TLP:CLEAR

การปรับสมดุลของความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์: หลักการและวิธีการสำหรับระบบความปลอดภัยโดยการออกแบบและโดยการตั้งค่าเริ่มต้น

ตีพิมพ์เผยแพร่เมื่อวันที่ 13 เมษายน 2023

คณะกรรมาธิการความมั่นคงปลอดภัยทางไซเบอร์และโครงสร้างพื้นฐาน

NSA | FBI | ACSC | NCSC-UK | CCCS | BSI | NCSC-NL | CERT NZ | NCSC-NZ

สารบัญ

ภาพรวม: จุดอ่อนที่เกิดจากการออกแบบ

เทคโนโลยีถูกผนวกรวมเข้ากับเกือบทุกแง่มุมของชีวิตประจำวัน ระบบที่ใช้อินเทอร์เน็ตเชื่อมต่อกับระบบต่าง ๆ ที่สำคัญซึ่งส่งผลกระทบโดยตรงต่อความมั่งคั่งทางเศรษฐกิจ การดำรงชีวิต และแม้แต่สุขภาพของเรา ตั้งแต่การจัดการอัตลักษณ์ส่วนบุคคลไปจนถึงการดูแลทางการแพทย์ ยกเพียงตัวอย่างเดียว เช่น การละเมิดทางไซเบอร์ได้ส่งผลให้โรงพยาบาลต้องยกเลิกการผ่าตัดและเปลี่ยนทิศทางการดูแลผู้ป่วยทั่วโลก เทคโนโลยีและจุดอ่อนที่ไม่มีความมั่นคงปลอดภัยในระบบที่สำคัญอาจเปิดทางให้เกิดการบุกรุกทางไซเบอร์ที่เป็นอันตรายซึ่งนำไปสู่ความเสี่ยงด้านความปลอดภัย[1]ที่อาจเกิดขึ้นอย่างรุนแรงได้

โดยเฉพาะอย่างยิ่งในปัจจุบันนี้ เป็นสิ่งสำคัญที่ผู้ผลิตเทคโนโลยีต้องสร้างระบบความปลอดภัยโดยการออกแบบ (Secure-by-Design) และความปลอดภัยโดยการตั้งค่าเริ่มต้น (Secure-by-Default) เป็นจุดสำคัญของกระบวนการออกแบบและพัฒนาผลิตภัณฑ์ ผู้จัดจำหน่ายบางรายได้ก้าวกระโดดโดยผลักดันอุตสาหกรรมไปข้างหน้าด้วยการรับประกันซอฟต์แวร์ในขณะที่บางรายยังล้าหลังอยู่ คณะผู้จัดทำเอกสารสนับสนุนให้ผู้ผลิตเทคโนโลยีทุกรายสร้างผลิตภัณฑ์ของตนในลักษณะที่ป้องกันไม่ให้ลูกค้าต้องดำเนินการเฝ้าระวัง การอัปเดตตามเวลา และการควบคุมความเสียหายของระบบอย่างต่อเนื่องเพื่อรับมือกับการบุกรุกทางไซเบอร์ ผู้ผลิตได้รับการสนับสนุนให้เกิดความรู้สึกของการเป็นเจ้าของเพื่อรับผิดชอบต่อการปรับปรุงผลลัพธ์ด้านความมั่นคงปลอดภัยให้กับลูกค้าของตน ในอดีต ผู้ผลิตเทคโนโลยีได้อาศัยการแก้ไขจุดอ่อนที่ลูกค้าพบหลังจากที่ได้นำผลิตภัณฑ์ไปปรับใช้งานแล้ว ซึ่งกำหนดให้ลูกค้าต้องแก้ไขด้วยการใช้แพตช์ (Patch) เหล่านั้นโดยเสียค่าใช้จ่ายเอง โดยการผสมผสานแนวปฏิบัติตามหลักความมั่นคงปลอดภัยด้วยการออกแบบเท่านั้นที่เราจะสามารถทำลายวงจรปัญหาของการสร้างและการหาทางแก้ไขได้

เพื่อให้บรรลุมาตรฐานความมั่นคงปลอดภัยของซอฟต์แวร์ระดับสูงได้สำเร็จ คณะผู้จัดทำเอกสารจึงสนับสนุนให้ผู้ผลิตจัดลำดับความสำคัญของการบูรณาการความมั่นคงปลอดภัยของผลิตภัณฑ์ให้เป็นข้อกำหนดเบื้องต้นที่สำคัญสำหรับคุณลักษณะและความรวดเร็วในการออกสู่ตลาด เมื่อเวลาผ่านไป ทีมวิศวกรจะสามารถสร้างจังหวะความสม่ำเสมอใหม่ที่ผนวกความมั่นคงปลอดภัยเข้ากับการออกแบบอย่างแท้จริงและใช้ความพยายามในการบำรุงรักษาน้อยลงเพื่อเป็นการสะท้อนถึงมุมมองนี้ สหภาพยุโรปได้เน้นย้ำถึงความสำคัญของความมั่นคงปลอดภัยของผลิตภัณฑ์ในพระราชบัญญัติความยืดหยุ่นทางไซเบอร์ (Cyber-Resilience-Act) โดยเน้นว่า ผู้ผลิตควรใช้หลักความมั่นคงปลอดภัยไปตลอดวงจรชีวิตการใช้งานของผลิตภัณฑ์เพื่อป้องกันไม่ให้ผู้ผลิตนำผลิตภัณฑ์ที่มีจุดอ่อนเข้าสู่ตลาด

เพื่อสร้างอนาคตที่เทคโนโลยีและผลิตภัณฑ์ที่เกี่ยวข้องให้มีความปลอดภัยมากขึ้นสำหรับลูกค้า คณะผู้จัดทำเอกสารจึงเรียกร้องให้ผู้ผลิตปรับปรุงโปรแกรมการออกแบบและการพัฒนาเพื่อให้เฉพาะผลิตภัณฑ์ที่มีความปลอดภัยโดยการออกแบบและการตั้งค่าเริ่มต้นเท่านั้นที่จะถูกจัดส่งไปให้กับลูกค้า ผลิตภัณฑ์ที่ใช้หลักความปลอดภัยโดยการออกแบบคือ ผลิตภัณฑ์ที่มีความมั่นคงปลอดภัยของลูกค้าเป็นเป้าหมายหลักทางธุรกิจ ไม่ใช่เพียงคุณลักษณะทางเทคนิคเท่านั้น ผลิตภัณฑ์ที่ใช้หลักความปลอดภัยโดยการออกแบบจะเริ่มต้นด้วยเป้าหมายนี้ก่อนที่จะเริ่มการพัฒนา ผลิตภัณฑ์ที่ใช้หลักความปลอดภัยโดยการตั้งค่าเริ่มต้นมีความมั่นคงปลอดภัยที่จะใช้งานเมื่อตอน "แกะกล่อง" โดยไม่จำเป็นต้องเปลี่ยนแปลงการกำหนดตั้งค่าและมีคุณลักษณะด้านความมั่นคงปลอดภัยให้ใช้งานได้โดยไม่จำเป็นต้องมีค่าใช้จ่ายเพิ่มเติม ทั้งสองหลักการนี้จะช่วยย้ายโอนภาระของความมั่นคงปลอดภัยไปยังผู้ผลิตและลดโอกาสที่ลูกค้าจะตกเป็นเหยื่อของเหตุการณ์ด้านความมั่นคงปลอดภัยซึ่งเกิดจากการกำหนดตั้งค่าผิดพลาด การแก้ไขโดยใช้แพตช์ (Patch) ที่ไม่รวดเร็วเพียงพอ หรือปัญหาทั่วไปอื่น ๆ อีกมากมาย

---

[1]คณะผู้จัดทำเอกสารตระหนักถึงคำว่า "ความปลอดภัย" มีความหมายหลายแง่ขึ้นอยู่กับบริบทที่ใช้งาน สำหรับวัตถุประสงค์ของคู่มือนี้ "ความปลอดภัย" จะหมายถึงการยกระดับมาตรฐานความมั่นคงปลอดภัยของเทคโนโลยี เพื่อให้การคุ้มครองลูกค้าจากการกิจกรรมทางไซเบอร์ที่เป็นอันตราย

คณะกรรมาธิการความมั่นคงปลอดภัยทางไซเบอร์และโครงสร้างพื้นฐาน หรือ Cybersecurity and Infrastructure Security Agency (CISA) คณะกรรมาธิการความมั่นคงปลอดภัยแห่งชาติ หรือ National Security Agency (NSA) สำนักงานสอบสวนกลาง หรือ Federal Bureau of Investigation (FBI) และพันธมิตรระหว่างประเทศ[2] ต่อไปนี้ ขอแนะนำให้ใช้คู่มือนี้เป็นแผนการทำงานสำหรับผู้ผลิตเทคโนโลยีเพื่อให้เกิดความมั่นใจในความมั่นคงปลอดภัยของผลิตภัณฑ์ของตน

