โดย นายสันติ พงค์เจริญพิทย์
อนุกรรมการควบคุมกำกับดูแลงานทะเบียน

Cybersecurity Checklist

แนวปฏิบัติ 22 ข้อ

รักษาความปลอดภัยไซเบอร์ซีคิวริตี้

อุบัติเหตุภัยที่เกิดขึ้นอย่างไม่คาดคิดกับชีวิตคนเราทุกวันนี้ อาจเกิดจากการกระทำของคนเรามากกว่าการกระทำของพระเจ้าหรือของคนอื่นแต่ที่คนเราคิดเช่นนั้น ทั้งนี้อาจเป็นเพราะคนเราจะมองไม่เห็นสาเหตุที่แท้จริงของภัยที่เกิดขึ้นและบางครั้งอุบัติเหตุที่เกิดขึ้นนั้นให้ความเสียหายอย่างมากจนกลายเป็นภัยพิบัติ ความเป็นจริงภัยที่เกิดขึ้นนั้นอาจเป็นเพราะความไม่ใส่ใจความประมาทเลินเล่อของตัวเราเองอย่างไม่รู้ตัวหรืออาจเกิดภาพลวงตามีเงินก้อนโตรออยู่ข้างหน้าเผลอตัวไปกดปุ่มที่ถูกวางกับดักไว้ บางครั้งโชคดีภัยที่เกิดขึ้นกับตัวเรานั้นอาจเป็นเรื่องเล็กน้อยแต่ก็มีบางครั้งโชคไม่ดีอาจเป็นเรื่องใหญ่ให้ความเสียหายใหญ่โตมากมายเหมือนภัยพิบัติได้เกิดขึ้นกับตัวเราหรือองค์กรที่เราสังกัดอยู่ อย่างเช่นที่ปรากฏในขณะที่เราทำงานอยู่บนโปรแกรมคอมพิวเตอร์ของบริษัทและบังเอิญเราอาจไปตอบรับอีเมลหรือโทรศัพท์ที่ได้วางกับดักหลอกล่อเราเพื่อเอาข้อมูลส่วนบุคคลหรือขององค์กรเพื่อประโยชน์บางอย่างโดยบุคคลนิรนามหรือบุคคลที่ไม่มีที่มาที่ไปของอีเมลหรือโทรศัพท์นั้นจนเป็นเหตุให้ข้อมูลส่วนตัวหรือขององค์กรที่อยู่ในระบบสารสนเทศของเราหรือขององค์กรถูกโจรกรรมโดยการแฮกเกอร์เพื่อการยักยอกเงินจากบัญชีเงินฝากในธนาคารของเราหรือองค์กรหรือล้วงความลับของเราหรือขององค์กรเพื่อเรียกค่าไถ่หรือไม่เช่นนั้นก็จะเปิดโปงข้อมูลที่เป็นความลับทำให้เราหรือองค์กรเกิดความเสียหายต่อสาธารณชนและนำไปสู่เสียชื่อเสียงของเราหรือองค์กรจนหมดความไว้วางใจของลูกค้าหรือผู้มีส่วนได้ส่วนเสียได้อย่างไม่ได้คาดคิดเป็นต้น อย่างที่ได้ปรากฏ

กระแสพาดหัวข่าวอย่างต่อเนื่องเกี่ยวกับการโจมตีโปรแกรมคอมพิวเตอร์ที่ออกแบบมาเพื่อขัดขวางการทำงานการเข้าถึงระบบคอมพิวเตอร์เพื่อเรียกค่าไถ่อย่างที่คนทั่วไปเรียกว่า (Ransomware) โดยบุกรุกละเมิดความปลอดภัยทางไซเบอร์ซึ่งทำให้ทุกคนรวมถึงนักบัญชีตกตลึงมึนงงกับเหตุการณ์ภัยคุกคามที่เกิดขึ้นนี้ ท่ามกลางสภาพแวดล้อมการเปลี่ยนแปลงเทคโนโลยีอย่างรวดเร็วและซับซ้อนมากขึ้นผู้นำหลายบริษัทได้มอบหมายความรับผิดชอบด้านการดูแลความปลอดภัยทางไซเบอร์นี้ให้กับบุคลากรด้านเทคโนโลยีสารสนเทศภายในของบริษัท (IT In-house) หรือผู้ให้บริการภายนอกด้านความปลอดภัยเทคโนโลยีสารสนเทศ (IT Outsource) ด้วยมีความคาดหวังว่า “งานที่มอบหมายนั้นได้รับการจัดการแล้ว” อย่างเพียงพอ แต่น่าเสียดายความเป็นจริงในปัจจุบันบุคลากรด้านเทคโนโลยีสารสนเทศภายในของหลายบริษัทไม่ได้รับการฝึกอบรมความรู้ ความสามารถด้านความปลอดภัยทางไซเบอร์หรือการเข้าถึงการใช้ทรัพยากรที่มีอยู่อย่างเพียงพอ อีกทั้งผู้ให้บริการภายนอกที่จะให้คำตอบในการแก้ไขปัญหาเหล่านั้นก็อาจไม่ทราบถึงข้อกำหนดด้านความปลอดภัยที่เป็นเฉพาะหรือข้อมูลสถานการณ์ที่เป็นปัจจุบันอยู่จริงของลูกค้าของสำนักงานสอบบัญชีที่ได้เผชิญอยู่

