TLP:CLEAR

ความปลอดภัยโดยการออกแบบ

การปรับสมดุลของความเสี่ยง

ด้านความมั่นคงปลอดภัยทางไซเบอร์:

หลักการและวิธีการสำหรับ ความปลอดภัยโดยการออกแบบซอฟต์แวร์

TLP:CLEAR

Communications Security Establishment

Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications

Centre canadien pour la cybersécurité

สารบัญ

ภาพรวม : ช่องโหว่ที่เกิดจากการออกแบบ

เทคโนโลยีถูกผนวกรวมให้เข้ากับชีวิตประจำวันเกือบทุกด้าน เนื่องจากระบบที่เชื่อมต่อกับอินเทอร์เน็ตเชื่อมโยงเราเข้ากับระบบต่าง ๆ ที่สำคัญซึ่งส่งผลกระทบโดยตรงต่อความมั่งคั่งทางเศรษฐกิจ การดำรงชีวิต และแม้แต่สุขภาพของเรา ตั้งแต่การจัดการอัตลักษณ์ส่วนบุคคลไปจนถึงการดูแลทางการแพทย์ ตัวอย่างหนึ่งของข้อเสียเปรียบของความสะดวกสบายดังกล่าวคือ การละเมิดทางไซเบอร์ที่ส่งผลให้โรงพยาบาลต้องยกเลิกการผ่าตัด และเปลี่ยนแนวทางการดูแลผู้ป่วยไปจากเดิม เทคโนโลยีและช่องโหว่หรือจุดบกพร่องต่าง ๆ ที่ไม่ปลอดภัยในระบบที่สำคัญอาจเปิดโอกาสให้เกิดการบุกรุกทางไซเบอร์ที่เป็นอันตราย ซึ่งนำไปสู่ความเสี่ยงด้านความปลอดภัย[1]ที่อาจเกิดขึ้นได้

ด้วยเหตุนี้ จึงเป็นสิ่งสำคัญที่ผู้ผลิตซอฟต์แวร์ต้องทำให้ระบบความปลอดภัยโดยการออกแบบ (Secure-by-Design) และความปลอดภัยโดยการตั้งค่าเริ่มต้น (Secure-by-Default) เป็นจุดสำคัญของกระบวนการออกแบบและพัฒนาผลิตภัณฑ์ ผู้จำหน่ายบางรายได้ก้าวกระโดดโดยผลักดันอุตสาหกรรมไปข้างหน้าด้วยการรับประกันซอฟต์แวร์ในขณะที่บางรายยังคงล้าหลังอยู่ คณะผู้จัดทำเอกสารสนับสนุนให้ผู้ผลิตเทคโนโลยีทุกรายสร้างผลิตภัณฑ์ของตนในลักษณะที่ช่วยลดภาระด้านความมั่นคงปลอดภัยทางไซเบอร์ให้กับลูกค้า รวมถึงช่วยป้องกันไม่ให้ลูกค้าต้องดำเนินการเฝ้าระวัง การอัปเดตตามเวลา และการควบคุมความเสียหายของระบบอย่างต่อเนื่องเพื่อรับมือกับการบุกรุกทางไซเบอร์ นอกจากนี้ เรายังสนับสนุนให้ผู้ผลิตซอฟต์แวร์สร้างผลิตภัณฑ์ของตนในลักษณะที่อำนวยความสะดวกให้กับระบบออโตเมชันในการกำหนดตั้งค่า การเฝ้าระวังระบบ และการอัปเดตตามเวลา ผู้ผลิตได้รับการสนับสนุนให้แสดงความเป็นเจ้าของรับผิดชอบการปรับปรุงผลลัพธ์ด้านความปลอดภัยให้กับลูกค้าของตน ในอดีต ผู้ผลิตซอฟต์แวร์ได้พึ่งพาการแก้ไขช่องโหว่ที่ลูกค้าพบหลังจากที่ได้นำผลิตภัณฑ์ไปปรับใช้งานแล้ว ซึ่งทำให้ลูกค้าต้องแก้ไขด้วยการใช้แพตช์ (Patch) เหล่านั้นโดยเสียค่าใช้จ่ายเอง โดยการผสมผสานแนวปฏิบัติตามหลักความปลอดภัยโดยการออกแบบเท่านั้นที่เราจะสามารถทำลายวงจรปัญหาของการสร้างและการหาทางแก้ไขที่ต้องทำอย่างต่อเนื่องเหล่านี้ **หมายเหตุ** คำว่า “ความปลอดภัยโดยการออกแบบ” หมายรวมถึงทั้งความปลอดภัยโดยการออกแบบ (Secure by design) และความปลอดภัยโดยการตั้งค่าเริ่มต้น (Secure by default)

เพื่อให้บรรลุมาตรฐานความปลอดภัยของซอฟต์แวร์ในระดับสูงเช่นนี้ คณะผู้จัดทำเอกสารจึงสนับสนุนให้ผู้ผลิตจัดลำดับความสำคัญของการบูรณาการความปลอดภัยของผลิตภัณฑ์ให้เป็นข้อกำหนดเบื้องต้นที่สำคัญสำหรับคุณลักษณะและความรวดเร็วในการออกสู่ตลาด เมื่อเวลาผ่านไป ทีมวิศวกรจะสามารถสร้างจังหวะความสม่ำเสมอใหม่ที่ผนวกความปลอดภัยเข้ากับการออกแบบอย่างแท้จริง และใช้ความพยายามในการบำรุงรักษาน้อยลง

เพื่อเป็นการสะท้อนถึงมุมมองนี้ สหภาพยุโรปได้เน้นย้ำถึงความสำคัญของความปลอดภัยของผลิตภัณฑ์ใน พระราชบัญญัติความยืดหยุ่นทางไซเบอร์ (Cyber Resilience Act) โดยเน้นว่า ผู้ผลิตควรใช้หลักความปลอดภัยนี้ไปตลอดวงจรชีวิตของผลิตภัณฑ์เพื่อป้องกันไม่ให้ผู้ผลิตนำผลิตภัณฑ์ที่มีความเสี่ยงเข้าสู่ตลาด เพื่อสร้างอนาคตที่เทคโนโลยีและผลิตภัณฑ์ที่เกี่ยวข้องมีความปลอดภัยมากขึ้นสำหรับลูกค้า คณะผู้จัดทำเอกสาร

[1] คณะผู้จัดทำเอกสารตระหนักดีว่าคำว่า “ความปลอดภัย” มีความหมายหลายแง่ขึ้นอยู่กับบริบทที่ใช้งาน สำหรับวัตถุประสงค์ของคำแนะนำนี้ “ความปลอดภัย” จะหมายถึงการยกระดับมาตรฐานความมั่นคงปลอดภัยของเทคโนโลยี เพื่อให้การคุ้มครองลูกค้าจากการกิจกรรมทางไซเบอร์ที่เป็นอันตราย

จึงเรียกร้องให้ผู้ผลิตปรับปรุงโปรแกรมการออกแบบและพัฒนาของตนเพื่อให้มีการจัดส่งผลิตภัณฑ์ที่มีความปลอดภัยโดยการออกแบบและโดยการตั้งค่าเริ่มต้นเท่านั้น ก่อนการพัฒนา ผลิตภัณฑ์ที่ใช้หลักความปลอดภัยโดยการออกแบบจะได้รับการค้นคิดโดยคำนึงถึงความปลอดภัยของลูกค้าเป็นเป้าหมายหลักทางธุรกิจ ไม่ใช่เพียงแค่คุณลักษณะทางเทคนิคเท่านั้น ผลิตภัณฑ์ที่ใช้หลักความปลอดภัยโดยการออกแบบจะเริ่มต้นด้วยเป้าหมายนี้ก่อนที่จะเริ่มการพัฒนา ส่วนผลิตภัณฑ์เดิมที่มีอยู่ก็สามารถวิวัฒนาการไปสู่สถานะตามหลักความปลอดภัยโดยการออกแบบได้โดยผ่านการปรับเปลี่ยนหลายครั้ง ผลิตภัณฑ์ที่ใช้หลักความปลอดภัยด้วยการตั้งค่าเริ่มต้นมีความปลอดภัยที่จะใช้งานเมื่อตอน “แกะกล่อง” โดยไม่จำเป็นต้องเปลี่ยนแปลงการกำหนดตั้งค่าหรือเปลี่ยนแปลงน้อย และมีคุณลักษณะด้านความปลอดภัยให้ใช้งานได้โดยไม่ต้องเสียค่าใช้จ่ายเพิ่ม ปรัชญาทั้งสองนี้จะร่วมกันย้ายโอนภาระของการรักษาความปลอดภัยไปยังผู้ผลิตและลดโอกาสที่ลูกค้าจะตกเป็นเหยื่อของเหตุการณ์ด้านความปลอดภัย ซึ่งเกิดจากการกำหนดตั้งค่าผิดพลาด การแก้ไขโดยใช้แพตช์ (Patch) ที่ไม่รวดเร็วเพียงพอ หรือปัญหาทั่วไปอื่น ๆ อีกมากมาย

คณะกรรมาธิการความมั่นคงปลอดภัยทางไซเบอร์และโครงสร้างพื้นฐาน (Cybersecurity and Infrastructure Security Agency - CISA) คณะกรรมาธิการความมั่นคงแห่งชาติ (National Security Agency - NSA) สำนักงานสอบสวนกลาง (Federal Bureau of Investigation - FBI) และพันธมิตรระหว่างประเทศ[2] ต่อไปนี้ ให้คำแนะนำในคู่มือนี้เพื่อใช้เป็นแผนการทำงานสำหรับผู้ผลิตซอฟต์แวร์ในการรับรองความปลอดภัยของผลิตภัณฑ์ของตน

- ศูนย์รักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งออสเตรเลีย (Australian Cyber Security Centre - ACSC)
- ศูนย์รักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งแคนาดา (Canadian Centre for Cyber Security - CCCS)
- ศูนย์รักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติสหราชอาณาจักร (United Kingdom’s National Cyber Security Centre - NCSC-UK)
- สำนักงานความมั่นคงปลอดภัยของข้อมูลแห่งสหพันธรัฐเยอรมนี (Germany’s Federal Office for Information Security - BSI)
- ศูนย์รักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติเนเธอร์แลนด์ (Netherlands’ National Cyber Security Centre - NCSC-NL)
- ศูนย์ความมั่นคงปลอดภัยทางไซเบอร์แห่งชาตินอร์เวย์ (Norway’s National Cyber Security Centre - NCSC-NO)
- ทีมช่วยเหลือฉุกเฉินทางคอมพิวเตอร์นิวซีแลนด์ (Computer Emergency Response Team New Zealand - CERT-NZ) และศูนย์รักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาตินิวซีแลนด์ (National Cyber Security Centre - NCSC-NZ)
- คณะกรรมาธิการอินเตอร์เน็ตและความมั่นคงปลอดภัยแห่งเกาหลี (Korea Internet & Security Agency - KISA)
- คณะกรรมาธิการไซเบอร์แห่งชาติอิสราเอล (Israel’s National Cyber Directorate - INCD)
- ศูนย์เตรียมความพร้อมเหตุการณ์และยุทธศาสตร์เพื่อความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติญี่ปุ่น (Japan’s National Center of Incident Readiness and Strategy for Cybersecurity - NISC) และศูนย์ประสานงานทีมตอบสนองเหตุฉุกเฉินคอมพิวเตอร์ญี่ปุ่น (Japan Computer Emergency Response Team Coordination Center - JPCERT/CC)
- เครือข่าย OAS/CICTE ทีมรับมือเหตุการณ์ไซเบอร์ของรัฐบาลทวีปอเมริกา (OAS/CICTE Network of Government Cyber Incident Response Teams (CSIRT) Americas)
- คณะกรรมาธิการความมั่นคงปลอดภัยทางไซเบอร์แห่งสิงคโปร์ (Cyber Security Agency of Singapore - CSA)
- คณะกรรมาธิการความมั่นคงปลอดภัยทางไซเบอร์และข้อมูลแห่งชาติสาธารณรัฐเช็ก (Czech Republic’s National Cyber and Information Security Agency - NÚKIB)

คณะผู้จัดทำเอกสารให้ความสำคัญกับการสนับสนุนจากพันธมิตรภาคเอกชนจำนวนมากในการปรับปรุงความปลอดภัยโดยการออกแบบและความปลอดภัยโดยการตั้งค่าเริ่มต้น เอกสารฉบับนี้มีวัตถุประสงค์เพื่อทำให้เกิดความก้าวหน้าในการสนทนาระหว่างประเทศเกี่ยวกับลำดับความสำคัญหลัก การลงทุน และการตัดสินใจที่จำเป็นเพื่อให้บรรลุเป้าหมายในอนาคตที่เทคโนโลยีจะมีความปลอดภัย มั่นคง และยืดหยุ่นตามการออกแบบและการตั้งค่าเริ่มต้น ด้วยเหตุนี้ คณะผู้จัดทำเอกสารจึงใคร่ขอความคิดเห็นเกี่ยวกับเอกสารฉบับนี้จากผู้สนใจ และเราตั้งใจที่จะจัดการประชุมรับฟังเพื่อปรับปรุง ระบุรายละเอียด และพัฒนาคำแนะนำเพิ่มเติมเพื่อให้บรรลุเป้าหมายที่มีร่วมกันของเรา

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับความสำคัญของความปลอดภัยของผลิตภัณฑ์ โปรดดูบทความโดย CISA ในเรื่อง ต้นทุนของเทคโนโลยีที่ไม่ปลอดภัยและสิ่งที่เราสามารถทำได้เกี่ยวกับเทคโนโลยีนั้น (The Cost of Unsafe Technology and What We Can Do About It.)

[2] ต่อจากนี้ จะเรียกว่า “คณะผู้จัดทำเอกสาร”

มีอะไรใหม่บ้าง

ในการตีพิมพ์ครั้งแรก ได้มีการสนทนาถึงรายงานฉบับนี้กันอย่างมากมายภายในอุตสาหกรรมซอฟต์แวร์ ข่าวรายวันที่องค์กรและบุคคลถูกละเมิดความปลอดภัยเน้นย้ำให้เห็นถึงความจำเป็นในการสนทนาเพิ่มเติมเกี่ยวกับวิธีแก้ไขปัญหาเชิงระบบที่เรื้อรังในผลิตภัณฑ์ซอฟต์แวร์

หลังจากการเผยแพร่ไปเมื่อเดือนเมษายน 2023 คณะผู้จัดทำเอกสาร (ต่อไปนี้จะกล่าวถึงว่า “เรา” และ “ของเรา”) ได้รับคำแนะนำจากการตอบรับที่เป็นประโยชน์มากมายจากบุคคล บริษัท และสมาคมการค้าหลายร้อยราย คำร้องขอที่พบบ่อยที่สุดในคำแนะนำที่ได้รับมาคือ การขอรายละเอียดเพิ่มเติมว่าหลักการสามประการเกี่ยวข้องกับทั้งผู้ผลิตซอฟต์แวร์และลูกค้าของพวกเขาอย่างไร ในเอกสารนี้ เราจะขยายความเพิ่มเติมจากที่ให้ไว้ในรายงานฉบับแรกเริ่มและกล่าวถึงประเด็นอื่น ๆ เช่น ขนาดของผู้ผลิตและลูกค้าที่ใช้ผลิตภัณฑ์ ประสบการณ์ของลูกค้า และขอบเขตของหลักการที่เรากำลังพูดคุยกัน

ซอฟต์แวร์มีอยู่ทุกที่และไม่มีรายงานใดเพียงฉบับเดียวที่สามารถครอบคลุมเนื้อหาทั้งหมดได้อย่างเพียงพอ ไม่ว่าจะเป็นเรื่องระบบซอฟต์แวร์ การพัฒนาผลิตภัณฑ์ซอฟต์แวร์ การปรับใช้งานและการบำรุงรักษาของลูกค้า และการเชื่อมต่อกับระบบอื่น ๆ สำหรับคำแนะนำด้านล่างนี้ ซึ่งอาจไม่ตรงกับสถานการณ์ใดอย่างเฉพาะเจาะจงนั้น เรายินดีรับฟังจากผู้คนในชุมชนว่าการปฏิบัติตามคำแนะนำในเอกสารนี้จะช่วยปรับปรุงความปลอดภัยประเภทนั้น ๆ ได้อย่างไร

รายงานนี้ยังใช้กับผู้ผลิตระบบและรุ่นหรือโมเดลซอฟต์แวร์ปัญญาประดิษฐ์ (Artificial Intelligence - AI) อีกด้วย แม้ว่าอาจมีความแตกต่างจากซอฟต์แวร์รูปแบบดั้งเดิม แต่แนวปฏิบัติขั้นพื้นฐานด้านความปลอดภัยยังคงมีความสำคัญสำหรับระบบและโมเดล AI อยู่ แนวปฏิบัติตามหลักความปลอดภัยโดยการออกแบบบางประการอาจต้องมีการปรับเปลี่ยนเพื่อคำนึงถึงข้อควรพิจารณาเฉพาะของ AI แต่หลักการที่ครอบคลุมทั้งสามประการด้านความปลอดภัยโดยการออกแบบยังนำไปใช้กับระบบ AI ได้ทั้งหมด

เราตระหนักดีว่าการเปลี่ยนแปลงวงจรชีวิตการพัฒนาซอฟต์แวร์ (Software Development Lifecycle - SDLC) เพื่อให้สอดคล้องตามหลักการความความปลอดภัยโดยการออกแบบเหล่านี้ไม่ใช่เรื่องง่ายและอาจต้องใช้เวลาพอสมควร นอกจากนี้ ผู้ผลิตซอฟต์แวร์ขนาดเล็กอาจพบว่าการนำคำแนะนำเหล่านี้ไปปฏิบัติเป็นเรื่องยาก เราเชื่อว่าอุตสาหกรรมซอฟต์แวร์จำเป็นต้องจัดให้มีเครื่องมือและขั้นตอนปฏิบัติต่าง ๆ เพื่อที่จะช่วยให้ผลิตภัณฑ์ปลอดภัยยิ่งขึ้นในวงกว้าง ในขณะที่ผู้คนและองค์กรมุ่งความสนใจไปสู่การปรับปรุงความปลอดภัยของซอฟต์แวร์มากขึ้น เราเชื่อว่ายังมีโอกาสสำหรับแนวคิดใหม่ ๆ ที่จะช่วยลดช่องว่างระหว่างผู้ผลิตซอฟต์แวร์รายใหญ่และรายเล็กให้แคบลงเพื่อประโยชน์ของลูกค้าโดยรวม

การอัปเดตรายงานความปลอดภัยโดยการออกแบบฉบับแรกเริ่มนี้ เป็นส่วนหนึ่งของความมุ่งมั่นของเราที่จะสร้างความร่วมมือกับชุมชนผู้มีส่วนได้ส่วนเสียที่เชื่อมต่อถึงกันจำนวนมากอันเป็นรากฐานของระบบนิเวศทางเทคโนโลยีของเรา ทั้งนี้ เป็นผลจากคำแนะนำที่เราได้รับมาจากหลายส่วนของระบบนิเวศนั้น และเราจะคอยรับฟังและเรียนรู้จากมุมมองเหล่านั้นต่อไป แม้ว่าจะมีความท้าทายมากมายรออยู่ข้างหน้า แต่เราก็ยังรักษามุมมองในแง่บวกอยู่เสมอในขณะที่เราเรียนรู้เพิ่มเติมเกี่ยวกับผู้คนและองค์กรที่ได้นำปรัชญาตามหลักความปลอดภัยโดยการออกแบบมาใช้แล้ว ซึ่งมักจะประสบผลสำเร็จ

วิธีใช้เอกสารนี้

เราขอแนะนำให้ผู้ผลิตซอฟต์แวร์ปฏิบัติตามหลักการในเอกสารนี้ ผู้ผลิตซอฟต์แวร์สามารถแสดงให้เห็นถึงความมุ่งมั่นของตนด้วยการเผยแพร่บันทึกการดำเนินการของตนต่อสาธารณะ ตามขั้นตอนที่ทำเป็นรายการด้านล่างนี้ เราสนับสนุนให้ผู้ผลิตซอฟต์แวร์หากลวิธีที่สอดคล้องกับเจตนารมณ์ตามหลักการนี้ และสร้างหลักฐานสิ่งประดิษฐ์ที่จะทำให้เกิดกรณีที่น่าสนใจเพื่อโน้มน้าวลูกค้าปัจจุบันและผู้ที่อาจมาเป็นลูกค้าในอนาคตที่ยังสงสัยอยู่ได้ว่าผู้ผลิตกำลังปฏิบัติตามปรัชญาความปลอดภัยโดยการออกแบบอย่างแท้จริง

นอกเหนือจากการดำเนินการที่ผู้ผลิตซอฟต์แวร์ควรทำแล้ว ลูกค้ายังสามารถใช้ประโยชน์จากเอกสารนี้ได้อีกด้วย บริษัทที่ซื้อซอฟต์แวร์ควรถามคำถามที่ตอบยากกับผู้จำหน่ายของตน โดยดึงแนวคิดจากตัวอย่างของการปฏิบัติตามหลักการที่กล่าวถึงในเอกสารนี้ ในการทำเช่นนี้ ลูกค้าสามารถมีส่วนช่วยทำให้ตลาดโน้มเอียงไปสู่ผลิตภัณฑ์ที่เป็นไปตามหลักความปลอดภัยโดยการออกแบบมากขึ้น ตัวอย่างคำถามที่ลูกค้าอาจถามผู้จำหน่ายมีอยู่ใน<u>คำแนะนำของ CISA สำหรับการจัดหาเทคโนโลยี K-12 (CISA's Guidance for K-12 Technology Acquisitions)</u>

เราสนับสนุนให้ลูกค้าประเภทองค์กรรวมแนวปฏิบัติเหล่านี้ไว้ในกระบวนการธุรกิจต่าง ๆ ไม่ว่าจะเป็นการจัดซื้อ การประเมินการตรวจสอบสถานะของผู้จำหน่าย การตัดสินใจเกี่ยวกับการยอมรับความเสี่ยงขององค์กร และขั้นตอนอื่น ๆ ที่ดำเนินการเมื่อประเมินผู้จำหน่าย ลูกค้ายังควรผลักดันให้ผู้จำหน่ายแบ่งปันข้อปฏิบัติตามหลักความปลอดภัยโดยการออกแบบที่ผู้จำหน่ายแต่ละรายทำเพื่อให้สาธารณะได้รับรู้ เมื่อทุกฝ่ายร่วมมือกัน ก็จะเป็นการส่งสัญญาณอันทรงพลังถึงความสำคัญเรื่องความปลอดภัย ซึ่งสามารถส่งเสริมและช่วยให้ผู้ผลิตซอฟต์แวร์ก้าวไปสู่การทำให้ผลิตภัณฑ์ของตนมีความปลอดภัยมากขึ้น หรืออีกนัยหนึ่ง เช่นเดียวกับที่เราพยายามก่อให้เกิดปรัชญาตามหลักความปลอดภัยโดยการออกแบบให้แพร่หลายในวงการผู้ผลิตซอฟต์แวร์แล้ว เรายังจำเป็นต้องสร้างวัฒนธรรม "ความปลอดภัยโดยการเรียกร้อง" ให้กับลูกค้าของพวกเขาอีกด้วย