- ศูนย์รักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งออสเตรเลีย หรือ Australian Cyber Security Centre (ACSC)
- ศูนย์รักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งแคนาดา หรือ Canadian Centre for Cyber Security (CCCS)
- ศูนย์ความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติสหราชอาณาจักร หรือ United Kingdom's National Cyber Security Centre (NCSC-UK)
- สำนักงานความมั่นคงปลอดภัยของข้อมูลแห่งสหพันธรัฐเยอรมนี หรือ Germany's Federal Office for Information Security (BSI)
- ศูนย์ความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติเนเธอร์แลนด์ หรือ Netherlands' National Cyber Security Centre (NCSC-NL)
- ทีมช่วยเหลือฉุกเฉินทางคอมพิวเตอร์นิวซีแลนด์ หรือ Computer Emergency Response Team New Zealand (CERT-NZ) และศูนย์ความมั่นคงปลอดภัยทางไซเบอร์แห่งชาตินิวซีแลนด์ หรือ National Cyber Security Centre (NCSC-NZ)

คณะผู้จัดทำเอกสารให้ความสำคัญกับการสนับสนุนจากพันธมิตรภาคเอกชนจำนวนมากในการปรับปรุงความปลอดภัยโดยการออกแบบและความปลอดภัยโดยการตั้งค่าเริ่มต้น เอกสารฉบับนี้มีวัตถุประสงค์เพื่อทำให้เกิดความก้าวหน้าในการสนทนาระหว่างประเทศเกี่ยวกับลำดับความสำคัญ การลงทุน และการตัดสินใจที่จำเป็นเพื่อให้บรรลุเป้าหมายในอนาคตที่เทคโนโลยีจะมีความปลอดภัย มั่นคง และยืดหยุ่นตามการออกแบบและการตั้งค่าเริ่มต้น เพื่อวัตถุประสงค์นี้ คณะผู้จัดทำเอกสารใคร่ขอความคิดเห็นเกี่ยวกับเอกสารฉบับนี้จากผู้สนใจและหน่วยงานยังมีความตั้งใจที่จะจัดการประชุมรับฟังเพื่อปรับปรุง ระบุรายละเอียด และพัฒนาคำแนะนำเพิ่มเติมเพื่อให้บรรลุเป้าหมายที่มีร่วมกันของเรา

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับความสำคัญของความมั่นคงปลอดภัยของผลิตภัณฑ์ โปรดดูบทความโดย CISA เรื่อง [ต้นทุนของเทคโนโลยีที่ไม่ปลอดภัยและสิ่งที่เราสามารถทำได้เกี่ยวกับเทคโนโลยีนั้น]

ความปลอดภัยโดยการออกแบบ (Secure-by-Design)

"ความปลอดภัยโดยการออกแบบ" หมายความว่า ผลิตภัณฑ์เทคโนโลยีถูกสร้างขึ้นในลักษณะที่สมเหตุสมผลเพื่อป้องกันไม่ให้ผู้กระทำการไซเบอร์ที่เป็นอันตรายประสบความสำเร็จในการเข้าถึงอุปกรณ์ ข้อมูล และโครงสร้างพื้นฐานที่เชื่อมต่อได้ ผู้ผลิตซอฟต์ท์แวร์ควรทำการประเมินความเสี่ยงเพื่อระบุและแจกแจงภัยคุกคามทางไซเบอร์ที่พบบ่อยไปยังระบบที่สำคัญ จากนั้นจึงรวมการป้องกันไว้ในพิมพ์เขียวของผลิตภัณฑ์ที่คำนึงถึงสภาพการณ์ของภัยคุกคามทางไซเบอร์ที่มีการพัฒนาอย่างต่อเนื่อง

แนวปฏิบัติในการพัฒนาเทคโนโลยีสารสนเทศ (IT) ที่มั่นคงปลอดภัยและการป้องกันหลายระดับชั้นที่เรียกว่าการป้องกันเชิงลึก (Defense-in-depth) ยังได้รับการแนะนำให้นำไปใช้เพื่อป้องกันกิจกรรมของฝ่ายตรงข้ามจากการจู่โจมระบบหรือการเข้าถึงข้อมูลที่สำคัญโดยไม่ได้รับอนุญาตอีกด้วย คณะผู้จัดทำเอกสารขอแนะนำผู้ผลิตให้ใช้

---

[2] ต่อจากนี้จะเรียกว่า "คณะผู้จัดทำเอกสาร"

แบบจำลองภัยคุกคามที่ปรับแต่งให้เหมาะสมในระหว่างขั้นตอนการพัฒนาผลิตภัณฑ์ เพื่อจัดการกับภัยคุกคามทั้งหมดที่อาจเกิดขึ้นกับระบบและเป็นเหตุผลสำหรับกระบวนการปรับใช้งานของแต่ละระบบ

คณะผู้จัดทำเอกสารเรียกร้องให้ผู้ผลิตใช้หลักความมั่นคงปลอดภัยแบบองค์รวมสำหรับผลิตภัณฑ์และแพลตฟอร์มของตน การพัฒนาตามหลักความปลอดภัยโดยการออกแบบต้องการการลงทุนด้านทรัพยากรอย่างมีนัยสำคัญจากผู้ผลิตซอฟต์แวร์ในแต่ละระดับชั้นของกระบวนการออกแบบและพัฒนาผลิตภัณฑ์ที่ไม่สามารถนำไป "พ่วงติด" ได้ในภายหลัง ผู้บริหารธุรกิจระดับสูงของผู้ผลิตจำเป็นต้องเป็นผู้นำที่แข็งแกร่งที่ตั้งความมั่นคงปลอดภัยเป็นความสำคัญทางธุรกิจ ไม่ใช่แค่เพียงคุณลักษณะหนึ่งทางเทคนิคเท่านั้น ความร่วมมือระหว่างผู้นำธุรกิจและทีมเทคนิคนี้ ครอบคลุมตั้งแต่ขั้นตอนแรกของการออกแบบและการพัฒนา ไปจนถึงการปรับใช้งานและการบำรุงรักษาของลูกค้า ผู้ผลิตจะได้รับการสนับสนุนให้ทำการแลกเปลี่ยนและลงทุนอย่างจริงจัง รวมถึงการลงทุนที่ลูกค้าจะ "มองไม่เห็น" เช่น การโยกย้ายไปยังภาษาการเขียนโปรแกรมที่จะช่วยกำจัดจุดอ่อนที่มีการแพร่กระจายได้ ผู้ผลิตควรจัดลำดับความสำคัญให้กับคุณลักษณะ กลไก และการใช้เครื่องมือที่จะช่วยปกป้องลูกค้า มากกว่าที่จะให้คุณลักษณะของผลิตภัณฑ์ที่ดูเหมือนจะดึงดูดลูกค้าแต่ไปขยายพื้นผิวการโจมตีแทน

ทางออกที่จะเอาชนะภัยคุกคามอย่างต่อเนื่องจากผู้กระทำการไซเบอร์ที่เป็นอันตรายโดยการใช้ประโยชน์จากจุดอ่อนทางเทคโนโลยีไม่ได้มีเพียงทางเดียว และผลิตภัณฑ์ที่มี "ความปลอดภัยโดยการออกแบบ" จะยังคงต้องประสบปัญหาจากจุดอ่อนอยู่ อย่างไรก็ตาม กลุ่มจุดอ่อนจำนวนมากเกิดจากสาเหตุส่วนย่อยของสาเหตุพื้นฐาน ผู้ผลิตควรพัฒนาแผนการทำงานที่เป็นลายลักษณ์อักษรเพื่อจัดกลุ่มพอร์ตผลงานผลิตภัณฑ์ที่มีอยู่ให้สอดคล้องกับแนวปฏิบัติตามหลักความปลอดภัยโดยการออกแบบ เพื่อให้เกิดความมั่นใจว่าจะมีการเบี่ยงเบนไปเฉพาะในสถานการณ์พิเศษเท่านั้น

คณะผู้จัดทำเอกสารยอมรับว่าการเป็นเจ้าของผลลัพธ์ด้านความมั่นคงปลอดภัยสำหรับลูกค้าและการสร้างความมั่นใจให้ลูกค้าต่อความมั่นคงปลอดภัยในระดับนี้ อาจทำให้ค่าใช้จ่ายในการพัฒนาผลิตภัณฑ์เพิ่มสูงขึ้นได้ อย่างไรก็ตาม การลงทุนในแนวปฏิบัติตามหลัก "ความปลอดภัยโดยการออกแบบ" ในขณะที่ทำการพัฒนาผลิตภัณฑ์เทคโนโลยีใหม่ ๆ และรักษาผลิตภัณฑ์ที่มีอยู่เดิมไว้จะสามารถช่วยปรับปรุงระบบความมั่นคงปลอดภัยของลูกค้าและลดโอกาสที่จะทำให้เป็นช่องโหว่ได้อย่างมีนัยสำคัญ หลักการความปลอดภัยโดยการออกแบบไม่เพียงแต่ช่วยเสริมสร้างระบบความมั่นคงปลอดภัยให้ลูกค้าและชื่อเสียงของแบรนด์สำหรับนักพัฒนาเท่านั้น แต่ยังช่วยลดค่าใช้จ่ายในการบำรุงรักษาและการแก้ไขโดยใช้แพตช์ (Patch) สำหรับผู้ผลิตในระยะยาวอีกด้วย

