ครั้งที่56 1/2567

3.1 กิจการทำธุรกิจโดยใช้ระบบออนไลน์ มีภัยคุกคามทาง cyber security จาก ransomware ให้ระบุการควบคุมทั่วไป 6 ข้อ อย่างละเอียดว่าจะตอบสนองต่อภัยคุกคาม ransomware อย่างไร (12 p)

3.2 ให้ท่านระบุ ก.วิธีการควบคุมทางกายภาพศูนย์คอม 2 ข้อ (4p)และ ข.วิธีการควบคุมสภาวะแวดล้อม 2 ข้อ(4p)

แนวคำตอบ

Ransomware คือ มัลแวร์ประเภทหนึ่ง ซึ่งวิธีการทำงานไม่ได้ออกแบบมาเพื่อขโมยข้อมูล แต่จะทำการเข้ารหัสหรือบล็อกการเข้าถึงไฟล์ทุกชนิดบนคอมพิวเตอร์ ทำให้ผู้ใช้งานไม่สามารถเปิดไฟล์ในเครื่องได้

3.1 การควบคุมทั่วไปเกี่ยวกับภัยคุกคามทาง cyber security จาก ransomware

1. **ติดตั้ง Firewall** ธุรกิจมีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์ได้ง่าย ต้องเสริมเกาะป้องกันความปลอดภัยโดยติดตั้ง Firewall ซอฟต์แวร์หรือฮาร์ดแวร์บนเครือข่าย ที่ทำหน้าที่ช่วยตรวจสอบข้อมูลของพนักงานที่ผ่านเข้า-ออกจากระบบเครือข่าย เพื่อเป็นการป้องกันHacker เข้ามาระบบเครือข่ายและระบบข้อมูลของกิจการ

2. **การสร้างความเข้าใจ และจิตสำนึกด้านความมั่นคงปลอดภัยระบบสารสนเทศให้ความรู้กับพนักงานทุกคนในองค์กรอย่างต่อเนื่อง และสม่ำเสมอ(Security Awareness Training)** เรื่องความปลอดภัยทางด้านข้อมูลนั้นสำคัญกับทั้งตัวบริษัทและพนักงานทุกคน ดังนั้นสิ่งที่จำเป็นมากที่สุดคือวางแนวทางการป้องกันความปลอดภัยบนโลกไซเบอร์ ด้วยการฝึกอบรม การสร้างความเข้าใจ และจิตสำนึกด้านความปลอดภัยระบบสารสนเทศให้กับพนักงานได้รับความรู้ทางด้านไอที เช่น ใช้อีเมลอย่างไรให้ปลอดภัย รวมถึงการใช้งานผ่านเว็บเบราว์เซอร์ ติดตามupdate ข้อมูลข่าวสารเกี่ยวกับMalware และการHack รูปแบบใหม่ๆ เพื่อป้องกันภัยคุกคามทางคอมพิวเตอร์

3. **กำหนดนโยบายการรักษาความปลอดภัยระบบสารสนเทศ (Security Policy)** ได้แก่นโยบายควบคุมการใช้ Password ธุรกิจต้องกำหนดให้พนักงานในองค์กรตั้งรหัสผ่านที่ปลอดภัยบนอุปกรณ์ที่เข้าถึงเครือข่ายขององค์กรได้โดยการตั้งรหัสผ่านที่เหมาะสมและปลอดภัย ไม่ควรที่จะใช้ตัวเลขหรือตัวอักษรที่คาดเดาได้ง่าย เช่น ตั้งตามเลขวันเกิด เลขซ้ำ เลขเรียงตามจำนวน ควรตั้งรหัสให้คาดเดาได้ยาก และควรตั้งตัวอักษรพิมพ์ใหญ่ พิมพ์เล็ก ตัวเลข และอักขระพิเศษ มาผสมผสานกันตั้งแต่ 10-12 ตัวขึ้นไป เพื่อเพิ่มความยากและป้องกันการใช้โปรแกรมคาดเดาของแฮกเกอร์

