7 รูปแบบทั่วไปของการโจมตี Cybersecurity

Highlight

– หากคุณได้เคยศึกษาเรื่องราวของภัยคุกคามในโลกไซเบอร์จะพบว่า “มีการโจมตีมากมายหลายรูปแบบ แตกไม่มีรูปแบบไหนเลยที่เหมือนกัน” แต่ละประเภทของภัยคุกคามจะมีลักษณะการโจมตีเป็นของตัวเองถึงแม้อาจจะมีความคล้ายคลึงกันบ้างก็ตาม

– ในทำนองเดียวกันหากผู้ไม่หวังที่ต้องการจะคุกคามข้อมูลขององค์กรและสร้างความเสียหายให้กับองค์กรของคุณ พวกเขาจะเตรียมข้อมูลและพัฒนารูปแบบอาวุธให้มีประสิทธิภาพที่มากพอในการคุกคาม

– ซึ่งหากคุณจะทำความเข้าใจเกี่ยวกับ “ภัยคุกคาม” เหล่านี้มากเพียงใด ก็อาจจะไม่มากพอ เพราะสิ่งเหล่านี้จะพยายามหาช่องโหว่ที่จะโจมตีอยู่เสมอ อย่างไรก็ตามนี่คือ 7 รูปแบบการโจมตีที่พบมากในปัจจุบัน

1. Malware
2. Phishing
3. SQL Injection Attack
4. Cross-Site Scripting (XSS)
5. Denial of Service (DoS)
6. Session Hijacking and Man-in-the-Middle Attacks
7. Credential Reuse

Malware

ภัยคุกคามรุ่นบุกเบิก Malware หากคุณเคยเห็นการแจ้งเตือนไวรัสที่มักปรากฏขึ้นเป็นหน้าจอของคุณ หรือในโปรแกรม Anti-Virus ขั้นพื้นฐานเมื่อเกิดความผิดปกติ หรือมีไวรัสปลอมแปลงเข้ามาในคอมพิวเตอร์ของคุณ ซึ่งมักแฝงตัวมากับไฟล์ที่ดาวน์โหลด อีเมล์ หรือแม้แต่การเชื่อมต่อของอุปกรณ์เสริมต่างๆ

“มัลแวร์” หมายถึงการรูปแบบหนึ่งของซอฟต์แวร์ ที่เป็นอันตรายต่อผู้ที่ได้รับ เช่น ไวรัส และ ransomware หากมีมัลแวร์อยู่ในคอมพิวเตอร์แล้วก็จะสามารถสร้างความเสียหายได้มากเลยทีเดียว ไม่ว่าจะเป็นการทำลายข้อมูล หรือแม้แต่การเข้าควบคุมระบบของคุณ ตัวอย่างที่ระบาดหนักก็คือ WannaCry ที่สร้างความเสียหายให้กับองค์กรทั้งในสหรัฐอเมริกา สหราชอาณาจักร จีน รัสเซีย สเปน อิตาลี และไต้หวัน โดยมีการเปิดเผยข้อมูลจากบริษัท Avast ซึ่งเชี่ยวชาญด้านความปลอดภัยทางไซเบอร์รายงานว่า พบกรณีการโจมตีด้วยมัลแวร์นี้ถึง 75,000 ครั้งทั่วโลกเลยทีเดียว

โดยวิธีพื้นฐานที่ “มัลแวร์” จะทำงานก็คือการแฝงตัวเข้ามาในรูปแบบต่างๆ เพื่อให้ผู้ใช้ดำเนินการเพื่อติดตั้งมัลแวร์ และ “วิธีที่นิยมมากที่สุดก็คือการแฝงระบบติดตั้งเข้ามาในลิงก์เพื่อดาวน์โหลดไฟล์หรือเปิดไฟล์แนบ (เช่นไฟล์เอกสาร Word หรือไฟล์ PDF)”

Phishing

แน่นอนว่า “ภัยคุกคาม” จะไม่มีวันเกิดขึ้นกับคุณแน่นอนหากไม่เปิดไฟล์หรือข้อมูลที่เป็นความเสี่ยงทั้งหลาย ! ซึ่งเหล่าอาชญากรไซเบอร์ก็เข้าใจประเด็นนี้เป็นอย่างดี จึงต้องมีระบบการ “Phishing” เพื่อสร้างแรงจูงใจในการเปิดไฟล์[ที่มีมัลแวร์อันตรายแนบไว้] และเมื่อเหยื่อหลงเชื่อและทำงานเปิดไฟล์เหล่านั้น “มัลแวร์” ก็จะถูกติดตั้งและพร้อมโจมตีคอมพิวเตอร์ของคุณได้ทันที