ความปลอดภัยโดยการออกแบบ (Secure by Design)

"ความปลอดภัยโดยการออกแบบ" หมายความว่าผลิตภัณฑ์เทคโนโลยีได้รับการสร้างขึ้นในลักษณะที่สามารถป้องกันไม่ให้ผู้กระทำการไซเบอร์ที่ไม่ประสงค์ดีเข้าถึงอุปกรณ์ ข้อมูล และโครงสร้างพื้นฐานที่เชื่อมต่อถึงกันได้ ผู้ผลิตซอฟต์แวร์ควรประเมินความเสี่ยงเพื่อระบุและแจกแจงภัยคุกคามทางไซเบอร์ที่เกิดขึ้นอย่างแพร่หลายต่อระบบที่สำคัญ และจากนั้นรวมการป้องกันไว้ในพิมพ์เขียวที่ใช้สร้างผลิตภัณฑ์ของตน แนวทางนี้ควรคำนึงถึงภาพรวมภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงได้ตลอดเวลา

แนวปฏิบัติในการพัฒนาเทคโนโลยีสารสนเทศ (Information Technology - IT) ที่ปลอดภัยและมีการป้องกันหลายระดับชั้นที่เรียกว่าการป้องกันเชิงลึก (Defense-in-Depth) ยังได้รับการแนะนำให้นำไปใช้เพื่อป้องกันผู้ไม่ประสงค์ดีจากการจู่โจมระบบหรือการเข้าถึงข้อมูลที่สำคัญโดยไม่ได้รับอนุญาตอีกด้วย คณะผู้จัดทำเอกสารยังแนะนำให้ผู้ผลิตใช้แบบจำลองภัยคุกคามที่ได้รับการปรับแต่งเพิ่มเติมในระหว่างขั้นตอนการพัฒนาผลิตภัณฑ์ เพื่อจัดการกับภัยคุกคามทั้งหมดที่อาจเกิดขึ้นกับระบบและเป็นเหตุผลสำหรับกระบวนการปรับใช้งานของแต่ละระบบ

คณะผู้จัดทำเอกสารเรียกร้องให้ผู้ผลิตใช้แนวปฏิบัติด้านความปลอดภัยแบบองค์รวมสำหรับผลิตภัณฑ์และแพลตฟอร์มของตน การพัฒนาตามหลักความปลอดภัยโดยการออกแบบต้องการการลงทุนเชิงกลยุทธ์ด้านทรัพยากรแบบเจาะจงเฉพาะจากผู้ผลิตซอฟต์แวร์ในแต่ละระดับชั้นของกระบวนการออกแบบและพัฒนาผลิตภัณฑ์ที่ไม่สามารถนำไป "พ่วงติด" ได้ในภายหลัง เป็นสิ่งจำเป็นที่ผู้บริหารธุรกิจระดับสูงสุดของผู้ผลิตต้องเป็นผู้นำที่แข็งแกร่งที่จัดลำดับให้ความปลอดภัยเป็นสิ่งสำคัญอันดับต้นของธุรกิจ ไม่ใช่แค่เพียงคุณลักษณะหนึ่งทางเทคนิคเท่านั้น ความร่วมมือระหว่างผู้นำธุรกิจและทีมเทคนิคนี้ ครอบคลุมตั้งแต่ขั้นตอนเบื้องต้นของการออกแบบและการพัฒนา ไปจนถึงการปรับใช้งานและการบำรุงรักษาของลูกค้า ผู้ผลิตได้รับการสนับสนุนให้ทำการประนีประนอมและลงทุนอย่างจริงจัง แม้ว่าจะเป็นการลงทุนที่ลูกค้า "มองไม่เห็น" ก็ตาม (เช่น การเปลี่ยนไปใช้ภาษาการเขียนโปรแกรมที่จะช่วยกำจัดช่องโหว่ทั่วไปที่พบกันอย่างแพร่หลาย) ผู้ผลิตควรมุ่งเน้นไปที่คุณลักษณะ กลไก และการนำเครื่องมือที่จะช่วยปกป้องลูกค้าออกใช้ มากกว่าคุณลักษณะของผลิตภัณฑ์ที่ดูน่าดึงดูดความสนใจแต่ไปขยายขอบเขตให้เสี่ยงต่อการถูกโจมตีมากขึ้น

ไม่มีวิธีแก้ปัญหาใดวิธีเดียวที่จะยุติภัยคุกคามที่เกิดขึ้นอย่างต่อเนื่องจากผู้กระทำการไซเบอร์ที่ไม่ประสงค์ดีซึ่งใช้ประโยชน์จากช่องโหว่ของเทคโนโลยี และผลิตภัณฑ์ที่มี "ความปลอดภัยโดยการออกแบบ" จะยังคงต้องประสบกับปัญหาจากช่องโหว่ต่อไป อย่างไรก็ตาม กลุ่มช่องโหว่หรือจุดบกพร่องจำนวนมากเกิดจากกลุ่มสาเหตุเบื้องหลังแท้จริงที่ค่อนข้างเล็ก ผู้ผลิตควรพัฒนาแผนการทำงานที่ชัดเจนเป็นลายลักษณ์อักษรเพื่อจัดกลุ่มผลิตภัณฑ์ที่มีอยู่ให้สอดคล้องกับแนวปฏิบัติตามหลักความปลอดภัยโดยการออกแบบมากขึ้น โดยให้แน่ใจว่าจะเบี่ยงเบนไปเฉพาะในสถานการณ์พิเศษเท่านั้น

คณะผู้จัดทำเอกสารยอมรับว่าการเป็นเจ้าของผลลัพธ์ด้านความปลอดภัยสำหรับลูกค้าและการสร้างความมั่นใจให้ลูกค้าต่อความปลอดภัยในระดับนี้ อาจทำให้ค่าใช้จ่ายในการพัฒนาผลิตภัณฑ์เพิ่มสูงขึ้น อย่างไรก็ตาม การลงทุนในแนวปฏิบัติตามหลักความปลอดภัยโดยการออกแบบไปพร้อมกับการพัฒนาผลิตภัณฑ์เทคโนโลยีที่เป็นนวัตกรรมใหม่และการบำรุงรักษาผลิตภัณฑ์ที่มีอยู่เดิมสามารถช่วยปรับปรุงจุดยืนด้านการรักษาความปลอดภัยให้ลูกค้าและลดโอกาสของการถูกละเมิดความปลอดภัยได้อย่างมีนัยสำคัญ หลักการความปลอดภัยโดยการออกแบบไม่เพียงแต่ช่วยเสริมสร้างจุดยืนด้านการรักษาความปลอดภัยให้ลูกค้าและชื่อเสียงของแบรนด์สำหรับนักพัฒนาเท่านั้น แต่แนวปฏิบัตินี้ยังช่วยลดค่าใช้จ่ายในการบำรุงรักษาและการแก้ไขโดยใช้แพตช์ (Patch) สำหรับผู้ผลิตในระยะยาวอีกด้วย

ส่วนคำแนะนำสำหรับผู้ผลิตซอฟต์แวร์ที่ระบุไว้ด้านล่างแสดงรายการแนวปฏิบัติและนโยบายการพัฒนาผลิตภัณฑ์ที่ให้ผู้ผลิตไว้พิจารณา

ความปลอดภัยโดยการตั้งค่าเริ่มต้น (Secure by Default)

"ความปลอดภัยโดยการตั้งค่าเริ่มต้น" หมายความว่าผลิตภัณฑ์มีความต้านทานต่อเทคนิคการหาประโยชน์ที่แพร่หลายตั้งแต่การแกะกล่องใช้งานโดยไม่ต้องมีค่าใช้จ่ายเพิ่มเติม ผลิตภัณฑ์เหล่านี้จะช่วยป้องกันภัยคุกคามและแก้ไขช่องโหว่ที่พบบ่อยที่สุดโดยผู้ใช้ปลายทางไม่ต้องดำเนินการเพื่อรักษาความปลอดภัยเพิ่มเติมใด ๆ ผลิตภัณฑ์ที่มีความปลอดภัยโดยการตั้งค่าเริ่มต้นได้รับการออกแบบมาเพื่อให้ลูกค้าตระหนักอย่างชัดเจนว่า หากพวกเขาเบี่ยงเบนไปจากการตั้งค่าเริ่มต้นที่ปลอดภัยแล้ว พวกเขาจะมีแนวโน้มที่จะถูกละเมิดความปลอดภัยมากขึ้น เว้นแต่จะใช้การควบคุมมาชดเชยเพิ่มเติม ความปลอดภัยโดยการตั้งค่าเริ่มต้นเป็นรูปแบบหนึ่งของความปลอดภัยโดยการออกแบบ

- การกำหนดตั้งค่าที่ปลอดภัยควรเป็นพื้นฐานเริ่มต้น ผลิตภัณฑ์ที่มีความปลอดภัยโดยการตั้งค่าเริ่มต้นเปิดใช้งานการควบคุมความปลอดภัยที่สำคัญที่สุดโดยอัตโนมัติ ซึ่งจำเป็นต่อการปกป้องค์กรจากผู้กระทำการไซเบอร์ที่ไม่ประสงค์ดี รวมถึงให้ความสามารถในการใช้งานและกำหนดตั้งค่าการควบคุมด้านความปลอดภัยเพิ่มเติมโดยไม่มีค่าใช้จ่ายเพิ่มเติม
- ความซับซ้อนของการกำหนดตั้งค่าความปลอดภัยไม่ควรเป็นปัญหาของลูกค้า เจ้าหน้าที่ไอทีขององค์กรมักมีภาระหน้าที่ด้านความปลอดภัยและการปฏิบัติงานมากเกินไป จึงส่งผลให้มีเวลาจำกัดในการทำความเข้าใจและดำเนินมาตรการทั้งหมดที่จำเป็นเพื่อให้แน่ใจว่าความปลอดภัยทางไซเบอร์ของบริษัทนั้นแข็งแกร่งและได้รับการปกป้องอย่างแท้จริง ผู้ผลิตสามารถช่วยเหลือลูกค้าได้โดยการเพิ่มประสิทธิภาพการกำหนดตั้งค่าผลิตภัณฑ์ให้มีความปลอดภัยสูงสุด หรือการรักษา "เส้นทางเริ่มต้น" นั่นเอง เพื่อให้มั่นใจได้ว่า ผลิตภัณฑ์ของตนได้รับการผลิต จัดจำหน่าย และใช้งานได้อย่างปลอดภัยตามมาตรฐาน "ความปลอดภัยโดยการตั้งค่าเริ่มต้น"

ผู้ผลิตผลิตภัณฑ์ที่มี "ความปลอดภัยโดยการตั้งค่าเริ่มต้น" จะไม่คิดค่าใช้จ่ายเพิ่มเติมสำหรับการกำหนดตั้งค่าความปลอดภัยที่มีเพิ่มมานี้ แต่จะคิดรวมอยู่ในผลิตภัณฑ์พื้นฐานแทน เช่นเดียวกับที่รถคันใหม่ทุกคันจะมีเข็มขัดนิรภัยติดมากับรถด้วย

ความปลอดภัยไม่ควรเป็นตัวเลือกที่หรูหรา แต่ควรได้รับการพิจารณาว่าเป็นสิทธิ์ที่ลูกค้าพึงได้รับโดยไม่ต้องเจรจาต่อรองหรือจ่ายเงินเพิ่มเติม

คำแนะนำสำหรับผู้ผลิตซอฟต์แวร์

คู่มือร่วมฉบับนี้ ให้คำแนะนำแก่ผู้ผลิตในการพัฒนาแผนการทำงานที่เป็นลายลักษณ์อักษรเพื่อนำออกใช้งานและรับประกันความปลอดภัยด้านไอทีของตน คณะผู้จัดทำเอกสารขอแนะนำให้ผู้ผลิตซอฟต์แวร์ปฏิบัติตามกลยุทธ์ที่ระบุไว้ในส่วนด้านล่างนี้ เพื่อแสดงความเป็นเจ้าของผลลัพธ์ด้านความปลอดภัยของลูกค้าผ่านหลักการความปลอดภัยโดยการออกแบบและการตั้งค่าเริ่มต้น

หลักการด้านความมั่นคงปลอดภัยของผลิตภัณฑ์ซอฟต์แวร์

เราขอสนับสนุนให้ผู้ผลิตซอฟต์แวร์ใช้กลยุทธ์ที่จัดลำดับความสำคัญให้กับความปลอดภัยของซอฟต์แวร์ คณะผู้จัดทำเอกสารได้พัฒนาหลักการสำคัญสามประการต่อไปนี้ เพื่อเป็นแนวทางให้กับผู้ผลิตซอฟต์แวร์ในการสร้างความปลอดภัยของซอฟต์แวร์เข้าไปในกระบวนการออกแบบก่อนการพัฒนา การกำหนดตั้งค่า และการจัดส่งผลิตภัณฑ์ของตน

1

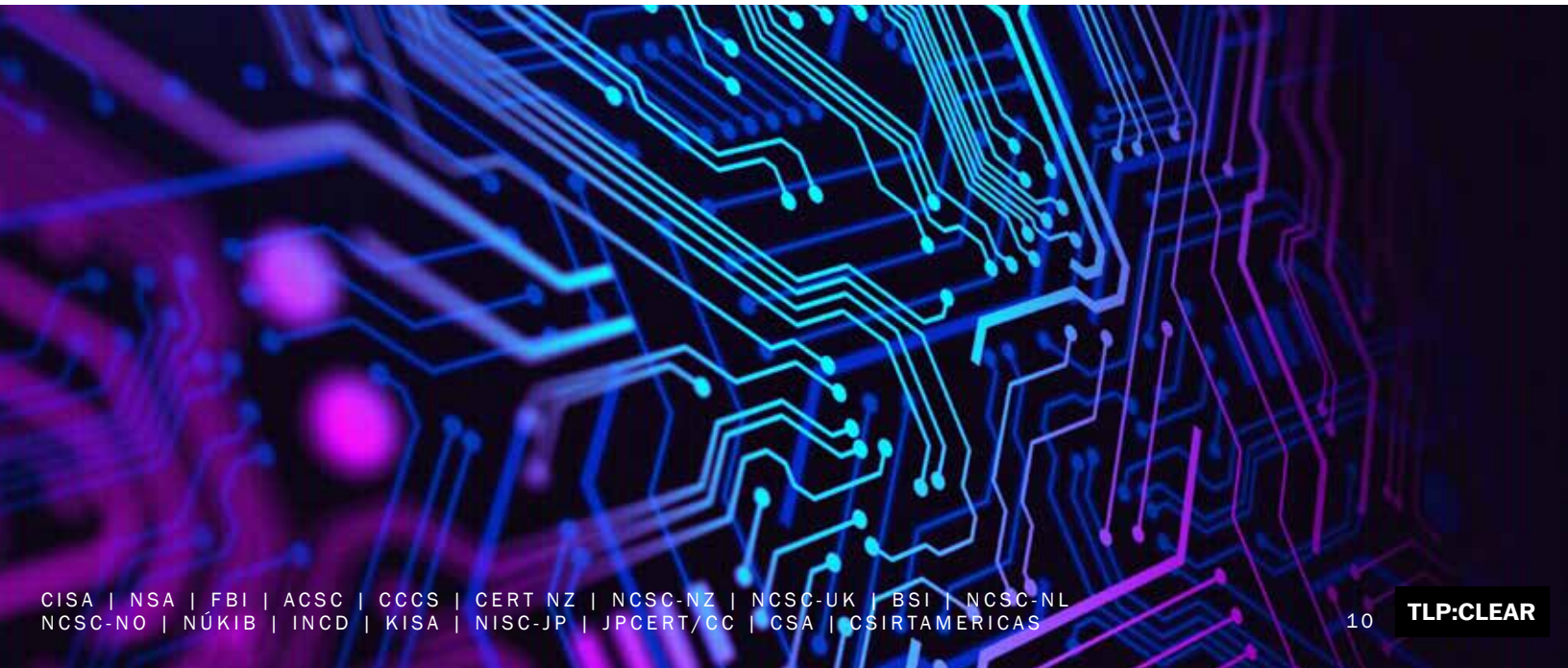
แสดงความเป็นเจ้าของผลลัพธ์ด้านความปลอดภัยของลูกค้า และพัฒนาสินค้าให้สอดคล้องกัน ภาระด้านความปลอดภัยไม่ควรตกอยู่ที่ลูกค้าเพียงฝ่ายเดียว

2

เปิดรับความโปร่งใสอย่างถึงแก่นและแสดงความรับผิดชอบต่อทุกสิ่งที่ทำ
ผู้ผลิตซอฟต์แวร์ควรภูมิใจที่ได้นำส่งผลิตภัณฑ์ที่ปลอดภัย ตลอดจนที่ได้สร้างความแตกต่างระหว่างตนเองกับผู้ผลิตรายอื่นในชุมชนจากความสามารถของตนที่ได้ปฏิบัติเช่นนั้น ซึ่งอาจรวมถึงการแบ่งปันข้อมูลที่พวกเขาเรียนรู้จากการปรับใช้งานของลูกค้า เช่น การใช้กลไกการยืนยันตัวตนที่รัดกุมด้วยการตั้งค่าเริ่มต้น นอกจากนั้น ยังรวมถึงความมุ่งมั่นอย่างแรงกล้าเพื่อให้แน่ใจว่าคำแนะนำเกี่ยวกับช่องโหว่ และการบันทึกช่องโหว่ทั่วไปและการเปิดเผยข้อมูล (Common Vulnerability and Exposure - CVE) ที่เกี่ยวข้องนั้นมีรายละเอียดครบถ้วนและถูกต้อง อย่างไรก็ตาม โปรดระวังเรื่องการคิดว่า CVE จำนวนมากนั้น เป็นตัวชี้วัดในเชิงลบ เนื่องจากตัวเลขดังกล่าวยังเป็นสัญญาณที่ดีที่บ่งบอกถึงชุมชนซึ่งกำลังวิเคราะห์และทดสอบรหัสอย่างขันแข็งอีกด้วย

3

สร้างโครงสร้างองค์กรและความเป็นผู้นำเพื่อบรรลุเป้าหมายเหล่านี้
แม้ว่าความเชี่ยวชาญด้านเทคนิคจะมีความสำคัญอย่างยิ่งต่อความปลอดภัยของผลิตภัณฑ์ แต่ผู้บริหารระดับสูงกลับเป็นผู้มีอำนาจตัดสินใจที่สำคัญที่สุดเมื่อต้องทำการเปลี่ยนแปลงในองค์กร ผู้บริหารจำเป็นต้องให้ความสำคัญกับความปลอดภัยเป็นองค์ประกอบอันดับแรกในการพัฒนาผลิตภัณฑ์ทั่วทั้งองค์กร และโดยการทำงานอย่างใกล้ชิดกับลูกค้า



เพื่อให้สามารถใช้หลักการสามประการนี้ ผู้ผลิตควรพิจารณากลวิธีการปฏิบัติงานหลาย ๆ ด้านเพื่อปรับกระบวนการพัฒนาของตน

จัดการประชุมร่วมกับผู้บริหารระดับสูงของบริษัทเป็นประจำเพื่อขับเคลื่อนความสำคัญของความปลอดภัยโดยการออกแบบและความปลอดภัยโดยการตั้งค่าเริ่มต้นภายในองค์กร ควรกำหนดนโยบายและขั้นตอนปฏิบัติในการให้รางวัลแก่ทีมผู้ผลิตที่พัฒนาผลิตภัณฑ์ตามหลักการเหล่านี้ ซึ่งอาจรวมถึงการให้รางวัลแก่การดำเนินการตามแนวปฏิบัติด้านความปลอดภัยของซอฟต์แวร์ที่โดดเด่น หรือเป็นสิ่งจูงใจสำหรับขั้นบันไดงานและเป็นเกณฑ์การเลื่อนตำแหน่ง

ให้ความสำคัญกับหลักความปลอดภัยของซอฟต์แวร์ต่อความสำเร็จของธุรกิจ ตัวอย่างเช่น พิจารณาแต่งตั้ง “ผู้นำด้านความปลอดภัยของซอฟต์แวร์” หรือ “ทีมความปลอดภัยของซอฟต์แวร์” ที่สนับสนุนแนวทางปฏิบัติด้านธุรกิจและไอที ที่เชื่อมโยงมาตรฐานความปลอดภัยของซอฟต์แวร์กับความรับผิดชอบของผู้ผลิตโดยตรง ผู้ผลิตควรตรวจสอบให้แน่ใจว่ามีการประเมินความปลอดภัยของผลิตภัณฑ์และโปรแกรมการประเมินผลที่แข็งแกร่งและเป็นอิสระสำหรับผลิตภัณฑ์ของตน

ใช้แบบจำลองภัยคุกคามที่ปรับแต่งให้เหมาะสมในระหว่างการจัดสรรทรัพยากรและการพัฒนาผลิตภัณฑ์เพื่อมุ่งเน้นไปที่คุณลักษณะที่สำคัญและมีผลกระทบมากที่สุดก่อน แบบจำลองภัยคุกคามจะพิจารณากรณีการใช้งานเฉพาะของผลิตภัณฑ์และช่วยให้ทีมพัฒนาสามารถเสริมความแข็งแกร่งให้กับผลิตภัณฑ์ได้ประการสุดท้าย ผู้นำระดับสูงควรมอบความรับผิดชอบให้ทีมงานในการส่งมอบผลิตภัณฑ์ที่ปลอดภัย ซึ่งเป็นองค์ประกอบสำคัญในการบรรลุความเป็นเลิศและคุณภาพของผลิตภัณฑ์

ในส่วนหนึ่งของการอัปเดตคำแนะนำเมื่อเดือนตุลาคม 2023 นี้ หลักการทั้งสามประการนี้ได้รับการขยายความผ่านคำอธิบาย การสาธิต และหลักฐานดังต่อไปนี้

หลักการที่ 1 แสดงความเป็นเจ้าของผลลัพธ์ด้านความปลอดภัยของลูกค้า

คำอธิบาย

แนวทางปฏิบัติสมัยใหม่ที่ดีที่สุดกำหนดว่า ผู้ผลิตซอฟต์แวร์ควรลงทุนในความพยายามด้านความปลอดภัยของผลิตภัณฑ์ ซึ่งรวมถึง**การเสริมความแข็งแกร่งของแอปพลิเคชัน คุณลักษณะของแอปพลิเคชัน** และ**การตั้งค่าเริ่มต้นของแอปพลิเคชัน**

