ด่วนที่สุด

สำเนาถูกต้อง

ที่ ๐๐๒๒(สพ).(๑๐)๑(๒)/ ๔๓๖๗

เรียน ผบก.ภ.จว.สุพรรณบุรี เพื่อโปรดทราบ

รอง ผบก.ภ.จว.สุพรรณบุรี เพื่อทราบ

ผกก.ฝอ.ฯ,ผกก.สืบสวนฯ, ผกก.สภ.ทุก สภ.ในสังกัดฯ

รอง ผกก.ฝอ.ฯ,สวญ.สภ.องค์พระ

เพื่อทราบและดำเนินการในส่วนที่เกี่ยวข้องตามหนังสือ ภ.๗ ด่วนที่สุด ที่ ๐๐๒๒.๑๖๒/๒๙๐๗ ลง ๓๐ ส.ค.๖๗ ต่อท้ายตามหนังสือสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ด่วนที่สุด ที่ สกมช ๐๘๑๐/ว๔๑๑๔ ลง ๒๘ ส.ค.๖๗ เรื่อง ขอทราบความคืบหน้าการดำเนินการตามแนวปฏิบัติขั้นพื้นฐานในการป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware) และการรั่วไหลของข้อมูลสำหรับหน่วยงาน ดังนี้

๑. ดำเนินการตามแนวปฏิบัติพื้นฐานในการป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware) และการรั่วไหลของข้อมูลสำหรับหน่วยงานให้มีความปลอดภัยมากยิ่งขึ้น

๒. ให้หัวหน้าหน่วยงานลงนามยืนยันแจ้งผลดำเนินการตามแบบตอบรับการดำเนินการแนวปฏิบัติพื้นฐานในการป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware) และการรั่วไหลของข้อมูล สำหรับหน่วยงาน

๓. ส่งรายงานแบบตอบรับฯ ให้ ภ.จว.สุพรรณบุรี ทราบ ภายใน ๒๐ ก.ย.๖๗ ทางไลน์กลุ่ม “เทคโนฯ ภ.จว.สุพรรณฯ” ตาม QR Code ด้านล่าง

รายละเอียดปรากฏตามเอกสารที่แนบมาพร้อมนี้

พ.ต.อ

(สมเพร พุกหอม)

รอง ผบก.ภ.จว.สุพรรณบุรีปรท.ผบก.ภ.จว.สุพรรณบุรี

๗ ก.ย.๖๗

กลุ่มไลน์ “เทคโนฯ ภ.จว.สุพรรณฯ”

ด่วนที่สุด

สำเนาถูกต้อง
ที่ ๐๐๒๒.๑๖๒/๒๙๐๗
เรียน ผบช.ภ.๗
ผทค.พิเศษ ตร. รรท.รอง ผบช.ภ.๗
รอง ผบช.ภ.๗

- เพื่อโปรดทราบ

ผบก.ในสังกัด ภ.๗

เพื่อโปรดทราบและดำเนินการในส่วนที่เกี่ยวข้องตามหนังสือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ด่วนที่สุด ที่ สกมช ๐๘๑๐/ว๔๑๑๔ ลง ๒๘ ส.ค.๖๗ เรื่อง ขอทราบความคืบหน้าการดำเนินการตามแนวปฏิบัติขั้นพื้นฐานในการป้องกันข้อมูลรั่วไหลและมัลแวร์เรียกค่าไถ่ (Ransomware) สำหรับหน่วยงาน โดยให้รายงานความคืบหน้าดำเนินการตอบตามแนวปฏิบัติขั้นพื้นฐานในการป้องกันข้อมูลรั่วไหลและมัลแวร์เรียกค่าไถ่ (Ransomware) สำหรับหน่วยงาน และนำไปดำเนินการให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น และขอให้ ผบก./หน.สภ. ในสังกัด ลงนามยืนยันแจ้งผลการดำเนินการตามแบบตอบรับการดำเนินการแนวปฏิบัติพื้นฐานในการป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware) และการรั่วไหลของข้อมูลสำหรับหน่วยงาน โดยให้ บก./ภ.จว. รวบรวมแบบตอบรับฯ ของหน่วยงานในสังกัด รายงานให้ บก.อก.ภ.๗ (ผ่าน ผอ.๖ บก.อก.ภ.๗) ทราบภายในวันที่ ๒๕ ก.ย.๖๗ ก่อน ๑๒.๐๐ น. (ห้ามผัดส่ง) เพื่อจะได้รวบรวมส่งให้ สกมช. ทราบ ต่อไป รายละเอียดปรากฏตามเอกสารที่แนบ

พ.ต.อ.
(ปรัชญา ทองน้ำวน)
รอง ผบก.อก.ภ.๗ ปรท.ผบก.อก.ภ.๗
๓๐ ส.ค.๖๗

แบบตอบรับฯ

NCS สกมช
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
๑๒๐ หมู่ ๓ อาคารรัฐประศาสนภักดี ชั้น ๗ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐ อีเมล saraban@ncsa.or.th

ด่วนที่สุด
ที่ สกมช ๐๘๑๐/๒ ๔๑๑๔

๒๗ สิงหาคม ๒๕๖๗

เรื่อง ขอทราบความคืบหน้าการดำเนินการตามแนวปฏิบัติขั้นพื้นฐานในการป้องกันข้อมูลรั่วไหลและมัลแวร์เรียกค่าไถ่ (Ransomware) สำหรับหน่วยงาน

เรียน หัวหน้าส่วนราชการ รัฐวิสาหกิจ องค์การมหาชน องค์กรอิสระ หน่วยงานภาคเอกชน และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

อ้างถึง หนังสือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่ สกมช ๐๘๑๐/ว๓๐๘๖ ลงวันที่ ๑๒ กรกฎาคม ๒๕๖๗

สิ่งที่ส่งมาด้วย แบบตอบรับการดำเนินการแนวปฏิบัติขั้นพื้นฐานในการป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware) และการรั่วไหลของข้อมูล สำหรับหน่วยงาน