แม้ว่าการปกป้องอาชญากรไซเบอร์จะไม่สามารถป้องกันได้เต็มอัตราร้อยเปอร์เซ็นต์ แต่การดำเนินการและการจัดทำเอกสารรายการต่อไปนี้สามารถช่วยปกป้องข้อมูลของบริษัทและผู้ใช้ได้อย่างมาก เจ้าของบริษัทควรพบบุคลากรด้านไอทีทั้งภายในและภายนอกเพื่อหารือในแต่ละประเด็นความปลอดภัยทางไซเบอร์เพื่อการพิจารณาการจัดลำดับความสำคัญและขั้นตอนในการแก้ไขความเสี่ยงด้านความปลอดภัยทางไซเบอร์ที่อาจจะเกิดขึ้นได้โดยสามารถสรุปลำดับขั้นตอนที่สำคัญแบ่งเป็น 22 ขั้นตอนดังต่อไปนี้

01 ควรจัดให้มีการล็อคหน้าจอคอมพิวเตอร์โดยอัตโนมัติทุกหน่วยพื้นที่ของการทำงาน

- หน้าจอคอมพิวเตอร์ควรถูกล็อคโดยอัตโนมัติหลังจากทิ้งช่วงไม่ได้ใช้งานเป็นระยะเวลา 5-10 นาที
- วิธีการเช่นนี้จะช่วยลดโอกาสในการเข้าถึงแอปพลิเคชันและข้อมูลโดยไม่ได้รับอนุญาตในขณะที่ผู้ใช้ไม่ได้อยู่ที่หน้าจอคอมพิวเตอร์

02 ตั้งค่าคอมพิวเตอร์การอัปเดตระบบความปลอดภัยปฏิบัติการและแอปพลิเคชันหลักโดยอัตโนมัติ

- หนึ่งในวิธีการที่นักโจรกรรมทำสำเร็จได้มากที่สุดโดยการบุกรุกระบบเครือข่ายด้วยการล่วงรู้ช่องโหว่ที่เป็นจุดอ่อนของระบบปฏิบัติการคือการที่บริษัทไม่ได้มีการอัปเดตระบบปฏิบัติการให้เป็นปัจจุบัน
- การตั้งค่าคอมพิวเตอร์ให้มีการอัปเดตระบบปฏิบัติการและแอปพลิเคชันคอมพิวเตอร์หลักที่สำคัญโดยอัตโนมัติเป็นวิธีการลดช่องโหว่การถูกโจมตีด้านความปลอดภัยไซเบอร์ให้เหลือน้อยที่สุด
- กำหนดให้พนักงานปิดเครื่องคอมพิวเตอร์ในเวลากลางคืนและรีบูท (Reboot) เครื่องคอมพิวเตอร์ทุกวันจะทำให้มีการอัปเดตระบบปฏิบัติการเหล่านี้มีการหมุนเวียนและจะช่วยขจัดความยุ่งเหยิงของระบบทำให้ระบบปฏิบัติการคอมพิวเตอร์มีประสิทธิภาพมากขึ้น

03 กำหนดการบังคับใช้นโยบายรหัสผ่าน

- อย่างน้อยสุด บริษัทควรกำหนดหลักเกณฑ์ในการตั้งรหัสผ่านดังต่อไปนี้
- การตั้งรหัสผ่านควรมีอักขระอักษรอย่างน้อย 14 ตัว
- กำหนดรหัสผ่านแต่ละตัวไม่ซ้ำกันและไม่นำกลับมาใช้อีกบนระบบบอื่น
- กำหนดความถี่ให้ผู้ใช้เปลี่ยนรหัสผ่านสี่ครั้งต่อปี
- โน้มน้าวให้การใช้รหัสผ่านที่ซับซ้อนหรือใช้เป็นคำวลี (เช่น ฉันเฝ้ามองว่าจะไม่มีแฮกเกอร์!) เป็นต้น
- ใช้ตัวเลข ตัวอักษร และอักขระที่มีลักษณะพิเศษเป็นเอกลักษณ์เฉพาะสำหรับแต่ละแอปพลิเคชันและไม่เป็นอนุพันธ์ตัวเลขรหัสผ่านที่เคยใช้ก่อนหน้านี้ (เช่น AiCPAGoPCPS!01, AiCPAGoPCPS!02, AiCPAGoPCPS!03) เป็นต้น
- กำหนดใช้รหัสผ่านทำหน้าที่เป็นผู้จัดการสามารถช่วยให้บุคลากรปฏิบัติตามนโยบายเหล่านี้ได้อย่างมีประสิทธิภาพ
- รหัสผ่านที่ทำหน้าที่เป็นผู้จัดการจะเป็นพื้นที่เก็บข้อมูลการเข้ารหัสสำหรับรหัสผ่านของผู้ใช้ทั้งหมดหรือข้อมูลอื่นที่สำคัญ วิธีการนี้ช่วยให้ผู้ใช้ไม่ต้องติดตามรหัสผ่านที่ซับซ้อนทั้งหมดที่ได้เคยสร้างขึ้นเพียงแค่จดจำและป้องกันรหัสผ่านหลักเท่านั้น
- เมื่อพนักงานลาออกจากบริษัท ฝ่ายไอทีควรยุติการทำงานของพนักงานที่ได้ลาออกในการเข้าถึงเครือข่าย และทรัพยากรข้อมูลของบริษัท และพิจารณาให้เป็นประจำการล็อคอินบัญชีที่ไม่ต้องการหรือไม่ได้รับอนุญาตออกจากระบบ

