

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 : กำหนดให้มีการยืนยันตัวตนหลายปัจจัยสำหรับผู้ใช้ทุกคนเพื่อเพิ่มความปลอดภัยเพิ่มเติม



5. อัปเดตระบบและซอฟต์แวร์อย่างสม่ำเสมอ

การปฏิบัติ : อัปเดตและติดตั้งแพทช์ระบบปฏิบัติการ ซอฟต์แวร์ และแอปพลิเคชันอย่างสม่ำเสมอเพื่อป้องกันช่องโหว่ที่ทราบ



6. ฝึกอบรมความปลอดภัยอย่างสม่ำเสมอ

การปฏิบัติ : ให้การฝึกอบรมเกี่ยวกับการรับรู้ความปลอดภัยอย่างต่อเนื่องแก่พนักงานเกี่ยวกับการโจมตีแบบฟิชซิง การวิศวกรรมสังคม และแนวปฏิบัติที่ดีที่สุด



7. ติดตั้งซอฟต์แวร์ป้องกันไวรัส

การปฏิบัติ : ติดตั้งโซลูชันการป้องกันอุปกรณ์ปลายทางเพื่อตรวจสอบและป้องกันอุปกรณ์จากมัลแวร์และแรนซัมแวร์



8. ฝึกระวังตรวจสอบและวิเคราะห์การจราจรในเครือข่าย ใช้ไฟร์วอลล์และระบบป้องกันการบุกรุก (IPS)

การปฏิบัติ : ใช้เครื่องมือตรวจสอบเครือข่ายเพื่อตรวจจับกิจกรรมที่ไม่ปกติและภัยคุกคามที่อาจเกิดขึ้นแบบเรียลไทม์ ติดตั้งและกำหนดค่าไฟร์วอลล์และ IPS เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตและตรวจจับการบุกรุก



9. ใช้การควบคุมการเข้าถึง

การปฏิบัติ : ใช้มาตรการควบคุมการเข้าถึงที่เข้มงวดและตรวจสอบสิทธิ์อย่างสม่ำเสมอเพื่อให้แน่ใจว่าผู้ใช้เข้าถึงเฉพาะทรัพยากรที่จำเป็น



10. พัฒนาและทดสอบแผนตอบสนองเหตุการณ์ รวบรวมผู้ให้บริการจากภายนอก

การปฏิบัติ : สร้างแผนตอบสนองเหตุการณ์ที่ครอบคลุมและดำเนินการฝึกซ้อมอย่างสม่ำเสมอเพื่อให้มั่นใจว่าพร้อมสำหรับการละเมิดข้อมูลและการโจมตีแรนซัมแวร์



11. ใช้การเข้ารหัสข้อมูล ข้อมูลส่วนบุคคล

การปฏิบัติ : เข้ารหัสข้อมูลที่จัดเก็บและที่ส่งเพื่อป้องกันการดักจับและการเข้าถึงที่ไม่ได้รับอนุญาต



12. บังคับใช้นโยบายการใช้ USB อย่างปลอดภัย

การปฏิบัติ : จำกัดการใช้และจัดการอุปกรณ์ USB อย่างปลอดภัยเพื่อป้องกันการติดมัลแวร์



13. ตรวจสอบบันทึกการเข้าใช้งาน

การปฏิบัติ : ดำเนินการตรวจสอบบันทึกการเข้าใช้งานอย่างสม่ำเสมอเพื่อตรวจจับกิจกรรมที่น่าสงสัย



14. ใช้การจัดการการกำหนดค่าอย่างปลอดภัย

การปฏิบัติ : กำหนดค่าระบบและอุปกรณ์ตามแนวปฏิบัติที่ดีที่สุดในการรักษาความปลอดภัย ค่าดีฟอลต์จากโรงงานจะเป็นสิ่งที่แฮกเกอร์ใช้การเข้าถึงระบบ



15. ใช้การแบ่งแยกเครือข่าย

การปฏิบัติ : แบ่งแยกเครือข่ายเพื่อจำกัดการแพร่กระจายของมัลแวร์และแรนซัมแวร์ในกรณีที่มีการโจมตี กันด้วยไฟร์วอลล์



16. ทำการทดสอบการเจาะระบบ

การปฏิบัติ : ดำเนินการทดสอบการเจาะระบบอย่างสม่ำเสมอเพื่อระบุช่องโหว่และปรับปรุงการป้องกัน และแก้ไขโดยเร็ว