ผู้ผลิตซอฟต์แวร์จำเป็นต้องนำหลัก**การเสริมความแข็งแกร่งของแอปพลิเคชัน**ออกใช้ โดยใช้กระบวนการและเทคโนโลยีที่ไปเพิ่มต้นทุนให้กับผู้ไม่ประสงค์ดีที่ต้องการจะละเมิดความปลอดภัยของแอปพลิเคลชัน โปรโตคอลและขั้นตอนการเสริมความแข็งแกร่งของแอปพลิเคชันช่วยผลิตภัณฑ์ให้ต้านทานการโจมตีจากผู้ไม่ประสงค์ดีที่ชาญฉลาดได้ คำศัพท์เช่นคำว่า การเสริมความแข็งแกร่ง ความปลอดภัยของผลิตภัณฑ์และความยืดหยุ่น ล้วนเกี่ยวข้องกับคุณภาพของผลิตภัณฑ์อย่างใกล้ชิดทั้งสิ้น แนวคิดก็คือความปลอดภัยจะต้อง “ประสานเข้าเป็นส่วนหนึ่ง” ตั้งแต่เริ่มต้นและไม่ใช่ “ส่วนที่พ่วงติด” เข้ามาในภายหลัง [1] ด้วยการประสานความปลอดภัยเข้าเป็นส่วนหนึ่งของกระบวนการ ผู้ผลิตซอฟต์แวร์ไม่เพียงแต่เพิ่มความปลอดภัยให้ลูกค้า แต่ยังเพิ่มคุณภาพให้ผลิตภัณฑ์ของตนอีกด้วย กลวิธีตัวอย่างได้แก่ การทำให้แน่ใจได้ว่าการป้อนข้อมูลของผู้ใช้ได้รับการตรวจสอบและคัดกรอง และไม่ได้ป้อนลงในรหัสโดยตรง (เช่น โดยใช้การสืบค้นแบบกำหนดพารามิเตอร์แทน) การใช้ภาษาการเขียนโปรแกรมที่ปลอดภัยสำหรับหน่วยความจำ การจัดการวงจรชีวิตการพัฒนาซอฟต์แวร์ (Software Development Life Cycle - SDLC) ที่เข้มงวด และการใช้วิธีการที่ปลอดภัยในการจัดการคีย์การเข้ารหัสด้วยความช่วยเหลือของฮาร์ดแวร์

แอปพลิเคชันจำเป็นต้องให้การสนับสนุน**คุณลักษณะของแอปพลิเคชัน**ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ บางครั้งคุณลักษณะเหล่านี้ก็เรียกว่า “ความสามารถ” ซึ่งขยายฟังก์ชันการทำงานของผลิตภัณฑ์หรือบริการในลักษณะที่ช่วยเพิ่มหรือรักษาจุดยืนด้านการรักษาความปลอดภัยให้กับลูกค้า ตัวอย่างคุณสมบัติที่เกี่ยวข้องกับความปลอดภัย

ได้แก่ ความปลอดภัยของชั้นการขนส่ง (Transport Layer Security - TLS) สำหรับการเชื่อมต่อเครือข่ายทั้งหมด การสนับสนุนการลงชื่อเข้าใช้ครั้งเดียว (Single Sign On - SSO) การสนับสนุนการยืนยันตัวตนโดยใช้หลากหลายปัจจัย (Multi-Factor Authentication - MFA) การบันทึกการตรวจสอบเหตุการณ์ความปลอดภัย การควบคุมการเข้าถึงตามบทบาท (Role-Based Access Control - RBAC) และการควบคุมการเข้าถึงตามคุณลักษณะ (Attribute-Based Access Control - ABAC)

คุณลักษณะบางอย่างของผลิตภัณฑ์เหล่านี้ สามารถกำหนดตั้งค่าเพื่อช่วยให้ลูกค้าสามารถปรับผลิตภัณฑ์ของตนให้เข้ากับสิ่งแวดล้อมและขั้นตอนการทำงานที่มีอยู่เดิมได้ง่ายขึ้น การกำหนดตั้งค่าเหล่านี้หมายถึงแอปพลิเคชันจะต้องมี**การตั้งค่าเริ่มต้น**ที่ตั้งไว้จนกว่าลูกค้าจะกำหนดตั้งค่าเอง การตั้งค่าเริ่มต้นเหล่านั้นจำเป็นต้องถูกตั้งค่ามาอย่างปลอดภัยตั้งแต่ “แกะกล่อง” เพื่อจะให้ลูกค้าใช้ทรัพยากรน้อยลงในการทำให้กลุ่มผลิตภัณฑ์เทคโนโลยีของตนมีความปลอดภัยมากขึ้น

องค์ประกอบแต่ละอย่างเหล่านี้ อันได้แก่ การเสริมความแข็งแกร่งของแอปพลิเคชัน คุณลักษณะด้านความปลอดภัยของแอปพลิเคชัน และการตั้งค่าเริ่มต้นของแอปพลิเคชัน มีบทบาททำให้แอปพลิเคชันมีความปลอดภัยและส่งผลต่อจุดยืนด้านการรักษาความปลอดภัยโดยรวมของลูกค้า ผู้ผลิตซอฟต์แวร์ควรคิดถึงแต่ละองค์ประกอบเหล่านี้และดูว่าองค์ประกอบเหล่านี้เกี่ยวข้องกันอย่างไร ผู้ผลิตควรต้องพิจารณามากกว่าแค่เรื่องการลงทุนเพื่อรวมองค์ประกอบเหล่านี้ให้เข้ากับผลิตภัณฑ์ของตน ผู้ผลิตควรคิดไปให้ไกลกว่านั้นอีกขั้นหนึ่งและพิจารณาว่าปัจจัยเหล่านั้นจะเปลี่ยนจุดยืนด้านการรักษาความปลอดภัยของลูกค้าในโลกแห่งความเป็นจริงให้ดีขึ้นหรือแย่ลงอย่างไร

ผู้ผลิตควรแสดงความเป็นเจ้าของผลลัพธ์ด้านการความปลอดภัยของลูกค้า แทนที่จะวัดผลตนเองจากความพยายามและการลงทุนเพียงอย่างเดียว ผู้ผลิตควรได้รับมอบความรับผิดชอบตั้งแต่ต้นสาย ซึ่งจะช่วยลดความเสี่ยงของการถูกละเมิดด้านความปลอดภัยได้มากที่สุด

แต่น่าเสียดายที่ทุกวันนี้ไม่ได้เป็นไปเช่นนั้น ผู้ผลิตจำนวนมากเกินไปผลักภาระด้านความปลอดภัยไปไว้ที่ลูกค้าแทนที่จะลงทุน**เสริมความแข็งแกร่งของแอปพลิเคชันให้ปลอดภัยเต็มที่** ตัวอย่างเช่น เมื่อผู้ผลิตแก้ไขช่องโหว่ด้วยแพตช์หนึ่งรายการ เรามักจะเห็นปัญหาช่องโหว่อื่นที่คล้ายกันปรากฏขึ้น เนื่องจากเป็นการจัดการกับอาการมากกว่าการหาสาเหตุเบื้องหลังแท้จริงของข้อบกพร่องนั้น ผลิตภัณฑ์อาจปรับใช้การแก้ปัญหาที่แตกต่างกันเพื่อจัดการกับส่วนต่าง ๆ ของรหัสพื้นฐานสำหรับช่องโหว่ประเภทเดียวกัน ยกตัวอย่างกรณีเช่น หลังจากที่ผู้ผลิตแก้ไขช่องโหว่ประเภทหนึ่งที่เกี่ยวข้องกับการคัดกรองอินพุตแล้ว นักวิจัยหรือผู้โจมตียังพบว่ามีเส้นทางรหัสที่ไม่ได้รับประโยชน์จากการปรับปรุงการคัดกรองอินพุตนั้นอีก ผู้ผลิตใช้การแก้ไขทีละรายการแทนที่จะรวมรหัสพื้นฐานทั้งหมดเพื่อกำจัดช่องโหว่ประเภทนั้นทั่วทั้งแอปพลิเคชัน

คุณลักษณะของแอปพลิเคชันสามารถก่อให้เกิดทั้งประโยชน์และความเสี่ยงให้กับลูกค้า คุณลักษณะที่ช่วยให้ผลิตภัณฑ์ทำงานร่วมกับระบบภายนอกและเวอร์ชันอื่น ๆ จำนวนมากนั้น สามารถเพิ่มมูลค่าของผลิตภัณฑ์ได้อย่างมาก แต่กระนั้นแล้ว การรองรับคุณลักษณะต่าง ๆ โดยไม่มีการวางแผนการเลิกใช้ เช่น โปรโตคอลเครือข่ายอาจทำให้ลูกค้าตกอยู่ในความเสี่ยงได้ หากลูกค้าขาดความเข้าใจถึงผลกระทบของการใช้คุณลักษณะเหล่านั้นต่อไป ตัวอย่างเช่น ผลิตภัณฑ์บางอย่างยังคงใช้โปรโตคอลเครือข่ายที่สร้างขึ้นในช่วงทศวรรษ 1990 หรือ 2000 และปัจจุบันเป็นที่ทราบแล้วว่าไม่ปลอดภัย มีหลายปัจจัยมากที่สามารถทำให้ความรวดเร็วในการอัปเดตและปรับใช้มาตรการรักษาความปลอดภัยที่ทันสมัยช้าลงได้ พวกเขาอาจใช้ผลิตภัณฑ์ที่บูรณาการมาให้เข้ากับส่วนที่เหลือของเครือข่ายขององค์กร แต่ขาดมาตรการรักษาความปลอดภัยที่ทันสมัย ซึ่งเป็นอุปสรรคทำให้ทีมไอทีไม่สามารถปรับปรุงสิ่งต่าง ๆ ให้ทันสมัยได้ ถึงกระนั้น ผู้ผลิตซอฟต์แวร์สามารถนำแนวโน้มเหล่านี้มาพิจารณาในกระบวนการวางแผนเพื่อจูงใจลูกค้าให้ปรับปรุงซอฟต์แวร์ของตนให้ทันสมัยอยู่เสมอ

การตั้งค่าเริ่มต้นของแอปพลิเคชั่นถือเป็นพื้นที่เสี่ยงเพิ่มเติมสำหรับลูกค้า ผู้ผลิตมักจะเลือกการตั้งค่าเริ่มต้นบางอย่าง เพื่อให้ลูกค้าสามารถใช้คุณลักษณะของแอปพลิเคชันที่ต้องการได้ง่ายขึ้น ข้อเสียคือแนวปฏิบัตินี้จะเพิ่มพื้นผิวการถูกโจมตีที่มากขึ้นสำหรับลูกค้าที่อาจไม่ต้องการคุณลักษณะและโปรโตคอลบางอย่างที่เปิดใช้งานตามการตั้งค่าเริ่มต้น นอกจากนี้ การควบคุมความปลอดภัยหลายอย่างไม่ได้เปิดเองโดยอัตโนมัติหรือลูกค้าจำเป็นต้องใช้เวลาในการปรับการกำหนดตั้งค่า เพื่อให้สิ่งต่าง ๆ มีความปลอดภัยมากขึ้น การสร้างแบบจำลองภัยคุกคามที่ชัดเจนเป็นกลวิธีที่อาจช่วยให้ตัดสินใจได้ว่า คุณลักษณะใดควรตั้งเป็นค่าเริ่มต้น หรือการกำหนดค่าใดที่จำเป็นเพื่อให้ปลอดภัยตามการตั้งค่าเริ่มต้น กลวิธีอีกประการหนึ่งคือการหาวิธีที่จะทำให้ผู้ดูแลระบบค้นหาและใช้คุณลักษณะต่าง ๆ ได้ง่ายขึ้น

ผู้ผลิตบางรายจัดส่งผลิตภัณฑ์ที่มีการตั้งค่าเริ่มต้นที่อาจก่อให้เกิดความเสี่ยงต่อลูกค้าบางรายหรือทั้งหมดได้ แทนที่จะตั้งค่าเริ่มต้นที่ปลอดภัยกว่า พวกเขามักเลือกที่จะจัดทำ**แนวทางการเสริมความแข็งแกร่ง**ที่ลูกค้าต้องปฏิบัติตามโดยออกค่าใช้จ่ายเอง แนวทางการเสริมความแข็งแกร่งประสบปัญหาทั่วไปหลายอย่าง แนวทางการเสริมความแข็งแกร่งที่ทำให้ผลิตภัณฑ์มีความปลอดภัยมากขึ้นบางฉบับนั้นหายากและไม่ได้รับการสนับสนุนมากนัก บางฉบับก็มีความซับซ้อนในการใช้งาน บางครั้งยังต้องให้ฝ่ายพัฒนาซอฟต์แวร์เขียนมอดูล (Module) ส่วนขยายเพิ่มเติมเข้าไปอีก ถึงกระนั้น คำแนะนำบางส่วนคาดหวังว่าผู้อ่านจะมีความรู้ด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์มากพอที่จะเข้าใจวิธีการตั้งค่าต่าง ๆ ว่าส่งผลต่อความเสี่ยงของการถูกโจมตีอย่างไร ผู้ใช้งานที่เข้าใจวิธีการทำงานของผู้โจมตีอย่างไม่ถ่องแท้อาจประสบปัญหาในการปฏิบัติตามคำแนะนำในแนวทางการเสริมความแข็งแกร่ง โดยเฉพาะอย่างยิ่งหากคำแนะนำนั้นไม่ได้อธิบายข้อดีข้อเสียที่เกี่ยวข้องไว้อย่างชัดเจน ยิ่งไปกว่านั้น ไม่ใช่แนวทางการเสริมความแข็งแกร่งทุกฉบับจะเขียนโดยวิศวกรที่เข้าใจกลวิธีและเศรษฐศาสตร์ของผู้โจมตีอย่างถ่องแท้ ซึ่งทำให้พวกเขาเขียนแนวทางการเสริมความแข็งแกร่งที่ไม่ได้ผล แม้ว่าจะถูกนำไปปฏิบัติใช้ตามอย่างเคร่งครัดก็ตาม ลูกค้าจำนวนนับล้านรายกำลังเป็นผู้รับผิดชอบในการปรับปรุงซอฟต์แวร์หรือระบบหลายรายการให้มีความปลอดภัยมากขึ้น แม้ว่าพวกเขาจะไม่มีทรัพยากรมากพอก็ตาม การพึ่งพาแนวทางการเสริมความแข็งแกร่งเพียงอย่างเดียวไม่ใช่วิธีแก้ปัญหาเมื่อต้องรับมือกับซอฟต์แวร์หรือระบบขนาดใหญ่

วิธีการกำหนดตั้งค่าของแอปพลิเคชันควรได้รับการประเมินอย่างต่อเนื่อง ไม่ว่าจะเป็นการตั้งค่าตามค่าเริ่มต้นหรือโดยลูกค้า โดยเทียบกับความรู้ในปัจจุบันของผู้ผลิตเกี่ยวกับภาพรวมภัยคุกคามที่อาจเกิดขึ้น แอปพลิเคชันควรถูกสร้างขึ้นให้มีตัวบ่งชี้ที่ชัดเจนเกี่ยวกับความเสี่ยงที่อาจเกิดขึ้น ซึ่งอาจเป็นผลมาจากการตั้งค่าเหล่านั้น และควรแจ้งให้ผู้ใช้ตระหนักถึงตัวบ่งชี้หรือสัญญาณเหล่านี้ เช่นเดียวกับรถยนต์สมัยใหม่ที่มีตัวบ่งชี้เกี่ยวกับเข็มขัดนิรภัยและมีการส่งเสียงเตือนหากคุณพยายามจะขับรถโดยไม่คาดเข็มขัด ซอฟต์แวร์ก็ควรมีตัวบ่งชี้หรือสัญญาณที่บ่งบอกถึงสถานะความปลอดภัยของระบบด้วย หากมีการกำหนดตั้งค่าแอปพลิเคชันให้บัญชีผู้ดูแลระบบที่ไม่ต้องใช้ MFA ก็ควรเตือนผู้ดูระบบเป็นประจำว่าพวกเขาและทั้งองค์กรจะตกอยู่ในอันตราย หากพวกเขาไม่ได้กำหนดตั้งค่า MFA ไว้ นอกจากนี้หากแอปพลิเคชันได้รับการกำหนดตั้งค่าให้รองรับโปรโตคอลรุ่นเก่าที่ขณะนี้ทราบว่ามีการใช้การเข้ารหัสที่มีความปลอดภัยต่ำ แอปพลิเคชันควรแจ้งให้ผู้ดูแลระบบทราบเป็นประจำว่าองค์กรกำลังตกอยู่ในอันตราย และเสนอคำแนะนำเพื่อแก้ไขสถานการณ์ เราขอแนะนำให้ผู้ผลิตซอฟต์แวร์ปรับใช้ระบบการแจ้งเตือนแบบเป็นประจำไว้ในตัวผลิตภัณฑ์แทนที่จะอาศัยผู้ดูแลระบบที่ต้องหาเวลา มีความเชี่ยวชาญ และมีความตระหนักในการตีความคำแนะนำในแนวทางการเสริมความแข็งแกร่ง เห็นได้ชัดว่ามีโอกาสสำหรับนวัตกรรมที่จะสร้างสมดุลระหว่างข้อพิจารณาด้านความปลอดภัยและความเป็นมิตรต่อผู้ใช้

ปัจจัยทั้งหมดที่กล่าวมาข้างต้นก่อให้เกิดสถานการณ์ที่ยากลำบากสำหรับลูกค้าที่จำเป็นต้องค้นคว้า หาทุน จัดซื้อ จ้างพนักงาน ปรับใช้ และคอยติดตามผลเพิ่มเติมกับ**ผลิตภัณฑ์รักษาความปลอดภัย**เพื่อลดโอกาสที่จะถูกละเมิดความปลอดภัย องค์กรขนาดเล็กและขนาดกลาง (SMO) มักไม่สามารถรับค่าใช้จ่ายสำหรับตัวเลือกเหล่านี้ได้ พวกเขาต้องเผชิญกับการขาดแคลนความเชี่ยวชาญ เงินทุน และเวลาซึ่งไปลดความสามารถในการจัดการความปลอดภัยโดยบังคับให้ความปลอดภัยได้รับลำดับความสำคัญน้อยลง และในที่สุดแล้วทำให้ความเสี่ยงโดยรวมรุนแรงยิ่งขึ้น ในทางกลับกัน หากมีผู้ผลิตจำนวนไม่มากลงทุนด้านความปลอดภัย ผลกระทบก็อาจขยายตัวมากขึ้นในวงกว้าง วลีทั่วไปที่สรุปปัญหานี้ คืออุตสาหกรรมซอฟต์แวร์ต้องการผลิตภัณฑ์ที่ปลอดภัยมากขึ้น ไม่ใช่ชนิดผลิตภัณฑ์ที่ไปเสริมความปลอดภัยมากขึ้น ผู้ผลิตซอฟต์แวร์ควรเป็นผู้นำการเปลี่ยนแปลงดังกล่าว

> ***“อุตสาหกรรมซอฟต์แวร์ต้องการผลิตภัณฑ์ที่ปลอดภัยมากขึ้น ไม่ใช่ชนิดผลิตภัณฑ์ที่ไปเสริมความปลอดภัยมากขึ้น ผู้ผลิตซอฟต์แวร์ควรเป็นผู้นำการเปลี่ยนแปลงดังกล่าว***

ทุกวันนี้ บางครั้งเราอ่านความคิดเห็นจากผู้ผลิตที่อธิบายว่าลูกค้าถูกละเมิดความปลอดภัยเนื่องจากไม่ได้เปิดใช้งานคุณลักษณะความปลอดภัยบางอย่าง หรือไม่ปฏิบัติตามคำแนะนำด้านการเสริมความแข็งแกร่งเฉพาะอย่าง แต่แทนที่จะโทษลูกค้า หลังจากที่มีการละเมิดความปลอดภัยเกิดขึ้น ผู้ผลิตควรอธิบายว่าคุณลักษณะด้านความปลอดภัยบางอย่างหรือคำแนะนำด้านการเสริมความแข็งแกร่งเฉพาะอย่างจะช่วยป้องกันการถูกละเมิดความปลอดภัยได้หรือไม่ และพิจารณากำหนดให้เป็นการตั้งค่าเริ่มต้นโดยไม่ต้องเรียกเก็บเงินเพิ่มเติม ในกรณีที่ตัวผลิตภัณฑ์ไม่ได้รับการเสริมความแข็งแกร่งเพียงพอในขั้นตอนการออกแบบและการนำออกใช้งาน ผู้ผลิตควรชี้แจงว่าตนกำลังทำงานเพื่อขจัดช่องโหว่ในประเภทนั้นให้ออกจากสายผลิตภัณฑ์ในอนาคตอย่างไร

ผู้ผลิตซอฟต์แวร์มีหน้าที่รับผิดชอบในการตรวจสอบว่าผลิตภัณฑ์ของตนได้รับการออกแบบและพัฒนาโดยเน้นไปที่ความปลอดภัยเป็นหลักสำคัญสูงสุด ด้วยเหตุนี้ ผู้ผลิตควรจะ**ประเมินผลอย่างเป็นกลาง**ต่อผลงานของตนในสถานการณ์จริง เราขอเรียกร้องให้ผู้ผลิตไม่เพียงแค่มุ่งเน้นความพยายามภายในองค์กรของตนเท่านั้น แต่ให้วัดผลอย่างเป็นกลางและรายงานผลลัพธ์และประสิทธิผลของความพยายามและการกำหนดตั้งค่าด้านความปลอดภัยของผลิตภัณฑ์อย่างสม่ำเสมอด้วย และเพื่อสร้างวงจรตอบรับความคิดเห็นที่ก่อให้เกิดการเปลี่ยนแปลงใน SDLC ที่จะนำไปสู่การปรับปรุงที่วัดผลได้ เพื่อความปลอดภัยของลูกค้าและผลิตภัณฑ์ที่ปลอดภัยยิ่งขึ้น การรายงานควรรวมข้อมูลที่ไม่ระบุตัวบุคคล ซึ่งชุมชนวิชาการและการวิจัยด้านความปลอดภัยสามารถนำไปใช้เพื่อติดตามดูแนวโน้มโดยรวมและวัดผลความก้าวหน้าในวงกว้างทั่วทั้งระบบนิเวศ

การสาธิตหลักการนี้

ผู้ผลิตซอฟต์แวร์และบริการออนไลน์ควรหาวิธีสาธิตว่าพวกเขานำหลักการนี้ไปปฏิบัติใช้อย่างไร โดยเน้นย้ำถึงความสำเร็จของพวกเขา พวกเขาควรหาหลักฐานในรูปแบบของหลักฐานสิ่งประดิษฐ์ที่คนภายนอกองค์กรสามารถตรวจสอบได้ การมีหลักฐานสิ่งประดิษฐเพียงชิ้นเดียวไม่สามารถพิสูจน์ได้ว่า ผู้ผลิตกำลังใช้โปรแกรมความปลอดภัยโดยการออกแบบที่เข้มแข็ง แต่ด้วยการจัดเตรียมหลักฐานสิ่งประดิษฐ์หลาย ๆ รายการ พวกเขาจะสามารถสร้างกรณีที่แสดงให้เห็นว่าผู้ผลิตทุ่มเทกับการพัฒนาผลิตภัณฑ์ที่ปลอดภัยอย่างแท้จริง แนวปฏิบัตินี้เป็นไปตามแนวคิดของ “การสาธิตผ่านการกระทำไม่ใช่แค่การบอกเล่า”