04 ยกระดับการควบคุมการใช้รหัสผ่าน

- ใช้เครื่องมือในการรับรองความถูกต้องด้วยหลายวิธีการที่เรียกว่า Multi Factor Authentication (MFA) เช่นวิธีการ ความปลอดภัยทางกายภาพ (Physical Security Fob) การสแกนทางชีวภาพ (Biometric Scan) หรือใช้แอปพลิเคชันด้วยการส่งรหัสผ่านหรือการยืนยันผ่านทางมือถือของผู้ใช้ เพื่อยืนยันความมีตัวตนของผู้ใช้ในการที่จะเข้าสู่ระบบ

05 รักษาความปลอดภัยของข้อมูลภายในองค์กร

- สถานที่เก็บแฟ้มข้อมูลในเซิร์ฟเวอร์ (Servers) ควรเป็นสถานที่ไม่เปิดเผย ปิดล็อคห้องป้องกันการถูกบุกรุกหรือการโจรกรรมทางกายภาพ
- คอมพิวเตอร์ควรมีแผ่นดิสก์ (Disks) ในการจัดเก็บข้อมูลการเข้ารหัสผ่านหรือการปฏิบัติการความปลอดภัยทุกด้านของเซิร์ฟเวอร์ (Servers) หรือในสถานที่ที่ดีกว่านั้น ควรเก็บอยู่ในระบบคลาวด์ (Cloud) ซึ่งจะปลอดภัยจากการถูกบุกรุกดีที่สุด
- ระบบเตือนภัยของสำนักงานควรมีรหัสผ่านเฉพาะสำหรับแต่ละพนักงานหรือบุคคลภายนอกที่มีการเข้า-ออกสำนักงานเพื่อสามารถระงับการเข้าออกสำนักงานของพนักงานหรือบุคคลที่เคยถูกว่าจ้างที่ได้ถูกยกเลิกการว่าจ้างแล้ว
- บริษัทควรทำลายเอกสารด้วยการบดข้อมูลในเอกสารก่อนการจำหน่ายออกจากระบบหรือการทิ้งเอกสารหลังจากที่ได้แปลงข้อมูลในเอกสารเหล่านั้นเป็นแฟ้มดิจิทัลแล้ว

06 บันทึกอุปกรณ์เครื่องมือที่เป็นของบริษัททั้งหมด

- ใช้บัตรระบุชื่อ ชนิด ลักษณะอุปกรณ์รายตัวในลักษณะเหมือนกับบัตรสินค้ารายตัว (Inventory Tags) เพื่อการติดตามค้นหาอุปกรณ์เครื่องมือของบริษัท
- บันทึกการได้มา การมอบหมาย การจ่ายจำหน่ายออก และการโอน รวมถึงวิธีการในการจำหน่ายอุปกรณ์เครื่องมือให้กับลูกค้าและข้อมูลเกี่ยวกับลูกค้าอย่างเหมาะสม

07 จัดเก็บข้อมูลของลูกค้าทั้งหมดและมั่นใจความปลอดภัย

- จัดลำดับความสำคัญของข้อมูลสำหรับการกู้คืนฉุกเฉินในกรณีระบบล่มหรือหยุดทำงานอย่างกระทันหัน
- สร้างแผนที่การจัดเก็บข้อมูล (Data Map) แสดงข้อมูลที่เก็บอยู่ภายในเซิร์ฟเวอร์ (Servers) ในคอมพิวเตอร์ มือถือ และการเก็บสำรอง/การจัดเก็บข้อมูลและผู้ให้บริการบนคลาวด์
- การเข้าถึงแต่ละระบบเหล่านี้ควรจำกัดจำนวนผู้ใช้เพื่อลดความเสี่ยงในการเข้าถึงระบบโดยไม่ได้รับอนุญาต
- เพิ่มมาตรการการป้องกันโดยการทำ USB พอร์ต (USB Ports) ไม่สามารถเข้าถึงข้อมูลที่จัดเก็บในไดรฟ์ (Drive)