ส่วนคำแนะนำสำหรับผู้ผลิตซอฟต์แวร์ที่ระบุไว้ด้านล่างแสดงรายการแนวปฏิบัติและนโยบายการพัฒนาผลิตภัณฑ์ที่แนะนำให้ผู้ผลิตไว้พิจารณา

ความปลอดภัยโดยการตั้งค่าเริ่มต้น (Secure-by-Default)

"ความปลอดภัยโดยการตั้งค่าเริ่มต้น" หมายความว่า ผลิตภัณฑ์มีความต้านทานต่อเทคนิคการหาประโยชน์ที่แพร่หลายตั้งแต่การแกะกล่องใช้งานโดยไม่ต้องมีค่าใช้จ่ายเพิ่มเติม ผลิตภัณฑ์เหล่านี้จะช่วยป้องกันภัยคุกคามและแก้ไขจุดอ่อนที่พบบ่อยที่สุดโดยผู้ใช้ปลายทางไม่ต้องดำเนินการใด ๆ เพิ่มเติมเพื่อรักษาความมั่นคงปลอดภัย ผลิตภัณฑ์ที่มีความปลอดภัยโดยการตั้งค่าเริ่มต้นได้รับการออกแบบมาเพื่อให้ลูกค้าตระหนักอย่างชัดเจนว่าหากพวกเขาเบี่ยงเบนไปจากการตั้งค่าเริ่มต้นที่ปลอดภัยแล้ว พวกเขาจะมีแนวโน้มที่จะทำให้เกิดช่องโหว่มากขึ้น เว้นแต่จะใช้การควบคุมมาชดเชยเพิ่มเติม

- การกำหนดตั้งค่าที่มั่นคงปลอดภัยควรเป็นพื้นฐานเริ่มต้น ผลิตภัณฑ์ที่มีความปลอดภัยโดยการตั้งค่าเริ่มต้นเปิดใช้งานการควบคุมความมั่นคงปลอดภัยที่สำคัญที่สุดโดยอัตโนมัติ ซึ่งจำเป็นต่อการปกป้องค์กรจากผู้กระทำการไซเบอร์ที่เป็นอันตรายได้ ตลอดจนให้สามารถใช้งานและกำหนดตั้งค่าการควบคุมด้านความมั่นคงปลอดภัยเพิ่มขึ้นได้โดยไม่มีค่าใช้จ่ายเพิ่มเติม
- ความซับซ้อนของการกำหนดตั้งค่าความมั่นคงปลอดภัยไม่ควรเป็นปัญหาของลูกค้า เจ้าหน้าที่สารสนเทศขององค์กรมักมีภาระงานด้านความมั่นคงปลอดภัยและการปฏิบัติงานมากเกินไป ส่งผลให้มีเวลาจำกัดในการทำความเข้าใจและปรับใช้ผลกระทบด้านความมั่นคงปลอดภัย ตลอดจนหามาตรการที่จำเป็นสำหรับระบบความมั่นคงปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพ ด้วยการเพิ่มประสิทธิภาพการกำหนดตั้งค่าผลิตภัณฑ์ให้มีความมั่นคงปลอดภัยสูงสุดหรือการรักษา "เส้นทางเริ่มต้น" ผู้ผลิตสามารถช่วยเหลือลูกค้าได้ด้วยการทำให้เกิดความมั่นใจว่าผลิตภัณฑ์ของตนได้รับการผลิต จัดจำหน่าย และใช้งานได้อย่างมั่นคงปลอดภัยตามมาตรฐาน "ความปลอดภัยโดยการตั้งค่าเริ่มต้น"

ผู้ผลิตของผลิตภัณฑ์ที่มี "ความปลอดภัยโดยการตั้งค่าเริ่มต้น"จะไม่คิดค่าใช้จ่ายเพิ่มเติมในการกำหนดตั้งค่าความมั่นคงปลอดภัย แต่จะคิดรวมอยู่ในผลิตภัณฑ์พื้นฐาน เช่นเดียวกับที่รถคันใหม่ทุกคันจะมีเข็มขัดนิรภัยติดมากับรถด้วย ความมั่นคงปลอดภัยไม่ใช่ตัวเลือกที่หรูหรา แต่ใกล้เคียงกับมาตรฐานที่ลูกค้าทุกคนควรคาดหวังได้โดยไม่ต้องเจรจาต่อรองหรือจ่ายเงินเพิ่ม

คำแนะนำสำหรับผู้ผลิตซอฟต์แวร์

เอกสารคู่มือร่วมฉบับนี้ ให้คำแนะนำแก่ผู้ผลิตในการพัฒนาแผนการทำงานที่เป็นลายลักษณ์อักษรเพื่อนำออกไปใช้งานและรับประกันความมั่นคงปลอดภัยด้านสารสนเทศ คณะผู้จัดทำเอกสารขอแนะนำให้ผู้ผลิตซอฟต์แวร์ใช้กลยุทธ์ที่ระบุไว้ในส่วนด้านล่างนี้ เพื่อแสดงความเป็นเจ้าของผลลัพธ์ด้านความมั่นคงปลอดภัยของลูกค้าผ่านหลักการตามความปลอดภัยโดยการออกแบบและการตั้งค่าเริ่มต้น

หลักการความมั่นคงปลอดภัยของผลิตภัณฑ์ซอฟต์แวร์

เราขอสนับสนุนให้ผู้ผลิตเทคโนโลยีปรับใช้กลยุทธ์ที่ให้ลำดับความสำคัญกับความมั่นคงปลอดภัยของซอฟต์แวร์ คณะผู้จัดทำเอกสารได้พัฒนาหลักการสำคัญสามประการด้านล่างนี้เพื่อเป็นแนวทางให้กับผู้ผลิตซอฟต์แวร์ในการสร้างความมั่นคงปลอดภัยของซอฟต์แวร์เข้าไปในกระบวนการออกแบบก่อนที่จะพัฒนา กำหนดตั้งค่า และจัดส่งผลิตภัณฑ์ของตน

1. ภาระด้านความมั่นคงปลอดภัยไม่ควรตกอยู่ที่ลูกค้าเพียงฝ่ายเดียว ผู้ผลิตซอฟต์แวร์ควรเป็นเจ้าของผลลัพธ์ด้านความมั่นคงปลอดภัยต่อสิ่งที่ลูกค้าซื้อและควรพัฒนาผลิตภัณฑ์ของตนให้สอดคล้องกัน
2. เปิดรับความโปร่งใสและการแสดงความรับผิดชอบอย่างถึงแก่น ผู้ผลิตซอฟต์แวร์ควรภูมิใจที่ได้ส่งมอบผลิตภัณฑ์ที่ปลอดภัยและมีความมั่นคง รวมทั้งสร้างความแตกต่างให้กับตนเองจากชุมชนผู้ผลิตรายอื่นตามความสามารถของตนที่ได้ปฏิบัติเช่นนั้น ซึ่งอาจรวมถึงการแบ่งปันข้อมูลที่พวกเขาเรียนรู้จากการปรับใช้งานของลูกค้า เช่น การยอมรับกลไกการยืนยันตัวตนที่รัดกุมด้วยการตั้งค่าเริ่มต้น นอกจากนั้นยังรวมถึงการมีความมุ่งมั่นอย่างแรงกล้าที่จะรับประกันคำแนะนำเกี่ยวกับจุดอ่อน และการบันทึกจุดอ่อนทั่วไปที่เกี่ยวข้องและการเปิดเผย (CVE) มีความสมบูรณ์และถูกต้อง อย่างไรก็ตาม โปรดให้ความระมัดระวังเรื่องการคำนวณ CVE เป็นตัวชี้วัดเชิงลบ เนื่องจากตัวเลขดังกล่าวยังเป็นสัญญาณของชุมชนการวิเคราะห์และทดสอบโค้ดที่มีประสิทธิภาพอีกด้วย