ตามหนังสืออ้างถึง หนังสือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ที่ สกมช ๐๘๑๐/ว๓๐๘๖ ลงวันที่ ๑๒ กรกฎาคม ๒๕๖๗ เรื่อง ขอให้หน่วยงานดำเนินการตามแนวปฏิบัติขั้นพื้นฐานในการป้องกันข้อมูลรั่วไหลและมัลแวร์เรียกค่าไถ่ (Ransomware) สำหรับหน่วยงาน ตามที่นายกรัฐมนตรีได้มอบนโยบายระบุถึงความสำคัญเรื่องความมั่นคงปลอดภัยทางไซเบอร์ โดยให้หน่วยงานรัฐและหน่วยงานที่เกี่ยวข้อง มีมาตรฐาน และเพิ่มการป้องกันภัยคุกคามทางไซเบอร์ ให้มีประสิทธิภาพมากยิ่งขึ้น นั้น

ในการนี้ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๕ กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน และจะต้องดำเนินการให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๑๓ วรรคหนึ่ง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) จึงขอให้หน่วยงานของท่าน ในฐานะหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รายงานความคืบหน้าดำเนินการตอบตามแนวปฏิบัติขั้นพื้นฐานในการป้องกันข้อมูลรั่วไหลและมัลแวร์เรียกค่าไถ่ (Ransomware) สำหรับหน่วยงาน และนำไปดำเนินการให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น เมื่อได้รับหนังสือฉบับนี้ ขอความอนุเคราะห์ยืนยันการรับทราบหนังสือให้ สกมช. ทางอีเมล Coordination@ncsa.or.th ทันที และขอให้หัวหน้าหน่วยลงนามยืนยันแจ้งผลการดำเนินการตามแบบตอบรับ (สิ่งที่ส่งมาด้วย) ให้ สกมช. ทราบทางอีเมล Coordination@ncsa.or.th อีกครั้ง ภายในวันที่ ๓๐ กันยายน ๒๕๖๗ ทั้งนี้ สกมช. จะได้รวบรวมรายงานผลให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) โดยมี นายกรัฐมนตรี เป็นประธานเพื่อรับทราบต่อไป

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการต่อไปด้วย จะขอบคุณยิ่ง

ขอแสดงความนับถือ

พลอากาศตรี อมร ชมเชย

(อมร ชมเชย)
เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ
โทรศัพท์ ๐ ๒๑๑๔ ๓๕๓๑
อีเมล coordination@ncsa.or.th

แบบตอบรับฯ (สิ่งที่ส่งมาด้วย)
https://drive.ncsa.or.th/s/HwakNE7B3fd2FrE

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
๑๒๐ หมู่ ๓ อาคารรัฐประศาสนภักดี ชั้น ๗ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐
ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐ ไปรษณีย์อิเล็กทรอนิกส์: saraban@ncsa.or.th

ที่ สกมช ๐๘๑๐/ว๓๐๘๖

๑๒ กรกฎาคม ๒๕๖๗

เรื่อง ขอให้หน่วยงานดำเนินการตามแนวปฏิบัติขั้นพื้นฐานในการป้องกันข้อมูลรั่วไหลและมัลแวร์เรียกค่าไถ่ (Ransomware) สำหรับหน่วยงาน

เรียน หัวหน้าส่วนราชการ รัฐวิสาหกิจ องค์การมหาชน องค์กรอิสระ หน่วยงานภาคเอกชน และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

อ้างถึง พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

สิ่งที่ส่งมาด้วย แบบตอบรับการดำเนินการแนวปฏิบัติขั้นพื้นฐานในการป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware) และการรั่วไหลของข้อมูล สำหรับหน่วยงาน

ตามที่นายกรัฐมนตรีได้มอบนโยบายระบุถึงความสำคัญเรื่องความมั่นคงปลอดภัยทางไซเบอร์ โดยให้หน่วยงานรัฐและหน่วยงานที่เกี่ยวข้อง มีมาตรฐาน และเพิ่มการป้องกันภัยคุกคามทางไซเบอร์ให้มีประสิทธิภาพมากยิ่งขึ้น ประกอบกับสถานการณ์ในห้วงเดือนมกราคม – เดือนมิถุนายน ๒๕๖๗ พบว่ามีหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศถูกโจมตีด้วยมัลแวร์เรียกค่าไถ่ (Ransomware) ได้รับผลกระทบเป็นจำนวนมาก และมีแนวโน้มว่าจะใช้ระยะเวลาในการดำเนินการแก้ไขปัญหาที่ซับซ้อน หากไม่ได้มีการเตรียมการหรือป้องกันอย่างถูกต้อง เหมาะสม และมีผลกระทบกับหน่วยงานอื่น ๆ เพิ่มขึ้น และใน**มาตรา ๔๕** แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้**หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ** มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน และจะต้องดำเนินการให้เป็นไปตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๑๓ วรรคหนึ่ง นั้น

ในการนี้ เพื่อให้สามารถป้องกัน รับมือ และลดความเสี่ยงจากข้อมูลรั่วไหลและมัลแวร์เรียกค่าไถ่ (Ransomware) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) จึงได้จัดทำแนวปฏิบัติขั้นพื้นฐานในการป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware) และการรั่วไหลของข้อมูล สำหรับหน่วยงาน ระยะเร่งด่วน เพื่อมิให้สร้างผลกระทบต่อระบบสารสนเทศหรือประชาชนที่มาใช้บริการหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จึงขอให้หน่วยงานของท่านนำไปดำเนินการให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น และเมื่อได้รับหนังสือฉบับนี้ ขอความอนุเคราะห์ยืนยันการรับทราบหนังสือให้ สกมช. ทางอีเมล thaicert@ncsa.or.th ทันที และขอให้หัวหน้าหน่วยลงนามยืนยันแจ้งผลการดำเนินการตามแบบตอบรับ (สิ่งที่ส่งมาด้วย) ให้ สกมช. ทราบทางอีเมล thaicert@ncsa.or.th อีกครั้ง ภายในวันที่ ๑๕ สิงหาคม ๒๕๖๗ ทั้งนี้ สกมช. จะได้รวบรวมรายงานผลให้คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) โดยมี นายกรัฐมนตรี เป็นประธาน เพื่อรับทราบต่อไป

จึงเรียนมาเพื่อโปรดพิจารณาดำเนินการต่อไปด้วย จะขอบคุณยิ่ง

ขอแสดงความนับถือ

พลอากาศตรี

(อมร ชมเชย)
เลขาธิการคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ
สำนักประสานงาน
โทรศัพท์ ๐ ๒๑๑๔ ๓๕๓๑
อีเมล thaicert@ncsa.or.th

แบบตอบรับฯ (สิ่งที่ส่งมาด้วย)

แบบตอบรับการดำเนินการแนวปฏิบัติพื้นฐานในการป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware) และการรั่วไหลของข้อมูล สำหรับหน่วยงาน

ชื่อหน่วยงาน..... .....

