เพื่อให้มั่นใจถึงประสิทธิภาพของการท าการรักษาความปลอดภัยและตรงตาม วัตถุประสงค์ของ CIA ทางองค์กรต้องทำการดำเนินการประเมินความปลอดภัยอยู่เป็น ประจำซึ่งรวมถึงการทดสอบการเจาะระบบอีกด้วย โดยการระบุช่องโหว่กับช่องว่างใน การควบคุมความปลอดภัยออกมาอย่างชัดเจน ทำให้องค์กรสามารถทำการปรับปรุงด้าน ความปลอดภัยได้อย่างเป็นขั้นเป็นตอน

Performance Development Review (PDR) เป็นกระบวนการประเมินผลและวางแผนพัฒนาทักษะของพนักงาน โดยมุ่งเน้นการตรวจสอบประสิทธิภาพการทำงาน ช่วยให้พนักงานเข้าใจเป้าหมายขององค์กรและหาวิธีการพัฒนา

63010519 นันทวัฒน์ รัตนเรืองวิมาน

63010519 นันทวัฒน์ รัตนเรืองวิมาน

ผลที่ตามมาของการโจมตีเครือข่ายที่ประสบความสำเร็จ อาจรุนแรงและรวมถึงการสูญเสียทางการเงิน ความ เสียหายต่อชื่อเสียง และผลทางกฎหมายและข้อบังคับ ตัวอย่างเช่น การโจมตีที่ประสบความสำเร็จอาจส่งผลให้ เกิดการขโมยข้อมูลที่ละเอียดอ่อน สิ่งนี้อาจนำไปสู่การ สูญเสียทางการเงิน นอกจากนี้ การโจมตีที่ประสบ ความสำเร็จอาจทำลายชื่อเสียงขององค์กรและทำลายความ ไว้วางใจของลูกค้า ซึ่งอาจส่งผลกระทบระยะยาวต่อผลกำไร ขององค์กร เพื่อลดผลกระทบเหล่านี้ องค์กรควรมีแผน รับมือเหตุการณ์ที่มีประสิทธิภาพซึ่งรวมถึงขั้นตอนในการ ตรวจจับและตอบสนองต่อเหตุการณ์ด้านความปลอดภัย ภายในองค์กร และส่งเสริมความตระหนักด้านความ ปลอดภัยและการศึกษาแก่พนักงานทุกระดับ

จุดประสงค์หลักของการทำ network topology diagram เนื่องจากเป็นรูปที่ แสดงระบบ network ทั้งแบบ physical ที่จะเห็นแค่รูปภาพโครงสร้างและในแบบ logical ที่จะแสดงทั้งรูปแบบการต่อต่ออย่างไรและมีเลข IP อะไรอยู่ตรงไหนบ้างอีกทั้งการทำ diagram ช่วยลดการผิดพลาดและช่วยทำให้การหาข้อผิดพลาดเมื่อเกิดขึ้น ทำได้ง่ายขึ้น

63010519 นันทวัฒน์ รัตนเรืองวิมาน

63010519 นันทวัฒน์ รัตนเรืองวิมาน

มีไฟร์วอลล์หลายประเภท เช่น packet filtering firewalls stateful inspection firewalls application layer firewalls และ next-generation firewalls แต่ละประเภทมีจุดแข็งและจุดอ่อน องค์กร ควรประเมินความต้องการอย่างรอบคอบและเลือก ประเภทไฟร์วอลล์ที่ตรงกับความต้องการมากที่สุด

Stateful firewall สามารถทำการติดตามสถานะของการเชื่อมต่อโดยการบันทึก เก็บไว้อยู่ในแพ็คเก็ตแต่เมื่อมองใน stateless firewall นั้นจะท าการดูทีละแพ็คเก็ต เป็นตัวๆ ไป โดยไม่รู้ว่ามีแพ็คเก็ตใดไปก่อนหน้าหรือกำลังจะมา อีกทั้ง stateful firewall นั้นมีความสามารถในการป้องกันได้ดีกว่า แต่ในเชิงประสิทธิภาพนั้น stateless firewall นั้นดีกว่า