ในรูปแบบการโจมตีนี้ “ผู้โจมตีอาจจะแสร้งส่งอีเมล์จากบุคคลที่สามารถไว้วางใจและสั่งการได้ เช่น ผู้บริหาร หรือองค์ที่น่าเชื่อถือของภาครัฐ” พร้อมแนบไฟล์ที่แฝงด้วยมัลแวร์ [ตัวอย่างเช่น รายละเอียดในอีเมล์จะทำงานแจ้งคุณว่า “มีการตรวจพบการฉ้อโกงในบัญชีของคุณ แนะนำให้คุณกรอกข้อมูลหรือเปิดไฟล์นี้เพื่อแสดงความบริสุทธิ์ใจ”] ซึ่งแน่นอนว่าสิ่งเหล่านี้ล้วนเป็นกับดัก เพื่อหลอกล่อให้คุณคลิกติดตั้งมัลแวร์นั่นเอง

SQL Injection Attack

SQL หมายถึงภาษาที่มีโครงสร้างที่เขียนด้วยภาษาของโปรแกรมที่ใช้สื่อสารกับฐานข้อมูลภายในเซิร์ฟเวอร์ และระบบ SQL นี้ถูกใช้เพื่อจัดการฐานข้อมูลของตนเอง ทำให้เมื่ออาชญาการไซเบอร์เปิดการโจมตีไปที่ SQL ก็จะส่งผลกระทบต่อระบบเซิร์ฟเวอร์โดยตรง

และการโจมตีในลักษณะนี้จะเป็นการสร้างปัญหาใหญ่ให้กับองค์กรได้มากมาย เนื่องจากภายในเซิร์ฟเวอร์ของแต่ละองค์กรมักจะรวบรวม “ข้อมูลของลูกค้า” “ข้อมูลส่วนบุคคล” “หมายเลขบัตรเครดิตและระบบการเงิน” อีกทั้งการโจมตีในลักษณะนี้จะสามารถเปิดช่องโหว่บนเซิร์ฟเวอร์ SQL ซึ่งสามารถสร้างปัญหาได้ในระยะยาวเลยทีเดียวหากไม่มีการแก้ไขที่ทันท่วงที

Cross-Site Scripting [XSS]

การโจมตีในลักษณะ SQL ผู้โจมตีจะทำการโจมตีผ่านเว็บไซต์และเซิร์ฟเวอร์ที่มีช่องโหว่ เพื่อคุกคามฐานข้อมูลสำคัญต่างๆ โดยเฉพาะข้อมูลด้านการเงิน แต่ถ้าผู้โจมตีมีจุดมุ่งหมายใน “การโจมตีคนที่เข้ามาใช้บริการเว็บไซต์” พวกเขาจะเลือกใช้การโจมตีแบบ XSS ซึ่งทำงานผ่านการเขียนสคริปต์ข้ามไซต์ โดยจะทำงานคล้ายคลึงกับการโจมตีแบบ SQL แต่จะแตกต่างกันที่ XSS จะไม่สร้างความเสียหายให้กับเว็บไซต์ที่เผยแพร่ข้อมูล

“สรุปได้ว่า เป้าหมายการโจมตีแบบ XSS จะโจมตีไปที่ผู้ใช้งานเว็บไซต์เท่านั้น ส่วนการโจมตีแบบ SQL จะเป็นการโจมตีที่ตัวเว็บไซต์และเซิร์ฟเวอร์” วิธีที่เหล่าผู้โจมตีเลือกใช้กันบ่อยที่สุดก็คือ “การใส่โค้ดที่เป็นอันตรายลงในช่องที่ผู้ใช้งานเว็บไซต์จะต้องเปิด หรือการฝังลิงค์ไปยัง JavaScript ภายในเว็บไซต์” ถึงแม้ว่าการโจมตีแบบ XSS จะไม่สร้างความเสียหายให้กับเว็บไซต์ แต่อย่างไรก็ตาม XSS จะสร้างความเสียหายให้กับ “ชื่อเสียงของเว็บไซต์เป็นอย่างมากเลยทีเดียว”

Denial of Service [DoS]

ลองจินตนาการว่า “ถนนหนึ่งเส้นที่ออกแบบขนาดมาให้เพียงพอต่อจำนวนรถที่วิ่งในทุกวัน แต่ถ้าวันหนึ่งจำนวนรถมากขึ้นกะทันหันย่อมสร้างปัญหาจราจรติดขัดให้เกิดขึ้นอย่างแน่นอน” ในทางเดียวกันหากเว็บไซต์ของคุณที่เคยรองรับจำนวนผู้ใช้งานได้ในจำนวนปกติ หากมีการเข้าใช้งานเยอะจนเกินไปก็จะทำให้เซิร์ฟเวอร์ของคุณเสียหายได้