ลำดับ	คำแนะนำ	ดำเนินการเรียบร้อย
1	การควบคุม และตรวจสอบการทำงานของ outsource ต้องมีการกำหนดสิทธิ์และควบคุมการเข้าถึงข้อมูลหรือระบบงาน รวมถึงมีการตรวจสอบการทำงานของทีม outsource ว่าเป็นไปตามข้อกำหนดหรือไม่ และควรมีมาตรการเอาผิดหรือบทลงโทษ หาก บริษัท outsource ละเมิดหรือทำผิดข้อกำหนดจนเป็นสาเหตุให้ถูกโจมตีทางไซเบอร์ รวมทั้งการละเมิด PDPA ด้วย	☐
2	สำรองข้อมูลที่สำคัญตามกฎ 3-2-1 โดยเก็บข้อมูลสำคัญเอาไว้ 3 ชุด ได้แก่ ข้อมูลหลัก 1 ชุด และข้อมูลสำรอง 2 ชุด เก็บไฟล์เหล่านั้นเอาไว้บนอุปกรณ์ที่แยกขาดจากกัน 2 ประเภท และข้อมูลสำรอง 1 ชุดเก็บไว้แบบ Offline และมีการดำเนินการสำรองข้อมูลเป็นประจำ	☐
3	บัญชีผู้ดูแล ผู้ใช้งาน ควรตั้งรหัสผ่านดังนี้ - ตั้งรหัสผ่านอย่างน้อย 8 ตัว โดยประกอบด้วยตัวอักษรเล็ก (abcd) ตัวอักษรใหญ่ (ABCD) ตัวเลข (1234) และสัญลักษณ์ ($#!?) เพื่อสร้างความหลากหลายให้กับรหัสผ่าน - มีการเก็บหรือจัดการกับรหัสผ่านที่มีความปลอดภัยจากการถูกแฮก - หลีกเลี่ยงการตั้งรหัสผ่านเดียวกันหลาย ๆ ระบบ - ปิดการใช้งาน "hint" หรือคำใบ้ของรหัสผ่าน - เปลี่ยนรหัสผ่านอย่างสม่ำเสมอ - การติดตั้งซอฟต์แวร์ทุกครั้งต้องใช้สิทธิ์ผู้ดูแลเสมอ	☐
4	เปิดการใช้งาน Multi-Factor Authentication (MFA) สำหรับผู้ดูแลระบบในการเข้าสู่ระบบรวมถึงระบบการเข้าถึงจากระยะไกล เพื่อป้องกันการโจมตีด้วย Phishing สำหรับทุกการใช้งาน โดยเฉพาะระบบอีเมล ระบบเครือข่ายภายใน และบัญชีการเข้าใช้งานระบบต่าง ๆ ที่สำคัญ	☐
5	อัปเดตแพตช์ของระบบปฏิบัติการและซอฟต์แวร์ รวมถึงติดตั้งโปรแกรมป้องกันมัลแวร์กับคอมพิวเตอร์ทุกเครื่อง และหมั่นอัปเดตโปรแกรมให้ทันสมัยอยู่เสมอ เช่น ระบบดูแลรักษา ESXi, Firewall และ VPN	☐
6	พิจารณาการใช้แผนความปลอดภัยแบบ Zero Trust บังคับใช้การยืนยันตัวตนและการอนุญาตที่เข้มงวดสำหรับการเข้าถึงทรัพยากรทุกครั้ง โดยให้สิทธิ์เข้าถึงตามหลักการของสิทธิ์น้อยที่สุด (least privilege) และตรวจสอบการเข้าถึง	☐
7	มีแผนการดำเนินการฝึกอบรมเกี่ยวกับการรู้เท่าทันภัยไซเบอร์ (Cyber Security Awareness) อย่างต่อเนื่องแก่พนักงาน	☐
8	ติดตั้ง SW ประเภท Antivirus/Anti Malware บนอุปกรณ์ เช่น โน๊ตบุค PC หรือมือถือ ที่ใช้ในหน่วยงาน เพื่อตรวจสอบและป้องกันอุปกรณ์จากมัลแวร์และแรนซัมแวร์	☐
9	ติดตั้งและกำหนดค่าไฟร์วอลล์และระบบป้องกันการบุกรุก (IPS) เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตและตรวจจับการบุกรุกที่อาจเกิดขึ้น เฝ้าระวังและตรวจสอบการจราจรในเครือข่ายอย่างต่อเนื่องเพื่อตรวจจับกิจกรรมที่ผิดปกติ	☐
10	ใช้นโยบายการควบคุมการเข้าถึง (access control policies) เพื่อให้แน่ใจว่าผู้ใช้สามารถเข้าถึงทรัพยากรที่จำเป็นหน้าที่ของตนเท่านั้น ตรวจสอบและปรับปรุงสิทธิ์การเข้าถึงอย่างสม่ำเสมอให้สอดคล้องกับความต้องการของงาน เพื่อลดความเสี่ยงจากการเข้าถึงที่ไม่ได้รับอนุญาต	☐