3. **สร้างโครงสร้างองค์กรและความเป็นผู้นำเพื่อบรรลุเป้าหมายเหล่านี้ แม้ว่าความเชี่ยวชาญเฉพาะทางด้านเทคนิคจะมีความสำคัญอย่างยิ่งต่อความมั่นคงปลอดภัยของผลิตภัณฑ์ ผู้บริหารระดับสูงก็จะยังเป็นผู้มีอำนาจตัดสินใจหลักในการดำเนินการเปลี่ยนแปลงองค์กร ความมุ่งมั่นในระดับผู้บริหารสำหรับผู้ผลิตซอฟต์แวร์ที่มีต่อการจัดลำดับความสำคัญของความมั่นคงปลอดภัยให้เป็นองค์ประกอบสำคัญของการพัฒนาผลิตภัณฑ์ จำเป็นต้องมีการพัฒนาความร่วมมือกับลูกค้าขององค์กรเพื่อทำความเข้าใจประเด็นดังนี้**
    a. **คำแนะนำด้านสถานการณ์การปรับใช้งานผลิตภัณฑ์พร้อมกับแบบจำลองภัยคุกคามที่ปรับแต่งตามความเหมาะสม**
    b. **การดำเนินการที่เสนอไว้ สำหรับการควบคุมความมั่นคงปลอดภัยเพื่อให้สอดคล้องกับหลักความปลอดภัยโดยการตั้งค่าเริ่มต้น**
    c. **กลยุทธ์การจัดสรรทรัพยากรที่ปรับแต่งให้เหมาะกับขนาดของบริษัทและความสามารถในการแทนที่แนวปฏิบัติด้านการพัฒนาแบบเดิมให้เป็นไปตามหลักความปลอดภัยโดยการออกแบบ**
    d. **ความจำเป็นในการรักษาช่องทางการสื่อสารแบบเปิดสำหรับความคิดเห็นทั้งภายในและภายนอกองค์กร (เช่น ความคิดเห็นของพนักงานและลูกค้า) เกี่ยวกับปัญหาด้านความมั่นคงปลอดภัยของผลิตภัณฑ์ ควรมีการเน้นย้ำถึงเรื่องความมั่นคงปลอดภัยของซอฟต์แวร์ในที่ประชุมภายในองค์กร (เช่น เมื่อมีการประชุมของบริษัท หรือ เวลาประชุมจัดเลี้ยงแก่พนักงาน) เช่นเดียวกับการทำการตลาดผลิตภัณฑ์ภายนอกและการให้ลูกค้ามีส่วนร่วม**
    e. **การวัดประสิทธิภาพด้วยการปรับใช้งานของลูกค้า ผู้บริหารระดับสูงจะต้องการที่จะทราบว่าการลงทุนด้านความปลอดภัยโดยการออกแบบและการตั้งค่าเริ่มต้นจะเป็นการช่วยเหลือลูกค้าได้อย่างไร โดยการชะลอความเร็วของแพตซ์ (Patch) การแก้ไขความมั่นคงปลอดภัย การลดข้อผิดพลาดในการกำหนดตั้งค่า และการลดพื้นผิวการโจมตีให้น้อยที่สุด**

เพื่อให้สามารถใช้หลักการสามข้อนี้ ผู้ผลิตควรพิจารณากลวิธีการปฏิบัติงานหลาย ๆ ด้านเพื่อปรับกระบวนการพัฒนาของตน

จัดการประชุมประจำร่วมกับผู้บริหารระดับสูงของบริษัทเพื่อขับเคลื่อนความสำคัญของหลักการตามความปลอดภัยโดยการออกแบบและการตั้งค่าเริ่มต้นภายในองค์กร ควรมีการกำหนดนโยบายและระเบียบปฏิบัติเพื่อให้รางวัลแก่ทีมผู้ผลิตที่พัฒนาผลิตภัณฑ์ตามหลักการเหล่านี้ ซึ่งอาจรวมถึงการให้รางวัลสำหรับการใช้แนวปฏิบัติตามหลักความมั่นคงปลอดภัยของซอฟต์แวร์ที่โดดเด่น หรือมอบสิ่งจูงใจสำหรับขั้นบันไดงานและใช้เป็นเกณฑ์การเลื่อนตำแหน่งงาน

ให้ความสำคัญกับหลักความมั่นคงปลอดภัยของซอฟต์แวร์ต่อความสำเร็จของธุรกิจ ตัวอย่างเช่น พิจารณาแต่งตั้ง "ผู้นำด้านความมั่นคงปลอดภัยของซอฟต์แวร์" หรือ "ทีมความมั่นคงปลอดภัยของซอฟต์แวร์"ซึ่งสนับสนุนแนวทางปฏิบัติด้านธุรกิจและสารสนเทศ โดยให้เชื่อมโยงกับมาตรฐานความมั่นคงปลอดภัยของซอฟต์แวร์และความรับผิดชอบของผู้ผลิตโดยตรง ผู้ผลิตควรทำให้เกิดความมั่นใจว่ามีระบบประเมินความมั่นคงปลอดภัยของผลิตภัณฑ์และโปรแกรมการประเมินผลที่แข็งแกร่งและเป็นอิสระสำหรับผลิตภัณฑ์ของพวกเขา

ใช้แบบจำลองภัยคุกคามที่ปรับแต่งให้เหมาะสมในระหว่างการพัฒนาเพื่อจัดลำดับความสำคัญของผลิตภัณฑ์ที่สำคัญและมีผลกระทบสูง แบบจำลองภัยคุกคามจะพิจารณากรณีการใช้งานเฉพาะของผลิตภัณฑ์และช่วยให้ทีมพัฒนาสามารถเสริมความแข็งแกร่งให้กับผลิตภัณฑ์ได้ ประการสุดท้าย ผู้นำระดับสูงควรให้ทีมรับผิดชอบในการส่งมอบผลิตภัณฑ์ที่ปลอดภัย ซึ่งเป็นองค์ประกอบสำคัญของผลิตภัณฑ์ที่ยอดเยี่ยมและมีคุณภาพ

กลวิธีความปลอดภัยโดยการออกแบบ

โครงร่างการพัฒนาซอฟต์แวร์ที่มั่นคงปลอดภัย หรือ Secure Software Development Framework (SSDF) ยังเป็นที่รู้จักกันในชื่อ สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ หรือ National Institute of Standards and Technology's (NIST) SP 800-218 เป็นชุดหลักปฏิบัติในการพัฒนาซอฟต์แวร์ที่มั่นคงปลอดภัยในระดับสูง ซึ่งสามารถผนวกรวมเข้ากับทุกขั้นตอนของวงจรชีวิตของการพัฒนาซอฟต์แวร์ (SDLC) การดำเนินการตามแนวปฏิบัติเหล่านี้สามารถช่วยให้ผู้ผลิตซอฟต์แวร์มีประสิทธิภาพมากขึ้นในการค้นหา และขจัดจุดอ่อนในซอฟต์แวร์ที่เผยแพร่ออกมา บรรเทาผลกระทบที่อาจเกิดขึ้นจากการใช้ประโยชน์จากจุดอ่อนต่าง ๆ และระบุสาเหตุพื้นฐานของจุดอ่อนเพื่อป้องกันมิให้เกิดซ้ำในอนาคต

คณะผู้จัดทำเอกสารสนับสนุนให้มีการใช้กลวิธีความปลอดภัยโดยการออกแบบ รวมถึงหลักการที่อ้างอิงแนวปฏิบัติ SSDF ผู้ผลิตซอฟต์แวร์ควรพัฒนาแผนการทำงานที่เป็นลายลักษณ์อักษร เพื่อนำแนวปฏิบัติในการพัฒนาซอฟต์แวร์ตามหลักความปลอดภัยโดยการออกแบบมาใช้ในพอร์ตผลงานของตนให้มากขึ้น ต่อไปนี้เป็นรายการของแผนการทำงานที่มีตัวอย่างประกอบเพียงบางตัวอย่าง ได้แก่

