สรุปเหตุการณ์ IT Supply Chain: Microsoft และ CrowdStrike

เผยแพร่วันที่ 20 กรกฎาคม 2567
ปรับปรุงล่าสุดวันที่ 20 กรกฎาคม 2567

ช่วงเวลาประมาณ 14:30น. ของวันที่ 19 กรกฎาคม 2567 ตามเวลาในประเทศไทย จากข่าวการเกิดเหตุการณ์ระบบไอทีหยุดชะงักซึ่งทำให้บริการของสายการบิน โรงพยาบาล ธนาคาร บริษัทสื่อ ฯลฯ ทั่วโลก ไม่สามารถให้บริการได้ซึ่งเป็นเวลาเดียวกันกับที่พบปัญหาหน้าจอของระบบปฏิบัติการ Microsoft Windows แสดงหน้าจอสีฟ้า (Blue Screen) มีผลทำให้เครื่องเหล่านั้นหยุดการทำงาน ซึ่งเกิดขึ้นพร้อมกันหลายเครื่องทั่วทั้งโลกนั้นเป็นเหตุการณ์สองเหตุการณ์ที่สร้างผลกระทบในวงกว้างมาก จึงควรจะต้องวิเคราะห์แยกแยะสาเหตุ และแนวทางในการจัดการปัญหา แม้ว่าสองเหตุการณ์ที่เกิดขึ้นนี้ไม่ใช่เหตุการณ์ที่เกิดการโจมตีทางไซเบอร์ แต่เป็นปัญหาในประเภท IT Supply Chain ที่ทุกหน่วยงานจะต้องให้ความสำคัญอย่างมาก

เหตุการณ์ที่ 1 Microsoft Azure Outage

Microsoft Azure ซึ่งเป็นแพล็ตฟอร์มประมวลผลในรูปแบบคลาวด์ (Cloud Platform) ที่ถือว่ามีผู้ใช้งานเป็นจำนวนมากทั่วโลกเกิดเหตุการณ์หยุดชะงักทำให้ในเวลาช่วงเช้าประมาณ 07:00 น. ของวันที่ 19 กรกฎาคม 2567 (เวลาประเทศไทย) ลูกค้าของ Microsoft Azure ที่ใช้บริการ ในแถบสหรัฐอเมริกากลาง (Central US region) ในเมืองไอโอวา ใช้บริการ Microsoft 365 หลายบริการไม่ได้ เช่น Office 365 ,SharePoint Online, OneDrive for Business, Teams, Intune, PowerBI, Microsoft Fabric, Microsoft Defender, และ Viva Engage

โดยบริษัท Microsoft อธิบายถึงสาเหตุของปัญหาที่เกิดขึ้นที่ทำให้บริการหยุดทำงานกว่า 5 ชั่วโมงนั้น เกิดจากการปรับค่า configuration ที่ผิดพลาด ทำให้การเชื่อมต่อระหว่างหน่วยประมวลผลและ Storage cluster* ขัดข้อง ส่งผลให้การบริการ Microsoft Azure ในแถบสหรัฐอเมริกากลาง (Central US region) ไม่สามารถใช้งานได้

*Storage Cluster คือ การจัดเก็บข้อมูลบนเครื่องคอมพิวเตอร์หลายเครื่องที่เชื่อมโยงกันเป็นกลุ่ม เพื่อช่วยกระจายการจัดเก็บข้อมูลและการเรียกใช้งานข้อมูล

ข้อแนะนำสำหรับการเตรียมพร้อมในการใช้งาน Cloud Service

1. สำหรับบริการที่สำคัญควรใช้งาน Cloud Service แบบ Multiple regions
2. มีการพัฒนาและกำหนดแผนสำรองสำหรับการรับมือกรณีที่ Cloud Service Provider ไม่สามารถให้บริการได้ รวมทั้งกำหนดให้มีการซักซ้อมแผนสำรองอย่างสม่ำเสมอ
3. ปรับปรุงข้อมูลที่ใช้ในการประสานงานกับ Cloud Service Provider ให้เป็นปัจจุบันเสมอ เช่น รายชื่อผู้ติดต่อและช่องทางในการติดต่อ

เหตุการณ์ที่ 2 Blue Screen of Death (BSOD) จากการ update ของ CrowdStrike Falcon software