ลำดับ	คำแนะนำ	ดำเนินการเรียบร้อย
11	ใช้การเข้ารหัสข้อมูล ทั้งในขณะจัดเก็บและระหว่างการส่ง เพื่อป้องกันการเข้าถึงและการดักจับที่ไม่ได้รับอนุญาต ใช้มาตรฐานการเข้ารหัสที่แข็งแกร่งและอัปเดตคีย์การเข้ารหัสอย่างสม่ำเสมอ พัฒนานโยบายความเป็นส่วนตัวของข้อมูลที่ครอบคลุม โดยกำหนดวิธีการเก็บรวบรวม ใช้ จัดเก็บ และปกป้องข้อมูล ให้แน่ใจว่าสอดคล้องกับกฎระเบียบการคุ้มครองข้อมูลที่เกี่ยวข้อง และตรวจสอบแนวปฏิบัติการเข้ารหัสและนโยบายความเป็นส่วนตัวของข้อมูลเป็นประจำ	☐
12	บังคับใช้นโยบายการใช้ USB อย่างปลอดภัย จำกัดหรือห้ามการใช้ USB ที่ไม่ได้รับการอนุญาตการใช้ USB ต้องปฏิบัติตามมาตรฐานการรักษาความปลอดภัยที่ได้รับการกำหนดและจะต้องมีการตรวจสอบและควบคุมเพื่อรักษาความปลอดภัยของระบบและข้อมูลอย่างสม่ำเสมอ	☐
13	มีแผนการตรวจสอบบันทึกการเข้าใช้งาน Audit log ที่เกิดขึ้นในระบบคอมพิวเตอร์หรือระบบเครือข่าย เช่น การเข้าถึงข้อมูล การเปลี่ยนแปลงข้อมูล หรือกิจกรรมที่เกี่ยวข้องกับความปลอดภัย อย่างสม่ำเสมอ	☐
14	ในการติดตั้งอุปกรณ์ IT ควรเปลี่ยนรหัสผ่านเริ่มต้น, ปิดการใช้งานบริการที่ไม่จำเป็น, ติดตั้งเครื่องมือป้องกัน, และใช้ความคุ้มครองการเข้าถึงเพื่อรักษาความปลอดภัยในองค์กรได้อย่างมีประสิทธิภาพ	☐
15	ใช้การแบ่งแยกเครือข่าย (network segmentation) โดยใช้ Firewall แยกแยะและกำหนดขอบเขตของเครือข่ายคอมพิวเตอร์ออกเป็นพื้นที่ย่อยที่เล็กกว่าภายในเครือข่ายใหญ่ โดยที่แต่ละพื้นที่นี้จะมีการกำหนดขอบเขตและการเข้าถึงที่เฉพาะเจาะจง ลดความเสี่ยงที่ข้อมูลสำคัญจะถูกขโมยหรือถูกเข้าถึงได้โดยไม่ได้รับอนุญาตและช่วยป้องกันไม่ให้การโจมตีขยายขึ้นไปสู่ส่วนอื่นของเครือข่ายได้	☐
16	ทำการทดสอบการเจาะระบบ (penetration testing) หลังจากที่การทดสอบเจาะระบบพบช่องโหว่แล้ว การแก้ไขช่องโหว่ที่พบจะต้องดำเนินการทันทีเพื่อลดความเสี่ยงและป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตในอนาคต	☐
17	มีการตรวจสอบและประเมินสิทธิ์การเข้าถึงที่ได้รับอนุญาต (privileged access) และสิทธิ์การเข้าถึงทั่วไปของผู้ใช้ทั้งในระบบและแอปพลิเคชันต่าง ๆ ในองค์กร และการทบทวนและปรับปรุงระบบการกำหนดสิทธิ์ให้เหมาะสม เช่นการกำหนดสิทธิ์ตามหลักการสัมพันธ์งาน (least privilege principle) ฯลฯ	☐
18	มีการทดสอบการโจมตีด้วยอีเมลฟิชชิ่ง สร้างอีเมลล์ฟิชชิ่งที่มีลักษณะเหมือนกับการโจมตีจริง และตรวจสอบว่าระบบป้องกันฟิชชิ่งสามารถตรวจจับและบล็อกการโจมตีนั้นได้หรือไม่ และมีพนักงานหรือผู้บริหารคนไหนที่หลงกดลิงค์ในอีเมล์ เพื่อจะได้สร้างความตระหนักรู้ต่อไป	☐
19	ใช้มาตรการรักษาความปลอดภัยสำหรับเครื่องคอมพิวเตอร์เสมือน (VM) เช่น การใช้ VM isolation ฯลฯ เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตและการแพร่กระจายของ ransomware	☐

ลงชื่อ .....

(.....)

ตำแหน่ง.....

วันที่.....

(หัวหน้าหน่วยงาน หรือผู้รับมอบอำนาจ)

19 ข้อ | รายการตรวจสอบ ตามมาตรา 45 *

1. การควบคุม และตรวจสอบการทำงานของ outsource

การปฏิบัติ : ต้องมีการกำหนดสิทธิ์และควบคุมการเข้าถึงข้อมูลหรือระบบงาน รวมถึงมีการตรวจสอบการทำงานของทีม outsource ว่าเป็นไปตามข้อกำหนดหรือไม่ และควรมีมาตรการเอาผิดหรือบทลงโทษ หาก บริษัท outsource ละเมิดหรือทำผิดข้อกำหนดจนเป็นสาเหตุให้ถูกโจมตีทางไซเบอร์ ใส่กฎหมายข้อมูลส่วนบุคคล

2. สำรองข้อมูลอย่างสม่ำเสมอ และมี airgap

การปฏิบัติ : ดำเนินการสำรองข้อมูลสำคัญทั้งหมดอย่างสม่ำเสมอและจัดเก็บสำรองข้อมูลแบบออฟไลน์หรือในเครือข่ายแยกต่างหาก

3. ใช้รหัสผ่านที่แข็งแกร่งและไม่ซ้ำกัน

การปฏิบัติ : ให้ผู้ใช้ทุกคนสร้างรหัสผ่านที่แข็งแกร่งและใช้โปรแกรมจัดการรหัสผ่านเพื่อรักษาข้อมูลที่ไม่ซ้ำกันสำหรับบริการต่างๆ

4. เปิดใช้งานการยืนยันตัวตนหลายปัจจัย (MFA)

การปฏิบัติ : กำหนดให้มีการยืนยันตัวตนหลายปัจจัยสำหรับผู้ใช้ทุกคนเพื่อเพิ่มชั้นความปลอดภัยเพิ่มเติม

5. อัพเดตระบบและซอฟต์แวร์อย่างสม่ำเสมอ

การปฏิบัติ : อัพเดตและติดตั้งแพทช์ระบบปฏิบัติการ ซอฟต์แวร์ และแอปพลิเคชันอย่างสม่ำเสมอเพื่อป้องกันช่องโหว่ที่ทราบ

6. ฝึกอบรมความปลอดภัยอย่างสม่ำเสมอ

การปฏิบัติ : ให้การฝึกอบรมเกี่ยวกับการรับรู้ความปลอดภัยอย่างต่อเนื่องแก่พนักงานเกี่ยวกับการโจมตีแบบฟิชชิ่ง การวิศวกรรมสังคม และแนวปฏิบัติที่ดีที่สุด

