847349333

Dear Esteemed Kasikorn Bank Customer,

Your Account requires Validation. We are having problems validating your accounnt. We would like you to validate your account with us to prevent account suspension.

To begin, log on to our secure server with your User ID and Password and proceed to updating your account information with us.

and verify your account.

กรุณาอย่าคลิกลิงค์ใดๆหรือยู่ในอีเมล์หลอกลวงนี้

Kasikorn Bank will bear no responsibility for any loss if no action is followed. This Email is subject to mndatory monitoring, Access to your online Banking will be suspended if no action is taken.

Kasikorn Bank , Thailand will Always send you Emails as regards to account maintainance.Please view our privcy policy statements

1 Soi Rat Burana 27/1, Rat Burana Road, Rat Burana Sub-District, Rat Burana District, Bangkok 10140, Thailand. Telephone: +66 2888 8800 Telefax : +66 2888 8882

Phishing และ Social Engineering

Phishing

Phishing คือ **การลวงเหยื่อให้เปิดเผยข้อมูลส่วนตัว** อาทิ รหัสผ่าน หมายเลขบัตรเครดิต เป็นต้น โดยมักมาใน**รูปแบบอีเมล** **หรือเว็บไซต์ปลอมที่ดูคล้ายของจริง** อาทิ อีเมลปลอมจากธนาคาร ที่แจ้งว่าบัญชีมีปัญหาและให้คลิกเพื่อยืนยันตัวตน เป็นต้น

Phishing และ Social Engineering

Spear Phishing

Spear Phishing คือ การโจมตีแบบฟิชชิ่งที่มีการเจาะจงเป้าหมาย อาทิ ระดับผู้บริหารหรือเจ้าหน้าที่ระดับสูง เป็นต้น โดยใช้ข้อมูลส่วนตัวของเหยื่อ เพื่อเพิ่มความน่าเชื่อถือในการโจมตี

Example

ผู้เจาะระบบ (Hacker) จะปลอมตัวเป็นบุคคลที่น่าเชื่อถือ และส่งอีเมลที่ดูเหมือนเป็นข้อความทางการ พร้อมลิงก์หรือไฟล์แนบที่แฝงมัลแวร์ เมื่อคลิกลิงก์หรือเปิดไฟล์แนบ จะสามารถเข้าถึงข้อมูลสำคัญหรือควบคุมระบบได้

Social Engineering

Social Engineering คือ เทคนิคการโจมตีที่ใช้มนุษย์เป็นช่องทาง โดยการปลอมตัวเป็นบุคคลหรือเจ้าหน้าที่ที่น่าเชื่อถือ อาทิ การปลอมตัวเป็นเจ้าหน้าที่ไอทีเพื่อขอรหัสผ่าน หรือโทรศัพท์มาหลอกขอรหัส OTP เทคนิคเหล่านี้ไม่ใช้เครื่องมือไอทีขั้นสูง แต่ใช้การหลอกลวงทางจิตวิทยาเพื่อให้เหยื่อเปิดเผยข้อมูลสำคัญ

Example

ผู้เจาะระบบ (Hacker) โทรปลอมแปลงเป็นเจ้าหน้าที่ธนาคาร แล้วหลอกล่อให้เหยื่อให้รหัส OTP เพื่อยืนยันการโอนเงิน ทั้งที่จริงคือการหลอกถอนเงิน

Insider Threats และ Human Error

Insider Threats คือ ภัยคุกคามที่เกิดจากบุคคลภายในองค์กร ไม่ว่าจะเป็นพนักงานประจำ พนักงานสัญญาจ้าง หรือบุคคลที่มีสิทธิ์เข้าถึงระบบหรือข้อมูลภายในองค์กร โดยภัยคุกคามประเภทนี้มักเกิดจากการใช้สิทธิ์หรือข้อมูลในทางที่ไม่เหมาะสม สามารถแบ่งออกเป็น 2 ประเภทหลัก ได้แก่

1

เจตนาไม่ดี (Malicious Insider)

บุคคลที่มีเจตนาขโมยข้อมูลหรือทำลายระบบ อาทิ การขโมยข้อมูลลูกค้าเพื่อนำไปขาย หรือการทำลายระบบก่อนการลาออกจากองค์กร เป็นต้น

2

ไม่เจตนา (Negligent Insider)

บุคคลที่ไม่มีเจตนาร้าย อาทิ การเผลอแชร์ไฟล์ที่มีข้อมูลลับกับบุคคลภายนอก หรือการโพสต์ข้อมูลภายในองค์กรลงในโซเชียลมีเดีย Ask ChatGPT เป็นต้น

ตัวอย่างกรณี

พนักงานฝ่ายไอทีที่ไม่พอใจองค์กรและจงใจลบข้อมูลในระบบเซิร์ฟเวอร์

พนักงานฝ่ายบัญชีที่ส่งข้อมูลเงินเดือนให้บุคคลที่ไม่เกี่ยวข้อง
ซึ่งส่งผลให้ข้อมูลส่วนบุคคลของพนักงานรั่วไหล

เจ้าหน้าที่ฝ่ายขายที่คัดลอกฐานข้อมูลลูกค้าออกไปใช้ประโยชน์
กับบริษัทคู่แข่งหลังจากการลาออกจากองค์กร

ความผิดพลาดของมนุษย์ (Human Error)

ความผิดพลาดของมนุษย์ (Human Error)

ข้อผิดพลาดจากบุคลากร (Human Error) ถือเป็นสาเหตุสำคัญของเหตุการณ์ด้านความมั่นคงปลอดภัยในหลายองค์กร แม้จะมีการติดตั้งระบบรักษาความปลอดภัยที่ทันสมัย หากบุคลากรขาดความเข้าใจหรือปฏิบัติไม่ถูกต้องตามมาตรการที่กำหนด อาจก่อให้เกิดช่องโหว่ซึ่งนำไปสู่เหตุการณ์ด้านความมั่นคงปลอดภัยได้

ตัวอย่างความผิดพลาดของมนุษย์ที่พบบ่อย

การใช้รหัสผ่านเดียวกัน ในหลายระบบ ทำให้หากรหัสรั่วจากระบบหนึ่ง ก็เข้าถึงระบบอื่นได้

การคลิกอีเมลฟิชชิ่ง ที่มีลิงก์หรือไฟล์แนบอันตราย โดยไม่ตรวจสอบก่อน

การละเลยในการล็อกหน้าจอคอมพิวเตอร์ขณะเปิดใช้งานเอกสารลับ อาจก่อให้เกิดความเสี่ยงต่อการรั่วไหลของข้อมูลอ่อนไหว

การส่งไฟล์หรืออีเมลไปยังผู้รับที่ไม่ถูกต้องโดยเฉพาะในกรณีที่ไฟล์นั้นประกอบด้วยข้อมูลที่มีความอ่อนไหว อาจก่อให้เกิดความเสี่ยงต่อการรั่วไหลของข้อมูลอ่อนไหว

การลบไฟล์สำคัญโดยไม่ตั้งใจ หรือการจัดการข้อมูลผิดขั้นตอน ซึ่งส่งผลให้ข้อมูลสูญหายและเป็นความเสี่ยงต่อความมั่นคงปลอดภัยของข้อมูล