“การโจมตีในลักษณะนี้คือการโจมตีแบบ DoS [Denial of Service] นั่นเอง” บ่อยครั้งที่เกิดเหตุการณ์เช่นนี้ขึ้น แต่ก็มักมีเหตุผลที่อ้างกันว่ามีผู้เข้าใช้บริการเว็บจนเยอะเกินไป แต่ในบางครั้งอาจจะเป็นอันตรายจากการคุกคามของ Dos ก็เป็นได้ที่ทำให้เกิดความผิดปกติของเซิร์ฟเวอร์

การโจมตีแบบ Dos หากเกิดขึ้นกับระบบคอมพิวเตอร์หลายๆส่วนพร้อมกันจะถูกเรียกว่า DDoS หรือ Distributed Denial of Service Attack ซึ่งการโจมตีในลักษณะอาจจะแก้ปัญหาได้ยากมากเลยทีเดียว เนื่องจากผู้โจมตีมี IP ที่หลากหลายจากทั่วโลกในการเข้ามาสร้างความหนาแน่นของ Traffic บนเซิร์ฟเวอร์

Session Hijacking and Man-in-the-Middle Attacks

ทุกครั้งที่คุณใช้งานอินเตอร์เน็ต ระบบคอมพิวเตอร์ของคุณจะทำการแจ้งไปยังเซิร์ฟเวอร์เพื่อยืนยันว่าคุณคือใคร และต้องการขอเข้าเว็บไซต์หรือธุรกรรมใดๆ บนอินเตอร์เน็ต ซึ่งในขณะเดียวกัน กระบวนการนี้หรือเซสชันนี้จะทำการเรียกดูข้อความของคอมพิวเตอร์ของคุณไม่ว่าจะเป็นเครือข่าย IP และรหัสผ่าน ซึ่งในกระบวนการนี้เซสชันระหว่างคอมพิวเตอร์และเว็บเซิร์ฟเวอร์ระยะไกลจะได้รับรหัสเซสชันที่ไม่ซ้ำกัน เพื่อการรักษาข้อมูลส่วนตัวเอวไว้ อย่างไรก็ตาม ในระหว่างกระบวนนี้ผู้บุกรุกจะสามารถโจมตีเซสชันได้ด้วยการจับรหัสเซสชัน และวางตัวเองคอมพิวเตอร์เครื่องที่ร้องขอการใช้งานเสียเอง ซึ่งแน่นอนว่าการโจมตีในลักษณะนี้จะสามารถดักจับและสกัดข้อมูลได้อย่างทั้งสองทิศทางเลยทีเดียว

Credential Reuse

ในทุกวันนี้การเข้าใช้ระบบต่างๆ จะมีการตั้งการเข้าสู่ระบบและรหัสผ่าน ซึ่งจะช่วยสร้างความภัยได้ในระดับหนึ่ง แต่อย่างไรก็ตามการรักษาความปลอดภัยที่ดีที่สุดในระดับสากลก็คือ “คุณจะต้องมีรหัสผ่านที่ไม่ซ้ำกันสำหรับแอปพลิเคชันเว็บไซต์ และการเข้าระบบทั้งหมดของคุณ”
ซึ่งหากคุณตั้งค่ารหัสผ่านไว้ในแบบเดียวกัน หากคุณโดนขโมยข้อมูลไปเพียงส่วนหนึ่ง ความเสียหายจะครอบคลุมไปได้ในหลายๆส่วนเลยทีเดียว บัญชีหลายๆบัญชีก็จะสามารถถูกแฮ็กเข้าได้อย่างง่ายดาย

Ref: https://monsterconnect.co.th/7-common-types-of-cybersecurity-attacks/

TYPES OF CYBER-ATTACKS

PHISHING

- Whale Phishing
- Spear Attack
- Pharming

MAN-IN-THE-MIDDLE ATTACK

- Session Hijacking
- IP Spoofing
- Replay

SQL INJECTION THREAT

DISTRIBUTED DENIAL OF SERVICE ATTACK (DDOS)

CROSS-SITE SCRIPTING (XSS)

PASSWORD ATTACK

- Brute Force Guessing
- Dictionary Attack

AI-POWERED ATTACKS

DRIVE-BY ATTACK

RANSOMWARE ATTACK

EAVESDROPPING ATTACK