7. ติดตั้งซอฟแวร์ป้องกันไวรัส

การปฏิบัติ : ติดตั้งโซลูชันการป้องกันอุปกรณ์ปลายทางเพื่อตรวจสอบและป้องกันอุปกรณ์จากมัลแวร์และแรนซัมแวร์

8. เฝ้าระวังตรวจสอบและวิเคราะห์การจราจรในเครือข่าย ใช้ไฟร์วอลล์และระบบป้องกันการบุกรุก (IPS)

การปฏิบัติ : ใช้เครื่องมือตรวจสอบเครือข่ายเพื่อตรวจจับกิจกรรมที่ไม่ปกติและภัยคุกคามที่อาจเกิดขึ้นแบบเรียลไทม์ ติดตั้งและกำหนดค่าไฟร์วอลล์และ IPS เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตและตรวจจับการบุกรุก

9. ใช้การควบคุมการเข้าถึง

การปฏิบัติ: ใช้มาตรการควบคุมการเข้าถึงที่เข้มงวดและตรวจสอบสิทธิ์อย่างสม่ำเสมอเพื่อให้แน่ใจว่าผู้ใช้เข้าถึงเฉพาะทรัพยากรที่จำเป็น

10. พัฒนาและทดสอบแผนตอบสนองเหตุการณ์ รวมทั้งผู้ให้บริการจากภายนอก

การปฏิบัติ : สร้างแผนตอบสนองเหตุการณ์ที่ครอบคลุมและดำเนินการฝึกซ้อมอย่างสม่ำเสมอเพื่อให้มั่นใจว่าพร้อมสำหรับการละเมิดข้อมูลและการโจมตีแรนซัมแวร์

11. ใช้การเข้ารหัสข้อมูล ข้อมูลส่วนบุคคล

การปฏิบัติ : ข้ารหัสข้อมูลที่จัดเก็บและที่ส่งเพื่อป้องกันการดักจับและการเข้าถึงที่ไม่ได้รับอนุญาต

12. บังคับใช้นโยบายการใช้ USB อย่างปลอดภัย

การปฏิบัติ : จำกัดการใช้และจัดการอุปกรณ์ USB อย่างปลอดภัยเพื่อป้องกันการติดมัลแวร์

13. ตรวจสอบบันทึกการเข้าใช้งาน

การปฏิบัติ : ดำเนินการตรวจสอบบันทึกการเข้าใช้งานอย่างสม่ำเสมอเพื่อตรวจจับกิจกรรมที่น่าสงสัย

14. ใช้การจัดการการกำหนดค่าอย่างปลอดภัย

การปฏิบัติ : กำหนดค่าระบบและอุปกรณ์ตามแนวปฏิบัติที่ดีที่สุดในการรักษาความปลอดภัย ค่าดีฟอลต์จากโรงงานจะเป็นสิ่งที่แฮกเกอร์ใช้การเข้าถึงระบบ

15. ใช้การแบ่งแยกเครือข่าย

การปฏิบัติ : แบ่งแยกเครือข่ายเพื่อจำกัดการแพร่กระจายของมัลแวร์และแรนซัมแวร์ในกรณีที่มีการโจมตี กั้นด้วยไฟร์วอล

16. ทำการทดสอบการเจาะระบบ

การปฏิบัติ : ดำเนินการทดสอบการเจาะระบบอย่างสม่ำเสมอเพื่อระบุช่องโหว่และปรับปรุงการป้องกัน และแก้ไขโดยเร็ว

17. ทดสอบการรับมือกับอีเมลหลอกลวง

การปฏิบัติ : ติดตั้งโซลูชันป้องกันฟิชชิ่งเพื่อตรวจจับและบล็อกอีเมลฟิชชิ่ง ทดสอบการรับมือกับเมลหลอกลวง

18. ปรับปรุงการจัดการสิทธิ์การเข้าถึง

การปฏิบัติ : ตรวจสอบและปรับปรุงการจัดการสิทธิ์การเข้าถึงของผู้ใช้เพื่อลดความเสี่ยงจากการเข้าถึงที่ไม่ได้รับอนุญาต

19. ใช้มาตรการรักษาความปลอดภัยสำหรับเครื่องคอมพิวเตอร์

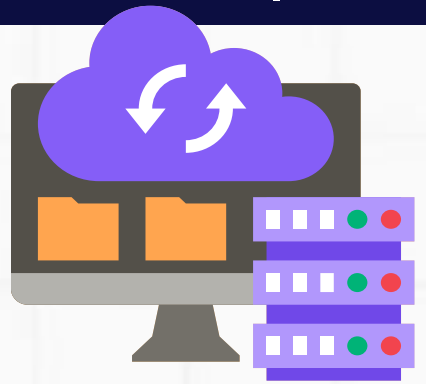
การใช้ VM isolation ฯลฯ เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตและการแพร่กระจายของ ransomware

***รายการตรวจสอบตาม มาตรา 45 ป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์**

1. การควบคุม และตรวจสอบการทำงานของ outsource

- **จำกัดการเข้าถึงข้อมูลและระบบ**ที่สำคัญเฉพาะที่จำเป็นสำหรับผู้ให้บริการในการปฏิบัติหน้าที่เท่านั้น
- ตรวจสอบว่าผู้ให้บริการ**ปฏิบัติตามมาตรฐาน**ความปลอดภัยทางไซเบอร์ที่เกี่ยวข้อง (เช่น ISO 27001, NIST)
- ดำเนินการ**ตรวจสอบและประเมินความปลอดภัย**ของผู้ให้บริการอย่างเป็นระยะเพื่อระบุและแก้ไขช่องโหว่

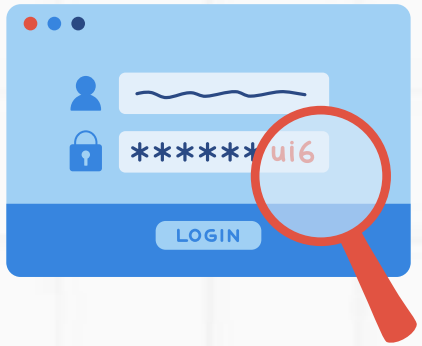
- **การปฏิบัติ** : ต้องมีการกำหนดสิทธิ์และควบคุมการเข้าถึงข้อมูลหรือระบบงาน รวมถึงมีการตรวจสอบการทำงานของทีม outsource ว่าเป็นไปตามข้อกำหนดหรือไม่ และควรมีมาตรการเอาผิดหรือบทลงโทษ หากบริษัท outsource ละเมิดหรือทำผิดข้อกำหนดจนเป็นสาเหตุให้ถูกโจมตีทางไซเบอร์



