ความปลอดภัยทางไซเบอร์ที่ไม่ใช่เรื่องไกลตัว

วันที่ 2 กุมภาพันธ์ 2026 เขียนโดยคุณอิชิคาวะ แผนกธุรการ

เมื่อปีที่ผ่านมา

ข่าวด้านไซเบอร์ซีเคียวริตี้ที่ถูกนำเสนอผ่านโทรทัศน์และหนังสือพิมพ์อย่างครึกโครมคงหนีไม่พ้นกรณีที่บริษัทเครื่องดื่มรายใหญ่และบริษัทจำหน่ายอุปกรณ์สำนักงานออนไลน์ตกเป็นเหยื่อแรนซัมแวร์ จนไม่สามารถจัดส่งสินค้าได้
สร้างความเสียหายอย่างหนัก อย่างไรก็ตาม
ยังมีความเสียหายอีกจำนวนมากที่ไม่ได้ถูกนำเสนอผ่านสื่อทำให้เรื่องความปลอดภัยทางไซเบอร์ไม่ใช่เรื่องของคนอื่นอีกต่อไปครับ

จำนวนคดีความเสียหายที่เกิดกับนิติบุคคลและองค์กร เฉพาะครึ่งแรกของปี 2025 มีถึง 116 กรณี เลยครับ
(ประกาศโดยสำนักงานตำรวจนครบาลญี่ปุ่น)

ทำไมจำนวนคดีจึงมากขนาดนี้? คำตอบคือ “เรียกค่าไถ่แล้วได้เงิน”
นี่คือแรงจูงใจของอาชญากรครับ และฝั่งอาชญากรก็ไม่ใช่มือสมัครเล่น
แต่เป็นกลุ่มมืออาชีพที่มีทักษะและความรู้ด้าน IT ในระดับที่แตกต่างกันอย่างสิ้นเชิง
เมื่อถูกเล็งเป้าแล้ว

บริษัทขนาดกลางและขนาดเล็กอย่างพวกเราก็ไม่ต่างจากการเอาไม้ไผ่มาสู้กับขีปนาวุธแทบไม่มีทางป้องกันได้เลย

แล้วถ้ามีแบ็กอัพจะปลอดภัยหรือไม่!?

คำตอบคือ ไม่เสมอไป จากการสำรวจพบว่า 60% ของบริษัทที่ได้รับความเสียหาย ไม่สามารถกู้คืนข้อมูลได้
แม้จะมีแบ็กอัพอยู่ก็ตามอาชญากรในปัจจุบันจะไม่ทำให้แรนซัมแวร์แสดงอาการทันที
แต่จะปล่อยให้แฝงตัวอยู่เป็นระยะเวลาหนึ่ง ดังนั้นแบ็กอัพที่ทำในช่วงนั้น ก็อาจติดไวรัสไปแล้วและไม่สามารถใช้งานได้

แล้วถ้าใช้แบ็กอัพก่อนติดเชื้อล่ะ? ปัญหาคือ แบ็กอัพต้องใช้พื้นที่จัดเก็บจำนวนมาก ยิ่งข้อมูลมาก
ค่าใช้จ่ายในการจัดเก็บก็ยิ่งสูงจึงมีข้อจำกัดด้านระยะเวลาในการเก็บรักษาแบ็กอัพ

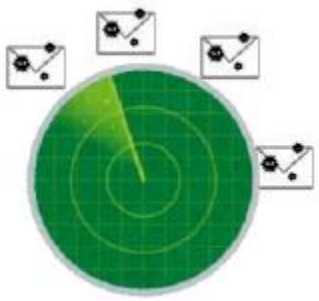
นอกจากนี้ หากกู้ข้อมูลจากแบ็กอัพที่เก่ามาก ข้อมูลในช่วงเวลานั้นจะหายไป ซึ่งยากต่อการนำกลับมาใช้งานในทันที

หากตกเป็นเหยื่อแรนซัมแวร์จะเกิดอะไรขึ้น ?