63010519 นันทวัฒน์ รัตนเรืองวิมาน

63010519 นันทวัฒน์ รัตนเรืองวิมาน

เป็น software ที่ใช้ในการรักษาความปลอดภัยที่จะช่วยเครื่องคอมพิวเตอร์จากการ โดน virus, malware และอื่นๆ โดยการทำงานจะทำการสแกนไฟล์และโปรแกรม บนเครื่องเพื่อหาสิ่งปกติและหากเจอจะทำการนำออกทันที

เพื่อให้มั่นใจถึงประสิทธิภาพของเครื่องมือรักษาความปลอดภัย องค์กร ควรทดสอบและประเมินสถานะการรักษาความปลอดภัยเป็นประจำผ่าน การทดสอบการเจาะระบบ การประเมินช่องโหว่ และการประเมินความ ปลอดภัยอื่นๆ พวกเขาควรตรวจสอบเครื่องมือรักษาความปลอดภัยเพื่อ หาผลบวกปลอมหรือผลลบปลอม และตรวจสอบนโยบายและขั้นตอน ความปลอดภัยเป็นประจำเพื่อให้แน่ใจว่ามีความทันสมัยและมี ประสิทธิภาพในการต่อต้านภัยคุกคามในปัจจุบัน เมื่อเลือกเครื่องมือ รักษาความปลอดภัยใหม่ องค์กรควรพิจารณาปัจจัยต่างๆ เช่น งบประมาณ ข้อกำหนดด้านความปลอดภัย การผสานรวมกับระบบที่มี อยู่ ข้อกำหนดด้านการจัดการและการบำรุงรักษา และชื่อเสียงและ ประวัติของผู้ขาย พวกเขาควรประเมินความสามารถและคุณลักษณะของ เครื่องมือรักษาความปลอดภัยต่างๆ และเลือกเครื่องมือที่เหมาะสมที่สุด กับความต้องการด้านความปลอดภัยและสภาพแวดล้อมเฉพาะของตน

63010519 นันทวัฒน์ รัตนเรืองวิมาน

63010519 นันทวัฒน์ รัตนเรืองวิมาน

เพื่อให้มั่นใจถึงประสิทธิผลของกระบวนการตอบสนองต่อเหตุการณ์ องค์กรควรทดสอบและประเมินincident response planอย่าง สม่ำเสมอผ่านการฝึกบนโต๊ะและการโจมตีจำลอง พวกเขาควรตรวจสอบ ให้แน่ใจว่าผู้มีส่วนได้ส่วนเสียทั้งหมดได้รับการฝึกอบรมอย่างถูกต้องและ ตระหนักถึงบทบาทและความรับผิดชอบของตนในระหว่างเหตุการณ์ ด้านความปลอดภัย นอกจากนี้ องค์กรควรตรวจสอบสภาพแวดล้อมของ ตนอย่างต่อเนื่องเพื่อหาสัญญาณของเหตุการณ์ด้านความปลอดภัย และ ดูแลรักษา playbooks การตอบสนองต่อเหตุการณ์ที่เป็นปัจจุบัน ซึ่ง สะท้อนถึงข่าวกรองภัยคุกคามในปัจจุบันและแนวทางปฏิบัติที่ดีที่สุด

แผนรับมือเหตุการณ์มักจะเกี่ยวข้องกับขั้นตอนสำคัญหลายขั้นตอน รวมถึงการเตรียมการ การระบุ การกักกัน การกำจัด การกู้คืน และ บทเรียนที่ได้รับ ในระหว่างขั้นตอนการเตรียมการ องค์กรต่างๆ จะ กำหนดนโยบายและขั้นตอนการตอบสนองต่อเหตุการณ์ ระบุผู้มีส่วนได้ ส่วนเสียและบทบาทที่สำคัญ และพัฒนาคู่มือการรับมือเหตุการณ์ ขั้นตอนการระบุเกี่ยวข้องกับการตรวจหาและจำแนกเหตุการณ์ด้าน ความปลอดภัย ในขณะที่ขั้นตอนการกักกันเกี่ยวข้องกับการแยกระบบที่ ได้รับผลกระทบและป้องกันความเสียหายเพิ่มเติม ขั้นตอนการกำจัด เกี่ยวข้องกับการลบต้นตอของเหตุการณ์ ในขณะที่ขั้นตอนการกู้คืน เกี่ยวข้องกับการคืนค่าการทำงานตามปกติและตรวจสอบให้แน่ใจว่า ข้อมูลได้รับการสำรองอย่างเหมาะสม ขั้นสุดท้าย บทเรียนที่ได้รับจะ เกี่ยวข้องกับการประเมินประสิทธิผลของincident response plan และระบุจุดที่ต้องปรับปรุง