- ภาษาโปรแกรมที่ปลอดภัยต่อหน่วยความจำ (Memory safe programming languages) (SSDF PW.6.1) จัดลำดับการใช้ภาษาที่ปลอดภัยของหน่วยความจำหากเป็นไปได้
  คณะผู้จัดทำเอกสารรับทราบว่าการบรรเทาปัญหาเฉพาะหน่วยความจำอื่น ๆ เช่น การสุ่มตำแหน่งพื้นที่ที่อยู่ (Address Space Layout
  Randomization - ASLR) ความสมบูรณ์ของโฟลว์ควบคุม (Control-flow Integrity - CFI) และการฟัสซิ่ง (fuzzing) มีประโยชน์สำหรับโค้ดเบสดั้งเดิม (Legacy codebase) แต่ไม่เพียงพอที่จะได้รับการพิจารณาว่ามีความปลอดภัยโดยการออกแบบ เนื่องจากไม่สามารถป้องกันการฉกฉวยประโยชน์ได้อย่างเพียงพอ ตัวอย่างของภาษาที่ปลอดภัยสำหรับหน่วยความจำสมัยใหม่ ได้แก่ C#, Rust, Ruby, Java, Go และ Swift สำหรับข้อมูลเพิ่มเติม โปรดอ่านแผ่นข้อมูลความปลอดภัยสำหรับหน่วยความจำของ NSA
- พื้นฐานฮาร์ดแวร์ที่มีความมั่นคงปลอดภัย (Secure Hardware Foundation) รวมคุณลักษณะสถาปัตยกรรมการใช้งานที่ช่วยให้เกิดการป้องกันหน่วยความจำขนาดละเอียดได้ เช่น คุณลักษณะที่อธิบายโดยคำสั่ง Capability Hardware Enhanced RISC Instructions (CHERI) ซึ่งสามารถขยายสถาปัตยกรรมการใช้งานด้วยชุดคำสั่ง (Instruction-Set Architectures- ISAs) ของฮาร์ดแวร์แบบดั้งเดิมได้ สำหรับข้อมูลเพิ่มเติม โปรดไปที่ CHERI ซึ่งเป็นเว็บไซต์ของมหาวิทยาลัย University of Cambridge
- ส่วนประกอบซอฟต์แวร์ที่มีความมั่นคงปลอดภัย (Secure Software Components) (SSDF PW 4.1) ซื้อหาและบำรุงรักษาส่วนประกอบซอฟต์แวร์ที่มีความมั่นคงปลอดภัยอย่างดี (เช่น ไลบรารีซอฟต์แวร์ โมดูลส์ มิดเดิลแวร์ เฟรมเวิร์ก) จากผู้พัฒนาซอฟต์แวร์เชิงพาณิชย์ จากแหล่งเปิดหรือโอเพ่นซอร์ส และผู้พัฒนาซอฟต์แวร์บุคคลที่สามอื่น ๆ ที่ผ่านการตรวจสอบเพื่อให้มั่นใจถึงความมั่นคงปลอดภัยที่แข็งแกร่งในผลิตภัณฑ์ซอฟต์แวร์สำหรับผู้บริโภค
- ชุดคำสั่งเทมเพลตเว็บ (Web template frameworks) (SSDF PW. 5.1) ใช้ชุดคำสั่งเทมเพลตเว็บที่เลี่ยงการป้อนข้อมูลจากผู้ใช้โดยอัตโนมัติเพื่อหลีกเลี่ยงการโจมตีทางเว็บ เช่น การเขียนสคริปต์ข้ามไซต์ (Cross-site Scripting)
- เควรีย์สที่มีการกำหนดพารามิเตอร์ (Parameterized queries) (SSDF PW 5.1) ใช้เควรีย์สที่มีการกำหนดพารามิเตอร์แทนที่จะรวมการป้อนข้อมูลของผู้ใช้ในเควรีย์ส เพื่อหลีกเลี่ยงการโจมตีแบบ SQL Injection
- การทดสอบความมั่นคงปลอดภัยของแอปพลิเคชันแบบคงที่และแบบไดนามิก (Static and dynamic application security testing) (SAST/DAST) (SSDF PW.7.2, PW.8.2)
  ใช้เครื่องมือเหล่านี้ในการวิเคราะห์ซอร์สโค้ดของผลิตภัณฑ์และลักษณะการทำงานของแอปพลิเคชัน

เพื่อตรวจหาแนวปฏิบัติที่อาจทำให้เกิดข้อผิดพลาด เครื่องมือเหล่านี้ ครอบคลุมปัญหาต่าง ๆ ตั้งแต่การจัดการหน่วยความจำที่ไม่เหมาะสมไปจนถึงการสร้างเคียวรีย์สฐานข้อมูลที่อาจเกิดข้อผิดพลาด (เช่น การป้อนข้อมูลของผู้ใช้ที่ไม่ได้รับอนุญาตซึ่งนำไปสู่การโจมตีแบบ SQL injection) เครื่องมือ SAST และ DAST สามารถนำมารวมเข้ากับกระบวนการพัฒนาและให้รันโดยอัตโนมัติในส่วนหนึ่งของการพัฒนาซอฟต์แวร์ SAST และ DAST ควรนำไปใช้ประกอบกับการทดสอบประเภทอื่น ๆ เช่น unit test และ integration text เพื่อให้แน่ใจว่าผลิตภัณฑ์เป็นไปตามข้อกำหนดด้านความมั่นคงปลอดภัยที่คาดไว้ เมื่อระบุปัญหาได้แล้ว ผู้ผลิตซอฟต์แวร์ควรทำการวิเคราะห์สาเหตุพื้นฐานเพื่อจัดการกับจุดอ่อนอย่างเป็นระบบ

- การทบทวนรหัส (Code review) (SSDF PW.7.1, PW.7.2) พยายามมุ่งมั่นเพื่อให้แน่ใจว่ารหัสที่ส่งเข้าไปยังผลิตภัณฑ์จะผ่านการตรวจสอบจากผู้พัฒนารายอื่น เพื่อให้แน่ใจว่ามีคุณภาพที่สูงขึ้น
- รายการวัสดุซอฟต์แวร์ (Software Bill of Materials -SBOM) (SSDF PS.3.2, PW.4.1) ผนวกการสร้าง SBOM[3] เข้าด้วยกันเพื่อให้สามารถมองเห็นชุดซอฟต์แวร์ที่เข้าสู่ผลิตภัณฑ์ได้อย่างชัดเจน
- โปรแกรมการบ่งชี้จุดอ่อน (Vulnerability disclosure programs) (SSDF RV.1.3) ก่อตั้งโปรแกรมการบ่งชี้จุดอ่อนที่ช่วยให้นักวิจัยด้านความมั่นคงปลอดภัยสามารถรายงานจุดอ่อนและได้รับความปลอดภัยทางกฎหมายในการดำเนินการเช่นนั้น ในฐานะที่เป็นส่วนหนึ่งของเรื่องนี้ ซัพพลายเออร์ควรสร้างกระบวนการเพื่อระบุสาเหตุพื้นฐานของจุดอ่อนที่ค้นพบ กระบวนการดังกล่าวควรรวมถึงการกำหนดว่าจะนำแนวปฏิบัติตามหลักความปลอดภัยโดยการออกแบบใด ๆ มาใช้ในเอกสารนี้ (หรือแนวปฏิบัติอื่น ๆ ที่คล้ายคลึงกัน) ซึ่งจะช่วยป้องกันไม่ให้นำจุดอ่อนเข้ามาในระบบหรือไม่
- ความสมบูรณ์แบบของ CVA (CVE completeness) ตรวจสอบให้แน่ใจว่า CVE ที่เผยแพร่ออกมานั้นรวมสาเหตุพื้นฐานหรือการระบุจุดอ่อนที่มีร่วมกัน (Common Weakness Enumeration - CWE) เพื่อให้สามารถวิเคราะห์สาเหตุพื้นฐานของความมั่นคงปลอดภัยซอฟต์แวร์ได้ทั่วทั้งอุตสาหกรรม ในขณะที่การตรวจสอบให้แน่ใจว่า CVE ทุกรายการมีความถูกต้องและสมบูรณ์แบบอาจต้องใช้เวลามากกว่าปกติ แต่การทำเช่นนั้นก็ช่วยให้หน่วยงานที่แตกต่างกันสามารถระบุแนวโน้มในอุตสาหกรรมที่เป็นประโยชน์ต่อผู้ผลิตและลูกค้าทั้งหมด สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการจุดอ่อน โปรดดู คำแนะนำ SVCC สำหรับผู้มีส่วนได้ส่วนเสียโดยเฉพาะของ CISA
- การป้องกันเชิงลึก (Defense-in-Depth) ออกแบบโครงสร้างพื้นฐานเพื่อให้การเสียงมีช่องโหว่ของความมั่นคงปลอดภัยเพียงจุดเดียวไม่ส่งผลให้เกิดเป็นช่องโหว่ต่อระบบทั้งหมด ตัวอย่างเช่น การตรวจสอบให้แน่ใจว่าสิทธิ์ของผู้ใช้ได้รับการจัดสรรไว้อย่างเคร่งครัดและการใช้รายการควบคุมการเข้าถึง ซึ่งสามารถลดผลกระทบของบัญชีผู้ใช้ที่อาจมีช่องโหว่ได้ นอกจากนี้ เทคนิค Sandbox หรือการทดสอบการทำงานของซอฟต์แวร์ยังสามารถกักกันจุดอ่อน เพื่อจำกัดการทำให้เกิดช่องโหว่ของแอปพลิเคชันทั้งหมดอีกด้วย

  บรรลุเป้าหมายประสิทธิภาพทางไซเบอร์ (Satisfy Cyber Performance Goals - CPG) ออกแบบผลิตภัณฑ์ที่ตรงตามแนวปฏิบัติพื้นฐานด้านความมั่นคงปลอดภัย เป้าหมายประสิทธิภาพความมั่นคงปลอดภัยทางไซเบอร์ของ CISA สรุปมาตรการต่อความมั่นคงปลอดภัยทางไซเบอร์ขั้นพื้นฐานที่องค์กรควรนำไปใช้ นอกจากนี้ สำหรับวิธีการเพิ่มความแข็งแกร่งให้กับระบบขององค์กรของคุณ โปรดดูที่ กรอบโครงสร้างความมั่นคงปลอดภัยทางไซเบอร์ของสหราชอาณาจักร (UK's Cyber Assessment Framework) ซึ่งมีความคล้ายคลึงกับ CPG ของ CISA หากผู้ผลิตไม่ได้ปฏิบัติตาม CPG เช่น ไม่บังคับให้พนักงานทุกคนใช้การยืนยันตัวตนโดยใช้หลายหลายปัจจัยที่สามารถต้านทานฟิชชิ่ง (phishing) ได้ พวกเขาก็จะไม่ถือว่ากำลังส่งมอบผลิตภัณฑ์ที่มีความปลอดภัยโดยการออกแบบ

---

[3] คณะผู้จัดทำเอกสารบางท่านกำลังสำรวจหาแนวทางเลือกอื่น เพื่อให้ได้การรับประกันความมั่นคงปลอดภัยรอบ ๆ ซัพพลายเชนของซอฟต์แวร์