2. สำรองข้อมูลอย่างสม่ำเสมอ และมี airgap

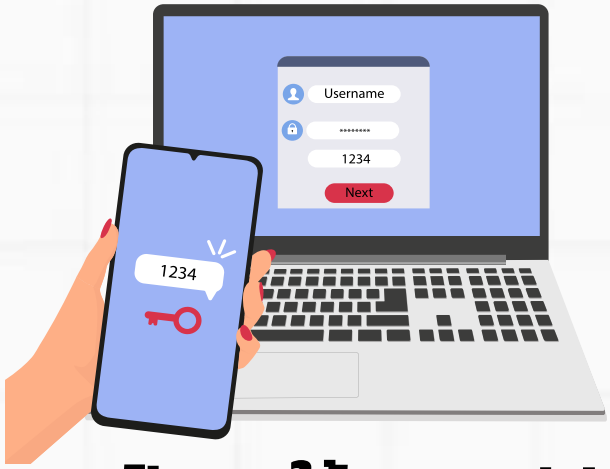
- สำรองข้อมูลที่สำคัญตามกฎ 3-2-1 โดยเก็บข้อมูลสำคัญเอาไว้ 3 ชุด ได้แก่ ข้อมูลหลัก 1 ชุด และข้อมูลสำรอง 2 ชุด
- เก็บไฟล์เหล่านั้นเอาไว้บนอุปกรณ์ที่แยกขาดจากกัน 2 ประเภท และข้อมูลสำรอง 1 ชุดเก็บไว้แบบ Offline และมีการดำเนินการสำรองข้อมูลเป็นประจำ

- **การปฏิบัติ** : ดำเนินการสำรองข้อมูลสำคัญทั้งหมดอย่างสม่ำเสมอและจัดเก็บสำรองข้อมูลแบบออฟไลน์หรือในเครือข่ายแยกต่างหาก



3. ใช้รหัสผ่านที่แข็งแกร่งและไม่ซ้ำกัน

- **บัญชีผู้ดูแล ผู้ใช้งาน ควรตั้งรหัสผ่านดังนี้**
  ตั้งรหัสผ่านอย่างน้อย 8 ตัว โดยประกอบด้วย
  ✓ตัวอักษรเล็ก (abcd)
  ✓ตัวอักษรใหญ่ (ABCD)
  ✓ตัวเลข (1234)
  ✓และสัญลักษณ์ ($#!?)
  เพื่อสร้างความหลากหลายให้กับรหัสผ่าน
- **มีการเก็บหรือจัดการกับรหัสผ่านให้มีความปลอดภัยจากการถูกแฮก**
- **หลีกเลี่ยงการตั้งรหัสผ่านเดียวกันหลายระบบ**
- **ปิดการใช้งาน "hint" หรือคำใบ้ของรหัสผ่าน**
- **เปลี่ยนรหัสผ่านอย่างสม่ำเสมอ**
- **การติดตั้งซอฟต์แวร์ทุกครั้งต้องใช้สิทธิ์ผู้ดูแลเสมอ**
- **การปฏิบัติ :** ให้ผู้ใช้สร้างรหัสผ่านที่แข็งแกร่งและใช้โปรแกรมจัดการรหัสผ่านเพื่อรักษาข้อมูลที่ไม่ซ้ำกันสำหรับบริการต่างๆ



4. เปิดใช้งานการยืนยันตัวตนหลายปัจจัย (MFA)

- **เปิดการใช้งาน Multi-Factor Authentication (MFA)** สำหรับผู้ดูแลระบบในการเข้าสู่ระบบ รวมถึงระบบการเข้าถึงจากระยะไกล
- **เพื่อป้องกันการโจมตีด้วย Phishing สำหรับทุกการใช้งานโดยเฉพาะ:**
  - ระบบอีเมล
  - ระบบเครือข่ายภายใน
  - บัญชีการเข้าใช้งานระบบต่าง ๆ ที่สำคัญ

- **การปฏิบัติ** :กำหนดให้ผู้ใช้ทุกคนต้องใช้การยืนยันตัวตนหลายปัจจัย (MFA) เพื่อเพิ่มความปลอดภัย

5. อัพเดตระบบและซอฟต์แวร์อย่างสม่ำเสมอ

- **อัปเดตแพตช์**ของระบบปฏิบัติการและซอฟต์แวร์
- **ติดตั้งโปรแกรมป้องกันมัลแวร์**กับคอมพิวเตอร์ทุกเครื่อง
- หมั่น**อัปเดตโปรแกรม**ให้ทันสมัยอยู่เสมอ เช่น:
  - ระบบดูแลรักษา ESXi
  - Firewall
  - VPN

- **การปฏิบัติ** :อัพเดตและติดตั้งแพทช์ระบบปฏิบัติการ ซอฟต์แวร์ และแอปพลิเคชันอย่างสม่ำเสมอเพื่อป้องกันช่องโหว่ที่ทราบ

6. ฝึกอบรมความปลอดภัยอย่างสม่ำเสมอ

- **จัดทำแผนการฝึกอบรมเกี่ยวกับการรู้เท่าทันภัยไซเบอร์ (Cyber Security Awareness) อย่างต่อเนื่องสำหรับพนักงาน :**
  - การระบุและหลีกเลี่ยงการโจมตีด้วยวิธี Phishing
  - การสร้างและจัดการรหัสผ่านที่ปลอดภัย
  - การใช้และรักษาอุปกรณ์ที่ปลอดภัย
  - การปฏิบัติตามนโยบายความปลอดภัยของบริษัท
  - การรายงานเหตุการณ์หรือกิจกรรมที่น่าสงสัย

- **การปฏิบัติ** : ให้การฝึกอบรมเกี่ยวกับการรับรู้ความปลอดภัยอย่างต่อเนื่องแก่พนักงานเกี่ยวกับการโจมตีแบบฟิชชิ่ง การวิศวกรรมสังคม และแนวปฏิบัติที่ดีที่สุด

7. ติดตั้งซอฟแวร์ป้องกันไวรัส

- **ติดตั้งซอฟต์แวร์ประเภท Antivirus/Anti Malware** บนอุปกรณ์ที่ใช้ในหน่วยงาน เช่น:
  - โน้ตบุ๊ก
  - PC
  - มือถือ
- **ตรวจสอบ**และป้องกันอุปกรณ์จากมัลแวร์และแรนซัมแวร์