บริษัท CrowdStrike เป็นบริษัทสัญชาติอเมริกัน ผู้ให้บริการเทคโนโลยีความปลอดภัยทางไซเบอร์ด้วยโปรแกรมป้องกันไวรัสหรือมัลแวร์ให้กับอุปกรณ์ของผู้ใช้งาน (Endpoint Device) เช่น คอมพิวเตอร์ แท็บเล็ต บริษัท CrowdStrike มีผลิตภัณฑ์ที่ชื่อว่า CrowdStrike Falcon ซึ่งเป็นผลิตภัณฑ์ที่รวมหลายโซลูชั่นความปลอดภัยไว้ด้วยกัน หนึ่งในนั้นคือระบบ Endpoint Detection Response หรือที่เรียกว่า EDR โดยทำหน้าที่ในการป้องกันมัลแวร์และการโจมตีทางไซเบอร์ ระบบ EDR เป็นที่นิยมใช้งานอย่างแพร่หลายในปัจจุบัน และถูกใช้อย่างแพร่หลายในธุรกิจจำนวนมากทั่วโลก เพื่อจัดการความปลอดภัยของคอมพิวเตอร์และเซิร์ฟเวอร์ โดยสามารถใช้ได้ในหลายระบบปฏิบัติการ ไม่ว่าจะ Windows, macOS, และ Linux

โดยปกติแล้ว CrowdStrike จะมีการทดสอบ Software ก่อนที่จะทำการ update ไฟล์ Configuration หรือที่เรียกว่า Channel Files แบบอัตโนมัติไปที่ Crowd Strike Falcon sensor ของระบบ EDR ที่ติดตั้งอยู่บนเครื่องของผู้ใช้งาน (Endpoint Device) โดยไฟล์ Configuration ดังกล่าวจะเป็นส่วนหนึ่งฟังก์ชันในการตรวจจบพฤติกรรมที่ผิดปกติของมัลแวร์ (Behavioral based malware protection)

แต่ช่วงเช้าของวันที่ 19 กรกฎาคม 2567 (เวลาประเทศไทย) เกิดเหตุการณ์คอมพิวเตอร์ที่ใช้ระบบปฏิบัติการ Windows และบนเครื่องติดตั้ง CrowdStrike เจอปัญหาหน้าจอฟ้าและหยุดการทำงาน (Blue Screen of Death : BSOD) ในหลายองค์กร โดยสาเหตุมาจากไฟล์ Configuration ที่ทาง CrowdStrike ได้ update มีข้อผิดพลาดทางตรรกะการทำงาน (Logic error) ทำให้ระบบปฏิบัติการ Windows หยุดทำงาน ส่งผลให้ไม่สามารถเรียกใช้งานระบบ (Boot System) ได้ตามปกติ ระบบปฏิบัติการWindows จึงแสดงหน้าจอฟ้าซึ่งแสดงถึงปัญหาที่ฮาร์ดแวร์หรือซอฟท์แวร์ที่ทำงานร่วมกับระบบปฏิบัติการ Windows ไม่ใช่เหตุการณ์ที่เกิดจากการโจมตีทางไซเบอร์

ระบบปฏิบัติการที่ได้รับผลกระทบ: ระบบปฏิบัติการ Windows ทุกรุ่น ยกเว้น Windows 7/2008 R2

แนวทางการดำเนินการแก้ไขปัญหาแบบ Workaround

โดยในปัจจุบันทาง CrowdStrike ได้ประกาศแนวทางการแก้ไขเบื้องต้นออกมาและ และทาง TB-CERT ได้มีข้อแนะนำเพิ่มในการแก้ไขแบบ Workaround ดังต่อไปนี้

1. ทำการ Boot เข้า Windows แบบ Safe Mode หรือเรียกว่า Windows Recovery Environment แล้ว ไปที่โฟลเดอร์ C:\Windows\System32\drivers\CrowdStrike และหาไฟล์ที่เป็นรูปแบบ "C-00000291*.sys" (คือขึ้นต้นด้วย C-00000291 แล้วตรง * คือเป็นตัวอะไรก็ได้ จบท้ายด้วย .sys) แล้วลบให้หมด เมื่อลบแล้วสามารถบูทเครื่องขึ้นมาใหม่ใช้งานได้ปกติ