08 ดำเนินการตรวจสอบประวัติทุกคนที่ได้รับสิทธิ์การเข้าถึงเครือข่ายระบบของบริษัท

- สถิติได้แสดงให้เป็นที่น่าประหลาดใจของผู้ที่สามารถบุกรุกละเมิดการเข้าถึงระบบที่เกิดขึ้นสูงนั้นล้วนมาจากการได้รับความช่วยเหลือจากบุคลากรภายใน (หนอนบ่อนไส้) ดังนั้นจึงเป็นเรื่องสำคัญที่จะต้องตรวจสอบประวัติของบุคคลที่ได้รับอนุญาตเข้าถึงสำนักงาน คอมพิวเตอร์และเครือข่ายระบบคอมพิวเตอร์ของบริษัท

09 พัฒนานโยบายการต้อนรับผู้เข้ามาติดต่อสำนักงาน

- พนักงานควรได้รับการฝึกอบรมในการต้อนรับบุคคลที่มาติดต่อสำนักงานด้วยการถามด้วยความอ่อนโยนและให้ความช่วยเหลือและหากเป็นไปได้พาผู้ที่มาติดต่อเข้าไปพบกับบุคคลที่ต้องการพบ
- หากมีข้อสงสัยผู้เข้ามาติดต่อเกี่ยวกับการยืนยันความมีตัวตนของผู้เข้ามาติดต่อบริษัท เจ้าหน้าที่ฝ่ายผู้จัดการที่รับผิดชอบหรือทีมงานฝ่ายธุรการควรได้รับแจ้งทันที

10 ให้มีความมั่นใจผู้ที่เข้าใช้อุปกรณ์ของบริษัทเป็นผู้ที่ได้รับอนุญาตเป็นผู้มีสิทธิ์ได้ผ่านการรับการอนุมัติอย่างถูกต้องเท่านั้นถึงจะสามารถเชื่อมโยงอุปกรณ์เครื่องมือไอทีของบริษัทได้

- อนุญาตผู้ใช้อุปกรณ์ของบริษัทเฉพาะผู้ที่ได้รับอนุญาตและมีสิทธิ์ผ่านการรับอนุมัติอย่างถูกต้องเท่านั้นถึงจะสามารถเชื่อมโยงต่อโครงสร้างพื้นฐานไอทีและการให้บริการบนคลาวด์ของบริษัทได้
- ใช้ระบบเน็ตเวิร์กส่วนตัวแบบจำลอง (Virtual Private Network) หรือที่เรียกว่า (VPN) หรือการจัดการอุปกรณ์เคลื่อนที่ (Mobile Device Management) กำหนดให้แต่ละอุปกรณ์ที่เป็นคอมพิวเตอร์ แท็บเล็ต (Tablet) และสมาร์ทโฟน (Smart Phone) ต้องลงทะเบียนเพื่อเชื่อมโยงกับระบบครือข่ายของบริษัท
- บุคลากรของบริษัทควรได้รับการเตือนถึงความสำคัญของการอัปเดตระบบปฏิบัติการให้เป็นปัจจุบันและการรักษาความปลอดภัยอุปกรณ์มือถืออย่างสม่ำเสมอ

11 ลดการเข้าถึงระบบในระดับเท่าที่จำเป็นที่สุดเท่านั้น

- นักโจรกรรมข้อมูลหรือที่เรียกว่าแฮกเกอร์นั้น สามารถเข้าถึงระบบเครือข่ายและคอมพิวเตอร์ ซึ่งจะมีอิทธิพลอย่างมากในการควบคุมเครือข่ายที่เป็นโครงสร้างพื้นฐานของบริษัท
- จำกัดจำนวนสิทธิ์ผู้ใช้ที่มีหน้าที่บริหารจัดการการเข้าถึงระบบและการตั้งค่าการเข้าถึงระบบของผู้ใช้แต่ละรายในระดับต่ำสุดพอเพียงผู้ใช้สามารถทำงานเสร็จสิ้นสมบูรณ์
- ฝ่ายไอทีต้องมีส่วนร่วมไม่เพียงแต่ให้ระดับการเข้าถึงขั้นต่ำเท่าที่จำเป็นแก่ผู้ใช้แต่ละรายในการทำงานเท่านั้น แต่ควรกำกับดูแลการเข้าถึงและยุติการเข้าถึงเมื่อไม่มีความจำเป็นในการเข้าถึงระบบอีกต่อไป