เพื่อเป็นการสาธิตหลักการนี้ ผู้ผลิตซอฟต์แวร์ควรพิจารณาดำเนินการตามรายการด้านล่างนี้ คณะผู้จัดทำเอกสารตระหนักดีว่ามีผู้ผลิตซอฟต์แวร์เพียงไม่กี่รายเท่านั้นที่สามารถนำแนวทางปฏิบัติเหล่านี้ไปใช้ได้ทันที และแสดงหลักฐานสิ่งประดิษฐ์ที่เกี่ยวข้องตั้งแต่เริ่มต้นเส้นทางตามหลักความปลอดภัยโดยการออกแบบได้ นอกจากนี้ผู้ผลิตซอฟต์แวร์จำเป็นต้องมุ่งเน้นที่การปรับปรุงคุณลักษณะด้านความปลอดภัยโดยพิจารณาจากวิธีที่ลูกค้าปรับใช้ผลิตภัณฑ์ในสถานการณ์จริง เพื่อให้บรรลุประโยชน์ด้านความปลอดภัยมากที่สุด

แนวปฏิบัติตามหลักความปลอดภัย โดยการตั้งค่าเริ่มต้น

1. **กำจัดรหัสผ่านเริ่มต้น** การใช้รหัสผ่านเริ่มต้นยังคงเป็นเหตุผลสำคัญที่ทำให้เกิดการโจมตีทางไซเบอร์หลายครั้งในแต่ละปี การตั้งความมุ่งมั่นที่จะขจัดปัญหาเรื้อรังนี้ จะทำให้ผู้โจมตีเข้าถึงระบบได้ยากขึ้น ในทำนองเดียวกัน ผู้ผลิตควรคำนึงถึงกฎเกณฑ์ในการตั้งรหัสผ่าน เช่น ความยาวขั้นต่ำของรหัสผ่าน และการไม่อนุญาตให้ใช้รหัสผ่านที่ถูกละเมิดมาก่อน

2. **ดำเนินการทดสอบภาคสนาม** ในขณะที่เทคโนโลยีพัฒนาและมีความซับซ้อนมากขึ้นไปอย่างต่อเนื่อง การที่ผู้ผลิตซอฟต์แวร์จะดำเนินการทดสอบโดยผู้ใช้งานที่เน้นความปลอดภัยเป็นหลัก เพื่อทำความเข้าใจจุดยืนด้านการรักษาความปลอดภัยของผลิตภัณฑ์ของตนในภาคสนามจึงเป็นสิ่งสำคัญมากขึ้นตามไปด้วย เช่นเดียวกับวิธีที่การวิจัยรวบรวมคำติชมจากผู้ใช้เพื่อปรับปรุงการพัฒนาซอฟต์แวร์ ผู้ผลิตซอฟต์แวร์ควรทำการวิจัยผู้ใช้ที่เน้นเรื่องความปลอดภัยด้วย เพื่อทำความเข้าใจว่าประสบการณ์ผู้ใช้ในด้านความปลอดภัย (User Experience - UX) มีปัญหาหรือข้อบกพร่องที่จุดใดบ้าง เมื่อผู้ผลิตซอฟต์แวร์สังเกตวิธีที่ลูกค้าใช้และปรับใช้ผลิตภัณฑ์ของตนในสถานการณ์จริง พวกเขาจะได้รับข้อมูลเชิงลึกในแง่ความเป็นมิตรต่อผู้ใช้และประสิทธิผลของคุณลักษณะและการควบคุมความปลอดภัยของผลิตภัณฑ์ ข้อมูลเชิงลึกเหล่านี้ สามารถช่วยบ่งบอกได้ว่าผลิตภัณฑ์ควรได้รับการปรับปรุงและปรับรายละเอียดตรงไหน เพื่อให้ตอบสนองความต้องการด้านความปลอดภัยของลูกค้าได้ดียิ่งขึ้น ตัวอย่างเช่น เมื่อทดสอบการใช้งานในภาคสนามแล้ว พวกเขาอาจพบว่าต้องปรับเปลี่ยนสิ่งต่าง ๆ ได้แก่ ลำดับการใช้งานผลิตภัณฑ์ของผู้ใช้ (UX Flow) การตั้งค่าเริ่มต้น การแจ้งเตือน และการเฝ้าระวัง การทดสอบในภาคสนามยังอาจชี้ให้เห็นว่า การปรับปรุงวิธีการออกแบบผลิตภัณฑ์ที่ผ่านมาช่วยลดความเร็วของการแก้ไขปัญหาด้านความปลอดภัยด้วยแพตช์ (Patch) ช่วยลดโอกาสผิดพลาดในการกำหนดตั้งค่า และลดโอกาสการถูกโจมตีให้เหลือน้อยที่สุดที่จุดใด

ผู้ผลิตควรพิจารณาปัจจัยต่อไปนี้

- ลูกค้าใช้แนวทางการเสริมความแข็งแกร่งอย่างถูกต้องหรือไม่?
- คุณลักษณะด้านความปลอดภัยที่มีอยู่ของผลิตภัณฑ์ทำงานได้ตามที่คาดหวังในสถานการณ์จริงหรือไม่?
- คุณลักษณะเหล่านี้สามารถต้านทานการโจมตีในโลกแห่งความเป็นจริงได้หรือไม่?
- คุณลักษณะใดที่จะลดโอกาสในการถูกละเมิดความปลอดภัยได้ดีกว่า?

หมายเหตุ เพื่อให้ได้ข้อมูลเชิงลึกเกี่ยวกับองค์ประกอบเหล่านี้ ผู้ผลิตซอฟต์แวร์อาจต้องการร่วมมือกับลูกค้าในการฝึกซ้อมการโจมตีจำลอง เพื่อดูว่าผลิตภัณฑ์ต้านทานการถูกโจมตีอย่างไร การทดสอบในภาคสนามเหล่านี้ อาจเกิดขึ้นที่สถานที่จริงของลูกค้า ทางออนไลน์หรือผ่านการตรวจวัดทางไกลโดยใช้แอปพลิเคชันในลักษณะที่มีการปกป้องความเป็นส่วนตัว

3. **ลดขนาดของแนวทางการเสริมความแข็งแกร่ง** ผู้ผลิตสามารถช่วยลูกค้าปรับปรุงจุดยืนด้านการรักษาความปลอดภัยได้โดยลดความซับซ้อนหรือแม้แต่ขจัดแนวทางการเสริมความแข็งแกร่งของผลิตภัณฑ์ไปเลย และมุ่งเน้นไปที่มาตรการรักษาความปลอดภัยที่สำคัญที่สุดที่ลูกค้าควรปฏิบัติก่อนเมื่อปรับใช้ผลิตภัณฑ์ แทนที่จะมอบหมายงานมาตรการรักษาความปลอดภัยให้ลูกค้าทำเป็นรายการจำนวนมาก ผู้ผลิตควรระบุความเสี่ยงด้านความปลอดภัยที่สำคัญที่สุดสำหรับผลิตภัณฑ์ของตน และให้คำแนะนำที่ชัดเจนและรัดกุมเกี่ยวกับวิธีการลดความเสี่ยงเหล่านี้ นอกจากนี้ ผู้ผลิตควรจัดหาเครื่องมือและระบบออโตเมชันให้ลูกค้าเพื่อลดความซับซ้อนของกระบวนการปรับใช้การควบคุมความปลอดภัย เช่น สคริปต์ที่ลูกค้าสามารถนำไปปรับใช้กับระบบของตนได้อย่างง่าย ๆ เครื่องมือเหล่านี้ควรสามารถตรวจสอบและแสดงการเปลี่ยนแปลงที่เกิดขึ้นได้อย่างชัดเจนด้วยเมื่อเปรียบเทียบกับการตั้งค่าดั้งเดิม ด้วยการลดความซับซ้อนของแนวทางการเสริมความแข็งแกร่งและและการมอบเครื่องมือและระบบออโตเมชั่นที่ใช้งานง่ายแก่ลูกค้า ผู้ผลิตสามารถลดภาระทำให้ลูกค้าใช้งานง่ายขึ้นและช่วยให้แน่ใจว่าผลิตภัณฑ์ของตนถูกนำไปปรับใช้ในลักษณะที่ปลอดภัย กลวิธีหนึ่งคือการพิจารณานำหลักการ Pareto ไปใช้คือ ลดขั้นตอนของงานให้ง่ายขึ้นในกรณีที่พบ

บ่อยที่สุด (80% ของกรณี) และเสนอความช่วยเหลือตามบริบทและให้เครื่องมือเพิ่มเติมสำหรับงานที่ไม่พบบ่อย (20% ของกรณี) ด้วยวิธีนี้ ผู้ผลิตซอฟต์แวร์จะสร้างผลิตภัณฑ์ที่เป็นมิตรต่อผู้ใช้สำหรับงานง่าย ๆ แต่ยังคงสามารถจัดการกับงานยาก ๆ ได้เมื่อจำเป็น การทดสอบในภาคสนามจะเป็นเครื่องมืออันทรงพลังที่จะวัดว่าลูกค้าต้องใช้เวลานานเท่าใดในการค้นหา ทำความเข้าใจ และนำแนวทางการเสริมความแข็งแกร่งออกใช้งาน ผู้ผลิตควรพิจารณาว่าผลิตภัณฑ์สามารถแจ้งเตือนให้ผู้ดูแลระบบดำเนินการโดยให้อยู่ภายในผลิตภัณฑ์โดยตรงได้อย่างไร แทนที่จะพึ่งพาพวกเขาให้ดำเนินการตามแนวทางการเสริมความแข็งแกร่ง

4. **ไม่สนับสนุนการใช้คุณลักษณะเดิมที่ไม่ปลอดภัยอย่างแข็งขัน**
   จัดลำดับความสำคัญของการรักษาความปลอดภัยโดยผ่านวิธีการอัปเกรดที่ชัดเจนแม้จะหมายความว่าไม่สามารถใช้งานร่วมกับเวอร์ชันเก่าได้อย่างสมบูรณ์ก็ตาม เผยแพร่บล็อกโพสต์ที่แสดงการนำคุณลักษณะและโปรโตคอลที่ปลอดภัยมาใช้ และแจ้งให้ผู้ใช้ทราบว่าจะเลิกใช้คุณลักษณะเก่าที่ไม่ปลอดภัยโดยผ่านการประกาศอย่างเป็นทางการ ซึ่งอาจปรากฏอยู่ในตัวผลิตภัณฑ์เอง ลูกค้าจำนวนมากได้แสดงให้เห็นว่าพวกเขาไม่ได้อัปเกรดระบบในปัจจุบันด้วยเครื่องข่ายที่ทันสมัย ข้อมูลประจำตัว และคุณลักษณะด้านความปลอดภัยที่สำคัญอื่น ๆ ในบางกรณี ลูกค้ากลัวว่าฟังก์ชันการทำงานที่ใช้งานอยู่อาจใช้งานไม่ได้หากมีการอัปเกรด การทำให้การอัปเกรดราบรื่นที่สุดเท่าที่จะเป็นไปได้ จะทำให้ลูกค้ามีแนวโน้มที่จะอัปเกรดและได้รับการแก้ไขด้านความปลอดภัยได้บ่อยขึ้นและรวดเร็วยิ่งขึ้น ผู้ผลิตซอฟต์แวร์ควรแจ้งเตือนลูกค้าอย่างจริงจังให้ปฏิบัติตามเส้นทางการอัปเกรดเพื่อลดความเสี่ยงของลูกค้า

5. **ใช้วิธีการแจ้งเตือนที่น่าดึงดูดความสนใจ**
   เช่นเดียวกับที่มีเสียงแจ้งเตือนให้รัดเข็มขัดนิรภัยในรถยนต์ที่ส่งเสียงดังไม่หยุดเมื่อคุณไม่ได้รัดเข็มขัด ผู้ผลิตควรใช้วิธีการแจ้งเตือนซ้ำ ๆ และทันเวลาเมื่อผู้ใช้หรือผู้ดูแลระบบกำลังตกอยู่ในสถานะที่ไม่ปลอดภัยอย่างเห็นได้ชัด โดยเตือนผู้ดูแลระบบว่าพวกเขากำลังใช้โปรโตคอลที่เลิกใช้ไปแล้วในขณะนั้น และแนะนำเส้นทางการอัปเกรดให้พวกเขา ใช้วิธีการแจ้งเตือนซ้ำ ๆ และทันเวลาเมื่อผู้ใช้หรือผู้ดูแลระบบ หรือการกำหนดตั้งค่าแอปพลิเคชัน กำลังตกอยู่ในสถานะที่ไม่ปลอดภัย แจ้งเตือนผู้ดูแลระบบอย่างชัดเจนเป็นประจำเมื่อระบบตกอยู่ในสถานะที่ไม่ปลอดภัย คุณลักษณะเพิ่มเติมอีกชั้นหนึ่งอาจกำหนดให้ผู้ดูแลระบบขั้นสูงรับทราบว่าพวกเขาขาด MFA ในบัญชีของตนทุกครั้งที่เข้าสู่ระบบ หรือแม้แต่ปิดคุณลักษณะหลักบางอย่างจนกว่าพวกเขาจะเปิดใช้งาน MFA มีพื้นที่สำหรับการปรับปรุงอย่างสร้างสรรค์เพื่อให้บรรลุเป้าหมายเหล่านี้โดยไม่ต้องแจ้งเตือนผู้คนมากเกินไป

6. **สร้างเทมเพลตการกำหนดตั้งค่าที่ปลอดภัย**
   เทมเพลตเหล่านี้สามารถกำหนดตั้งค่าบางอย่างไว้ล่วงหน้าตามการตั้งค่าที่ปลอดภัยโดยพิจารณาจากระดับความเสี่ยงที่องค์กรรับได้ แม้ว่าอาจจะธรรมดาเกินไปที่มีเทมเพลตสำหรับใช้แบ่งความปลอดภัยเป็นระดับต่ำ กลาง หรือสูง แต่ตัวอย่างดังกล่าวแสดงให้เห็นว่ามีการตั้งค่าแบบใดบ้างที่สามารถอัปเดตเพื่อจัดการความเสี่ยงให้กับองค์กรได้ แนวทางการเสริมความแข็งแกร่งสามารถให้การรองรับเทมเพลตต่าง ๆ ได้โดยอิงตามความเสี่ยงที่ผู้ผลิตระบุไว้

แนวปฏิบัติในการพัฒนาผลิตภัณฑ์ที่มีความปลอดภัย

1. **ความสอดคล้องของเอกสารกับกรอบงาน SDLC ที่มีความปลอดภัย** กรอบงาน SDLC ที่ปลอดภัยให้เป้าหมายและตัวอย่างสำหรับวิธีจัดการความปลอดภัยในแง่ของบุคลากร กระบวนการ และเทคโนโลยีในระหว่างการพัฒนาซอฟต์แวร์ ลองพิจารณาเผยแพร่คำอธิบายโดยละเอียดว่ามีการควบคุมกรอบงาน SDLC ที่มีความปลอดภัยใดถูกนำมาใช้แล้วบ้าง นอกจากนี้ ให้อธิบายการควบคุมสำรองใด ๆ ที่เคยใช้ในกรณีที่การควบคุมหลักไม่สามารถใช้งานได้ หากอยู่ในสหรัฐอเมริกา ให้พิจารณาใช้กรอบงานพัฒนาซอฟต์แวร์ที่ปลอดภัย (Secure Software Development Framework - SSDF) ของ NIST แม้ว่าจะไม่ใช่รายการตรวจสอบ แต่ SSDF ก็ “อธิบายถึงชุดแนวปฏิบัติที่ดีและเหมาะสมสำหรับการพัฒนาซอฟต์แวร์ที่คำนึงถึงความปลอดภัย”

2. **บันทึกเป้าหมายประสิทธิภาพความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Performance Goals - CPG) หรือความสอดคล้องที่เทียบเท่า** เมื่อองค์กรยืนยันว่าปฏิบัติตามมาตรฐาน NIST SSDF พวกเขากำลังระบุว่ากระบวนการ SDLC ของตนเป็นไปตามแนวปฏิบัติที่ดีที่สุดที่ได้รับการยอมรับอย่างกว้างขวาง อย่างไรก็ตาม การมีกระบวนการ SDLC ที่แข็งแกร่งเพียงอย่างเดียวนั้นไม่เพียงพอ พวกเขายังจำเป็นต้องปกป้ององค์กรและสภาพแวดล้อมการพัฒนาของตนเองจากผู้ไม่ประสงค์ดีที่อาจพยายามยุ่งเกี่ยวกับคุณสมบัติด้านความปลอดภัยของผลิตภัณฑ์ในขณะที่ยังอยู่ในระหว่างการพัฒนา นี่ไม่ใช่แค่ความเป็นไปได้ทางทฤษฎีเท่านั้น เป็นการโจมตีประเภทหนึ่งที่เกิดขึ้นจริง ซึ่งก่อให้เกิดผลเสียต่อลูกค้าและขยายผลกระทบถึงความมั่นคงระดับประเทศด้วย องค์กรควรพิจารณาเผยแพร่รายละเอียดเกี่ยวกับการดำเนินการขององค์กรที่สอดคล้องตาม CISA CPGs, กรอบงานด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Framework - CSF) ของ NIST หรือกรอบงานโปรแกรมการรักษาความมั่นคงปลอดภัยทางไซเบอร์อื่น ๆ

3. **การจัดการกับช่องโหว่ของระบบ** ผู้ผลิตบางรายมีโปรแกรมสำหรับจัดการกับช่องโหว่ของระบบที่มุ่งเน้นไปที่การแก้ไขช่องโหว่ด้วยการใช้แพตช์ที่ค้นพบทั้งภายในและภายนอกองค์กรเป็นหลัก และอื่น ๆ อีกเล็กน้อย โปรแกรมขั้นสูงที่พัฒนากว่าจะรวมการวิเคราะห์ข้อมูลที่เกี่ยวข้องกับช่องโหว่และสาเหตุเบื้องหลังแท้จริง นอกจากนี้ ยังดำเนินการตามขั้นตอนเพื่อกำจัดช่องโหว่ให้กับทั้งประเภทอย่างเป็นระบบ[3] โปรแกรมเหล่านี้ใช้โปรแกรมอย่างเป็นทางการเพื่อกำหนดการวางแผนคุณภาพ ควบคุมคุณภาพงาน ค้นหาวิธีปรับปรุงคุณภาพ และวัดผลคุณภาพของงาน โปรแกรมเหล่านี้มองว่าการจัดการข้อบกพร่องไม่เพียงแต่เป็นปัญหาด้านความปลอดภัยเท่านั้น แต่ยังเป็นเรื่องทางธุรกิจอีกด้วย โปรแกรมเหล่านี้ไม่แตกต่างไปจากโปรแกรมคุณภาพและความปลอดภัยในอุตสาหกรรมอื่น ๆ ในบางด้าน

4. **ใช้ซอฟต์แวร์โอเพนซอร์สอย่างมีความรับผิดชอบ** เมื่อใช้ซอฟต์แวร์โอเพนซอร์ส ผู้ใช้จะต้องรับผิดชอบโดยการตรวจสอบแพ็คเกจโอเพนซอร์สอย่างรอบคอบ มีส่วนร่วมในการปรับปรุงรหัสเมื่อเป็นไปได้ และช่วยสนับสนุนการพัฒนาและการบำรุงรักษาส่วนประกอบที่สำคัญอย่างต่อเนื่อง เพื่อเป็นข้อมูลอ้างอิง กระทรวงเศรษฐกิจ การค้า และอุตสาหกรรม (Ministry of Economy, Trade, and Industry - METI) ของญี่ปุ่นได้เผยแพร่เอกสารที่ชื่อว่า "Collection of Use Case Examples Regarding Management Methods for Utilizing OSS and Ensuring Its Security"

5. **ให้ค่าเริ่มต้นที่ปลอดภัยสำหรับนักพัฒนา** ทำให้เส้นทางเริ่มต้นในระหว่างการพัฒนาซอฟต์แวร์มีความปลอดภัย โดยจัดเตรียมบล็อคส่วนประกอบที่ปลอดภัยสำหรับนักพัฒนา ตัวอย่างเช่น ด้วยเหตุที่ช่องโหว่ของการแทรก SQL ก่อให้เกิดอันตรายในโลกแห่งความเป็นจริงอย่างแพร่หลาย จึงจำเป็นต้องตรวจสอบให้แน่ใจว่านักพัฒนาใช้ไลบรารีที่ได้รับการดูแลอย่างดีเพื่อป้องกันช่องโหว่ประเภทนั้น แนวปฏิบัตินี้เรียกอีกอย่างหนึ่งว่า “ถนนบุผิว” หรือ “เส้นทางที่มีแสงสว่างเพียงพอ” และให้ทั้งความรวดเร็ว ความปลอดภัย และลดข้อผิดพลาดที่เกิดจากมนุษย์

6. **ส่งเสริมบุคลากรนักพัฒนาซอฟต์แวร์ที่เข้าใจหลักปฏิบัติด้านความปลอดภัย** ตรวจสอบให้แน่ใจว่านักพัฒนาซอฟต์แวร์ของคุณเข้าใจหลักปฏิบัติด้านความปลอดภัย โดยการฝึกอบรมให้พวกเขามีความพร้อมในการเขียนโค้ดสร้างซอฟต์แวร์ที่ปลอดภัยตามแนวปฏิบัติที่ดีที่สุด นอกจากนี้ คุณยังสามารถช่วยเปลี่ยนแปลงบุคลากรในวงกว้างขึ้นด้วยการเปลี่ยนวิธีการจ้างงาน โดยพิจารณาประเมินความรู้ด้านความปลอดภัย และทำงานร่วมกับมหาวิทยาลัย วิทยาลัยชุมชน ค่ายฝึกอบรม และนักการศึกษาอื่น ๆ เพื่อรวมการฝึกอบรมด้านความปลอดภัยเข้าไปในหลักสูตรวิทยาการคอมพิวเตอร์และการพัฒนาซอฟต์แวร์

[3] NIST SSDF, PO 1.2, ตัวอย่างที่ 2 “กำหนดนโยบายที่ระบุความต้องการด้านความปลอดภัยสำหรับซอฟต์แวร์ขององค์กร และตรวจสอบการปฏิบัติตามข้อกำหนดที่จุดสำคัญ ๆ ของ SDLC (เช่น การใช้เกต (Gate) ระบุประเภทของข้อบกพร่องของซอฟต์แวร์ และการจัดการตอบสนองต่อช่องโหว่ที่พบหลังจากที่เปิดตัวซอฟต์แวร์ไปแล้ว)”