17. ทดสอบการรับมือกับอีเมลหลอกลวง

การปฏิบัติ : ติดตั้งโซลูชันป้องกันฟิชซิงเพื่อตรวจจับและบล็อกอีเมลฟิชซิง **ทดสอบการรับมือกับเมลหลอกลวง**



18. ปรับปรุงการจัดการสิทธิ์การเข้าถึง

การปฏิบัติ : ตรวจสอบและปรับปรุงการจัดการสิทธิ์การเข้าถึงของผู้ใช้เพื่อลดความเสี่ยงจากการเข้าถึงที่ไม่ได้รับอนุญาต

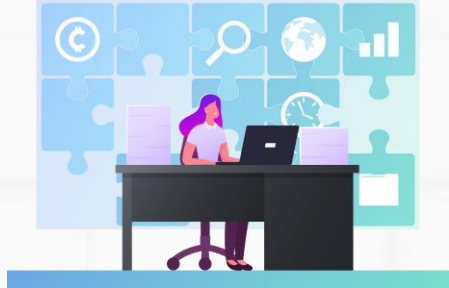
19. ใช้มาตรการรักษาความปลอดภัยสำหรับเครื่องคอมพิวเตอร์

การใช้ VM isolation ฯลฯ เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตและการแพร่กระจายของ ransomware

***รายการตรวจสอบตาม มาตรา 45 ป้องกัน รับมือและลด**

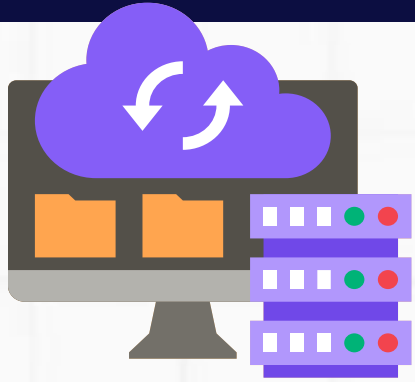
ความเสี่ยงจากภัยคุกคามทางไซเบอร์

OUTSOURCING



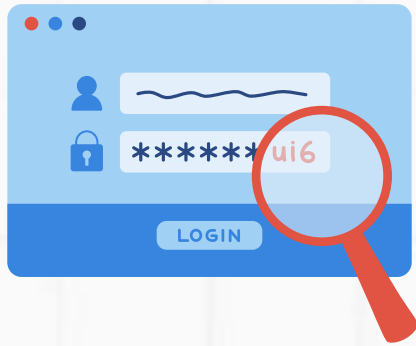
1. การควบคุม และตรวจสอบการ ทำงานของ outsource

- **จำกัดการเข้าถึงข้อมูลและระบบที่สำคัญ**
เฉพาะที่จำเป็นสำหรับผู้ให้บริการในการปฏิบัติหน้าที่เท่านั้น
- ตรวจสอบว่าผู้ให้บริการ**ปฏิบัติตามมาตรฐาน**ความปลอดภัยทางไซเบอร์ที่เกี่ยวข้อง (เช่น ISO 27001, NIST)
- ดำเนินการ**ตรวจสอบและประเมินความปลอดภัย**ของผู้ให้บริการอย่างเป็นระยะเพื่อระบุและแก้ไขช่องโหว่
- **การปฏิบัติ** : ต้องมีการกำหนดสิทธิ์และควบคุมการเข้าถึงข้อมูลหรือระบบงาน รวมถึงมีการตรวจสอบการทำงานของทีม outsource ว่าเป็นไปตามข้อกำหนดหรือไม่ และควรมีมาตรการเอาผิดหรือบทลงโทษ หากบริษัท outsource ละเมิดหรือทำผิดข้อกำหนดจนเป็นสาเหตุให้ถูกโจมตีทางไซเบอร์



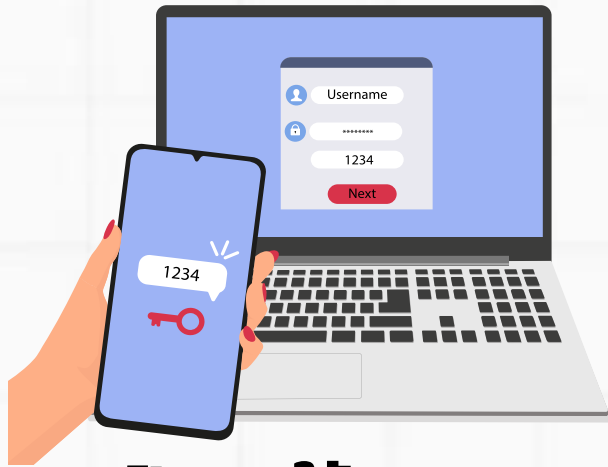
2. สำรองข้อมูลอย่างสม่ำเสมอ และมี airgap