12 ตรวจสอบความเชื่อมั่นว่าอุปกรณ์ระบบปฏิบัติการเครือข่ายทั้งหมดเป็นปัจจุบัน

- อุปกรณ์ระบบปฏิบัติการเครือข่ายทั้งหมด เช่นเซิร์ฟเวอร์ไฟล์ (File Servers), ไฟร์วอลล์ (Firewalls), เราเตอร์ (Routers), อุปกรณ์เครือข่ายพ่วง (Internet of Things (IoT)) ควรได้รับการสอบทานเป็นประจำ เพื่อให้มีความเชื่อมั่นระบบการปฏิบัติการมีการอัปเดตเป็นปัจจุบันอยู่เสมอ
- สิ่งสำคัญอย่างยิ่งที่จะต้องอัพเดตระบบเครือข่าย (Firmware) ให้เป็นปัจจุบันและกำหนดการเปลี่ยนรหัสผ่านบนอุปกรณ์ทั้งหมดที่เชื่อมโยงต่อกับบริษัทและที่ผ่านเครือข่ายในบ้านหรือในระยะไกล ซึ่งรวมถึงเครื่องพิมพ์แบบไร้สายและอุปกรณ์ระบบเครือข่ายพ่วง (IoT) รวมถึงกล้องรักษาความปลอดภัย, เครื่องใช้ภาพในบ้านที่เชื่อมต่อและอุปกรณ์ที่เปิดใช้งานด้วยเสียงอย่างสม่ำเสมอ.

13 ยืนยันให้มีความเชื่อมั่นแต่ละไฟล์เซิร์ฟเวอร์ (Fileserver) คอมพิวเตอร์และอุปกรณ์มือถือติดตั้งที่เป็นซอฟต์แวร์ป้องกันไวรัส/ความปลอดภัยแล้ว

- ซอฟต์แวร์ที่ติดตั้งควรได้รับการอัพเดตให้เป็นปัจจุบันอย่างสม่ำเสมอโดยอัตโนมัติและอุปกรณ์กลั่นกรองการเข้าถึงมีการสแกนผ่านมัลแวร์ (Malware) ตามตารางเวลาที่ตั้งไว้ล่วงหน้า
- เพิ่มขีดความสามารถในการใช้อุปกรณ์เครือข่ายแอปพลิเคชันเหล่านี้ ในการตรวจจับและการป้องกันการบุกรุกและการปิดกันภัยคุกคามที่คาดไม่ถึง
- คอมพิวเตอร์ควรมีการตั้งค่าการสแกนที่เป็นสื่อภายนอกโดยอัตโนมัติ เช่นแฟลชไดรฟ์ (Flash Drive) อุปกรณ์เพิ่มหน่วยความจำที่จัดหาโดยลูกค้าก่อนการโหลดข้อมูลลงในไฟล์ ไม่อนุญาตให้ใช้ยูเอสบี (USB) เพื่อการจัดเก็บข้อมูล (USB Storage Drives) และให้ความรู้แก่ลูกค้าเกี่ยวกับการใช้ดิจิทัลพอร์ทัล (Digital Portals) และอีเมลที่ปลอดภัย

14 สอบทานการสำรองข้อมูลเป็นประจำ ทดสอบความสามารถการเข้าถึงข้อมูลและทำสำเนาไฟล์ที่มีการเปลี่ยนแปลงตลอดวันการปฏิบัติการ

- สำรองข้อมูลไม่เพียงแต่การปกป้องการสูญหายของข้อมูล/เสียหายจากการถูกทำลาย แต่มีความสำคัญในการกู้คืนข้อมูลฉุกเฉินในยามวิกฤตจากความพยายามการถูกบุกรุกโจมตีระบบการปฏิบัติการเพื่อการเรียกค่าไถ่ด้วยวิธีการที่เรียกว่าแรนซัมแวร์ (Ransomware)
- ฝ่ายไอทีควรสอบทานการสำรองข้อมูลเป็นประจำ โดยการทดสอบความครบถ้วนการสำรองข้อมูลและสุ่มเลือกการกู้คืนแฟ้มข้อมูลเพื่อทดสอบความสามารถการเข้าถึงข้อมูลเหล่านั้นได้
- สำเนาแฟ้มข้อมูลที่เปลี่ยนแปลงทั้งหมดตลอดวันแล้วจัดเก็บแยกต่างหากให้อยู่นอกสถานที่ใกลตา
- ข้อมูลสำรองทั้งหมดควรได้รับการเข้ารหัสผ่าน รวมถึงข้อมูลสำรองที่อยู่นอกสถานที่ผ่านอินเทอร์เน็ตหรือสื่อจัดเก็บข้อมูลทางกายภาพ รวมถึงการสำรองข้อมูลบางอย่างที่ “Air Gapped” ซึ่งหมายถึงการจัดเก็บทางกายภาพแยกต่างหากและไม่สามารถเข้าถึงเครือข่ายได้

15 ใช้รหัสผ่านอีเมลและ/หรือด้วยวิธีพอร์ทัลโซลูชั่น (Portal Solutions) ในการส่งแฟ้มข้อมูล