63010519 นันทวัฒน์ รัตนเรืองวิมาน

63010519 นันทวัฒน์ รัตนเรืองวิมาน

เป็นช่องโหว่ของเว็บที่อนุญาตให้มีการใส่ code ที่เป็นอันตรายลงไปในหน้าเว็บที่ผู้ใช้ รายอื่นก าลังใช้งานอยู่ สิ่งนี้ท าเพื่อขโมยข้อมูลที่มีความละเอียดอ่อนอย่าง password ในการป้องกันการโจมตีต้องมีการตรวจสอบ input ของผู้ใช้งานก่อนท าการแสดงผล หน้าเว็บ

ช่องโหว่ด้านความปลอดภัยของเว็บประเภททั่วไป ได้แก่ injection attacks cross-site scripting (XSS) broken authentication and session management การอ้างอิง วัตถุโดยตรงที่ไม่ปลอดภัย, การกำหนดค่าความปลอดภัย ผิดพลาด และการบันทึกและการตรวจสอบไม่เพียงพอ

63010519 นันทวัฒน์ รัตนเรืองวิมาน

63010519 นันทวัฒน์ รัตนเรืองวิมาน

WPA2 ย่อมาจาก Wi-Fi Protected Access 2 ซึ่งเป็นโปรโตคอลความ ปลอดภัยที่ใช้ในเครือข่าย LAN ไร้สาย ช่วยเพิ่มความปลอดภัยโดยใช้ AES และให้การ ควบคุมความปลอดภัยที่แข็งแกร่งขึ้นสำหรับการตรวจสอบผู้ใช้WPA2 ยังใช้ keyที่ไม่ ซ้ำกันสำหรับการเชื่อมต่อแต่ละครั้งซึ่งทำให้แฮกเกอร์สามารถถอดรหัสการรับส่งข้อมูลไร้ สายและเข้าถึงเครือข่ายได้ยากขึ้น.

ปัจจุบัน WPA2 เป็นโปรโตคอลการเข้ารหัส WLAN ที่ปลอดภัย ที่สุด เนื่องจากมีการเข้ารหัสที่แรงกว่าและคุณสมบัติด้านความ ปลอดภัยที่ดีกว่า WEP และ WPA อย่างไรก็ตาม สิ่งสำคัญคือ ต้องทราบว่าแม้แต่ WPA2 ก็สามารถเสี่ยงต่อการโจมตีบางอย่าง ได้ เช่น การโจมตีด้วยกำลังดุร้ายกับรหัสผ่านที่ไม่รัดกุม นอกจากนี้ องค์กรควรอัปเดตโปรโตคอลความปลอดภัย WLAN อย่างสม่ำเสมอ และตรวจสอบปัญหาด้านความปลอดภัยที่อาจ เกิดขึ้นเพื่อรักษาความปลอดภัยของ WLAN

63010519 นันทวัฒน์ รัตนเรืองวิมาน

63010519 นันทวัฒน์ รัตนเรืองวิมาน

เป็น access point ที่ไม่ได้รับการยืนยันหรือทราบจากผู้ดูแลระบบ access point นี้สามารถใช้งานได้เหมือน access point ปกติแต่เมื่อเชื่อมต่อแล้วทำให้ผู้ โจมตีสามารถเข้าไปล้วงข้อมูลละเอียดอ่อนอย่าง password หรือเลขบัตรเครดิต ซึ่ง ควรใช้ระบบการป้องกันแบบไร้สาย (WIPS) ซึ่งมีความสามารถในการตรวจจับและ ป้องกัน access point ที่อยู่นอกเครือข่าย และสามารถลบ access point ที่ถูก แอบเข้ามาติดตั้งรวมทั้งระบุจุดได้ด้วย