7. **ทดสอบการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัย(Security Incident Event Management - SIEM) และการบูรณาการระหว่างการประสานงานเพื่อตอบสนองปัญหาด้านความปลอดภัย ระบบออโตเมชันและการตอบสนอง (SOAR)** นอกเหนือจากการดำเนินการทดสอบภาคสนามแล้ว ให้ร่วมมือกับผู้ให้บริการที่มีชื่อเสียงในด้าน SIEM และ SOAR โดยเรียนรู้พร้อมกับลูกค้าเฉพาะรายเพื่อดูว่าทีมที่ตอบสนองต่อเหตุการณ์ด้านความปลอดภัยใช้ข้อมูลบันทึก (Logs) เพื่อตรวจสอบและแก้ไขปัญหาด้านความปลอดภัยที่คาดว่าจะเกิดหรือเกิดขึ้นจริงได้อย่างไร มีนักพัฒนาซอฟต์แวร์จำนวนไม่น้อยที่มีประสบการณ์รู้จักวิธีจัดการกับเหตุการณ์ด้านความปลอดภัย และบางครั้งบันทึกที่สร้างขึ้นอาจไม่ได้ช่วยเหลือผู้ที่ตอบสนองต่อเหตุการณ์ได้มากเท่าที่พวกเขาคิด ด้วยการทำงานร่วมกับทั้งเทคโนโลยี SIEM และ SOAR และผู้เชี่ยวชาญด้านการตอบสนองต่อเหตุการณ์จริง ทีมพัฒนาจึงสามารถสร้างบันทึกที่อธิบายถึงสิ่งที่เกิดขึ้นอย่างแม่นยำและครบถ้วน ซึ่งจะช่วยประหยัดเวลา และลดความไม่แน่นอนเมื่อต้องรับมือกับเหตุการณ์ด้านความปลอดภัย

8. **ทำงานสอดคล้องกับ Zero Trust Architecture (ZTA)** จัดแนวทางการปรับใช้ผลิตภัณฑ์ให้สอดคล้องกับโมเดล ZTA ของ NIST และโมเดล Zero Trust Maturity ของ CISA สนับสนุนให้ลูกค้านำหลักการเหล่านี้ไปใช้ในสภาพแวดล้อมของพวกเขา

แนวปฏิบัติทางธุรกิจ ที่ให้ความสำคัญกับความปลอดภัย

1. **ให้การจัดเก็บบันทึกโดยไม่มีค่าใช้จ่ายเพิ่มเติม** บริการคลาวด์ควรมุ่งมั่นที่จะรวมการสร้างและบันทึกข้อมูลที่เกี่ยวข้องกับความปลอดภัยเข้าเป็นส่วนหนึ่งของบริการโดยไม่มีค่าใช้จ่ายเพิ่มเติม ผลิตภัณฑ์ที่ใช้ภายในสำนักงานควรสร้างบันทึกข้อมูลที่เกี่ยวข้องกับความปลอดภัย โดยไม่มีค่าใช้จ่ายเพิ่มเติมเช่นกัน นอกจากนี้ ผลิตภัณฑ์ควรเก็บบันทึกเหตุการณ์ด้านความปลอดภัยตามค่าเริ่มต้นโดยอัตโนมัติ เนื่องจากลูกค้าจำนวนมากอาจไม่เข้าใจว่าบันทึกเหล่านี้มีความสำคัญเพียงใดจนกว่าจะเกิดปัญหาด้านความปลอดภัยขึ้น กลวิธีเหล่านี้อาจต้องมีการทบทวนอย่างรอบคอบว่าเหตุการณ์ด้านความปลอดภัยใดที่ควรบันทึกไว้เพื่อติดตามสถานะความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งรวมถึงวิธีที่ลูกค้าสามารถกำหนดตั้งค่าการบันทึกเอง ระยะเวลาในการเก็บรักษาบันทึก การป้องกันความสมบูรณ์และพื้นที่จัดเก็บของบันทึก และวิธีการวิเคราะห์บันทึก ในบางกรณี การทบทวนนี้อาจบ่งบอกถึงความจำเป็นในการปรับโครงสร้างสถาปัตยกรรมใหม่ที่แอปพลิเคชันจัดการการบันทึกเพื่อให้แน่ใจว่าบันทึกไม่เพียงแต่มีประโยชน์ แต่ยังเป็นค่าใช้จ่ายที่เหมาะสมสำหรับผู้ผลิตอีกด้วย การทำงานร่วมกับผู้เชี่ยวชาญด้านการตอบสนองต่อเหตุการณ์ (Incident Response - IR) สามารถเพิ่มโอกาสที่บันทึกจะเป็นประโยชน์ต่อผู้ตรวจสอบในภาคสนามหรือสถานการณ์จริง ดูหัวข้อเกี่ยวกับ SIEM

2. **กำจัดค่าใช้จ่ายต่าง ๆ ที่ซ่อนอยู่** ให้คำมั่นสัญญาอย่างเป็นทางการด้วยการประกาศว่าจะไม่เรียกเก็บเงินสำหรับคุณลักษณะหรือส่วนที่มาเสริมผสานด้านความปลอดภัยหรือความเป็นส่วนตัว ตัวอย่าง เช่น ภายในขอบเขตวงกว้างของการจัดการข้อมูลประจำตัวและการเข้าถึง (Identity and Access Management - IAM) มีบริการที่เรียกว่าบริการการลงชื่อเข้าใช้ครั้งเดียว (Single Sign-On - SSO) ซึ่งเหมือนกับการมีกุญแจดอกเดียวสำหรับประตูหลายบาน ผู้ผลิตบางรายจะเรียกเก็บเงินเพิ่มหากต้องการเชื่อมต่อระบบของตนกับบริการ SSO (บางครั้งเรียกว่าผู้ให้บริการข้อมูลประจำตัว) ส่วย หรือ "ภาษี SSO" นี้ ทำให้ธุรกิจขนาดเล็กยากที่จะมีข้อมูลประจำตัวและการจัดการการเข้าถึงที่ดีได้ ทำให้พวกเขาไม่สามารถบรรลุจุดยืนด้านการรักษาความปลอดภัยที่แข็งแกร่งจริง ๆ ได้ บางบริการเรียกเก็บเงินเพิ่มเพื่อเปิดใช้งาน MFA สำหรับผู้ใช้ **ไม่ควรตั้งราคาระบบความปลอดภัยเป็นสินค้าฟุ่มเฟือย ทุกคนควรเข้าถึงได้โดยถือเป็นสิทธิพื้นฐานของลูกค้า** ผู้ผลิตบางรายแย้งว่ามีลูกค้าเพียงไม่กี่รายที่ขอใช้คุณลักษณะเหล่านี้ ซึ่งมีค่าใช้จ่ายในการบำรุงรักษาสูงกว่า ข้อโต้แย้งเหล่านี้ไม่ได้พิจารณาถึงความจริงที่ว่ามีลูกค้าเพียงไม่กี่รายเท่านั้นที่จะโทรเข้ามาเพื่อร้องเรียนหรือต่อรองราคา ไม่ใช่ลูกค้าทั้งหมดจะเข้าใจถึงประโยชน์ของคุณลักษณะเหล่านี้อย่างเต็มที่ และเข้าใจว่าทุกคุณลักษณะต้องเสียค่าใช้จ่ายในการบำรุงรักษา ถึงกระนั้น เราไม่เห็นผู้ผลิตหลายรายนักที่เรียกเก็บเงินเพิ่มเติมสำหรับความพร้อมใช้งานหรือความสมบูรณ์ของข้อมูล ค่าใช้จ่ายในการสนับสนุนคุณสมบัติหลัก ๆ เหล่านั้นรวมอยู่ในราคาที่ลูกค้าทุกคนจ่าย เช่นเดียวกับค่าใช้จ่ายสำหรับอุปกรณ์ด้านความปลอดภัยในรถยนต์ เช่น เข็มขัดนิรภัย คอพวงมาลัยแบบยุบได้ และถุงลมนิรภัยที่ช่วยชีวิตผู้คนหากมีอุบัติเหตุ

3. **ยอมรับมาตรฐานแบบเปิด** ใช้มาตรฐานแบบเปิดที่ทุกคนใช้ได้ โดยเฉพาะอย่างยิ่งกับระบบเครือข่ายและโปรโตคอลการระบุข้อมูลประจำตัว หลีกเลี่ยงการใช้โปรโตคอลที่เป็นกรรมสิทธิ์เฉพาะ หากมีมาตรฐานแบบเปิดที่ทุกคนสามารถใช้ได้

4. **มอบเครื่องมือสำหรับการอัปเกรด** ลูกค้าจำนวนมากลังเลที่จะใช้ผลิตภัณฑ์เวอร์ชันใหม่ล่าสุด รวมถึงการปรับใช้คุณลักษณะที่ใหม่กว่าและปลอดภัยยิ่งขึ้น เช่น การเชื่อมต่อเครือข่ายที่ปลอดภัย ผู้ผลิตซอฟต์แวร์สามารถสนับสนุนให้ลูกค้าใช้การอัปเดตใหม่ ๆ มากขึ้นได้ โดยการจัดหาเครื่องมือที่จะช่วยลดความไม่แน่นอนและความเสี่ยงให้ลูกค้า มอบใบอนุญาตใช้งานให้กับลูกค้าโดยไม่เสียค่าใช้จ่าย เพื่อทดลองใช้การอัปเกรดและการแก้ไขโดยใช้แพตช์ในสภาพแวดล้อมการทดสอบ เพื่อเป็นแนวทางในการจูงใจให้ลูกค้า

หลักการที่ 2 เปิดรับความโปร่งใสอย่างถึงแก่นและแสดงความรับผิดชอบต่อทุกสิ่งที่ทำ

คำอธิบาย

ผู้ผลิตซอฟต์แวร์ควรภูมิใจที่ได้นำส่งผลิตภัณฑ์ที่ปลอดภัย ตลอดจนที่ได้ สร้างความแตกต่างระหว่างตนเองกับผู้ผลิตรายอื่นในชุมชนจากความสามารถของตนที่ได้ปฏิบัติเช่นนั้น

มาพูดถึงข้อกังวลที่เรามีร่วมกันเกี่ยวกับความโปร่งใส เมื่อผู้ปฏิบัติงานพูดถึงความโปร่งใสอย่างถึงแก่น การสนทนามีแนวโน้มจะติดขัดด้วยความกังวลที่ว่า พวกเขากำลังจัดเตรียม "แผนการทำงานให้กับผู้โจมตีระบบ" อย่างไรก็ตาม หลักฐานที่ชัดเจนก็คือผู้โจมตีระบบก็ยังดำเนินการไปได้โดยไม่มีแผนการทำงานนี้ และข้อกังวลดังกล่าวควรได้รับความสำคัญน้อยกว่าความโปร่งใส ซึ่งเป็นประโยชน์ต่อลูกค้าทั้งทางตรงและทางอ้อม ซัพพลายเชน และอุตสาหกรรมซอฟต์แวร์โดยรวมทั้งหมด

ความโปร่งใสช่วยให้อุตสาหกรรมกำหนดแบบแผนเป็นมาตรฐานได้ หรืออีกนัยหนึ่งคือ แสดงให้ทุกคนเห็นว่าการทำสิ่งต่าง ๆ ที่ "ดี" นั้นมีลักษณะเช่นใด ซึ่งช่วยให้แบบแผนเหล่านั้นเปลี่ยนแปลงไปตามกาลเวลาโดยตอบสนองต่อสิ่งที่ลูกค้าต้องการ การเปลี่ยนแปลงกลวิธีหรือเศรษฐศาสตร์ของผู้โจมตี หรือความก้าวหน้าทางเทคโนโลยี ความโปร่งใสช่วยให้ผู้ผลิตที่มีทรัพยากรน้อยกว่าเรียนรู้จากผู้ที่มีประสบการณ์และความสมบูรณ์ทางทรัพยากรมากกว่า เมื่อพูดถึงการแบ่งปันข้อมูล เราควรขยายความไปให้ไกลกว่าคำเตือนที่ชี้ถึงภัยคุกคามในเวลาจริง เพื่อรวมองค์ประกอบด้านล่างนี้

ความโปร่งใสบังคับให้มีการตัดสินใจเลือกความปลอดภัยในกระบวนการพัฒนาตั้งแต่เนิ่น ๆ และเป็นกิจกรรมต่อเนื่องของผู้นำธุรกิจ เช่นเดียวกับวิศวกรและผู้เชี่ยวชาญด้านความปลอดภัย ความโปร่งใสสร้างความรับผิดชอบพร้อมไปในตัวผลิตภัณฑ์

หมายเหตุเกี่ยวกับการเลือกคำคุณศัพท์ "อย่างถึงแก่น (Radical)" ที่ใช้กับ "ความโปร่งใส่ (Transparency)" ทุกวันนี้ ไม่ใช่เรื่องปกติที่ผู้ผลิตซอฟต์แวร์จะเผยแพร่ข้อมูลโดยละเอียดเกี่ยวกับวิธีการพัฒนาและบำรุงรักษาซอฟต์แวร์ และวิธีที่พวกเขาพัฒนาโปรแกรมโดยใช้ข้อมูลตามเวลาที่ผ่านไป ในอุตสาหกรรมซอฟต์แวร์มีผู้ผลิตเพียงไม่กี่รายที่เสนอทัวร์พาชมวิธีการออกแบบซอฟต์แวร์ของตน ผู้ผลิตซอฟต์แวร์มักไม่มีโอกาสได้เห็นว่าองค์กรอื่น ๆ ที่คล้ายคลึงกันจัดโครงสร้างโปรแกรม SDLC ของตนอย่างไร และโปรแกรมเหล่านั้นทำงานอย่างไรเพื่อรับมือกับผู้โจมตีจริงในสภาพแวดล้อมของลูกค้า อุตสาหกรรมส่วนรวมจะได้รับประโยชน์จากการแบ่งปันข้อมูลเพิ่มเติมเกี่ยวกับหัวข้อต่าง ๆ เช่น กลยุทธ์ในการคำนวณต้นทุนของข้อบกพร่องด้านความปลอดภัย และเพื่อกำจัดประเภทต่าง ๆ ของช่องโหว่ จากผลของแนวปฏิบัติทั่วไปเหล่านี้ ผู้ผลิตซอฟต์แวร์ทุกรายจึงต้องเรียนรู้วิธีจัดการกับความปลอดภัยของผลิตภัณฑ์ด้วยตนเอง หากบริษัทไม่คิดค่าใช้จ่ายเพิ่มเติมสำหรับคุณลักษณะด้านความปลอดภัยเหมือนการเก็บภาษีสินค้าฟุ่มเฟือย ความปลอดภัยจะกลายเป็นศูนย์ต้นทุนแทนที่จะเป็นแหล่งที่มาของผลกำไร และบริษัทต่าง ๆ ก็จะได้รับประโยชน์จากการแบ่งเบาภาระผ่านการทำงานร่วมกันและการใช้ความโปร่งใส

เราต้องการมุ่งเน้นกลวิธีที่จะเร่งความก้าวหน้าของอุตสาหกรรมซอฟต์แวร์อย่างมีนัยสำคัญ เราไม่สามารถปรับปรุงแบบค่อยเป็นค่อยไปและทำงานแบบฉวยโอกาสได้อีกต่อไป หากเราต้องการเอาชนะภัยคุกคามด้วยกัน ซึ่งเกิดจากศัตรูที่ชาญฉลาดและปรับตัวได้นั้น เราต้องเปิดรับระดับความโปร่งใสแม้ว่าอาจรู้สึกอึดอัดในวันนี้ แต่สิ่งนี้จะช่วยขับเคลื่อนอุตสาหกรรมไปข้างหน้า ปัจจุบันมีผู้ผลิตหลายรายที่ปฏิบัติการตามหลักความปลอดภัยโดยการออกแบบอยู่แล้ว ดังที่ William Gibson กล่าวไว้ว่า “อนาคตมาถึงแล้ว เพียงแต่ไม่ได้กระจายออกไปอย่างเท่าเทียมกันทุกที่เท่านั้น” **ความโปร่งใสอย่างถึงแก่นนี้จะช่วยกระจายข้อมูลดังกล่าวและเป็นประโยชน์ต่อผู้ที่ป้องกันภัยคุกคามมากกว่าช่วยเหลือศัตรูของเรา**

ความโปร่งใสสามารถบรรลุผลได้มากกว่าแค่ช่วยเหลือองค์กรระดับเดียวกันพัฒนา SDLC ของตน ลูกค้าและนักลงทุนในอนาคตสามารถเรียนรู้เพิ่มเติมเกี่ยวกับการลงทุนและการประนีประนอมที่ผู้ผลิตได้ทำไว้ รวมถึงจุดยืนด้านการรักษาความปลอดภัยที่การลงทุนเหล่านั้นสร้างไว้ให้กับลูกค้า ผู้ผลิตที่เปิดรับความโปร่งใสอย่างถึงแก่นจะให้ข้อมูลแก่ลูกค้าเพื่อช่วยพวกเขาตัดสินใจว่าจะซื้ออะไร ซึ่งไม่เพียงแต่ขึ้นอยู่กับราคาและคุณลักษณะเท่านั้น แต่ยังรวมถึงความปลอดภัยของผลิตภัณฑ์ด้วย

แม้ว่าองค์กรต่าง ๆ จะทำงานหนักเพื่อรักษาความปลอดภัยให้กับซัพพลายเชนและ SDLC ของตนก็ตาม แต่ในอดีตที่เพิ่งผ่านมา บางบริษัทก็ยังประสบปัญหาที่กระบวนการสร้างซอฟต์แวร์ถูกละเมิดความปลอดภัย การเปิดรับความโปร่งใสอย่างถึงแก่นนี้ หมายถึงการแจ้งให้สาธารณชนทราบเกี่ยวกับการโจมตีนั้น รวมถึงการปรับปรุงที่บริษัททำเพื่อป้องกันและตรวจจับการโจมตีที่คล้ายกันในอนาคต การแบ่งปันข้อมูลประเภทนี้จะช่วยให้องค์กรอื่นเรียนรู้จากประสบการณ์โดยไม่ต้องประสบชะตากรรมเดียวกัน

การสาธิตหลักการนี้

เพื่อสาธิตให้เห็นถึงหลักการนี้ ผู้ผลิตซอฟต์แวร์ควรดำเนินการตามขั้นตอนดังต่อไปนี้

แนวปฏิบัติตามหลักความปลอดภัย โดยการตั้งค่าเริ่มต้น

1. **เผยแพร่สถิติและแนวโน้มที่เกี่ยวข้องกับความปลอดภัยโดยรวม** หัวข้อตัวอย่าง ได้แก่ จำนวนลูกค้าและผู้ดูแลระบบที่ใช้ MFA และการใช้โปรโตคอลล้าสมัยที่ไม่ปลอดภัย
2. **เผยแพร่สถิติการใช้แพตช์** ให้รายละเอียดสัดส่วนร้อยละของจำนวนลูกค้าที่ใช้ผลิตภัณฑ์เวอร์ชันใหม่ล่าสุด และสิ่งที่คุณกำลังทำเพื่อให้การอัปเดตง่ายขึ้นและเชื่อถือได้มากขึ้น
3. **เผยแพร่ข้อมูลเกี่ยวกับสิทธิพิเศษที่ผู้คนมีแต่ไม่ได้ใช้** เผยแพร่ข้อมูลโดยรวมเกี่ยวกับการอนุญาตที่มากเกินไปทั่วทั้งฐานลูกค้าของคุณ ตลอดจนการแจ้งเตือนและการเปลี่ยนแปลงอื่น ๆ ในผลิตภัณฑ์ที่คุณกำลังทำเพื่อลดโอกาสที่ลูกค้าจะถูกโจมตี สำหรับสิทธิพิเศษที่ไม่ได้ใช้เหล่านี้ เราสามารถใช้เป็นการแจ้งเตือนผู้ดูแลระบบได้เช่นเดียวกับเสียงเตือนให้รัดเข็มขัดนิรภัย

แนวปฏิบัติในการพัฒนาผลิตภัณฑ์ที่มีความปลอดภัย

1. **สร้างการควบคุมความปลอดภัยภายในองค์กร** บริษัทหลายแห่งเล็งเห็นประโยชน์ของการย้ายข้อมูลไปยังผู้ให้บริการระบบคลาวด์ ตอนนี้ผู้ให้บริการระบบคลาวด์จึงกลายเป็นจุดสนใจและเป็นเป้าหมายของผู้โจมตีทางไซเบอร์ ผู้ให้บริการซอฟต์แวร์เป็นบริการออนไลน์ (SaaS) ควรเผยแพร่ข้อมูลสถิติการควบคุมภายในของตน ตัวอย่างเช่น ผู้ให้บริการซอฟต์แวร์ที่เป็นบริการออนไลน์ (SaaS) ควรเผยแพร่ข้อมูลสถิติเกี่ยวกับการปรับใช้งาน MFA ภายในองค์กรที่ป้องกันการฟิชชิ่งได้ (phishing-resistant MFA) เช่น FIDO (Fast Identity Online - FIDO) ตามหลักการแล้ว บริษัทควรสามารถระบุได้อย่างมั่นใจว่าไม่มีพนักงานคนใดสามารถเข้าถึงข้อมูลลูกค้าหรือข้อมูลที่ละเอียดอ่อนได้โดยไม่ต้องยืนยันตัวตนผ่าน MFA ที่ป้องกันการฟิชชิ่ง

2. **เผยแพร่โมเดลที่เป็นภัยคุกคามระดับสูง** ผลิตภัณฑ์ตามหลักความปลอดภัยโดยการออกแบบเริ่มต้นด้วยโมเดลภัยคุกคามที่เขียนขึ้นเพื่ออธิบายถึงสิ่งที่ผู้สร้างต้องการป้องกันและต้องการป้องกันจากใคร โมเดลภัยคุกคามที่มีประสิทธิภาพมาจากการทำความเข้าใจว่าการโจมตีที่แท้จริงเกิดขึ้นได้อย่างไร และควรครอบคลุมทั้งสภาพแวดล้อมขององค์กรและการพัฒนา ตลอดจนวิธีที่ผู้ผลิตซอฟต์แวร์ตั้งใจที่จะใช้ในสภาพแวดล้อมของลูกค้า

3. **เผยแพร่การรับรองตนเองอย่างละเอียดเกี่ยวกับ SDLC ที่ปลอดภัย** ผู้ผลิตที่ปฏิบัติตามมาตรฐาน NIST SSDF หรือกรอบงานอื่น ๆ ที่คล้ายคลึงกัน กำลังทำงานกันอย่างมุ่งมั่นเพื่อที่จะเติบโตและทำให้วงจรการพัฒนาซอฟต์แวร์สมบูรณ์ตั้งแต่ต้นจนจบ การเผยแพร่การรับรองตนเองต่อสาธารณะว่าการควบคุมใดที่ผู้ผลิตได้บังคับใช้ และใช้กับผลิตภัณฑ์ใด จะแสดงให้เห็นถึงความมุ่งมั่นที่ผู้ผลิตได้ปฏิบัติตามแนวปฏิบัติที่ดีที่สุดเหล่านี้ ความโปร่งใสนี้สามารถทำให้ลูกค้าไว้วางใจผู้ผลิตมากขึ้น นอกจากนี้ยังมีโปรแกรมการรับรองอื่น ๆ เช่น ระเบียบวิธีซัพพลายเชนทางไซเบอร์ของอิสราเอล (Israel Cyber Supply Chain Methodology) เป็นต้น