- บุคลากรของบริษัททุกคนควรได้รับการฝึกอบรมเกี่ยวกับการเข้ารหัสผ่านอีเมลและ/หรือด้วยวิธีพอร์ทัลโซลูชั่น (Portal Solutions) ในการส่งแฟ้มข้อมูลไปยังลูกค้าและจากลูกค้าด้วยความปลอดภัย
- บริษัทควรลงทุนเวลาในการอบรมลูกค้าในการใช้ระบบดิจิทัลที่บริษัทนำมาใช้ให้ถูกต้อง

16 ส่งเสริมการตระหนักรู้ถึงรูปแบบการหลอกล่อการเข้าถึงข้อมูลด้วยวิธีการที่เรียกว่าการตกเบ็ดที่กำลังถูกใช้อย่างแพร่หลายในปัจจุบัน (Phishing Schemes) และแนะนำการตอบสนองอย่างถูกต้องให้กับพนักงาน

- รูปแบบการหลอกล่อการเข้าถึงข้อมูลด้วยวิธีการที่เรียกว่า การตกเบ็ด (Phishing Schemes) นั้นมีความชาญฉลาดความสามารถมากขึ้นโดยวิธีการที่เรียกว่าการตกเบ็ดแบบ “ปาหอก” (Spear) เจาะจงไปยังผู้ตกเป็นเหยื่อด้วยการส่งอีเมลตรงไปยังเป้าหมายเฉพาะเจาะจงผู้ที่ตกเป็นเหยื่อ ข้อมูลของผู้ที่ตกเป็นเหยื่อมักมาจากเพื่อนร่วมงานที่รู้อีเมลหลอก “ด้วยการปลอมแปลง” หรือการบุกรุก
- พนักงานจำเป็นต้องทำการอัปเดตเป็นประจำเป็นปกติเกี่ยวกับรูปแบบการถูกล่อเหยื่อโดยวิธีการตกเบ็ดด้วยการปักธง “ธงแดง”เป็นการเตือนชักชวนให้มีการวิเคราะห์พิจารณาเพิ่มเติมและการศึกษาเพิ่มเติมควรทำอะไรหากได้รับอีเมลหรือโทรศัพท์ที่น่าสงสัย
- พนักงานไม่ควรคลิกลิงก์หรือเปิดไฟล์แนบอยู่ในอีเมลหรือมีข้อความชักชวนการกระทำอย่างใดอย่างหนึ่งโดยไม่มีการยืนยันความมีตัวตนกับผู้ส่งก่อนหรือด้วยวิธีการอื่นนอกเหนือรูปแบบที่ถูกส่งเข้ามา
- หากผู้ใช้มีข้อกังวลใด ๆ ควรมีกระบวนการแจ้งให้สมาชิกทีมงานไอทีตรวจสอบอีเมลหรือติดต่อผู้ส่งเพื่อยืนยันเจตนา
- พิจารณาการใช้บริการที่ให้การฝึกอบรมการตกเบ็ด/การรักษาความปลอดภัยอย่างต่อเนื่องและการทดสอบการตอบสนองของพนักงานต่ออีเมลตกเบ็ด

17 ฝึกอบรมพนักงานการตรวจสอบการเชื่อมต่อที่ปลอดภัยหรือการใช้การเชื่อมต่ออุปกรณ์ที่เป็นส่วนบุคคลที่เรียกว่า Virtual Private Network (VPN) เมื่ออยู่นอกสำนักงาน

- พนักงานทุกคนควรได้รับการฝึกอบรมการตรวจสอบการเชื่อมต่อที่ปลอดภัยไปยังเว็บไซต์ หรือใช้การเชื่อมต่อส่วนบุคคลแบบวิธี Virtual Private Network (VPN) เมื่อทำงานนอกสถานที่สำนักงานและในการที่จะเข้าถึงอินเทอร์เน็ตและ/หรือข้อมูลทรัพยากรของบริษัท
- เมื่อทำงานจากระยะไกลบุคลากรควรตรวจสอบ SSID/รหัสผ่านสำหรับการเข้าถึง Wi-Fi ที่จัดหาให้ลูกค้าหรือการใช้ Hotspot มือถือเซลลูลาร์ดิจิทัลที่ปลอดภัยแทนที่จะเป็น Wi-Fi สาธารณะ เช่น โรงแรม ร้านกาแฟ หรือสนามบินซึ่งอาจถูกบุกรุกอย่างลับ ๆ
- วิธีการที่ดีกว่า ส่งเสริมการใช้ Hotspot มือถือ (4G/5G) สำหรับการเข้าถึงอินเทอร์เน็ตมาตรฐานแทนที่จะใช้อินเตอร์เน็ตที่จัดหาให้เพื่อสาธารณะหรือเพื่อลูกค้าหรือ Wi-Fi สาธารณะ