คณะผู้จัดทำเอกสารตระหนักว่าการเปลี่ยนแปลงเหล่านี้มีผลต่อระบบการทำงานขององค์กรอย่างมีนัยสำคัญ ด้วยเหตุนี้ การนำการเปลี่ยนแปลงนี้เข้ามาในองค์กรควรได้รับการจัดลำดับตามความสำคัญ ความซับซ้อน และผลกระทบทางธุรกิจ แนวปฏิบัติเหล่านี้สามารถนำมาใช้กับซอฟต์แวร์ตัวใหม่และค่อย ๆ ขยายอย่างต่อเนื่อง เพื่อให้ครอบคลุมกรณีการใช้งานและผลิตภัณฑ์เพิ่มเติม ในบางกรณี วิกฤตและระบบความเสี่ยงของผลิตภัณฑ์บางอย่างอาจคุ้มค่ากับตารางเวลาที่เร่งรัดให้เร็วขึ้นเพื่อนำแนวปฏิบัติเหล่านี้ออกใช้ ส่วนในกรณีอื่น แนวปฏิบัติสามารถนำไปปรับใช้กับโค้ดเบสดั้งเดิม (Legacy codebase) และปรับปรุงแก้ไขตามเวลาที่ผ่านไป

กลวิธีความปลอดภัยโดยการตั้งค่าเริ่มต้น

นอกจากการนำแนวปฏิบัติการพัฒนาตามหลักความปลอดภัยโดยการออกแบบ (Secure-by-Design) มาใช้แล้ว คณะผู้จัดทำเอกสารยังขอแนะนำให้ผู้ผลิตซอฟต์แวร์จัดลำดับความสำคัญของการกำหนดตั้งค่าตามหลักความปลอดภัยโดยการตั้งค่าเริ่มต้น (Secure-by-Default) ในผลิตภัณฑ์ของตนอีกด้วย ซึ่งควรจะพยายามปรับผลิตภัณฑ์เพื่อให้สอดคล้องกับแนวปฏิบัติเหล่านี้เมื่อมีการปรับปรุงใหม่ ตัวอย่างเช่น

- กำจัดรหัสผ่านเริ่มต้น ผลิตภัณฑ์ไม่ควรมาพร้อมกับรหัสผ่านเริ่มต้นที่สามารถใช้แชร์ร่วมกันได้ทั่วไปในระดับสากล ในการกำจัดรหัสผ่านเริ่มต้น คณะผู้จัดทำเอกสารขอแนะนำว่าผลิตภัณฑ์ต้องใช้ผู้ดูแลระบบมาตั้งรหัสผ่านที่รัดกุมยากต่อการคาดเดาในระหว่างการติดตั้งและการกำหนดตั้งค่าต่าง ๆ
    - บังคับใช้การยืนยันตัวตนโดยใช้หลากหลายปัจจัย (MFA) สำหรับผู้ใช้ที่มีสิทธิ์ เราสังเกตว่าการปรับใช้งานขององค์กรจำนวนมากได้รับการจัดการโดยผู้ดูแลระบบที่ไม่ได้ปกป้องบัญชีของตนด้วย MFA เนื่องจากผู้ดูแลระบบเป็นเป้าหมายที่มีมูลค่าสูง ผลิตภัณฑ์จึงควรกำหนดให้ MFA เป็นแบบให้เลือกออก (Opt-out) แทนที่จะเป็นแบบให้เลือกเข้า (Opt-in) นอกจากนี้ ระบบควรแจ้งให้ผู้ดูแลระบบลงทะเบียนใน MFA ทุกครั้ง จนกว่าพวกเขาจะเปิดใช้งานบนบัญชีผู้ใช้ของพวกเขาได้สำเร็จ NCSC ของเนเธอร์แลนด์มีคำแนะนำที่คล้ายคลึงกับของ CISA โปรดดูแผ่นข้อมูลยืนยันตัวตนที่พร้อมใช้งาน (Mature Authentication) หากต้องการข้อมูลเพิ่มเติม
- การลงชื่อเข้าใช้ครั้งเดียว (Single sign-on - SSO) แอปพลิเคชันด้านสารสนเทศควรใช้เทคโนโลยีการลงชื่อเข้าใช้เพียงครั้งเดียวผ่านมาตรฐานแบบเปิดสมัยใหม่ ตัวอย่างเช่น Security Assertion Markup Language (SAML) หรือ OpenID Connect (OIDC) ความสามารถนี้ ควรจัดให้ใช้งานได้ตั้งแต่ค่าเริ่มต้นโดยไม่มีค่าใช้จ่ายเพิ่มเติม
- การบันทึกที่มั่นคงปลอดภัย (Secure Logging) จัดให้มีบันทึกการตรวจสอบ (Audit logs) ที่มีคุณภาพสูงให้แก่ลูกค้าโดยไม่มีค่าใช้จ่ายเพิ่มเติม บันทึกการตรวจสอบมีความสำคัญต่อการตรวจจับและยกระดับเหตุการณ์ด้านความมั่นคงปลอดภัยที่อาจเกิดขึ้น นอกจากนี้ ยังมีความสำคัญอย่างยิ่งในระหว่างการสืบสวนเหตุการณ์ด้านความปลอดภัยที่ต้องสงสัยหรือต้องการการยืนยัน พิจารณาแนวปฏิบัติที่ดีที่สุด เช่น บูรณาการให้กับระบบข้อมูลความปลอดภัยและการจัดการเหตุการณ์ (Security Information and Event Management - SIEM) ที่ง่ายดายด้วยการเข้าถึงอินเตอร์เฟซการเขียนโปรแกรมแอปพลิเคชัน (Application Programming Interface - API) ที่ใช้เวลาสากลเชิงพิกัด (Coordinated Universal Time - UTC) การจัดรูปแบบเขตเวลาแบบมาตรฐาน และเทคนิคการจัดทำเอกสารที่มีประสิทธิภาพ
- โปรไฟล์การยืนยันตัวตนด้วยการใช้ซอฟต์แวร์ (Software Authorization Profile) ซัพพลายเออร์ซอฟต์แวร์ควรให้คำแนะนำเกี่ยวกับบทบาทโปรไฟล์ที่ได้รับอนุมัติและกรณีการใช้งานกำหนดไว้ ผู้ผลิตควรให้คำเตือนที่มองเห็นได้ชัด ซึ่งแจ้งให้ลูกค้าทราบถึงความเสี่ยงที่เพิ่มขึ้น ในกรณีที่พวกเขาเบี่ยงเบนไปจากการอนุมัติโปรไฟล์ที่แนะนำมาให้ ตัวอย่างเช่น แพทย์สามารถเข้าดูบันทึกผู้ป่วยได้ทั้งหมด แต่ผู้จัดตารางเวลาทางการแพทย์มีข้อจำกัดในการเข้าถึงข้อมูลเท่าที่จำเป็นต่อการจัดตารางนัดหมายเท่านั้น

- ความมั่นคงปลอดภัยที่มุ่งไปข้างหน้าเหนือความเข้ากันได้กับผลิตภัณฑ์รุ่นเก่า บ่อยครั้งที่มีการรวมหรือเปิดใช้งานร่วมในคุณลักษณะของผลิตภัณฑ์รุ่นดั้งเดิมที่เข้ากันได้กับรุ่นเก่า แม้ว่าจะทำให้เกิดความเสี่ยงต่อความมั่นคงปลอดภัยของผลิตภัณฑ์ก็ตาม จัดลำดับความสำคัญของความมั่นคงปลอดภัยให้อยู่เหนือความเข้ากันได้กับรุ่นเก่า โดยให้ทีมความมั่นคงปลอดภัยสามารถลบคุณลักษณะที่ไม่ปลอดภัยออกไปได้ แม้ว่าจะเป็นการเปลี่ยนแปลงครั้งใหญ่ก็ตาม
- ติดตามและลดขนาดของ "แนวทางที่เพิ่มความเข้มงวด" ลดขนาดของ "แนวทางที่เพิ่มความเข้มงวด" ที่ผลิตขึ้นสำหรับผลิตภัณฑ์และพยายามทำให้แน่ใจว่าขนาดจะลดลงตามเวลาเมื่อมีการเปิดตัวซอฟต์แวร์เวอร์ชันใหม่ บูรณาการส่วนประกอบของ "แนวทางที่เพิ่มความเข้มงวด" ให้เป็นส่วนหนึ่งของการกำหนดตั้งค่าเริ่มต้นของผลิตภัณฑ์ คณะผู้จัดทำเอกสารตระหนักว่าการทำให้แนวทางที่เพิ่มความเข้มงวดนี้สั้นลงเป็นผลมาจากความร่วมมืออย่างต่อเนื่องกับลูกค้าที่มีอยู่ และรวมถึงความพยายามของทีมผลิตภัณฑ์จำนวนมาก รวมถึงประสบการณ์ผู้ใช้ (User experience - UX)
- พิจารณาประสบการณ์ผู้ใช้ที่เป็นผลเนื่องมาจากการตั้งค่าความมั่นคงปลอดภัย ในการตั้งค่าใหม่แต่ละครั้งจะไปเพิ่มภาระด้านการรับรู้ของผู้ใช้ปลายทาง และควรได้รับการประเมินร่วมกับประโยชน์ทางธุรกิจที่จะได้รับด้วย ตามหลักการแล้วไม่ควรมีการตั้งค่า แต่ควรรวมการตั้งค่าที่มั่นคงปลอดภัยที่สุดไว้ในผลิตภัณฑ์ตามการตั้งค่าเริ่มต้นแทน เมื่อจำเป็นต้องกำหนดตั้งค่า
  ทางเลือกการตั้งค่าเริ่มต้นควรมีความมั่นคงปลอดภัยในวงกว้างจากภัยคุกคามทั่วไป