- สำรองข้อมูลที่สำคัญตามกฎหมาย 3-2-1 โดยเก็บข้อมูลสำคัญเอาไว้ 3 ชุด ได้แก่ ข้อมูลหลัก 1 ชุด และข้อมูลสำรอง 2 ชุด
- เก็บไฟล์เหล่านั้นเอาไว้บนอุปกรณ์ที่แยกขาดจากกัน 2 ประเภท และข้อมูลสำรอง 1 ชุดเก็บไว้แบบ Offline และมีการดำเนินการสำรองข้อมูลเป็นประจำ
- **การปฏิบัติ :** ดำเนินการสำรองข้อมูลสำคัญทั้งหมดอย่างสม่ำเสมอและจัดเก็บสำรองข้อมูลแบบออฟไลน์หรือในเครือข่ายแยกต่างหาก



3. ใช้รหัสผ่านที่แข็งแกร่ง และไม่ซ้ำกัน

- **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 :** กำหนดให้ผู้ใช้ทุกคน ต้องใช้การยืนยันตัวตนหลายปัจจัย (MFA) เพื่อเพิ่มความปลอดภัย



5. อัปเดตระบบและซอฟต์แวร์ อย่างสม่ำเสมอ

- อัปเดตแพตช์ของระบบปฏิบัติการและซอฟต์แวร์
- ติดตั้งโปรแกรมป้องกันมัลแวร์กับคอมพิวเตอร์ทุกเครื่อง
- หมั่นอัปเดตโปรแกรมให้ทันสมัยอยู่เสมอ เช่น:
 - ระบบดูแลรักษา ESXi
 - Firewall
 - VPN

- **การปฏิบัติ** : อัปเดตและติดตั้งแพทช์ระบบปฏิบัติการซอฟต์แวร์ และแอปพลิเคชันอย่างสม่ำเสมอเพื่อป้องกันช่องโหว่ที่ทราบ



6. ฝึกอบรมความปลอดภัย อย่างสม่ำเสมอ

- จัดทำแผนการฝึกอบรมเกี่ยวกับการรู้เท่าทันภัยไซเบอร์ (Cyber Security Awareness) อย่างต่อเนื่องสำหรับพนักงาน :

- การระบุและหลีกเลี่ยงการโจมตีด้วยวิธี Phishing
- การสร้างและจัดการรหัสผ่านที่ปลอดภัย
- การใช้และรักษาอุปกรณ์ที่ปลอดภัย
- การปฏิบัติตามนโยบายความปลอดภัยของบริษัท
- การรายงานเหตุการณ์หรือกิจกรรมที่น่าสงสัย

- **การปฏิบัติ** : ให้การฝึกอบรมเกี่ยวกับการรับรู้ความปลอดภัยอย่างต่อเนื่องแก่พนักงานเกี่ยวกับการโจมตีแบบฟิชซึ่งการวิศวกรรมสังคม และแนวปฏิบัติที่ดีที่สุด



7. ติดตั้งซอฟต์แวร์ ป้องกันไวรัส

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

- **การปฏิบัติ** : ใช้เครื่องมือตรวจสอบเครือข่ายเพื่อตรวจจับกิจกรรมที่ไม่ปกติและภัยคุกคามที่อาจเกิดขึ้นแบบเรียลไทม์



8. เฝ้าระวังตรวจสอบและวิเคราะห์ การจราจรในเครือข่าย ใช้ไฟร์วอลล์และระบบป้องกัน การบุกรุก (IPS)

- **ติดตั้งและกำหนดค่าไฟร์วอลล์และระบบ** ป้องกันการบุกรุก (IPS)
- **ป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตและ** ตรวจจับการบุกรุกที่อาจเกิดขึ้น
- **เฝ้าระวังและตรวจสอบ** การจราจรใน เครือข่ายอย่างต่อเนื่องเพื่อตรวจจับ กิจกรรมที่ผิดปกติ
- **การปฏิบัติ :** ติดตั้งและ กำหนดค่าไฟร์วอลล์และ IPS เพื่อ ป้องกันการเข้าถึงที่ไม่ได้รับ อนุญาตและตรวจจับการบุกรุก



9.