18 จ้างผู้เชี่ยวชาญด้านความปลอดภัยไซเบอร์

- หากบุคลากรด้านไอทีภายในของบริษัท ไม่มีความเชี่ยวชาญด้านความปลอดภัยไซเบอร์ในระดับที่ไว้วางใจได้เพียงพอและเหมาะสมในการปกป้องด้านความปลอดภัยไซเบอร์ของบริษัท บริษัทควรมีพันธมิตรภายนอกที่มีความเชี่ยวชาญและไว้ใจได้ร่วมมือด้านความปลอดภัยไซเบอร์เพื่อเน้นการให้บริการความปลอดภัยไซเบอร์แบบบูรณาการ
- ผู้เชี่ยวชาญเหล่านี้สามารถช่วยสอบทานด้านความปลอดภัยเครือข่ายอินเตอร์เน็ตของบริษัทและให้แนวทางและช่วยเหลือการติดตั้งเพื่อการใช้งานรวมถึงการสอบทานเพื่อการตรวจพบการบุกรุก การป้องกันและการกำกับดูแลติดตามอย่างต่อเนื่อง
- หากภายในของบริษัทไม่มีความเชี่ยวชาญด้านความปลอดภัยทางไซเบอร์เพียงพอก็ควรพิจารณาการใช้การจัดการจากบุคคลภายนอกในการให้บริการและแม้บริษัทมีผู้เชี่ยวชาญด้านไอทีภายในดีอยู่แล้วอาจว่าจ้างผู้เชี่ยวชาญด้านไอทีภายนอกมาสอบทานระบบความปลอดภัยด้านไซเบอร์เป็นครั้งคราวก็จะช่วยกระชับความปลอดภัยด้านไซเบอร์ที่เป็นปัจจุบันชัดเจนมากขึ้น

19 พัฒนาแผนการตอบสนองการรับมือกับการถูกบุกรุกหรือการถูกละเมิด

- เวลาที่ดีที่สุดของการพัฒนาแผนการตอบสนองการรับมือต่อเหตุการณ์ด้านความปลอดภัยไซเบอร์ คือ เวลาก่อนที่บริษัทจะพบว่าความปลอดภัยไซเบอร์ดังกล่าวถูกบุกรุกหรือถูกละเมิด
- ผู้นำของบริษัทและบุคลากรด้านไอทีควรจัดทำบันทึกกระบวนการแผนรักษาความปลอดภัย (WISP) เป็นลายลักษณ์อักษรเป็นเอกสารส่วนหนึ่งของบริษัทซึ่งถือเป็นข้อกำหนดหนึ่งในกระบวนการรายงานการแสดงแบบภาษีให้กับกรมสรรพกรของบริษัทเช่นกัน
- พนักงานควรได้รับการให้การศึกษาและอบรมควรทำอย่างไรในกรณีเกิดข้อสงสัยว่าระบบความปลอดภัยถูกการบุกรุกหรือการละเมิด
- การฝึกอบรมนี้ควรรวมถึงขั้นตอนการปฏิบัติงานของทีมงานไอทีในการที่จะดำเนินการเพื่อตรวจสอบและบรรเทาการถูกละเมิดรวมถึงมีรายละเอียดทรัพยากรอุปกรณ์ภายนอกและการปฏิบัติตามข้อกำหนดการประกันภัย
- บริษัทควรตระหนักรู้ถึงข้อกำหนดการรายงานทางกฎหมายทั้งหมดสำหรับการแจ้งเตือนการถูกบุกรุกหรือการละเมิดในเขตอำนาจศาลสถานที่ตั้งของบริษัทที่ได้ดำเนินงานอยู่

20 สอบทานนโยบายด้านไอทีประจำปีสม่ำเสมอและเตือนผู้ใช้การเปลี่ยนแปลง

- เทคโนโลยีมีการพัฒนาอย่างรวดเร็วและปัจจุบันมีการนำเทคโนโลยีการทำงานระยะไกลมาใช้เกิดขึ้นอย่างรวดเร็ว มีบริษัทจำนวนมากได้ปรับสภาพแวดล้อมการทำงานสองระบบทำงานนอกสถานที่ได้ในทุกสถานที่กับการทำงานสถานที่ในออฟฟิศ
- บริษัทควรทบทวนนโยบายด้านไอทีเป็นประจำทุกปีหรือตามความจำเป็น และปรับปรุงนโยบายด้านไอที/ทรัพยากรบุคคลเพื่อให้สอดคล้องกับสภาพแวดล้อมปัจจุบัน สื่อสารการเปลี่ยนแปลงใด ๆ ให้กับผู้ใช้อย่างเป็นทางการและอัปเดตนโยบายการใช้งานอินเทอร์เน็ตและคอมพิวเตอร์พร้อมกับการฝึกอบรมกาอัปเดตความปลอดภัยเป็นประจำทุกปี

21 ให้มีการอบรมด้านความปลอดภัยเป็นส่วนหนึ่งการเก็บคะแนนสะสมการศึกษาต่อเนื่องประจำปีของบริษัท

นอกเหนือจากการอัปเดตนโยบายด้านไอทีให้เป็นปัจจุบันแล้ว บุคลากรทุกคนควรได้รับการศึกษาต่อเนื่องเกี่ยวกับภัยคุกคามในปัจจุบัน ได้แก่ :