การกำหนดเป้าหมายการบริหารความเสี่ยง (Objective Setting)

63010519 นันทวัฒน์ รัตนเรืองวิมาน

63010519 นันทวัฒน์ รัตนเรืองวิมาน

63010519 นันทวัฒน์ รัตนเรืองวิมาน

63010519 นันทวัฒน์ รัตนเรืองวิมาน

63010519 นันทวัฒน์ รัตนเรืองวิมาน

63010519 นันทวัฒน์ รัตนเรืองวิมาน

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ของไทย มีผลบังคับใช้กับบริษัทต่างชาติที่ดำเนินธุรกิจใน ประเทศไทย และต้องรับโทษและดำเนินการบังคับเช่นเดียวกับ บริษัทไทย ซึ่งรวมถึงค่าปรับที่อาจเกิดขึ้น การจำคุก และการ ยึดระบบและข้อมูลคอมพิวเตอร์ กฎหมายดังกล่าวถูกนำมาใช้ เพื่อดำเนินคดีกับบุคคลและบริษัทต่างชาติสำหรับกิจกรรม ออนไลน์ที่ละเมิดกฎหมาย เช่น การโพสต์เนื้อหาที่ถือว่าหมิ่น ประมาทหรือวิพากษ์วิจารณ์สถาบันกษัตริย์ บริษัทต่างชาติที่ ดำเนินกิจการในประเทศไทยจึงต้องรับทราบข้อกำหนดของ CCA และตรวจสอบให้แน่ใจว่ากิจกรรมออนไลน์ของพวกเขา เป็นไปตามกฎหมาย

พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลของไทย ( PDPA ) เป็นกฎหมายคุ้มครอง ข้อมูลและกฎหมายความเป็นส่วนตัวที่ดำเนินการในประเทศไทยในปี 2563 บทบัญญัติที่ สำคัญของมันรวมถึงข้อกำหนดสำหรับการได้รับความยินยอมสำหรับการประมวลผล ข้อมูลสิทธิการปกป้องข้อมูลที่เพิ่มขึ้นสำหรับบุคคลและเพิ่มความรับผิดชอบและ บทลงโทษสำหรับองค์กรที่ไม่ปฏิบัติตามกฎระเบียบ. PDPA ใช้กับทุกองค์กรที่ ประมวลผลข้อมูลส่วนบุคคลของบุคคลในประเทศไทยโดยไม่คำนึงถึงองค์กรที่เป็นฐาน. ธุรกิจที่ไม่ปฏิบัติตาม PDPA อาจต้องเสียค่าปรับจ าคุกหรือทั้งสองอย่าง.

เป็นมาตรฐานสากลสำหรับระบบการจัดการความปลอดภัยของข้อมูล ( ISMS ) สำหรับองค์กรในการสร้างด าเนินการบำรุงรักษาและปรับปรุงแนวทางปฏิบัติด้านความ ปลอดภัยของข้อมูลอย่างต่อเนื่อง วัตถุประสงค์ของการรับรอง ISO 27001 คือเพื่อ แสดงให้เห็นถึงความสนใจว่าองค์กรได้ใช้ระบบการจัดการความปลอดภัยข้อมูลที่ ครอบคลุมและมีประสิทธิภาพ ในการขอรับการรับรององค์กรจะต้องได้รับการตรวจสอบ อย่างจากหน่วยงานรับรองบุคคลที่สามเพื่อตรวจสอบว่า ISMS ขององค์กรสอดคล้อง กับข้อกำหนดของมาตรฐาน ISO 27001

ส่วนประกอบที่สำคัญของ ISMS ที่เป็นไปตามมาตรฐาน ISO 27001 ได้แก่ การประเมินความเสี่ยง การรักษาความเสี่ยง นโยบายและขั้นตอนการรักษาความปลอดภัยของข้อมูล การ ควบคุมการเข้าถึง และการฝึกอบรมและการรับรู้ การนำ องค์ประกอบเหล่านี้ไปใช้ องค์กรสามารถสร้าง ISMS ที่มี ประสิทธิภาพซึ่งช่วยให้พวกเขาจัดการความเสี่ยงด้านความ ปลอดภัยของข้อมูลได้