ใช้การควบคุมการเข้าถึง

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

- **การปฏิบัติ** : ใช้มาตรการควบคุมการเข้าถึงที่เข้มงวดและตรวจสอบสิทธิ์อย่างสม่ำเสมอ เพื่อให้แน่ใจว่าผู้ใช้เข้าถึงเฉพาะทรัพยากรที่จำเป็น



10. พัฒนาและทดสอบแผน ตอบสนองเหตุการณ์ รวมทั้งผู้ให้บริการจากภายนอก

- ฝึกอบรมและเพิ่มความตระหนักรู้ด้านไซเบอร์ให้แก่เจ้าหน้าที่และผู้ให้บริการ
- พัฒนาแผนการตอบสนองเหตุการณ์ (Incident Response Plan)
- ฝึกซ้อมตามแผนการตอบสนองเหตุการณ์

- **การปฏิบัติ** : สร้างแผนตอบสนองเหตุการณ์ที่ครอบคลุมและดำเนินการฝึกซ้อมอย่างสม่ำเสมอเพื่อให้มั่นใจว่าพร้อมสำหรับการละเมิดข้อมูลและการโจมตีแรนซัมแวร์



11. ใช้การเข้ารหัสข้อมูล ข้อมูลส่วนบุคคล

- 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. ตรวจสอบบันทึก การเข้าใช้งาน

- มีแผนการตรวจสอบบันทึกการเข้าใช้งาน (Audit log) อย่างสม่ำเสมอ โดยครอบคลุม:
 - การเข้าถึงข้อมูล
 - การเปลี่ยนแปลงข้อมูล
 - กิจกรรมที่เกี่ยวข้องกับความปลอดภัย

- **การปฏิบัติ** : ดำเนินการตรวจสอบบันทึกการเข้าใช้งานอย่างสม่ำเสมอเพื่อตรวจจับกิจกรรมที่น่าสงสัย

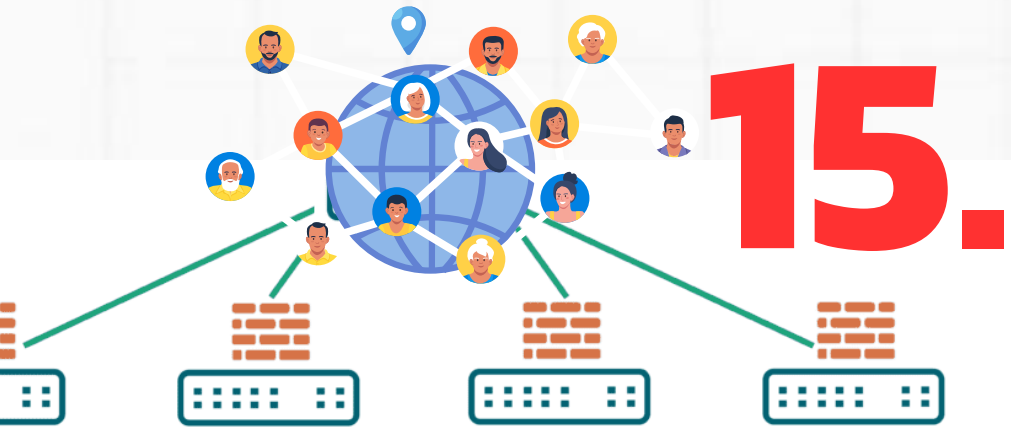


14. ใช้การจัดการการ กำหนดค่าอย่างปลอดภัย

ในการติดตั้งอุปกรณ์ IT

- ค่าเริ่มต้นจากโรงงานจะเป็นสิ่งที่แฮกเกอร์
ใช้การเข้าถึงระบบ
- ปกป้องการเข้าถึงข้อมูลเพื่อรักษาความ
ปลอดภัยในองค์กรได้อย่างมีประสิทธิภาพ
- อัปเดตเฟิร์มแวร์และซอฟต์แวร์ของอุปกรณ์
อย่างสม่ำเสมอ เพื่อแก้ไขช่องโหว่และ
ปรับปรุงความปลอดภัย

- การปฏิบัติ : เปลี่ยนรหัสผ่าน
เริ่มต้น, ติดตั้งเครื่องมือป้องกัน
, ปิดการใช้งานบริการที่ไม่จำเป็น
, กำหนดค่าระบบและอุปกรณ์
ตามแนวปฏิบัติที่ดีที่สุดในการ
รักษาความปลอดภัย