4. **การสำรองข้อมูล และการนำข้อมูลสำรองกลับมาใช้ใหม่ (Backup & Recovery)** โดยจัดเก็บข้อมูลสำรองไว้ในที่ปลอดภัยทั้งภายในและนอกสถานที่มากกว่า 1 แห่ง รวมทั้งมีการทดสอบแผ่นสำรองข้อมูล และทดสอบกู้ข้อมูลเป็นระยะ ปัจจุบันนิยมสำรองข้อมูล หรือฐานข้อมูลที่สำคัญต่าง ๆ ไว้บนระบบCloud เพื่อให้การสำรองข้อมูลมีประสิทธิภาพสูงสุดและมั่นใจว่าข้อมูลจะไม่สูญหาย เพราะการสำรองข้อมูลถือเป็นหนึ่งในการปฏิบัติงานด้านความมั่นคงปลอดภัยที่ทุกองค์กรพึงกระทำเป็นประจำ และสม่ำเสมอ โดยเฉพาะอย่างยิ่งในยุคปัจจุบันที่ Ransomware กำลังแพร่ระบาดไปทั่ว การสำรองข้อมูลช่วยให้องค์กรสามารถนำข้อมูลสำรองกลับมาใช้ใหม่ หลังจากถูกโจมตี

5. **ติดตั้งซอฟต์แวร์ป้องกัน มัลแวร์ (Anti-malware)** โดยทั่วไปพนักงานที่ได้รับเมลไม่สามารถดูออกว่าอีเมลไหนเป็นอีเมลหลอก การมีซอฟต์แวร์ป้องกันมัลแวร์ติดตั้งในทุกอุปกรณ์และเครือข่าย ก็จะช่วยเสริมความปลอดภัยมากยิ่งขึ้น Anti-malware จะช่วยscanว่าไฟล์ไหนมี Ransomwareติดมาด้วย

6. **กำหนดให้ยืนยันตัวตน(Authentication)** พนักงานทุกคนต้องพิสูจน์เป็นวิธีการเพิ่มความปลอดภัยในการเข้าใช้งานในระบบ โดยกำหนดให้ผู้ใช้ป้อนข้อมูลที่นอกเหนือจากรหัสผ่านแบบ 2 ชั้น ตัวอย่างเช่น ระบบอาจขอให้ผู้ใช้ป้อนรหัสที่ส่งไปยังอีเมล, SMS หรือ App Authentication ที่ใช้คู่กับการป้อนรหัสผ่าน รูปแบบที่เพิ่มขึ้นนี้มาจะช่วยป้องกันการเข้าถึงบัญชีโดยไม่ได้รับอนุญาตได้ในกรณีที่รหัสผ่านเกิดช่องโหว่

3.2 **ก. การควบคุมทางกายภาพห้องคอมพิวเตอร์**

1) การควบคุมการเข้าถึงทางกายภาพของระบบคอมพิวเตอร์และอุปกรณ์ต่าง ๆ เช่น จัดให้ห้องคอมพิวเตอร์อยู่ในสถานที่ที่เหมาะสม เช่น ไม่เป็นที่ที่พลุกพล่านด้วยผู้คนจำนวนมากและถ้าอยู่ในอาคาร ก็ไม่ควรอยู่ชั้นที่สูงหรือต่ำเกินไป

2) กำหนดให้เป็นพื้นที่รักษาความปลอดภัย (Securities Area) ห้ามผู้ที่ไม่เกี่ยวข้องเข้าห้องคอมพิวเตอร์

ข. การควบคุมด้านสภาวะแวดล้อมการทำงานของระบบคอมพิวเตอร์

1) จัดให้มีการติดตั้งและทดสอบอุปกรณ์ควบคุมสภาวะแวดล้อมของการทำงานของระบบคอมพิวเตอร์ในห้องคอมพิวเตอร์อย่างเพียงพอ เช่น มีการติดตั้งระบบปรับอุณหภูมิ ความชื้นและคลื่นแม่เหล็ก และอุปกรณ์ในการควบคุมความคงที่และจัดให้มีไฟฟ้าใช้อย่างต่อเนื่อง

2) ระบบปรับอากาศควรจะต่อเข้ากับระบบไฟฟ้าจากแหล่งเดียวกันกับระบบคอมพิวเตอร์ เพื่อทำให้มั่นใจว่าระบบปรับอากาศสามารถทำงานได้ในกรณีไฟฟ้าปกติขัดข้อง และระบบคอมพิวเตอร์จะต้องใช้ไฟฟ้าจากแหล่งไฟฟ้าสำรอง (UPS)

.....