**กรณีศึกษา การโจมตีทางไซเบอร์**

**สถานการณ์:**บริษัท B เป็นบริษัทให้บริการด้านการเงินออนไลน์ซึ่งใช้ระบบเครือข่ายในการจัดการธุรกรรมของลูกค้า วันหนึ่ง บริษัทได้รับแจ้งว่าระบบถูกโจมตีทางไซเบอร์ (Cyber Attack) โดยผู้โจมตีสามารถเข้าถึงข้อมูลที่มีความละเอียดอ่อนของลูกค้า เช่น ข้อมูลบัญชีธนาคาร และรหัสผ่าน โดยผ่านทางการโจมตีแบบ Phishing ที่หลอกพนักงานให้คลิกลิงก์ที่เป็นอันตราย ทำให้ระบบถูกเจาะและข้อมูลถูกขโมย

**คำถามที่ต้องการให้นักศึกษาตอบ:**

1. **การโจมตีไซเบอร์ในกรณีนี้เป็นรูปแบบใด? (เช่น Phishing, Malware, หรืออื่น ๆ)**

**ตอบ** การโจมตีนี้เป็นการโจมตีรูปแบบ Phishing

1. **บริษัท B ควรมีมาตรการใดบ้างในการป้องกันการโจมตีในอนาคต**

**ตอบ**

* ปรับระบบให้มีการยืนยันตัวตนหลายชั้น (MFA) เพื่อทำให้แฮกเกอร์จะได้ไม่สามารถเข้าถึงระบบได้ หากไม่มีการยืนยันขั้นเพิ่มเติม
* อัปเดตระบบอย่างสม่ำเสมอเพื่อลดช่องโหว่ทางเทคนิค
* ให้พนักงานเข้าถึงเฉพาะข้อมูลที่จำเป็นต้องใช้ในการทำงานเท่านั้น

1. **การฝึกอบรมพนักงานเกี่ยวกับความปลอดภัยไซเบอร์มีความสำคัญอย่างไรในกรณีนี้**

**ตอบ**

* พนักงานจะเข้าใจวิธีสังเกตและสามารถหลีกเลี่ยงลิงก์หรืออีเมล Phishing
* พนักงานจะรู้ขั้นตอนในการแจ้งและจัดการปัญหาอย่างมีประสิทธิภาพ

1. **หากคุณเป็นผู้จัดการความปลอดภัยไซเบอร์ของบริษัท B คุณจะดำเนินการอย่างไรในการรับมือกับเหตุการณ์นี้**

**ตอบ**

* ระงับการเข้าถึงระบบ เพื่อลดความเสียหายและป้องกันการขยายตัวของการโจมตี
* แจ้งเตือนลูกค้า ให้ลูกค้ารับทราบถึงเหตุการณ์เพื่อให้ลูกค้าดำเนินการป้องกันเพิ่มเติม เช่น เปลี่ยนรหัสผ่าน
* พัฒนาแนวทางป้องกันใหม่

1. **มาตรการทางกฎหมายใดบ้างที่สามารถนำมาใช้เพื่อคุ้มครองข้อมูลของลูกค้า และบริษัท B ควรทำอย่างไรให้เป็นไปตามกฎหมายเหล่านี้**

**ตอบ**

* พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA)
* บริษัทต้องได้รับความยินยอมจากลูกค้าในการเก็บและประมวลผลข้อมูล
* แจ้งเตือนลูกค้าเมื่อเกิดเหตุละเมิดข้อมูลส่วนบุคคลภายในระยะเวลาที่กำหนด
* พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
* รายงานความผิดที่เกี่ยวข้องกับการโจมตีทางไซเบอร์ไปยังเจ้าหน้าที่ตำรวจหรือหน่วยงานที่เกี่ยวข้อง
* ความร่วมมือกับเจ้าหน้าที่ ให้ข้อมูลและหลักฐานที่เกี่ยวข้องกับการโจมตี
* ปฏิบัติตามมาตรการรักษาความปลอดภัย