4. **เปิดรับความโปร่งใสโดยไม่ปกปิดช่องโหว่** ให้คำมั่นสัญญาอย่างเป็นทางการด้วยการประกาศว่าจะทำให้แน่ใจว่า ช่องโหว่ของผลิตภัณฑ์ที่ระบุจะถูกเผยแพร่เป็นรายการ CVE ที่ถูกต้องและครบถ้วน โดยเฉพาะอย่างยิ่งสำหรับหมวดหมู่การระบุจุดอ่อนที่มีร่วมกัน (Common Weakness Enumeration - CWE) ซึ่งระบุสาเหตุเบื้องหลังแท้จริงของช่องโหว่ต่าง ๆ ยิ่งรายการจุดอ่อนหรือฐานข้อมูล CVE สาธารณะมีความถูกต้องและครบถ้วนมากขึ้น อุตสาหกรรมก็จะยิ่งสามารถติดตามได้มากขึ้นด้วยว่าผลิตภัณฑ์มีความปลอดภัยมากขึ้นอย่างไร และช่องโหว่ประเภทใดที่พบบ่อยที่สุด อย่างไรก็ตาม โปรดระวังเรื่องการคิดว่า CVE จำนวนมากนั้น เป็นตัวชี้วัดในเชิงลบ เนื่องจากตัวเลขดังกล่าวยังเป็นสัญญาณที่ดีที่บ่งบอกถึงชุมชน ซึ่งกำลังวิเคราะห์และทดสอบรหัสอย่างขันแข็งอีกด้วย เมื่อผู้ผลิตใช้หลักปรัชญาความปลอดภัยโดยการออกแบบพวกเขาอาจพบว่ามีช่องโหว่หรือจุดบกพร่องที่รายงานเพิ่มขึ้นในช่วงแรก ๆ เนื่องจากพวกเขากำลังค้นพบและแก้ไขปัญหาเพิ่มเติมในรหัสที่มีอยู่อย่างครอบคลุมยิ่งขึ้น ผู้ผลิตควรเผยแพร่การวิเคราะห์ช่องโหว่ในอดีต รวมถึงรูปแบบและมาตรการใด ๆ ที่ดำเนินการเพื่อแก้ไขปัญหาช่องโหว่ประเภทคล้ายคลึงกันในทุกระดับ ตัวอย่างเช่น หาก CVE ของบริษัทส่วนใหญ่เกี่ยวข้องกับสคริปต์ข้ามไซต์ (Cross-Site Scripting - XSS) การจัดทำเอกสารการวิเคราะห์สาเหตุเบื้องหลังแท้จริง การตอบสนอง (เช่น การเปลี่ยนไปใช้กรอบงานเทมเพลตเว็บที่ป้องกัน XSS) และผลลัพธ์จะส่งสัญญาณให้ลูกค้าทราบว่าพวกเขาจะไม่ตกเป็นเหยื่อของช่องโหว่ประเภทใดประเภทหนึ่ง ซึ่งการบรรเทาผลกระทบนั้นเป็นที่เข้าใจกันมานานหลายทศวรรษแล้ว

5. **เผยแพร่รายการวัสดุซอฟต์แวร์ (Software Bills of Materials - SBOM)** ผู้ผลิตควรรู้และควบคุมซัพพลายเชนของตน องค์กรควรสร้างและบำรุงรักษา SBOM [2] สำหรับแต่ละผลิตภัณฑ์ พวกเขายังควรขอข้อมูลจากซัพพลายเออร์ และทำให้ SBOM พร้อมใช้งานสำหรับลูกค้าและผู้ใช้ขั้นปลายน้ำ การทำเช่นนี้แสดงให้เห็นว่าองค์กรใส่ใจต่อการทำความเข้าใจส่วนประกอบที่พวกเขาใช้ในสร้างผลิตภัณฑ์ของตน นอกจากนี้ ยังแสดงให้เห็นว่าพวกเขาสามารถตอบสนองกับความเสี่ยงที่ระบุใหม่ได้ และสามารถช่วยให้ลูกค้าเข้าใจวิธีการตอบสนองหากเพิ่งมีการค้นพบช่องโหว่ใหม่ในมอดูลของซัพพลายเชน

เพื่อเป็นข้อมูลอ้างอิง กระทรวงเศรษฐกิจ การค้า และอุตสาหกรรม (METI) ของญี่ปุ่นได้เผยแพร่แนวทางที่ชื่อว่า "Guide of Introduction of Software Bill of Materials (SBOM) for Software Management" ความโปร่งใสนี้ ควรให้ข้อมูลที่ขยายไปถึงเฟิร์มแวร์ที่ติดตั้งในอุปกรณ์ ข้อมูล และโมเดลที่ใช้ในการเรียนรู้ของ AI หรือการเรียนรู้ของเครื่อง (Machine Learning - ML) นอกเหนือจากการช่วยในการตัดสินใจซื้อและความสามารถในการปฏิบัติงานแล้ว SBOM ยังมีบทบาทสำคัญในโครงสร้างพื้นฐานที่จะตรวจจับและตอบสนองการโจมตีต่อซัพพลายเชนที่เป็นอันตราย

6. **เผยแพร่นโยบายการเปิดเผยช่องโหว่** เผยแพร่นโยบายการเปิดเผยช่องโหว่ที่ (1) อนุญาตให้ทำการทดสอบกับผลิตภัณฑ์ทั้งหมดที่นำเสนอโดยผู้ผลิตและเงื่อนไขสำหรับการทดสอบเหล่านั้น (2) ให้ความคุ้มครองตามกฎหมายสำหรับการดำเนินการที่สอดคล้องกับนโยบาย และ (3) อนุญาตให้เปิดเผยช่องโหว่ต่อสาธารณะหลังจากช่วงระยะเวลาหนึ่งที่กำหนด ผู้ผลิตควรทำการวิเคราะห์สาเหตุเบื้องหลังแท้จริงของช่องโหว่ที่ค้นพบและดำเนินการเพื่อกำจัดประเภทช่องโหว่ทั้งหมดให้ได้มากที่สุด ดู เทมเพลตนโยบายการเปิดเผยช่องโหว่ (Vulnerability Disclosure Policy Template) ของ CISA สำหรับภาษาอ้างอิง

แนวปฏิบัติทางธุรกิจ ที่ให้ความสำคัญกับความปลอดภัย

1. **ประกาศแต่งตั้งผู้สนับสนุนที่เป็นผู้บริหารระดับสูงเพื่อรับผิดชอบด้านความปลอดภัยโดยการออกแบบ** ในองค์กรจำนวนมาก การรักษาความปลอดภัย (เช่นเดียวกับคุณภาพ) มักมอบหมายให้กับทีมงานด้านเทคนิคที่อาจไม่มีอำนาจในการเปลี่ยนแปลงในระดับโครงสร้างเพื่อเพิ่มความปลอดภัยของผลิตภัณฑ์อย่างมีนัยสำคัญ การประกาศต่อสาธารณะแต่งตั้งให้ผู้บริหารธุรกิจระดับสูงสุดดูแลโปรแกรมความปลอดภัยโดยการออกแบบจะเปลี่ยนความปลอดภัยของผลิตภัณฑ์ให้กลายเป็นข้อกังวลทางธุรกิจระดับสูงสุดได้

2. **เผยแพร่แผนการทำงานตามหลักความปลอดภัยโดยการออกแบบ** ผู้ผลิตควรจดบันทึกการเปลี่ยนแปลงใด ๆ ที่ทำกับ SDLC ของตนเพื่อปรับปรุงความปลอดภัยของลูกค้า รวมถึงรายละเอียดเกี่ยวกับรายงานการทดสอบในสภาพใช้งานจริง ขั้นตอนดำเนินการเพื่อกำจัดช่องโหว่ประเภทต่าง ๆ ทั้งหมด และรายการอื่น ๆ ที่กล่าวถึงในหลักการอื่น เช่นเดียวกับกรณีของความพยายามทำให้สิ่งต่าง ๆ ดีขึ้นในแง่ของคุณภาพ โปรแกรมการปรับปรุงความความปลอดภัยยังต้องผ่านขั้นตอนที่ชัดเจนด้วย เช่น การวางแผน การควบคุมให้เป็นไปตามแผน และการปรับปรุงให้ดีขึ้นอย่างต่อเนื่อง ตามแนวคิดการลงมือทำแทนการบอกเล่าเป็นคำพูด การเผยแพร่แผนการทำงานและรายละเอียดเบื้องหลังขั้นตอนเหล่านี้ จะทำให้ผู้คนมั่นใจว่าผลิตภัณฑ์เป็นไปตามหลักความปลอดภัยโดยการออกแบบอย่างแท้จริง เมื่อผู้ผลิตทำการปรับปรุงที่สำคัญได้สำเร็จแล้ว พวกเขาควรให้รายละเอียดในรายงานเพื่อความโปร่งใสได้ การแบ่งปันรายละเอียดเช่นนี้ ไม่เพียงแต่พิสูจน์ให้เห็นถึงความมุ่งมั่นตามหลักความปลอดภัยโดยการออกแบบ แต่ยังเป็นแรงบันดาลใจสนับสนุนให้ผู้อื่นปฏิบัติตามด้วยการเป็นตัวอย่างแห่งความสำเร็จที่แท้จริงให้กับผู้อื่น

3. **เผยแพร่แผนการทำงานด้านความปลอดภัยสำหรับหน่วยความจำ** ผู้ผลิตสามารถดำเนินการเพื่อกำจัดช่องโหว่ประเภทใหญ่ที่สุดกลุ่มหนึ่งได้โดยการย้ายผลิตภัณฑ์ที่มีอยู่และสร้างผลิตภัณฑ์ใหม่ด้วยการใช้ภาษาการเขียนโปรแกรมที่มีปลอดภัยสำหรับหน่วยความจำ แม้ว่าการดำเนินการนี้อาจเป็นไปไม่ได้ในทุกกรณี แต่ผู้ผลิตสามารถพิจารณาการพัฒนาแอปพลิเคชันแรปเปอร์ (Application Wrapper) ในภาษาที่ปลอดภัยสำหรับหน่วยความจำ แทนที่จะเขียนแอปพลิเคชันทั้งหมดใหม่ นอกจากนี้ ยังอาจเกี่ยวข้องกับวิธีที่ผู้ผลิตอัปเดตการจ้างงาน การฝึกอบรม ตรวจสอบรหัสและจัดการกระบวนการอื่น ๆ ภายในองค์กรตลอดจนวิธีที่พวกเขาจะช่วยสนับสนุนให้ชุมชนโอเพนซอร์สดำเนินการเช่นเดียวกัน

4. **เผยแพร่ผลลัพธ์** ในขณะที่มีการอัปเดต SDLC เพื่อปฏิบัติตามหลักความปลอดภัยโดยการออกแบบนั้น องค์กรต่าง ๆ จะได้พบกับผลสำเร็จที่รวดเร็ว ผลสำเร็จที่ต้องใช้ทรัพยากรมากขึ้น และความล้มเหลวที่ไม่คาดคิดบางประการในระหว่างทาง ด้วยการนำเสนอความสำเร็จและอุปสรรคภายในต่าง ๆ อุตสาหกรรมโดยรวมทั้งหมดจะได้เรียนรู้จากผลลัพธ์นี้ด้วย

หลักการที่ 3 นำจากระดับบนสุดสู่ล่าง

คำอธิบาย

แม้ว่าปรัชญาโดยรวมจะชื่อว่า "ความปลอดภัยโดยการออกแบบ" แต่แรงจูงใจเพื่อความปลอดภัยของลูกค้าเริ่มต้นก่อนที่จะมีการออกแบบผลิตภัณฑ์เสียอีก โดยเริ่มต้นด้วยการหาเป้าหมายทางธุรกิจและวัตถุประสงค์โดยนัยและโดยแจ้ง ตลอดจนผลลัพธ์ที่คาดหวัง เมื่อผู้นำระดับสูงให้ความสำคัญของความปลอดภัยเป็นอันดับแรกในทางธุรกิจ สร้างแรงจูงใจภายในองค์กร และส่งเสริมวัฒนธรรมที่ทั่วถึงเพื่อทำให้ความปลอดภัยเป็นข้อกำหนดในการออกแบบเท่านั้น พวกเขาจึงจะบรรลุผลลัพธ์ที่ดีที่สุด

แม้ว่าความเชี่ยวชาญด้านเทคนิคมีความสำคัญอย่างยิ่งต่อความปลอดภัยของผลิตภัณฑ์ แต่ก็ไม่ใช่เรื่องที่จะปล่อยให้เป็นหน้าที่ของเจ้าหน้าที่ด้านเทคนิคเพียงฝ่ายเดียว ถือเป็นลำดับความสำคัญทางธุรกิจที่ต้องเริ่มต้นจากผู้นำระดับสูงสุด

บางคนสงสัยว่าหากผู้ผลิตซอฟต์แวร์กำลังยอมรับหลักการสองข้อแรกและสร้างหลักฐานสิ่งประดิษฐ์ที่มีความหมายแล้ว หลักการที่สามจำเป็นหรือไม่ วิธีที่บริษัทกำหนดวิสัยทัศน์ พันธกิจ ค่านิยม และวัฒนธรรมของตนจะส่งผลต่อผลิตภัณฑ์อย่างไร และปัจจัยเหล่านี้ส่วนใหญ่ถูกกำหนดโดยผู้นำที่อยู่ระดับสูงสุด เราสังเกตเห็นรูปแบบเดียวกันนี้ในอุตสาหกรรมอื่น ๆ ที่มีการปรับปรุงด้านความปลอดภัยและคุณภาพอย่างมีนัยสำคัญ J.M. Juran ผู้เชี่ยวชาญด้านคุณภาพที่มีชื่อเสียง เขียนไว้ว่า

> ***การบรรลุความเป็นผู้นำที่มีคุณภาพ หมายถึง ผู้จัดการระดับสูงจำเป็นต้องเป็นผู้นำและจัดการเพื่อคุณภาพด้วยตนเองอย่างแข็งขัน ในบริษัทที่ประสบความสำเร็จและมีความเป็นผู้นำที่มีคุณภาพ ผู้จัดการระดับสูงเองก็เป็นผู้นำในความคิดริเริ่มนี้ด้วยตนเอง ผมไม่ทราบถึงข้อยกเว้นใด ๆ [3]***

เราเชื่อว่าความปลอดภัยเป็นหมวดหมู่ย่อยของคุณภาพผลิตภัณฑ์ เมื่อความปลอดภัยและคุณภาพกลายเป็นความจำเป็นทางธุรกิจ แทนที่จะเป็นเพียงงานทางเทคนิคสำหรับทีมเทคนิคเท่านั้น องค์กรต่าง ๆ จะสามารถตอบสนองความต้องการด้านความปลอดภัยของลูกค้าได้อย่างรวดเร็วและมีประสิทธิภาพมากขึ้น นอกจากนี้ การลงทุนทรัพยากรที่จำเป็นเพื่อให้แน่ใจว่าความปลอดภัยของซอฟต์แวร์เป็นลำดับความสำคัญทางธุรกิจตั้งแต่เริ่มต้นจะช่วยลดต้นทุนระยะยาวในการแก้ไขข้อบกพร่องของซอฟต์แวร์ และเป็นผลให้ลดความเสี่ยงด้านความมั่นคงระดับประเทศ

เช่นเดียวกับที่ทีมผู้นำได้นำโปรแกรมความรับผิดชอบต่อสังคมขององค์กร (Corporate Social Responsibility - CSR) ออกใช้ ก็มีความตระหนักเพิ่มมากขึ้นว่า คณะกรรมการขององค์กร รวมถึงผู้ผลิตซอฟต์แวร์ควรมีบทบาทเชิงรุกมากขึ้นในการชี้แนะโปรแกรมการรักษาความมั่นคงปลอดภัยทางไซเบอร์ บางครั้งมีการใช้คำว่าความรับผิดชอบทางไซเบอร์ขององค์กร (Corporate Cyber Responsibility - CCR) เพื่ออธิบายแนวคิดที่เกิดขึ้นใหม่นี้

การสาธิตหลักการนี้

เพื่อสาธิตให้เห็นถึงหลักการนี้ ผู้ผลิตซอฟต์แวร์ควรดำเนินการตามขั้นตอนดังต่อไปนี้

1. **รวมรายละเอียดของโปรแกรมความปลอดภัยโดยการออกแบบไว้ในรายงานทางการเงินขององค์กร** หากผู้ผลิตเป็นบริษัทจดทะเบียนในตลาดหลักทรัพย์ ให้เพิ่มส่วนหนึ่งไว้ในรายงานประจำปีทุกปีที่พูดถึงความพยายามที่บริษัทได้ทำตามหลักความปลอดภัยโดยการออกแบบ เป็นเรื่องปกติที่บริษัทรถยนต์มักรวมรายงานทางการเงินประจำปีที่มีรายละเอียดเกี่ยวกับความปลอดภัยของผู้ขับขี่และผู้โดยสาร รวมถึงข้อมูลเกี่ยวกับคณะกรรมการคุณภาพและความปลอดภัยแบบรวมศูนย์และแบบกระจายไปตามแผนก การให้รายละเอียดเกี่ยวกับโปรแกรมความปลอดภัยโดยการออกแบบในรายงานทางการเงินจะแสดงให้เห็นว่าองค์กรกำลังเชื่อมโยงความปลอดภัยของลูกค้ากับผลลัพธ์ทางการเงินขององค์กร และแสดงให้เห็นถึงความมุ่งมั่นอย่างแท้จริงมากกว่าการใช้คำที่นิยมใช้กันในด้านการตลาด
2. **รายงานต่อคณะกรรมการบริหารของคุณอย่างสม่ำเสมอ** เมื่อประธานเจ้าหน้าที่ความปลอดภัยด้านสารสนเทศ (Chief Information Security Officer - CISO) รายงานต่อคณะกรรมการบริหารของบริษัท พวกเขามักจะนำเสนอรายละเอียดเกี่ยวกับโปรแกรมความปลอดภัยในปัจจุบันและที่วางแผนไว้ ตลอดจนภัยคุกคาม เหตุการณ์ด้านความปลอดภัยที่ต้องสงสัยและได้รับการยืนยัน และการอัปเดตที่สำคัญอื่น ๆ ที่เน้นจุดยืนด้านการรักษาความปลอดภัยโดยรวมและสถานภาพของบริษัท นอกเหนือไปจากการรับข้อมูลเกี่ยวกับจุดยืนด้านการรักษาความปลอดภัยขององค์กรแล้ว คณะกรรมการบริหารของบริษัทควรขอข้อมูลเกี่ยวกับความปลอดภัยของผลิตภัณฑ์และผลกระทบที่ข้อมูลมีต่อความปลอดภัยของลูกค้าด้วย คณะกรรมการบริหารของบริษัทไม่ควรพึ่งพาแค่เพียงประธาน CISO เท่านั้น แต่ควรมองไปที่สมาชิกฝ่ายบริหารของบริษัทรายอื่น ๆ เป็นหลักในการทำงานเพื่อลดความเสี่ยงที่อาจส่งผลกระทบต่อลูกค้า
3. **มอบอำนาจให้ผู้บริหารด้านความปลอดภัยโดยการออกแบบ** มีความแตกต่างที่มีนัยสำคัญระหว่างองค์กรมีทีมงานด้านเทคนิคที่ได้รับ "การยอมรับจากผู้บริหาร" และองค์กรที่ผู้นำธุรกิจจัดการกับกระบวนการปรับปรุงความปลอดภัยของลูกค้าด้วยตนเองโดยใช้กระบวนการทางธุรกิจตามมาตรฐานปกติ คำว่า "การยอมรับจากผู้บริหาร" หมายความว่าต้องมีคนคอยโน้มน้าวให้ผู้บริหารระดับสูงสนับสนุนแนวคิดเกี่ยวกับโปรแกรมความปลอดภัยของลูกค้า แทนที่จะเป็นเป้าหมายทางธุรกิจจากระดับสูงสุด ผู้บริหารท่านนี้จะต้องได้รับมอบอำนาจให้มีอิทธิพลต่อการกำหนดรูปแบบการลงทุนในผลิตภัณฑ์เพื่อให้บรรลุผลลัพธ์ด้านความปลอดภัยของลูกค้า
4. **สร้างแรงจูงใจภายในองค์กรที่มีความหมาย** ให้แน่ใจว่ารางวัลที่มอบให้กับพนักงานที่ทำงานดีด้านความปลอดภัยของลูกค้านั้นมีความสมดุล และไม่สนับสนุนพฤติกรรมที่ไม่ถูกต้องโดยไม่ได้ตั้งใจ จัดรางวัลเหล่านี้ให้สอดคล้องกับพฤติกรรมและผลลัพธ์อื่น ๆ ที่บริษัทให้ความสำคัญ เริ่มต้นจากผู้บริหารด้านความปลอดภัยโดยการออกแบบไปจนถึงฝ่ายจัดการผลิตภัณฑ์ การพัฒนาซอฟต์แวร์ การสนับสนุน การขาย กฎหมาย และองค์กรอื่น ๆ การผสานสิ่งจูงใจด้านความปลอดภัยของลูกค้าเข้ากับการจ้างงาน การเลื่อนตำแหน่ง เงินเดือน โบนัส ตัวเลือกหุ้น และกระบวนการทั่วไปอื่น ๆ ในการดำเนินธุรกิจ ตัวอย่างเช่น เมื่อกำหนดเกณฑ์สำหรับการเลื่อนตำแหน่งสนับสนุนนักพัฒนาซอฟต์แวร์ ให้พิจารณาว่าพวกเขามีส่วนปรับปรุงความปลอดภัยของผลิตภัณฑ์อย่างไร ควบคู่ไปกับสิ่งต่าง ๆ เช่น การปรับปรุงสถานะการออนไลน์ ประสิทธิภาพ และคุณลักษณะ
5. **ก่อตั้งคณะกรรมการด้านความปลอดภัยโดยการออกแบบ** ในบางอุตสาหกรรม เป็นเรื่องปกติที่องค์กรต่าง ๆ จะแต่งตั้งคณะกรรมการดูแลคุณภาพไว้ที่ส่วนกลางและยังจัดจ้างบุคลากรตัวแทนที่เชี่ยวชาญด้านคุณภาพไว้ในแผนกหรือหน่วยธุรกิจหลัก ด้วยการรวมตัวของสมาชิกทั้งแบบรวมศูนย์และแบบกระจายเช่นนี้ ทั้งกลุ่มทำงานเพื่อปรับปรุงคุณภาพโดยเทียบกับเป้าหมายระดับสูงสุด ขณะเดียวกันก็รวบรวมข้อมูลจากส่วนต่าง ๆ ขององค์กรเพื่อติดตามว่าทุกสิ่งทำงานได้ดีเพียงใด ในทำนองเดียวกัน คณะกรรมการด้านความปลอดภัยโดยการออกแบบจะปรับปรุงความปลอดภัยด้วยการมุ่งเน้นไปที่การทำให้แน่ใจว่าการออกแบบบรรลุเป้าหมายด้านความปลอดภัยไปทั่วทั้งองค์กร
6. **ก่อตั้งและพัฒนาคณะกรรมการดูแลลูกค้า** ผู้ผลิตซอฟต์แวร์หลายรายมีคณะกรรมการดูแลลูกค้าที่ประกอบด้วยลูกค้าจากภูมิภาค ประเภทธุรกิจและขนาดจำนวนลูกค้าที่แตกต่างกันไป คณะกรรมการลูกค้าเหล่านี้สามารถให้ข้อมูลมากมายเกี่ยวกับความสำเร็จและความท้าทายของลูกค้าในการปรับใช้ผลิตภัณฑ์ของบริษัท จัดโครงสร้างวาระการประชุมของคณะกรรมการดูแลลูกค้าด้วยหัวข้อเฉพาะที่เกี่ยวข้องกับความปลอดภัยของลูกค้า แม้ว่าผู้เข้าร่วมประชุมจะไม่ได้คำนึงถึงเรื่องนี้เป็นอันดับแรกก็ตาม พิจารณาว่าคณะกรรมการดูแลลูกค้ารายงานที่ใด และทำอย่างไรจึงจะสามารถข้อมูลเชิงลึกจากผู้เข้าร่วมประชุมเกี่ยวกับความปลอดภัยของผลิตภัณฑ์โดยพิจารณาจากการปรับใช้งานของลูกค้า ตัวอย่างเช่น คณะกรรมการดูแลลูกค้ามีความโน้มเอียงไปทางการตลาดและการขาย หรือการจัดการผลิตภัณฑ์หรือไม่? ผู้บริหารด้านความปลอดภัยโดยการออกแบบควรช่วยควบคุมบทสนทนาของลูกค้าเหล่านี้ และเชื่อมโยงพวกเขากับปัจจัยอื่น ๆ ที่กล่าวถึงในเอกสารนี้ เช่น การศึกษาจากสถานการณ์จริง