2. ในปัจจุบันทาง CrowdStrike ได้แก้ไขปัญหา (Fixed issue) ของ file C-00000291*.sys เป็นเวอร์ชั่นใหม่เรียบร้อยแล้ว หากกรณีเครื่องที่ update และมีปัญหาก่อนหน้านี้ จะต้องไป delete file C-00000291*.sys อกจาก C:\windows\system32\drivers\crowdstrike\ ก่อนจึงสามารถ Update ได้ตามปกติ

3. หากยังพบปัญหาให้ทำการ Roll back ไปใช้ snapshot ก่อนเวลาเกิดเหตุการณ์คือเวลา 04:09 (UTC)

4. ควรติดตามการประกาศการแก้ไขจาก CrowdStrike อย่างใกล้ชิด

ข้อควรระวัง

1. ติดตามข่าวจากแหล่งที่เชื่อถือได้ โดยเฉพาะการ download program เพื่อแก้ไขปัญหา เพื่อป้องกันการสวมรอยโจมตีด้วย Phishing หรือหลอกให้ลงโปรแกรมมัลแวร์ในองค์กร

2. ติดตามข่าวสารข้อมูลจาก TB-CERT ในเหตุการณ์ดังกล่าวเพื่อได้รับข้อมูลสถานการณ์เพิ่มเติม

3. หากพบสัญญาณการโจมตีใดๆ จากเหตุการณ์ให้รีบแจ้งให้ TB-CERT ทราบเพื่อใช้วิเคราะห์การโจมตีในภาพรวม และแบ่งปันสัญญาณการโจมตีให้หน่วยงานสมาชิกรับทราบเพื่อใช้งานการป้องกัน ช่องทางในการแจ้ง TB-CERT ผ่านทางอีเมล incident@tb-cert.or.th

สรุปแนวทางป้องกันความเสี่ยงจาก IT Supply Chain

เหตุการณ์ 2 เหตุการณ์นี้แม้ว่าไม่มีหลักฐานยืนยันว่าเกี่ยวข้องกัน แต่ทั้ง 2 เหตุการณ์นี้ส่งผลกระทบทั่วโลก ซึ่งถือว่าเป็นเหตุการณ์ IT ประเภท IT Supply Chain ที่รุนแรงมาก หลายหน่วยงานใช้งานไม่ได้ ก็ส่งผลต่อไปยังการให้บริการต่าง ๆ ของหน่วยงานนั้น และโยงต่อกันไปเรื่อย ๆ เป็นเหมือนกับ Ripple effect ที่เหตุการณ์นั้นเกิดจากจุดเล็ก ๆ แต่ส่งผลกระจายต่อเป็นวงกว้าง

แนวทางการเตรียมความพร้อมสำหรับการใช้บริการจากผู้ให้บริการภายนอกมีดังนี้

1. การประเมินความเสี่ยงของผู้ให้บริการกับความสำคัญของบริการ (Risk assessment and management) เช่น สูง กลาง ต่ำ เพื่อกำหนดการจัดลำดับความสำคัญของบริการ
2. การใช้บริการจากหลายผู้ให้บริการหรือใช้หลาย Region (Diversify)
3. การมีความสัมพันธ์ที่ดีกับผู้ให้บริการ (Supplier relationship)
4. ควรใช้เทคโนโลยีในการตรวจสอบสถานะการให้บริการแบบ real time (Supply chain visibility)
5. การเตรียมแผนฉุกเฉิน (Contingency planning) กำหนดแผนฉุกเฉินให้สอดคล้องกับระดับความเสี่ยง โดยคำนึงถึงเหตุการณ์ที่อาจเกิดผลกระทบเป็นวงกว้าง เช่น มีระบบสำคัญล่มพร้อม ๆ กัน และไม่สามารถ remote ทำงานเพื่อเข้าแก้ไขปัญหาได้ และเหตุการณ์ที่ต้องมีการกู้คืนระบบที่อยู่ต่างที่
6. การปฏิบัติตามกฎหมาย ข้อกำหนด และ ด้านความมั่นคงปลอดภัย (Compliance and Security)

ข้อมูลอ้างอิง

1. https://www.crowdstrike.com/blog/statement-on-windows-sensor-update/
2. https://www.hindustantimes.com/business/microsoft-cloud-outage-grounds-flights-and-disrupts-airlines-in-us-what-we-know-101721371273020.html
3. https://www.datacenterdynamics.com/en/news/microsoft-azure-outage-grounds-flights-delays-trains-impacts-banks-around-the-world/
4. https://www.theregister.com/2024/07/19/microsoft_365_azure_outage_central_us/