- **การปฏิบัติ** : ใช้เครื่องมือตรวจสอบเครือข่ายเพื่อตรวจจับกิจกรรมที่ไม่ปกติและภัยคุกคามที่อาจเกิดขึ้นแบบเรียลไทม์

8. เฝ้าระวังตรวจสอบและวิเคราะห์การจราจรในเครือข่าย ใช้ไฟร์วอลล์และระบบป้องกันการบุกรุก (IPS)

- **ติดตั้งและกำหนดค่า**ไฟร์วอลล์และระบบป้องกันการบุกรุก (IPS)
- **ป้องกัน**การเข้าถึงที่ไม่ได้รับอนุญาตและตรวจจับการบุกรุกที่อาจเกิดขึ้น
- **เฝ้าระวังและตรวจสอบ**การจราจรในเครือข่ายอย่างต่อเนื่องเพื่อตรวจจับกิจกรรมที่ผิดปกติ

- **การปฏิบัติ** : ติดตั้งและกำหนดค่าไฟร์วอลล์และ IPS เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตและตรวจจับการบุกรุก

9. ใช้การควบคุมการเข้าถึง

- พิจารณาการใช้แผนความปลอดภัยแบบ Zero Trust บังคับใช้การยืนยันตัวตน
- การอนุญาตที่เข้มงวดสำหรับการเข้าถึงทรัพยากรทุกครั้ง โดยให้สิทธิ์เข้าถึงตามหลักการของสิทธิ์น้อยที่สุด (least privilege) และตรวจสอบการเข้าถึง

- **การปฏิบัติ** : ใช้มาตรการควบคุมการเข้าถึงที่เข้มงวดและตรวจสอบสิทธิ์อย่างสม่ำเสมอ เพื่อให้แน่ใจว่าผู้ใช้เข้าถึงเฉพาะทรัพยากรที่จำเป็น

10. พัฒนาและทดสอบแผนตอบสนองเหตุการณ์ รวมทั้งผู้ให้บริการจากภายนอก

- ฝึกอบรมและเพิ่มความตระหนักรู้ด้านไซเบอร์ให้แก่เจ้าหน้าที่และผู้ให้บริการ
- พัฒนาแผนการตอบสนองเหตุการณ์ (Incident Response Plan)
- ฝึกซ้อมตามแผนการตอบสนองเหตุการณ์

- **การปฏิบัติ** : สร้างแผนตอบสนองเหตุการณ์ที่ครอบคลุมและดำเนินการฝึกซ้อมอย่างสม่ำเสมอเพื่อให้มั่นใจว่าพร้อมสำหรับการละเมิดข้อมูลและการโจมตีแรนซัมแวร์

11. ใช้การเข้ารหัสข้อมูลข้อมูลส่วนบุคคล

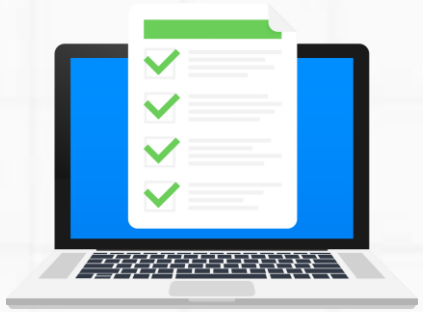
- กำหนดนโยบายการเข้ารหัสข้อมูล
- กำหนดบทบาทและสิทธิ์การเข้าถึงข้อมูลเข้ารหัส
- ทำการเข้ารหัสข้อมูลทั้งขณะเก็บรักษาและขณะถ่ายโอน
- ฝึกอบรมพนักงานเกี่ยวกับการเข้ารหัสข้อมูลเป็นระยะ

- **การปฏิบัติ** : เข้ารหัสข้อมูลที่จัดเก็บและที่ส่งเพื่อป้องกันการดักจับและการเข้าถึงที่ไม่ได้รับอนุญาต

12. บังคับใช้นโยบายการใช้ USB อย่างปลอดภัย

- **บังคับใช้นโยบายการใช้ USB** อย่างปลอดภัย โดย:
  - **จำกัดหรือห้าม**การใช้ USB ที่ไม่ได้รับการอนุญาต
  - กำหนดให้การใช้ USB ต้อง**ปฏิบัติตามมาตรฐานการรักษาความปลอดภัย**ที่กำหนด
  - **ตรวจสอบและควบคุม**การใช้ USB เพื่อรักษาความปลอดภัยของระบบและข้อมูลอย่างสม่ำเสมอ

- **การปฏิบัติ** : จำกัดการใช้และจัดการอุปกรณ์ USB อย่างปลอดภัยเพื่อป้องกันการติดมัลแวร์



13. ตรวจสอบบันทึกการเข้าใช้งาน

- มี**แผนการตรวจสอบ**บันทึกการเข้าใช้งาน (Audit log) อย่างสม่ำเสมอ โดยครอบคลุม:
  - การเข้าถึงข้อมูล
  - การเปลี่ยนแปลงข้อมูล
  - กิจกรรมที่เกี่ยวข้องกับความปลอดภัย

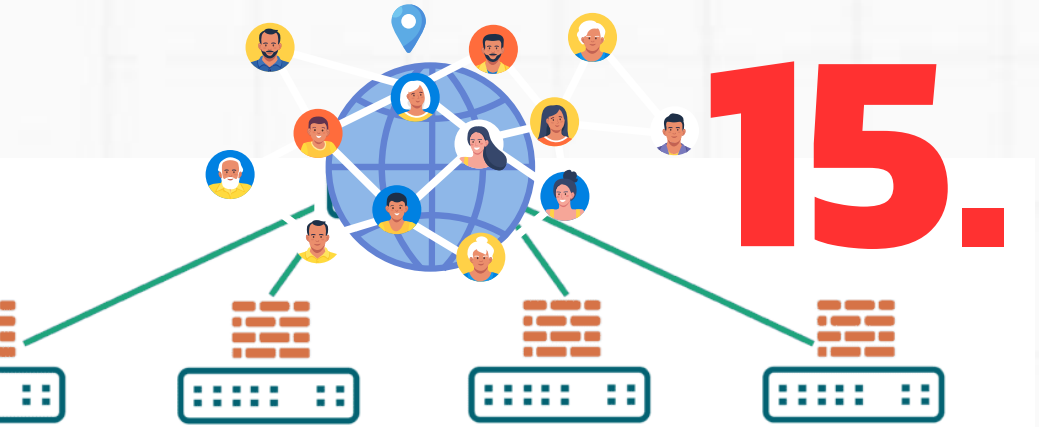
- **การปฏิบัติ** : ดำเนินการตรวจสอบบันทึกการเข้าใช้งานอย่างสม่ำเสมอเพื่อตรวจจับกิจกรรมที่น่าสงสัย