- แรนซัมแวร์ (Ransomware)
- การหลอกล่อด้วยวิธีการตกเบ็ด (Phishing)
- ส่งเอสเอ็มเอสหรือข้อความในรูปแบบวิธีการตกเบ็ด (SMiShing (SMS/Text Phishing))
- การหลอกล่อด้วยวิธีการตกเบ็ดด้วยเสียง (Vishing (Voice Mail Phishing))

ตัวอย่างอื่น ๆ ด้านวิศวกรรมตามสภาพแวดล้อมของสังคม (Social Engineering) ที่ออกแบบมาเพื่อให้พนักงานดาวน์โหลดมัลแวร์ (Malware) มีผลกระทบต่อความปลอดภัยของบริษัทหรือให้ข้อมูลที่ละเอียดอ่อนของบริษัทอย่างไม่ได้ตั้งใจ

- พนักงานควรได้รับการอบรมการเตือนให้สงสัยจากการได้รับโทรศัพท์จากบุคคลที่ไม่รู้แหล่งที่มาของบุคคลและอย่าให้มีการเข้าสู่ระบบรหัสผ่านหรือข้อมูลทางการเงินหรือดาวน์โหลดไฟล์โดยไม่มีการยืนยันความมีตัวตนของบุคคลที่ผู้โทรเข้ามาก่อนการตอบรับการโทรศัพท์

22 สอบทานทบทวนกรมธรรม์ประกันภัย

- บริษัทควรสอบทานนโยบายการประกันของตนเพื่อทำความเข้าใจว่าบริษัทได้รับความคุ้มครองประกันภัยสำหรับเหตุการณ์แรนซัมแวร์ (Ransomware) ในระดับใดและความเสียหายที่เกิดขึ้นจากการสูญเสียรายได้ซึ่งเป็นผลมาจากการถูกบุกรุกละเมิดด้านความปลอดภัยไซเบอร์
- บริษัทควรพิจารณารวมถึงความคุ้มครองความเสียหายที่เกิดขึ้นกับลูกค้าที่ตกเป็นเหยื่อของการถูกโจรกรรมข้อมูลสืบเนื่องมาจากข้อมูลของบริษัทถูกบุกรุกหรือการถูกละเมิดข้อมูลของบริษัท

บทสรุประดับสูงโดยสังเขป (Executive Summary)

ในขณะที่บริษัทส่วนใหญ่ถูกการบุกรุกด้วยการถูกแฮกข้อมูลจากแฮกเกอร์ (Hackers) ซึ่งผู้ที่มีความเชี่ยวชาญด้านเทคนิคชั้นสูงและด้วยวิธีการที่สลับซับซ้อนอย่างมากในการบุกรุกข้อมูลในระบบนั้น ผลของการสำรวจข้อเท็จจริงส่วนใหญ่ตรวจพบว่ามีรากฐานมาจากความผิดพลาดของมนุษย์ (Human Error) เช่น การคลิกที่ไฟล์ที่แนบมากับอีเมลโดยไม่ได้ตั้งใจหรือการให้ข้อมูลแก่ผู้บุกรุกโดยไม่ได้ตั้งใจหรือความประมาทเลินเล่อละเลยการอัปเดตซอฟต์แวร์ในเวลาที่เหมาะสม ดังนั้น การบันทึกโครงสร้างการจัดการความปลอดภัยทางไซเบอร์เชิงรุกเป็นลายลักษณ์อักษรนั้นไม่เพียงแต่มีความสำคัญและมีความจำเป็นอย่างมากเท่านั้น แต่ยังช่วยการปกป้องได้ตลอดเส้นทางของการป้องกันระบบไซเบอร์ให้กับบริษัท

ตามที่ได้กล่าวข้างต้นแนวทางการรักษาความปลอดภัยทางไซเบอร์การป้องกันและการแก้ไขเยียวยาข้อผิดพลาดและความเสียหายที่อาจเกิดขึ้นนั้นได้ระบุเป็นรายละเอียด 22 ข้อเพื่อเป็นแนวปฏิบัติการป้องกันและการรักษาความปลอดภัยไซเบอร์อย่างต่อเนื่องสำหรับผู้ที่มีหน้าที่ด้านไอทีและพนักงานของบริษัทและจะมีคุณค่ามากยิ่งขึ้นหากการปกป้องและการรักษาความปลอดภัยไซเบอร์ได้เริ่มต้นจากตัวเราซึ่งเป็นผู้ใช้คอมพิวเตอร์

Roman H. Kepczyk, CPA.CITP, CGMA is Director of Firm Technology Strategy for Right Networks and partners exclusively with accounting firms on production automation, application optimization and practice transformation. He has been consistently listed as one of INSIDE Public Accounting's Most Recommended Consultants, Accounting Today's Top 100 Most Influential People, and CPA Practice Advisor's Top Thought Leaders.