กลวิธีตามหลักความปลอดภัยโดยการออกแบบ

กรอบงานพัฒนาซอฟต์แวร์ที่ปลอดภัย (Secure Software Development Framework - SSDF) ยังเป็นที่รู้จักกันในชื่อ สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology's - NIST) SP 800-218 เป็นชุดแนวปฏิบัติในการพัฒนาซอฟต์แวร์ที่มีความปลอดภัยในระดับสูง ซึ่งสามารถบูรณาการเข้ากับทุกขั้นตอนของวงจรชีวิตของการพัฒนาซอฟต์แวร์ (SDLC) การดำเนินการตามแนวปฏิบัติเหล่านี้สามารถช่วยให้ผู้ผลิตซอฟต์แวร์มีประสิทธิภาพมากขึ้นในการค้นหา และขจัดช่องโหว่ในซอฟต์แวร์ที่เผยแพร่ออกมา บรรเทาผลกระทบที่อาจเกิดขึ้นจากการใช้ประโยชน์จากช่องโหว่ต่าง ๆ และระบุสาเหตุเบื้องหลังแท้จริงของช่องโหว่เพื่อป้องกันมิให้เกิดซ้ำในอนาคต

คณะผู้จัดทำเอกสารสนับสนุนให้มีการใช้กลวิธีตามหลักความปลอดภัยโดยการออกแบบ รวมถึงหลักการที่อ้างอิงแนวปฏิบัติตามกรอบงาน SSDF ผู้ผลิตซอฟต์แวร์ควรพัฒนาแผนการทำงานที่เป็นลายลักษณ์อักษร เพื่อนำแนวปฏิบัติในการพัฒนาซอฟต์แวร์ตามหลักความปลอดภัยโดยการออกแบบมาใช้ในพอร์ตผลงานของตนให้มากขึ้น
ต่อไปนี้เป็นรายการของแนวปฏิบัติที่ดีที่สุดในด้านแผนการทำงานที่มีตัวอย่างประกอบเพียงบางตัวอย่าง ได้แก่

- **ภาษาโปรแกรมที่ปลอดภัยต่อหน่วยความจำ** (Memory safe programming languages) (SSDF PW.6.1) จัดลำดับความสำคัญให้กับการใช้ภาษาที่ปลอดภัยของหน่วยความจำ หากเป็นไปได้ คณะผู้จัดทำเอกสารรับทราบว่าการบรรเทาปัญหาเฉพาะหน่วยความจำอื่น ๆ อาจมีประโยชน์สำหรับกลวิธีระยะสั้นสำหรับรหัสพื้นฐานดั้งเดิม (Legacy Codebase) ตัวอย่างรวมถึงการปรับปรุงภาษา C/C++ การบรรเทาปัญหาฮาร์ดแวร์ การสุ่มตำแหน่งพื้นที่ที่อยู่ (Address Space Layout Randomization - ASLR) ความสมบูรณ์ของโฟลว์ควบคุม (Control-Flow Integrity - CFI) และการฟัสซิ่ง (Fuzzing) อย่างไรก็ตาม มีผู้คนจำนวนมากขึ้นยอมรับว่าการใช้ภาษาการเขียนโปรแกรมที่ปลอดภัยสำหรับหน่วยความจำของคอมพิวเตอร์สามารถกำจัดข้อบกพร่องประเภทนี้ได้ และผู้ผลิตซอฟต์แวร์ควรพิจารณาปรับใช้ภาษาเหล่านี้ ตัวอย่างของภาษาที่ปลอดภัยสำหรับหน่วยความจำสมัยใหม่ ได้แก่ภาษา C#, Rust, Ruby, Java, Go และ Swift สำหรับข้อมูลเพิ่มเติม โปรดอ่านแผ่นข้อมูลความปลอดภัยสำหรับหน่วยความจำของ NSA
- **พื้นฐานฮาร์ดแวร์ที่มีความปลอดภัย (Secure Hardware Foundation)** รวมคุณลักษณะสถาปัตยกรรมการใช้งานที่ช่วยให้เกิดการป้องกันหน่วยความจำขนาดละเอียดได้ เช่น คุณลักษณะที่อธิบายโดยคำสั่ง Capability Hardware Enhanced RISC Instructions (CHERI) ซึ่งสามารถขยายสถาปัตยกรรมการใช้งานด้วยชุดคำสั่ง (Instruction-Set Architectures- ISAs) ของฮาร์ดแวร์แบบดั้งเดิมได้ รวมถึงคุณสมบัติอื่น ๆ เช่น Trusted Platform Modules และ Hardware Security Modules สำหรับข้อมูลเพิ่มเติมโปรดไปที่เว็บไซต์ CHERI ของมหาวิทยาลัยแคมบริดจ์
- **ส่วนประกอบซอฟต์แวร์ที่มีความปลอดภัย (Secure Software Components) (SSDF PW 4.1)** ซื้อหาและบำรุงรักษาส่วนประกอบซอฟต์แวร์ที่มีความปลอดภัยดี (เช่น ไลบรารีซอฟต์แวร์ มอดูล มิดเดิลแวร์ เฟรมเวิร์ก) จากผู้พัฒนาซอฟต์แวร์เชิงพาณิชย์ จากแหล่งเปิดหรือโอเพนซอร์ส และผู้พัฒนาซอฟต์แวร์บุคคลที่สามอื่น ๆ ที่ผ่านการตรวจสอบเพื่อให้มั่นใจถึงความปลอดภัยที่แข็งแกร่งในผลิตภัณฑ์ซอฟต์แวร์สำหรับผู้บริโภค
- **เฟรมเวิร์กเทมเพลตเว็บ (SSDF PW.5.1)** ใช้เฟรมเวิร์กเทมเพลตเว็บที่เลี่ยงการป้อนข้อมูลจากผู้ใช้โดยอัตโนมัติเพื่อหลีกเลี่ยงการโจมตีทางเว็บ เช่น การเขียนสคริปต์ข้ามไซต์ (Cross-Site Scripting)
- **เควียรีย์สที่มีการกำหนดพารามิเตอร์ (Parameterized queries) (SSDF PW 5.1)** ใช้เควียรีย์สที่มีการกำหนดพารามิเตอร์แทนที่จะรวมการป้อนข้อมูลของผู้ใช้ในเควียรีย์ส เพื่อหลีกเลี่ยงการโจมตีแบบ SQL Injection
- **การทดสอบความปลอดภัยของแอปพลิเคชันแบบคงที่และแบบไดนามิก (Static and dynamic application security testing) (SAST/DAST)** (SSDF PW.7.2, PW.8.2) ใช้เครื่องมือเหล่านี้ในการวิเคราะห์รหัสซอร์สโค้ดของผลิตภัณฑ์และลักษณะการทำงานของแอปพลิเคชัน เพื่อตรวจหาแนวปฏิบัติที่อาจเกิดข้อผิดพลาดได้ เครื่องมือเหล่านี้ ครอบคลุมปัญหาต่าง ๆ ตั้งแต่การจัดการหน่วยความจำที่ไม่เหมาะสมไปจนถึงการสร้างเควียรีย์สฐานข้อมูลที่อาจเกิดข้อผิดพลาดได้ (เช่น การป้อนข้อมูลของผู้ใช้ที่ไม่ได้รับอนุญาตซึ่งนำไปสู่การโจมตีแบบ SQL injection) เครื่องมือ SAST และ DAST สามารถนำมารวมไว้ในกระบวนการพัฒนาซอฟต์แวร์และตั้งค่าให้ทำงานโดยอัตโนมัติโดยเป็นส่วนหนึ่งของกิจกรรมการพัฒนาซอฟต์แวร์ SAST และ DAST ควรนำไปใช้ประกอบกับการทดสอบประเภทอื่น ๆ เช่น unit test และ integration text เพื่อให้แน่ใจว่าผลิตภัณฑ์เป็นไปตามข้อกำหนดด้านความปลอดภัยที่คาดไว้ เมื่อระบุปัญหาได้แล้ว ผู้ผลิตซอฟต์แวร์ควรทำการวิเคราะห์สาเหตุพื้นฐานเพื่อจัดการกับช่องโหว่ต่าง ๆ อย่างเป็นระบบ

- **การทบทวนรหัส (Code review)** (SSDF PW.7.1, PW.7.2) พยายามตรวจสอบให้แน่ใจว่ารหัสที่ส่งไปยังผลิตภัณฑ์ต้องผ่านเทคนิคการควบคุมคุณภาพ ซึ่งอาจรวมถึงการให้นักพัฒนาทรงคุณวุฒิรายอื่นตรวจสอบ หรือที่เรียกกว่า "จงใจทดสอบหาข้อผิดพลาด (Error Seeding)"

- **รายการวัสดุซอฟต์แวร์ (Software Bill of Materials - SBOM)** (SSDF PS.3.2, PW.4.1) สร้างรายการวัสดุซอฟต์แวร์หรือ SBOM[4] เพื่อช่วยให้มองเห็นและเข้าใจส่วนประกอบซอฟต์แวร์ทั้งหมดที่ใช้ในการผลิตผลิตภัณฑ์

- **โปรแกรมการบ่งชี้ช่องโหว่ (Vulnerability disclosure programs)** (SSDF RV.1.3) ก่อตั้งโปรแกรมการบ่งชี้ช่องโหว่ที่ช่วยให้นักวิจัยด้านความปลอดภัยสามารถรายงานช่องโหว่และได้รับความปลอดภัยทางกฎหมายในการดำเนินการเช่นนั้น ในฐานะที่เป็นส่วนหนึ่งของเรื่องนี้ ซัพพลายเออร์ควรสร้างกระบวนการเพื่อระบุสาเหตุเบื้องหลังแท้จริงของช่องโหว่ที่ค้นพบ กระบวนการดังกล่าวควรรวมถึงการกำหนดว่าการนำแนวปฏิบัติตามหลักความปลอดภัยโดยการออกแบบใด ๆ (หรือแนวปฏิบัติอื่น ๆ ที่คล้ายคลึงกัน) ในเอกสารนี้มาใช้จะช่วยป้องกันไม่ให้นำช่องโหว่เข้ามาในระบบได้หรือไม่

- **ความสมบูรณ์แบบของ CVA (CVE completeness)** ตรวจสอบให้แน่ใจว่า CVE ที่เผยแพร่ออกมานั้น รวมสาเหตุที่เบื้องหลังแท้จริงหรือการระบุจุดอ่อนที่มีร่วมกัน (Common Weakness Enumeration - CWE) เพื่อให้สามารถวิเคราะห์ข้อบกพร่องของการออกแบบความปลอดภัยของซอฟต์แวร์ได้ทั่วทั้งอุตสาหกรรม ในขณะที่การตรวจสอบให้แน่ใจว่า CVE ทุกรายการมีความถูกต้องและสมบูรณ์แบบอาจต้องใช้เวลามากกว่าปกติ แต่การทำเช่นนั้นก็ช่วยให้หน่วยงานที่แตกต่างกันสามารถระบุแนวโน้มในอุตสาหกรรมที่เป็นประโยชน์ต่อผู้ผลิตและลูกค้าทั้งหมด สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการช่องโหว่ โปรดดู คำแนะนำการจัดประเภทของช่องโหว่เฉพาะกลุ่มผู้มีส่วนได้ส่วนเสีย (Stakeholder-Specific Vulnerability Categorization - SSVC) ของ CISA

- **การป้องกันเชิงลึก (Defense-in-Depth)** ออกแบบโครงสร้างพื้นฐานเพื่อให้การเสี่ยงถูกละเมิดเพียงจุดเดียวไม่ส่งผลให้เกิดการประนีประนอมด้านความปลอดภัยไปทั้งระบบ ตัวอย่างเช่น การตรวจสอบให้แน่ใจว่าสิทธิ์ของผู้ใช้ได้รับการจัดสรรเฉพาะที่จำเป็นเท่านั้น และการใช้รายการควบคุมการเข้าถึงที่สามารถลดผลกระทบของบัญชีผู้ใช้ที่อาจถูกบุกรุกได้ นอกจากนี้ เทคนิค Sandbox หรือการทดสอบการทำงานของซอฟต์แวร์ยังสามารถกักกันช่องโหว่ เพื่อจำกัดโอกาสการถูกละเมิดความปลอดภัยของแอปพลิเคชันทั้งหมดอีกด้วย

- **บรรลุเป้าหมายประสิทธิภาพความมั่นคงปลอดภัยทางไซเบอร์ (Satisfy Cybersecurity Performance Goals - CPGs)** ออกแบบผลิตภัณฑ์ที่ตรงตามแนวปฏิบัติพื้นฐานด้านความปลอดภัย เป้าหมายประสิทธิภาพความมั่นคงปลอดภัยทางไซเบอร์ ของ CISA สรุปมาตรการต่อความมั่นคงปลอดภัยทางไซเบอร์ขั้นพื้นฐานที่องค์กรควรนำไปใช้ นอกจากนี้ สำหรับวิธีการเพิ่มความแข็งแกร่งให้กับระบบขององค์กรของคุณ โปรดดูที่ กรอบงานการประเมินทางไซเบอร์ของสหราชอาณาจักร (UK's Cyber Assessment Framework) ซึ่งมีส่วนคล้ายคลึงกับ CPGs ของ CISA หากผู้ผลิตไม่ได้ปฏิบัติตาม CPGs เช่น ไม่บังคับให้พนักงานทุกคนใช้ MFA ที่ป้องกันการฟิชชิ่ง (phishing) สำหรับพนักงานทั้งหมดได้ พวกเขาก็จะไม่ถือว่ากำลังส่งมอบผลิตภัณฑ์ที่มีความปลอดภัยโดยการออกแบบ

คณะผู้จัดทำเอกสารตระหนักดีว่าการเปลี่ยนแปลงเหล่านี้มีผลต่อระบบการทำงานขององค์กรอย่างมีนัยสำคัญ ด้วยเหตุนี้ การนำการเปลี่ยนแปลงเข้ามาในองค์กรควรได้รับการจัดลำดับความสำคัญโดยพิจารณาจากแบบจำลองภัยคุกคามที่ปรับแต่งโดยเฉพาะ ภาวะวิกฤต ความซับซ้อน และผลกระทบต่อธุรกิจ แนวปฏิบัติเหล่านี้สามารถนำมาใช้กับซอฟต์แวร์ตัวใหม่และค่อย ๆ ขยายอย่างต่อเนื่อง เพื่อให้ครอบคลุมกรณีการใช้งานและผลิตภัณฑ์เพิ่มเติม ในบางกรณี วิกฤตและจุดยืนด้านความเสี่ยงของผลิตภัณฑ์บางตัวอาจคุ้มค่ากับการนำแนวปฏิบัติเหล่านี้ออกใช้ตามตารางเวลาที่เร่งรัดให้เร็วขึ้น ส่วนในกรณีอื่น แนวปฏิบัตินี้สามารถนำไปปรับใช้กับรหัสพื้นฐานดั้งเดิม (Legacy Codebase) หรือซอฟต์แวร์รุ่นเก่า และปรับปรุงแก้ไขให้ปลอดภัยตามเวลาที่เหมาะสมต่อไป

[4] คณะผู้จัดทำเอกสารบางท่านกำลังสำรวจหาแนวปฏิบัติทางเลือกอื่น เพื่อให้ได้การรับประกันความปลอดภัยรอบ ๆ ซัพพลายเชนของซอฟต์แวร์

กลวิธีตามหลักความปลอดภัยโดยการตั้งค่าเริ่มต้น

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

- **ขจัดรหัสผ่านเริ่มต้น** ผลิตภัณฑ์ไม่ควรมาพร้อมกับรหัสผ่านเริ่มต้นที่สามารถใช้แชร์ร่วมกันได้ทั่วไป เพื่อกำจัดรหัสผ่านเริ่มต้น คณะผู้จัดทำเอกสารขอแนะนำให้ผลิตภัณฑ์กำหนดให้ผู้ดูแลระบบตั้งรหัสผ่านที่รัดกุมระหว่างการติดตั้งและกำหนดตั้งค่า หรือเพื่อให้ผลิตภัณฑ์จัดส่งด้วยรหัสผ่านที่รัดกุมและไม่ซ้ำกันสำหรับอุปกรณ์แต่ละเครื่อง

- **บังคับให้มีการใช้การยืนยันตัวตนโดยใช้หลากหลายปัจจัย (MFA) สำหรับผู้ใช้ที่มีสิทธิพิเศษ** เราสังเกตว่าการปรับใช้งานขององค์กรจำนวนมากได้รับการจัดการโดยผู้ดูแลระบบที่ไม่ได้ปกป้องบัญชีของตนด้วย MFA เนื่องจากผู้ดูแลระบบเป็นเป้าหมายที่มีมูลค่าสูงสำหรับการโจมตี จึงเป็นการดีกว่าถ้าผลิตภัณฑ์จะเปิด MFA ไว้เป็นค่าเริ่มต้นโดยอัตโนมัติ และผู้ใช้จะต้องเลือกที่จะปิดหากไม่ต้องการใช้ (opt-out) แทนที่จะให้ผู้ใช้เลือกใช้ด้วยตนเอง (opt-in) นอกจากนี้ ระบบควรคอยเตือนผู้ดูแลระบบเป็นประจำให้ลงทะเบียนตั้งค่า MFA จนกว่าพวกเขาจะเปิดใช้งานในบัญชีของตนได้สำเร็จ NCSC ของเนเธอร์แลนด์มีคำแนะนำที่คล้ายคลึงกับของ CISA โปรดดูข้อมูลเพิ่มเติมได้ที่ แผ่นข้อมูลยืนยันตัวตนที่พร้อมใช้งาน (Mature Authentication)

- **การลงชื่อเข้าใช้ครั้งเดียว (Single Sign-On - SSO)** แอปพลิเคชันไอทีควรปรับใช้การสนับสนุนการลงชื่อเข้าใช้ครั้งเดียวผ่านมาตรฐานแบบเปิดสมัยใหม่ ตัวอย่างเช่น Security Assertion Markup Language (SAML) หรือ OpenID Connect (OIDC) ความสามารถนี้ ควรจัดให้ใช้งานได้ตั้งแต่ค่าเริ่มต้นโดยไม่มีค่าใช้จ่ายเพิ่มเติม

- **การบันทึกที่ปลอดภัย (Secure Logging)** จัดให้มีบันทึกการตรวจสอบ (Audit Logs) ที่มีคุณภาพสูงให้แก่ลูกค้าโดยไม่มีค่าใช้จ่ายเพิ่มเติมหรือไม่มีการกำหนดตั้งค่าเพิ่มเติม บันทึกการตรวจสอบมีความสำคัญต่อการตรวจจับและยกระดับเหตุการณ์ด้านความปลอดภัยที่อาจเกิดขึ้น นอกจากนี้ ยังมีความสำคัญอย่างยิ่งในระหว่างการสืบสวนเหตุการณ์ด้านความปลอดภัยที่ต้องสงสัยหรือได้รับการยืนยันแล้ว พิจารณาแนวปฏิบัติที่ดีที่สุด เช่น บูรณาการให้กับระบบข้อมูลความปลอดภัยและการจัดการเหตุการณ์ (Security Information and Event Management) ที่ง่ายดายด้วยการเข้าถึงอินเตอร์เฟซการเขียนโปรแกรมแอปพลิเคชัน (Application Programming Interface - API) ที่ใช้เวลาสากลเชิงพิกัด (Coordinated Universal Time - UTC) การจัดรูปแบบเขตเวลาแบบมาตรฐาน และเทคนิคการจัดทำเอกสารที่มีประสิทธิภาพ

- **โปรไฟล์การยืนยันตัวตนด้วยการใช้ซอฟต์แวร์ (Software Authorization Profile)** ซัพพลายเออร์ซอฟต์แวร์ควรให้คำแนะนำเกี่ยวกับบทบาทโปรไฟล์ที่ได้รับอนุมัติและกรณีการใช้งานที่ถูกกำหนดมา ผู้ผลิตควรให้การเตือนที่มองเห็นได้ชัด ซึ่งแจ้งให้ลูกค้าทราบถึงความเสี่ยงที่เพิ่มขึ้น ในกรณีที่พวกเขาเบี่ยงเบนไปจากการอนุมัติโปรไฟล์ที่แนะนำมาให้ ตัวอย่างเช่น แพทย์สามารถเข้าดูบันทึกผู้ป่วยได้ทั้งหมด แต่ผู้จัดตารางเวลาทางการแพทย์มีข้อจำกัดในการเข้าถึงข้อมูลเพียงบางรายการเท่าที่จำเป็นต่อการจัดตารางนัดหมายเท่านั้น

- **ความปลอดภัยที่มุ่งไปข้างหน้าเหนือความเข้ากันได้กับผลิตภัณฑ์รุ่นเก่า** บ่อยครั้งคุณลักษณะดั้งเดิมที่สามารถสร้างความเสี่ยงด้านความปลอดภัยจะยังถูกเก็บไว้ในผลิตภัณฑ์ และบางครั้งก็เปิดใช้งานด้วย แม้ว่าอาจไม่จำเป็นแล้วก็ตาม จัดลำดับความสำคัญของความปลอดภัยให้อยู่เหนือความเข้ากันได้กับรุ่นเก่า โดยให้ทีมความปลอดภัยสามารถลบคุณลักษณะที่ไม่ปลอดภัยออกไปได้ แม้ว่าจะเป็นการเปลี่ยนแปลงครั้งใหญ่ก็ตาม