คณะผู้จัดทำเอกสารยอมรับว่าการเปลี่ยนแปลงเหล่านี้อาจมีผลต่อการดำเนินการใช้งานของซอฟต์แวร์ ดังนั้น ข้อมูลจากลูกค้าจึงมีความสำคัญอย่างยิ่งในการสร้างความสมดุลในระหว่างการพิจารณาด้านการปฏิบัติงานและความมั่นคงปลอดภัย คณะผู้จัดทำเอกสารเชื่อว่าการพัฒนาแผนการทำงานที่เป็นลายลักษณ์อักษรและการสนับสนุนจากผู้บริหารที่จัดลำดับความสำคัญของแนวคิดเหล่านี้ลงในผลิตภัณฑ์ที่สำคัญที่สุดขององค์กรเป็นขั้นตอนแรกในการปรับเปลี่ยนไปสู่แนวปฏิบัติการพัฒนาซอฟต์แวร์ที่มีความมั่นคงปลอดภัย แม้ว่าความคิดเห็นของลูกค้าจะมีความสำคัญ แต่คณะผู้จัดทำเอกสารได้สังเกตเห็นกรณีสำคัญที่ลูกค้าไม่เต็มใจหรือไม่สามารถนำมาตรฐานที่ได้รับการปรับปรุงแล้วมาใช้ ซึ่งมักจะเป็นโปรโตคอลเครือข่าย เป็นสิ่งสำคัญสำหรับผู้ผลิตที่จะสร้างแรงจูงใจที่มีความหมายเพื่อให้ลูกค้าได้ติดตามข่าวสารปัจจุบันเสมอ และไม่ปล่อยให้พวกเขาอยู่ในภาวะเปราะบางอย่างไม่มีที่สิ้นสุด

เปรียบเทียบแนวทางที่เพิ่มความเข้มงวดกับแนวทางที่ลดความเข้มงวด

แนวทางที่เพิ่มความเข้มงวดอาจเป็นผลมาจากการขาดการควบคุมความมั่นคงปลอดภัยของผลิตภัณฑ์ที่ฝังอยู่ในสถาปัตยกรรมการใช้งานของผลิตภัณฑ์ตั้งแต่เริ่มต้นการพัฒนา ด้วยเหตุนี้ แนวทางที่เพิ่มความเข้มงวดยังสามารถนำมาใช้เป็นแผนการทำงานที่ตรงข้ามได้ในการระบุและใช้ประโยชน์จากคุณสมบัติที่ไม่ปลอดภัยได้อีกด้วย เป็นเรื่องปกติสำหรับองค์กรจำนวนมากที่จะไม่ทราบเกี่ยวกับแนวทางที่เพิ่มความเข้มงวดนี้ ดังนั้นพวกเขาจึงปล่อยให้การกำหนดตั้งค่าอุปกรณ์ไว้ในระบบที่ไม่ปลอดภัย แบบจำลองที่ย้อนแย้งกัน ซึ่งเรียกกันว่าแนวทางที่ลดเข้มงวดควรจะนำมาแทนที่แนวทางที่เพิ่มความเข้มงวดดังกล่าว และให้คำอธิบายแก่ผู้ใช้ว่าควรทำการเปลี่ยนแปลงอะไรบ้าง ขณะเดียวกันก็แสดงรายการความเสี่ยงด้านความมั่นคงปลอดภัยที่เป็นผลตามมาด้วย

แทนที่จะพัฒนาแนวทางที่เพิ่มความเข้มงวด ซึ่งแสดงรายการรักษาความมั่นคงปลอดภัยของผลิตภัณฑ์ คณะผู้จัดทำเอกสารขอแนะนำให้ผู้ผลิตซอฟต์แวร์เปลี่ยนไปใช้แนวทางตามหลักความปลอดภัยโดยการตั้งค่าเริ่มต้นโดยให้แนวทางที่ลดเข้มงวดกับผู้ใช้ไปด้วย แนวทางเหล่านี้อธิบายถึงการตัดสินใจด้านความเสี่ยงทางธุรกิจในภาษาที่เข้าใจง่าย และสามารถเพิ่มความตระหนักระดับองค์กรเกี่ยวกับความเสี่ยงต่อการบุกรุกทางไซเบอร์ที่เป็นอันตราย การแลกเปลี่ยนความมั่นคงปลอดภัยควรถูกกำหนดโดยผู้บริหารระดับสูงของลูกค้า โดยพิจารณาความสมดุลระหว่างความมั่นคงปลอดภัยกับความต้องการทางธุรกิจด้านอื่น

คำแนะนำสำหรับลูกค้า

คณะผู้จัดทำเอกสารขอแนะนำให้องค์กรถือว่าผู้ผลิตเทคโนโลยีที่ให้บริการนั้นเป็นผู้รับผิดชอบต่อผลลัพธ์ด้านความมั่นคงปลอดภัยของผลิตภัณฑ์ของตน ในฐานะที่เป็นส่วนหนึ่งของเรื่องนี้ คณะผู้จัดทำเอกสารจึงขอแนะนำให้ผู้บริหารองค์กรจัดลำดับความสำคัญของการซื้อผลิตภัณฑ์ที่มีความปลอดภัยโดยการออกแบบ (Secure-by-Design) และมีความปลอดภัยโดยการตั้งค่าเริ่มต้น (Secure-by-Default) ซึ่งสามารถแสดงออกผ่านนโยบายที่กำหนดให้ฝ่ายสารสนเทศต้องประเมินความมั่นคงปลอดภัยของซอฟต์แวร์จากผู้ผลิตก่อนที่จะซื้อ รวมทั้งให้อำนาจฝ่ายสารสนเทศในการปฏิเสธได้หากจำเป็น ฝ่ายสารสนเทศควรมีอำนาจในการพัฒนาเกณฑ์การจัดซื้อที่เน้นความสำคัญของแนวปฏิบัติตามหลักความปลอดภัยโดยการออกแบบและความปลอดภัยโดยการตั้งค่าเริ่มต้น (ทั้งที่ระบุไว้ในเอกสารฉบับนี้และฉบับอื่น ๆ ที่พัฒนาโดยองค์กร) นอกจากนี้ ฝ่ายสารสนเทศควรได้รับการสนับสนุนจากฝ่ายบริหารเมื่อมีการบังคับใช้เกณฑ์เหล่านี้ในการตัดสินใจจัดซื้อ การตัดสินใจขององค์กรในการยอมรับความเสี่ยงที่เกี่ยวข้องกับผลิตภัณฑ์เทคโนโลยีเฉพาะควรได้รับการบันทึกอย่างเป็นทางการ ได้รับการอนุมัติโดยผู้บริหารระดับสูงของธุรกิจ และนำเสนอต่อคณะกรรมการบริษัทอย่างสม่ำเสมอ

บริการด้านสารสนเทศขององค์กรขนาดใหญ่ที่สนับสนุนระบบการรักษาความมั่นคงปลอดภัยขององค์กร เช่น เครือข่ายขององค์กร การจัดการข้อมูลอัตลักษณ์ขององค์กรและการเข้าถึง และการดำเนินการด้านความมั่นคงปลอดภัยและความสามารถในการตอบสนอง ควรได้รับการพิจารณาว่าเป็นหน้าที่ทางธุรกิจที่สำคัญ ซึ่งได้รับทุนสนับสนุนเพื่อให้สอดคล้องกับความสำคัญต่อความสำเร็จของภารกิจองค์กร องค์กรควรพัฒนาแผนในการอัปเกรดความสามารถเหล่านี้เพื่อใช้ประโยชน์จากผู้ผลิตที่ใช้หลักการตามความปลอดภัยโดยการออกแบบ และความปลอดภัยโดยการตั้งค่าเริ่มต้น