14. ใช้การจัดการการกำหนดค่าอย่างปลอดภัย

ในการติดตั้งอุปกรณ์ IT

- ค่าเริ่มต้นจากโรงงานจะเป็นสิ่งที่แฮกเกอร์ใช้การเข้าถึงระบบ
- ปกป้องการเข้าถึงข้อมูลเพื่อรักษาความปลอดภัยในองค์กรได้อย่างมีประสิทธิภาพ
- อัปเดตเฟิร์มแวร์และซอฟต์แวร์ของอุปกรณ์อย่างสม่ำเสมอ เพื่อแก้ไขช่องโหว่และปรับปรุงความปลอดภัย

- **การปฏิบัติ : เปลี่ยนรหัสผ่านเริ่มต้น, ติดตั้ง**เครื่องมือป้องกัน , **ปิด**การใช้งานบริการที่ไม่จำเป็น , **กำหนด**ค่าระบบและอุปกรณ์ตามแนวปฏิบัติที่ดีที่สุดในการรักษาความปลอดภัย



15. ใช้การแบ่งแยกเครือข่าย <Network Segmentation>

- ใช้การแบ่งแยกเครือข่าย (network segmentation) โดยใช้ Firewall กำหนดขอบเขตของเครือข่ายคอมพิวเตอร์ออกเป็นพื้นที่ย่อย
- กำหนดขอบเขตและการเข้าถึงที่เฉพาะเจาะจงแต่ละพื้นที่
- ติดตามและวิเคราะห์กิจกรรมในแต่ละโซนของเครือข่ายอย่างต่อเนื่อง เพื่อตรวจจับและตอบสนองต่อความเสี่ยงและการบุกรุกที่เป็นไปได้

- **การปฏิบัติ** : แบ่งแยกเครือข่ายเพื่อจำกัดการแพร่กระจายของมัลแวร์และแรนซัมแวร์ในกรณีที่มีการโจมตี กั้นด้วยไฟร์วอล ลดความเสี่ยงที่ข้อมูลสำคัญจะถูกขโมยหรือถูกเข้าถึงได้โดยไม่ได้รับอนุญาตและช่วยป้องกันไม่ให้การโจมตีขยายขึ้นไปสู่ส่วนอื่นของเครือข่ายได้

16. ทำการทดสอบการเจาะระบบ

- ทำการ**ทดสอบการเจาะระบบ (Penetration Testing)** อย่างสม่ำเสมอ
- เมื่อพบช่องโหว่จากการทดสอบ:
  - **แก้ไข**ช่องโหว่ที่พบทันที
  - **ลดความเสี่ยงและป้องกัน**การเข้าถึงที่ไม่ได้รับอนุญาตในอนาคต

- **การปฏิบัติ** :ดำเนินการทดสอบการเจาะระบบอย่างสม่ำเสมอ เพื่อระบุช่องโหว่และปรับปรุงการป้องกัน และแก้ไขโดยเร็ว

17. ทดสอบการรับมือกับอีเมลหลอกลวง

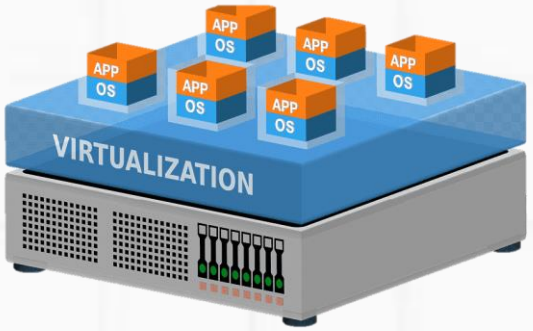
- **ตรวจสอบ**ที่อยู่อีเมลของผู้ส่ง
- **อย่าคลิกลิงก์**หรือแนบไฟล์จากอีเมลที่ไม่คุ้นเคย
- **อย่าตอบกลับ**หรือส่งข้อมูลส่วนตัวหากไม่แน่ใจ
- ใช้เทคโนโลยีตรวจสอบและ**บล็อก**อีเมลสแปม

- **การปฏิบัติ** :ติดตั้งโซลูชันป้องกันฟิชชิ่งเพื่อตรวจจับและบล็อกอีเมลฟิชชิ่งและทดสอบการรับมือกับเมลหลอกลวงเพื่อการพร้อมรับมือต่อการโจมตี

18. ปรับปรุงการจัดการสิทธิ์การเข้าถึง

- **ตรวจสอบและประเมินสิทธิ์**การเข้าถึงที่ได้รับอนุญาต (privileged access) และสิทธิ์การเข้าถึงทั่วไปของผู้ใช้ทั้งในระบบและแอปพลิเคชันต่าง ๆ ในองค์กร
- **ทบทวนและปรับปรุง**ระบบการกำหนดสิทธิ์ให้เหมาะสม โดยใช้หลักการต่าง ๆ เช่น:
  - กำหนดสิทธิ์ตามหลักการสัมพันธ์งาน (least privilege principle)

- **การปฏิบัติ** :ตรวจสอบและปรับปรุงการจัดการสิทธิ์การเข้าถึงของผู้ใช้เพื่อลดความเสี่ยงจากการเข้าถึงที่ไม่ได้รับอนุญาต



19. ใช้มาตรการรักษาความปลอดภัยสำหรับเครื่องคอมพิวเตอร์

- ใช้มาตรการรักษาความปลอดภัยสำหรับพื้นที่ของเครื่องคอมพิวเตอร์เสมือน (VM isolation) เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต
- ควบคุมการเข้าถึงและการใช้งานของ VM อย่างเข้มงวด
- ติดตั้งระบบป้องกัน malware เพื่อลดความเสี่ยงจากการแพร่กระจายของ ransomware

- **การปฏิบัติ** : ใช้ VM isolation เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต จำกัดการแพร่กระจายของ Malware