เหตุการณ์จะเกิดขึ้นอย่างกะทันหัน แม้ความเสียหายที่ปรากฏภายนอกจะเป็นเพียงส่วนหนึ่ง
แต่จนกว่าจะพิสูจน์ได้ว่าไม่มีการติดไวรัส

คอมพิวเตอร์ทุกเครื่องจะถูกห้ามใช้งานอย่างน้อย 1–2 สัปดาห์ และอาจยาวนานเป็นเดือน
ไม่เพียงแต่คอมพิวเตอร์สำนักงาน แม้แต่คอมพิวเตอร์ที่ควบคุมเครื่องจักรและอุปกรณ์ต่าง ๆ
ก็อาจไม่สามารถใช้งานได้เช่นกัน เราจะต้องย้อนกลับไปใช้ยุคกระดาษ โทรศัพท์ และแฟกซ์ สำหรับผู้ที่ไม่เคยผ่านยุคนั้นมา
คงต้องตั้งคำถามว่า “จะทำอย่างไรดี?” หากสถานการณ์ยืดเยื้ออาจต้องใช้เวลาหลายเดือนกว่าจะฟื้นฟูได้
ไม่สามารถผลิตสินค้า ไม่สามารถจัดส่ง ไม่เพียงเท่านั้น ระบบลงเวลาทำงาน การคำนวณเงินเดือน และการโอนเงินเดือน
ล้วนพึ่งพาคอมพิวเตอร์ทั้งหมด ย่อมส่งผลกระทบต่อเงินเดือนของทุกคนอย่างแน่นอนครับ

มาตรการป้องกัน — เริ่มจากไม่ให้ตกเป็นเป้าหมาย !



อีเมลฟิชชิ่งหรืออีเมลขยะ เปรียบเสมือนเซนเซอร์ของอาชญากร หากเปิดอีเมล คลิกลิงก์
หรือเปิดไฟล์แนบ อาชญากรจะรู้ทันทีว่า ใคร ที่ไหน และเมื่อใด จากนั้นพวกเขาจะคิดว่า
“บริษัทนี้ระบบความปลอดภัยอ่อนแอแน่” และเริ่มเล็งเป้า ไม่ใช่แค่บริษัทเท่านั้น
อีเมลส่วนบุคคลก็มีความเสี่ยงเช่นเดียวกันครับ

ปัจจุบันอาชญากร**ใช้ AI** เพื่อสร้างกับดักที่แนบเนียนยิ่งขึ้น ทำให้อุปสรรคด้านภาษาอย่าง
“ภาษาญี่ปุ่น” แทบหมดไป ทำให้ตกเป็นเป้าได้ง่ายขึ้น และหลงกลได้ง่ายขึ้น
ต้องระมัดระวังอย่างยิ่งครับ !

ตัวอย่างเช่น

อดีต (ภาษาญี่ปุ่นผิดธรรมชาติ)	ปัจจุบัน (ภาษาญี่ปุ่นถูกต้อง)
คุณสามารถเปิดไฟล์แนบได้	กรุณาตรวจสอบไฟล์แนบ

ระวังอีเมลที่สร้างความกังวล เร่งด่วน หรือดูน่าดึงดูดเกินจริง

ตัวอย่างเช่น “บัตรเครดิตของคุณถูกใช้งานโดยมิชอบ”, ”ไม่สามารถยืนยันการชำระเงินได้”, “พบการเข้าสู่ระบบจากสถานที่อื่น”, “บัญชีถูกระงับการใช้งาน”, “พัสดุถูกจัดส่งแต่ไม่มีผู้รับ”, “[ชื่อบริษัท] กรุณาติดต่อโดยด่วน”, “คุณได้รับรางวัล”, “มีค่าล่วงเวลาที่ยังไม่ได้รับการชำระ” เป็นต้น แม้อีเมลจะอ้างชื่อบริษัทใหญ่ คู่ค้า หรือบริษัทที่คุ้นเคย ขอให้ตั้งสติและตรวจสอบให้รอบคอบครับ

การยืนยันตัวตนสองขั้นตอน ก็ไม่ปลอดภัยเสมอไป

หากคลิกลิงก์ในอีเมลและถูกนำไปยังเว็บไซต์ปลอมของอาชญากร แม้จะกรอก ID รหัสผ่าน และรหัสยืนยันครบทุกขั้นตอน ระบบยืนยันตัวตนสองขั้นตอนก็ไร้ความหมาย โปรดใช้ความระมัดระวังอย่างที่สุด ก่อนคลิกลิงก์ในอีเมลและตรวจสอบ URL ปลายทางทุกครั้ง ！

ติดตามข่าวจากโทรทัศน์และหนังสือพิมพ์

มีข้อมูลที่ระบุว่าคนรุ่นใหม่กลับตกเป็นเหยื่อฟิชชิ่งได้มากกว่า
สิ่งที่กล่าวมาทั้งหมดมีการรายงานผ่านข่าวโทรทัศน์และหนังสือพิมพ์อยู่เสมอครับ
อย่ารับข่าวสารเฉพาะจาก YouTube หรือ SNS แต่ควรรับฟังข่าวจากสื่อกระแสหลัก แม้จะไม่ใช่เรื่องที่สนใจก็ตามครับ นี่คือการป้องกันตัวเองที่สำคัญนะครับ