หากเป็นไปได้ องค์กรควรพยายามสร้างความสัมพันธ์เชิงกลยุทธ์กับซัพพลายเออร์ด้านสารสนเทศที่สำคัญของพวกเขา ความสัมพันธ์ดังกล่าวรวมถึงความไว้วางใจในระดับต่าง ๆ ขององค์กรและใช้เป็นเครื่องมือให้สามารถแก้ไขปัญหาและระบุลำดับความสำคัญที่มีร่วมกันได้ ความมั่นคงปลอดภัยควรเป็นองค์ประกอบที่สำคัญของความสัมพันธ์และองค์กรดังกล่าวควรพยายามอย่างเต็มที่ที่จะส่งเสริมความสำคัญของแนวปฏิบัติตามหลักความปลอดภัยโดยการออกแบบและความปลอดภัยโดยการตั้งค่าเริ่มต้น ทั้งในรูปแบบที่เป็นทางการ (เช่น การทำสัญญาหรือข้อตกลงกับผู้ขาย) และในมิติความสัมพันธ์แบบไม่เป็นทางการ องค์กรควรคาดหวังความโปร่งใสจากซัพพลายเออร์ด้านเทคโนโลยีเกี่ยวกับระบบควบคุมภายในของพวกเขา รวมทั้งแผนการทำงานเพื่อนำมาปรับใช้ในแนวปฏิบัติตามหลักความปลอดภัยโดยการออกแบบและความปลอดภัยโดยการตั้งค่าเริ่มต้น

นอกจากการกำหนดให้ความสำคัญตามหลักความปลอดภัยโดยการตั้งค่าเริ่มต้นภายในองค์กรแล้ว ผู้นำด้านสารสนเทศควรร่วมมือกับเพื่อนร่วมอาชีพในอุตสาหกรรมของตนเพื่อทำความเข้าใจว่าผลิตภัณฑ์และบริการใดที่รวมอยู่ในหลักการออกแบบเหล่านี้ได้ดีที่สุด ผู้นำเหล่านี้ ควรประสานงานด้านคำร้องขอของพวกเขาเพื่อช่วยให้ผู้ผลิตจัดลำดับความสำคัญของความคิดริเริ่มด้านความมั่นคงปลอดภัยที่กำลังจะเกิดขึ้น โดยการทำงานร่วมกัน ลูกค้าจะสามารถให้ข้อมูลที่มีความหมายต่อผู้ผลิตและสร้างแรงจูงใจให้พวกเขาเพื่อจัดลำดับความสำคัญด้านความมั่นคงปลอดภัยขึ้นมา

เมื่อใช้ประโยชน์จากระบบคลาวด์ (Cloud) องค์กรควรตรวจสอบเพื่อให้เกิดความมั่นใจว่าตนเองเข้าใจรูปแบบความรับผิดชอบร่วมกันกับซัพพลายเออร์ด้านเทคโนโลยีของตน นั่นคือ องค์กรควรมีความชัดเจนเกี่ยวกับความรับผิดชอบด้านความมั่นคงปลอดภัยของซัพพลายเออร์ไม่ใช่เพียงแค่ความรับผิดชอบของลูกค้าเท่านั้น องค์กรควรจัดลำดับความสำคัญของผู้ให้บริการระบบคลาวด์ (Cloud) ที่ต้องมีความโปร่งใสเกี่ยวกับระบบความมั่นคงปลอดภัย การควบคุมภายใน และความสามารถในการปฏิบัติตามภาระหน้าที่ของตนภายใต้แบบจำลองความรับผิดชอบที่มีร่วมกัน

ข้อจำกัดความรับผิดชอบ (Disclaimer)

ข้อมูลในเอกสารนี้ได้รับการจัดหา "ตามสภาพที่เป็น" เพื่อวัตถุประสงค์ในการให้ข้อมูลเท่านั้น CISA และคณะผู้จัดทำเอกสารไม่ขอรับรองผลิตภัณฑ์หรือบริการเชิงพาณิชย์ รวมถึงหัวข้อการวิเคราะห์ใด ๆ การอ้างอิงถึงองค์กรหรือผลิตภัณฑ์เชิงพาณิชย์ กระบวนการ หรือบริการโดยเครื่องหมายบริการ เครื่องหมายการค้า ผู้ผลิต หรืออื่น ๆ ไม่ถือว่าเป็นการรับรอง การแนะนำ หรือการทำให้เกิดความลำเอียงโดย CISA และคณะผู้จัดทำเอกสาร เอกสารนี้เป็นความคิดริเริ่มร่วมกันของ CISA ซึ่งไม่ได้ทำหน้าที่เป็นเอกสารกำกับดูแลโดยอัตโนมัติ

ทรัพยากรข้อมูล

CISA

- คำแนะนำ SBOM โดย CISA
- เป้าหมายประสิทธิภาพการทำงานด้านความมั่นคงปลอดภัยทางไซเบอร์ระหว่างภาคธุรกิจ โดย CISA
- แนวทางเกี่ยวกับการทำงานร่วมกันของเทคโนโลยี
- การป้องกันการโจมตีต่อซอฟต์แวร์ซัพพลายเชน โดย CISA และ NIST
- ต้นทุนของเทคโนโลยีที่ไม่ปลอดภัยและสิ่งที่เราสามารถทำได้ | โดย CISA
- หยุดการกล่าวโทษกันในด้านความมั่นคงปลอดภัยทางไซเบอร์
  เหตุใดบริษัทจึงต้องสร้างความปลอดภัยในผลิตภัณฑ์เทคโนโลยี (เว็บไซต์ foreignaffairs.com)
- คำแนะนำเกี่ยวกับการจัดประเภทของจุดอ่อนเฉพาะกลุ่มผู้มีส่วนได้ส่วนเสีย (SSVC) โดย CISA
- ข้อเท็จจริง MFA เกี่ยวกับต้านการฟิชชิ่ง โดย CISA
- คำแนะนำทางไซเบอร์สำหรับธุรกิจขนาดเล็ก |โดย CISA

NSA

- เอกสารข้อมูลความมั่นคงปลอดภัยทางไซเบอร์เรื่องความปลอดภัยของหน่วยความจำ โดย NSA
- ความมั่นคงปลอดภัยด้าน ESF สำหรับซัพพลายเชนของซอฟต์แวร์ โดย NSA
  วิธีปฏิบัติที่ดีที่สุดสำหรับซัพพลายเออร์

FBI

- การทำความเข้าใจและตอบสนองต่อการโจมซัพพลายเชน SolarWinds มุมมองจากสำนักงานสอบสวนกลาง
- การคุกคามทางไซเบอร์ - การตอบสนองและการรายงาน
- กลยุทธ์ไซเบอร์ของ FBI

สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology - NIST)

- แนวปฏิบัติเกี่ยวกับข้อมูลจำแนกตัวตนดิจิตอล โดย NIST
- กรอบโครงสร้างความมั่นคงปลอดภัยทางไซเบอร์ โดย NIST
- กรอบโครงสร้างการพัฒนาซอฟต์แวร์อย่างปลอดภัย (SSDF) โดย NIST

ศูนย์รักษาความปลอดภัยทางไซเบอร์แห่งออสเตรเลีย(ACSC)

- แนวทางปฏิบัติสำหรับโค้ด IoT สำหรับบริษัทผู้ผลิต โดย ACSC

ศูนย์รักษาความปลอดภัยไซเบอร์แห่งชาติสหราชอาณาจักร(UK)

- กรอบโครงสร้างความมั่นคงปลอดภัยทางไซเบอร์ของสหราชอาณาจักร
- คำแนะนำการพัฒนาและการปรับใช้งานที่ปลอดภัย โดย NCSC แห่งสหราชอาณาจักร
- คำแนะนำในการจัดการจุดอ่อน โดย NCSC แห่งสหราชอาณาจักร
- ชุดเครื่องมือการเปิดเผยจุดอ่อน โดย NCSC แห่งสหราชอาณาจักร
- หลักการ CHERI โดยมหาวิทยาลัยแคมบริดจ์
- ลาก่อนและขอขอบคุณสำหรับทุกสิ่ง NCSC.GOV.UK

ศูนย์รักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งแคนาดา หรือ Canadian Centre for Cyber Security (CCS)

- คู่มือการป้องกันการโจมตีต่อซัพพลายเชนของซอฟต์แวร์ โดย CCCS
- ซัพพลายเชนทางไซเบอร์แนวทางการประเมินความเสี่ยง
- คำแนะนำเกี่ยวกับแรนซัมแวร์ CONTI โดยศูนย์รักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งแคนาดา

สำนักงานความมั่นคงปลอดภัยของข้อมูลแห่งสหพันธรัฐเยอรมนี หรือ Germany’s Federal Office for Information Security (BSI)

- บทสรุป BSI Grundschutz (module CON.8)
- มาตรฐานระหว่างประเทศ IEC 62443 ตอนที่ 4-1
- รายงานสถานการณ์ความมั่นคงปลอดภัยด้านไอทีของประเทศเยอรมนีปี 2022
- แนวปฏิบัติ BSI ในการรักษาความปลอดภัยแอปพลิเคชันบนเว็บ

ศูนย์ความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติเนเธอร์แลนด์ หรือ Netherlands’ National Cyber Security Centre

- แผ่นข้อมูลการยืนยันตัวตนที่พร้อมใช้งาน โดย NCSC-NL

อื่น ๆ

- ระบบที่ซับซ้อนล้มเหลวอย่างไร
- รูปลักษณ์ใหม่ในความล้มเหลวของระบบที่ซับซ้อน