15. ใช้การแบ่งแยกเครือข่าย <Network Segmentation>

- ใช้การแบ่งแยกเครือข่าย (network segmentation) โดยใช้ Firewall กำหนดขอบเขตของเครือข่ายคอมพิวเตอร์ออกเป็นพื้นที่ย่อย
- กำหนดขอบเขตและการเข้าถึงที่เฉพาะเจาะจงแต่ละพื้นที่
- ติดตามและวิเคราะห์กิจกรรมในแต่ละโซนของเครือข่ายอย่างต่อเนื่อง เพื่อตรวจจับและตอบสนองต่อความเสี่ยงและการบุกรุกที่เป็นไปได้
- **การปฏิบัติ :** แบ่งแยกเครือข่ายเพื่อจำกัดการแพร่กระจายของมัลแวร์และแรนซัมแวร์ในกรณีที่มีการโจมตี กันด้วยไฟร์วอลล์ ลดความเสี่ยงที่ข้อมูลสำคัญจะถูกขโมยหรือถูกเข้าถึงได้โดยไม่ได้รับอนุญาตและช่วยป้องกันไม่ให้การโจมตีขยายขึ้นไปยังส่วนอื่นของเครือข่ายได้



16. **ทำการทดสอบการเจาะระบบ**

- **ทำการทดสอบการเจาะระบบ (Penetration Testing) อย่างสม่ำเสมอ**
- เมื่อพบช่องโหว่จากการทดสอบ:
 - **แก้ไขช่องโหว่ที่พบทันที**
 - **ลดความเสี่ยงและป้องกันการเข้าถึงที่ไม่ได้รับอนุญาตในอนาคต**

- **การปฏิบัติ** :ดำเนินการทดสอบการเจาะระบบอย่างสม่ำเสมอเพื่อระบุช่องโหว่และปรับปรุงการป้องกัน และแก้ไขโดยเร็ว



17. ทดสอบการรับมือกับอีเมล หลอกลวง

- ตรวจสอบที่อยู่อีเมลของผู้ส่ง
- อย่าคลิกลิงก์หรือแนบไฟล์จากอีเมลที่ไม่คุ้นเคย
- อย่าตอบกลับหรือส่งข้อมูลส่วนตัวหากไม่แน่ใจ
- ใช้เทคโนโลยีตรวจสอบและบล็อกอีเมลสแปม

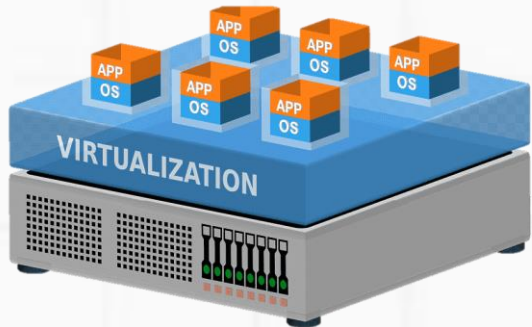
- **การปฏิบัติ** : ติดตั้งโซลูชันป้องกันฟิชชิ่งเพื่อตรวจจับและบล็อกอีเมลฟิชชิ่งและทดสอบการรับมือกับเมลหลอกลวงเพื่อการพร้อมรับมือต่อการโจมตี



18. ปรับปรุงการจัดการสิทธิ์การเข้าถึง

- **ตรวจสอบและประเมินสิทธิ์การเข้าถึง** ที่ได้รับอนุญาต (privileged access) และสิทธิ์การเข้าถึงทั่วไปของผู้ใช้ทั้งในระบบและแอปพลิเคชันต่าง ๆ ในองค์กร
- **ทบทวนและปรับปรุง** ระบบการกำหนดสิทธิ์ให้เหมาะสม โดยใช้หลักการต่าง ๆ เช่น:
 - กำหนดสิทธิ์ตามหลักการสัมพันธงาน (least privilege principle)

- **การปฏิบัติ** : ตรวจสอบและปรับปรุงการจัดการสิทธิ์การเข้าถึงของผู้ใช้เพื่อลดความเสี่ยงจากการเข้าถึงที่ไม่ได้รับอนุญาต



19. ใช้มาตรการรักษาความปลอดภัย ปลอดภัยสำหรับเครื่อง คอมพิวเตอร์

- ใช้มาตรการรักษาความปลอดภัยสำหรับพื้นที่ของเครื่องคอมพิวเตอร์เสมือน (VM isolation) เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต
- ควบคุมการเข้าถึงและการใช้งานของ VM อย่างเข้มงวด
- ติดตั้งระบบป้องกัน malware เพื่อลดความเสี่ยงจากการแพร่กระจายของ ransomware
- **การปฏิบัติ** : ใช้ VM isolation เพื่อป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต จำกัดการแพร่กระจายของ Malware