- **ติดตามและลดขนาดของ “แนวทางการเสริมความแข็งแกร่ง”** ลดขนาดของ “แนวทางการเสริมความแข็งแกร่ง” ที่รวมอยู่กับผลิตภัณฑ์และพยายามทำให้แน่ใจว่าขนาดจะลดลงตามเวลาเมื่อมีการเปิดตัวซอฟต์แวร์เวอร์ชันใหม่ บูรณาการส่วนประกอบของ “แนวทางการเสริมความแข็งแกร่ง” ให้เป็นส่วนหนึ่งของการกำหนดตั้งค่าเริ่มต้นของผลิตภัณฑ์ คณะผู้จัดทำเอกสาร ตระหนักดีว่าการทำให้แนวทางการเสริมความแข็งแกร่งนี้สั้นลงเป็นผลมาจากความร่วมมืออย่างต่อเนื่องกับลูกค้าเดิมที่มีอยู่ และรวมถึงความพยายามของทีมผลิตภัณฑ์ และประสบการณ์ผู้ใช้ (User Experience - UX) เข้าด้วยกันเป็นจำนวนมาก

- **พิจารณาประสบการณ์ผู้ใช้ที่เป็นผลเนื่องมาจากการตั้งค่าความปลอดภัย** ในการตั้งค่าใหม่แต่ละครั้งจะไปเพิ่มภาระด้านการรับรู้ของผู้ใช้ขั้นปลายและควรได้รับการประเมินร่วมกับประโยชน์ทางธุรกิจที่จะได้รับด้วยตามหลักการแล้ว ไม่ควรมีการตั้งค่า แต่ควรรวมการตั้งค่าที่ปลอดภัยที่สุดไว้ในผลิตภัณฑ์ตามการตั้งค่าเริ่มต้นแทนเมื่อจำเป็นต้องกำหนดตั้งค่า ทางเลือกการตั้งค่าเริ่มต้นควรมีความปลอดภัยในวงกว้างจากภัยคุกคามทั่วไป

คณะผู้จัดทำเอกสารยอมรับว่าการเปลี่ยนแปลงเหล่านี้อาจมีผลต่อการดำเนินการใช้งานของซอฟต์แวร์ ดังนั้น ข้อมูลจากลูกค้าจึงมีความสำคัญอย่างยิ่งในการสร้างความสมดุลในระหว่างการพิจารณาด้านการปฏิบัติงานและความปลอดภัย เราเชื่อว่าการพัฒนาแผนการทำงานที่เป็นลายลักษณ์อักษรและการสนับสนุนจากผู้บริหารที่จัดลำดับความสำคัญของแนวคิดเหล่านี้ลงในผลิตภัณฑ์ที่สำคัญที่สุดขององค์กรเป็นขั้นตอนแรกของการปรับเปลี่ยนไปสู่แนวปฏิบัติการพัฒนาซอฟต์แวร์ที่มีความปลอดภัย แม้ว่าความคิดเห็นของลูกค้าจะมีความสำคัญ แต่เราได้สังเกตเห็นกรณีสำคัญที่ลูกค้าไม่เต็มใจหรือไม่สามารถนำมาตรฐานที่ได้รับการปรับปรุงแล้วมาใช้ ซึ่งมักจะเป็นโปรโตคอลเครือข่าย เป็นสิ่งสำคัญสำหรับผู้ผลิตที่จะสร้างแรงจูงใจที่มีความหมาย เพื่อให้ลูกค้าได้ติดตามข่าวสารปัจจุบันเสมอ และไม่ปล่อยให้พวกเขาอยู่ในภาวะเปราะบางอย่างไม่มีที่สิ้นสุด

เปรียบเทียบแนวทางการเสริมความแข็งแกร่งกับแนวทางลดความเข้มงวด

แนวทางการเสริมความแข็งแกร่งอาจเป็นผลมาจากการขาดการควบคุมความปลอดภัยของผลิตภัณฑ์ที่ฝังอยู่ในสถาปัตยกรรมการใช้งานของผลิตภัณฑ์ตั้งแต่เริ่มต้นการพัฒนา ด้วยเหตุนี้ แนวทางการเสริมความแข็งแกร่งจึงสามารถนำไปใช้เป็นแผนการทำงานโดยศัตรูในการระบุและใช้ประโยชน์จากคุณสมบัติที่ไม่ปลอดภัยได้อีกด้วย เป็นเรื่องปกติสำหรับองค์กรจำนวนมากที่จะไม่ทราบเกี่ยวกับแนวทางการเสริมความแข็งแกร่งนี้ ดังนั้นพวกเขาจึงปล่อยการกำหนดตั้งค่าอุปกรณ์ไว้ในระบบที่ไม่ปลอดภัย แบบจำลองที่ย้อนแย้งกัน ซึ่งเรียกกันว่าแนวทางที่ลดความเข้มงวด ควรจะนำมาแทนที่แนวทางการเสริมความแข็งแกร่งดังกล่าว และให้คำอธิบายแก่ผู้ใช้ว่าควรทำการเปลี่ยนแปลงอะไรบ้าง ขณะเดียวกันก็แสดงรายการความเสี่ยงด้านความปลอดภัยที่เป็นผลตามมาด้วย ผู้ที่ทำงานด้านความปลอดภัยควรเป็นผู้เขียนคำแนะนำที่เป็นแนวทางในคู่มือเหล่านี้ เนื่องจากสามารถอธิบายข้อดีข้อเสียเป็นภาษาง่าย ๆ ได้ ซึ่งจะช่วยเพิ่มโอกาสที่ผู้อื่นจะนำไปใช้ได้อย่างถูกต้อง

แทนที่จะพัฒนาแนวทางการเสริมความแข็งแกร่ง ซึ่งแสดงรายการรักษาความปลอดภัยของผลิตภัณฑ์ คณะผู้จัดทำเอกสารขอแนะนำให้ผู้ผลิตซอฟต์แวร์เปลี่ยนไปใช้แนวปฏิบัติตามหลักความปลอดภัยโดยการตั้งค่าเริ่มต้นโดยให้ “แนวทางที่ลดความเข้มงวด” กับผู้ใช้ไปด้วย แนวทางเหล่านี้อธิบายถึงการตัดสินใจด้านความเสี่ยงทางธุรกิจในภาษาที่เข้าใจง่าย และสามารถเพิ่มความตระหนักระดับองค์กรเกี่ยวกับความเสี่ยงต่อการบุกรุกทางไซเบอร์จากผู้ไม่ประสงค์ดี การประนีประนอมด้านความปลอดภัยควรกำหนดโดยผู้บริหารระดับสูงของลูกค้า โดยพิจารณาความสมดุลระหว่างความปลอดภัยกับความต้องการทางธุรกิจด้านอื่น

คำแนะนำสำหรับลูกค้า

คณะผู้จัดทำเอกสารขอแนะนำให้องค์กรถือว่าผู้ผลิตซอฟต์แวร์ที่ให้บริการนั้นเป็นผู้รับผิดชอบต่อผลลัพธ์ด้านความปลอดภัยของผลิตภัณฑ์ของตน ในฐานะที่เป็นส่วนหนึ่งของประเด็นนี้ คณะผู้จัดทำเอกสารจึงขอแนะนำให้ผู้บริหารองค์กรจัดลำดับความสำคัญของการซื้อผลิตภัณฑ์ที่มีความปลอดภัยโดยการออกแบบ (Secure-by-Design) และมีความปลอดภัยโดยการตั้งค่าเริ่มต้น (Secure-by-Default) ซึ่งสามารถแสดงออกผ่านนโยบายที่กำหนดให้ฝ่ายไอทีต้องประเมินความปลอดภัยของซอฟต์แวร์ก่อนที่จะซื้อ รวมทั้งให้อำนาจฝ่ายไอทีในการปฏิเสธได้หากจำเป็น ฝ่ายไอทีควรมีอำนาจในการพัฒนาเกณฑ์การจัดซื้อที่เน้นความสำคัญของแนวปฏิบัติตามหลักความปลอดภัยโดยการออกแบบและความปลอดภัยโดยการตั้งค่าเริ่มต้น (ทั้งที่ระบุไว้ในเอกสารฉบับนี้และฉบับอื่น ๆ ที่พัฒนาโดยองค์กร) นอกจากนี้ ฝ่ายไอทีควรได้รับการสนับสนุนจากฝ่ายบริหารเมื่อมีการบังคับใช้เกณฑ์เหล่านี้ในการตัดสินใจจัดซื้อ การตัดสินใจขององค์กรในการยอมรับความเสี่ยงที่เกี่ยวข้องกับผลิตภัณฑ์เทคโนโลยีเฉพาะควรได้รับการบันทึกอย่างเป็นทางการ ได้รับการอนุมัติโดยผู้บริหารระดับสูงของธุรกิจ และนำเสนอต่อคณะกรรมการบริษัทอย่างสม่ำเสมอ

บริการด้านไอทีขององค์กรขนาดใหญ่ที่สนับสนุนจุดยืนด้านการรักษาความปลอดภัยขององค์กร เช่น เครือข่ายขององค์กร การจัดการข้อมูลอัตลักษณ์ขององค์กรและการเข้าถึง และการดำเนินการด้านความปลอดภัยและความสามารถในการตอบสนองควรได้รับการพิจารณาว่าเป็นหน้าที่ทางธุรกิจที่สำคัญ ซึ่งได้รับทุนสนับสนุนเพื่อให้สอดคล้องกับความสำคัญต่อความสำเร็จของพันธกิจองค์กร องค์กรควรพัฒนาแผนในการอัปเกรดความสามารถเหล่านี้เพื่อใช้ประโยชน์จากผู้ผลิตที่ใช้หลักการตามความปลอดภัยโดยการออกแบบ และความปลอดภัยโดยการตั้งค่าเริ่มต้น

หากเป็นไปได้ องค์กรต่าง ๆ ควรพยายามสร้างความสัมพันธ์ที่เข้มแข็งกับซัพพลายเออร์ด้านไอทีที่สำคัญของตน ความสัมพันธ์ดังกล่าวรวมถึงความไว้วางใจในระดับต่าง ๆ ขององค์กรและใช้เป็นเครื่องมือให้สามารถแก้ไขปัญหาและระบุลำดับความสำคัญที่มีร่วมกันได้ ความปลอดภัยควรเป็นปัจจัยที่สำคัญของความสัมพันธ์ และองค์กรดังกล่าวควรพยายามอย่างเต็มที่ที่จะส่งเสริมความสำคัญของแนวปฏิบัติตามหลักความปลอดภัยโดยการออกแบบและความปลอดภัยโดยการตั้งค่าเริ่มต้น ทั้งในรูปแบบที่เป็นทางการ (เช่น การทำสัญญาหรือข้อตกลงกับผู้ขาย) และในมิติความสัมพันธ์แบบไม่เป็นทางการ องค์กรควรคาดหวังความโปร่งใสจากซัพพลายเออร์ด้านเทคโนโลยีเกี่ยวกับระบบควบคุมภายในของพวกเขา รวมทั้งแผนการทำงานเพื่อนำมาปรับใช้ในแนวปฏิบัติตามหลักความปลอดภัยโดยการออกแบบและความปลอดภัยโดยการตั้งค่าเริ่มต้น

นอกจากการกำหนดให้ความสำคัญตามหลักความปลอดภัยโดยการตั้งค่าเริ่มต้นภายในองค์กรแล้ว ผู้นำด้านไอทีควรร่วมมือกับเพื่อนร่วมอาชีพในอุตสาหกรรมของตนเพื่อทำความเข้าใจว่าผลิตภัณฑ์และบริการใดที่รวมอยู่ในหลักการออกแบบเหล่านี้ได้ดีที่สุด ผู้นำเหล่านี้ ควรประสานงานด้านคำร้องขอของพวกเขาเพื่อช่วยให้ผู้ผลิตจัดลำดับความสำคัญของความคิดริเริ่มด้านความปลอดภัยที่กำลังจะเกิดขึ้นโดยการทำงานร่วมกัน ลูกค้าจะสามารถให้ข้อมูลที่มีความหมายต่อผู้ผลิตและสร้างแรงจูงใจให้พวกเขาเพื่อจัดลำดับความสำคัญด้านความปลอดภัยขึ้นมา

เมื่อใช้ประโยชน์จากระบบคลาวด์ (Cloud) องค์กรควรตรวจสอบเพื่อให้เกิดความมั่นใจว่าตนเองเข้าใจรูปแบบความรับผิดชอบร่วมกันกับซัพพลายเออร์ด้านเทคโนโลยีของตน นั่นคือ องค์กรควรมีความชัดเจนเกี่ยวกับความรับผิดชอบด้านความปลอดภัยของซัพพลายเออร์ไม่ใช่เพียงแค่ความรับผิดชอบของลูกค้าเท่านั้น

องค์กรควรจัดลำดับความสำคัญของผู้ให้บริการระบบคลาวด์ (Cloud) ที่ต้องมีความโปร่งใสเกี่ยวกับจุดยืนด้านการรักษาความปลอดภัย การควบคุมภายใน และความสามารถในการปฏิบัติตามภาระหน้าที่ของตนภายใต้แบบจำลองความรับผิดชอบที่มีร่วมกัน

ข้อจำกัดความรับผิดชอบ

ข้อมูลในเอกสารนี้ได้รับการจัดหา “ตามสภาพที่เป็น” เพื่อวัตถุประสงค์ในการให้ข้อมูลเท่านั้น CISA และคณะผู้จัดทำเอกสารไม่ขอรับรองผลิตภัณฑ์หรือบริการเชิงพาณิชย์ รวมถึงหัวข้อการวิเคราะห์ใด ๆ การอ้างอิงถึงองค์กรหรือผลิตภัณฑ์เชิงพาณิชย์ กระบวนการ หรือบริการโดยเครื่องหมายบริการ เครื่องหมายการค้า ผู้ผลิต หรืออื่น ๆ ไม่ถือว่าเป็นการรับรอง การแนะนำหรือการทำให้เกิดความลำเอียงโดย CISA และคณะผู้จัดทำเอกสาร เอกสารนี้เป็นความคิดริเริ่มร่วมกันโดย CISA ซึ่งไม่ได้ทำหน้าที่เป็นเอกสารกำกับดูแลที่ต้องปฏิบัติตามโดยอัตโนมัติ

การพัฒนาร่วมกัน

CISA

- คำแนะนำ SBOM โดย CISA
- เป้าหมายประสิทธิภาพการทำงานด้านความมั่นคงปลอดภัยทางไซเบอร์ระหว่างภาคธุรกิจ (Cross-Sector Cybersecurity Performance Goals) ของ CISA
- แนวทางเกี่ยวกับการทำงานร่วมกันของเทคโนโลยี (Guidelines on Technology Interoperability)
- การป้องกันการโจมตีต่อซอฟต์แวร์ซัพพลายเชน (Defending Against Software Supply Chain Attacks) ของ CISA และ NIST
- ต้นทุนของเทคโนโลยีที่ไม่ปลอดภัยและสิ่งที่เราสามารถทำได้ | โดย CISA (The Cost of Unsafe Technology and What We Can Do About It | CISA)
- หยุดการกล่าวโทษกันในด้านความมั่นคงปลอดภัยทางไซเบอร์ (Stop Passing the Buck on Cybersecurity) เหตุใดบริษัทจึงต้องสร้างความปลอดภัยในผลิตภัณฑ์เทคโนโลยี (Why Companies Must Build Safety Into Tech Products (foreignaffairs.com))
- คำแนะนำเกี่ยวกับการจัดประเภทของช่องโหว่เฉพาะกลุ่มผู้มีส่วนได้ส่วนเสีย (SSVC) (Stakeholder-Specific Vulnerability Categorization (SSVC) Guidance) ของ CISA
- แผ่นข้อมูล MFA ที่ป้องกันการฟิชชิ่ง (Phishing Resistant MFA Fact Sheets) ของ CISA
- คำแนะนำด้านไซเบอร์สำหรับธุรกิจขนาดเล็ก | โดย CISA (Cyber Guidance for Small Businesses | CISA)

NSA

- เอกสารข้อมูลความมั่นคงปลอดภัยทางไซเบอร์เรื่องความปลอดภัยของหน่วยความจำ (Cybersecurity Information Sheet on Memory Safety) ของ NSA
- ความมั่นคงปลอดภัยด้าน ESF สำหรับซัพพลายเชนของซอฟต์แวร์ (ESF Securing the Software Supply Chain) ของ NSA แนวปฏิบัติที่ดีที่สุดสำหรับซัพพลายเออร์ (Best Practices for Suppliers)

FBI

- การทำความเข้าใจและตอบสนองต่อการโจมตีซัพพลายเชน SolarWinds (Understanding and Responding to the SolarWinds Supply Chain Attack) มุมมองจากรัฐบาลกลาง (The Federal Perspective)
- การคุกคามทางไซเบอร์ - การตอบสนองและการรายงาน (The Cyber Threat - Response and Reporting)
- กลยุทธ์ไซเบอร์ (Cyber Strategy) ของ FBI

สถาบันมาตรฐานและเทคโนโลยีแห่งชาติ (National Institute of Standards and Technology - NIST)

- แนวทางเกี่ยวกับข้อมูลยืนยันตัวตนด้วยระบบดิจิทัล (Digital Identity Guidelines) ของ NIST
- กรอบงานความปลอดภัยทางไซเบอร์ (Cyber Security Framework) ของ NIST
- กรอบงานพัฒนาซอฟต์แวร์ที่ปลอดภัย (Secure Software Development Framework - SSDF) ของ NIST

ศูนย์รักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งออสเตรเลีย (Australian Cyber Security Centre - ACSC)

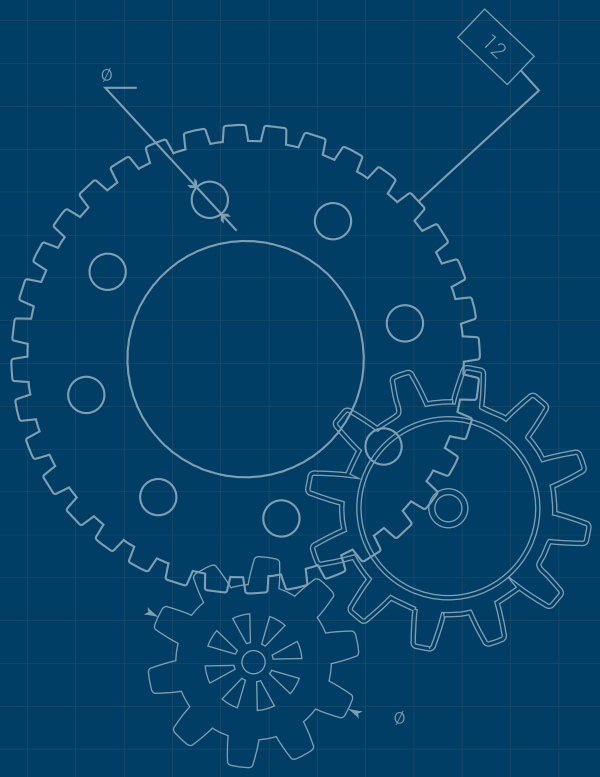
- คำแนะนำเกี่ยวกับหลักปฏิบัติ IoT สำหรับผู้ผลิต (IoT Code of Practice Guidance for Manufacturers) ของ ACSC

ศูนย์รักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติสหราชอาณาจักร (The United Kingdom's National Cyber Security Centre – NCSC-UK)

- กรอบงานการประเมินทางไซเบอร์ (Cyber Assessment Framework) ของสหราชอาณาจักร
- คำแนะนำการพัฒนาและการปรับใช้งานที่ปลอดภัย (Secure Development and Deployment guidance) ของ NCSC-UK
- คำแนะนำในการจัดการช่องโหว่ (Vulnerability Management guidance) ของ NCSC-UK
- ชุดเครื่องมือการเปิดเผยช่องโหว่ (Vulnerability Disclosure Toolkit) ของ NCSC-UK
- หลักการ CHERI โดยมหาวิทยาลัยแคมบริดจ์ (University of Cambridge)
- ลาก่อนและขอบคุณสำหรับทุกสิ่ง (So long and thanks for all the bits) - NCSC.GOV.UK

ศูนย์รักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งแคนาดา (Canadian Centre for Cyber Security - CCCS)

- คำแนะนำเกี่ยวกับการป้องกันการโจมตีต่อซัพพลายเชนของซอฟต์แวร์ (Guidance on Protecting Against Software Supply Chain Attacks) ของ CCCS
- ซัพพลายเชนทางไซเบอร์: แนวทางการประเมินความเสี่ยง (Cyber supply chain: An approach to assessing risks)
- คำแนะนำเกี่ยวกับแรนซัมแวร์ CONTI (CONTI ransomware guidance) ของศูนย์รักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งแคนาดา



สำนักงานความมั่นคงปลอดภัยของข้อมูลแห่งสหพันธรัฐเยอรมนี (Germany's Federal Office for Information Security - BSI)

- บทสรุป BSI Grundschutz compendium (module CON.8)
- มาตรฐานระหว่างประเทศ IEC 62443 ตอนที่ 4-1 (The international standard IEC 62443, part 4-1)
- รายงานสถานการณ์ความมั่นคงปลอดภัยด้านไอทีของประเทศเยอรมนี ปี 2022 (State of IT-security in Germany report)
- แนวปฏิบัติ BSI ในการรักษาความปลอดภัยแอปพลิเคชันบนเว็บ (BSI practices of web application security)

ศูนย์รักษาความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติเนเธอร์แลนด์ (Netherlands' National Cyber Security Centre - NCSC-NL)

- แผ่นข้อมูลการยืนยันตัวตนที่พร้อมใช้งาน (Mature Authentication Factsheet) ของ NCSC-NL

ศูนย์เตรียมความพร้อมเหตุการณ์และยุทธศาสตร์เพื่อความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติของญี่ปุ่น (Japan's National Center of Incident Readiness and Strategy for Cybersecurity - NISC)

- กลยุทธ์เพื่อความมั่นคงปลอดภัยทางไซเบอร์แห่งชาติญี่ปุ่น (Japan's National Cybersecurity Strategy)

กระทรวงเศรษฐกิจ การค้า และอุตสาหกรรม (Ministry of Economy, Trade and Industry - METI) ของญี่ปุ่น

- คู่มือคำแนะนำรายการวัสดุซอฟต์แวร์ (SBOM) สำหรับการจัดการซอฟต์แวร์ (Guide of Introduction of Software Bill of Materials (SBOM) for Software Management)
- การรวบรวมตัวอย่างกรณีการใช้งานเกี่ยวกับวิธีการจัดการสำหรับการใช้ OSS และการรับรองความปลอดภัย (Collection of Use Case Examples Regarding Management Methods for Utilizing OSS and Ensuring Its Security)

คณะกรรมาธิการความมั่นคงปลอดภัยทางไซเบอร์แห่งสิงคโปร์ (Cyber Security Agency of Singapore)

- ที่ปรึกษาทางเทคนิคเกี่ยวกับการพัฒนา API ที่ปลอดภัย (Technical Advisory on Secure API Development)
- นโยบายการเปิดเผยช่องโหว่ที่รับรองโดย SingCERT ของ CSA (CSA SingCERT Vulnerability Disclosure Policy)
- รายการตรวจสอบการตอบสนองต่อเหตุการณ์ที่รับรองโดย SingCERT ของ CSA (CSA SingCERT Incident Response Checklist)
- คู่มือการตอบสนองต่อเหตุการณ์รับรองโดย SingCERT ของ CSA (CSA SingCERT Incident Response Playbooks)
- กรอบงานความปลอดภัยโดยการออกแบบของ CSA (CSA Security by Design Framework)
- รายการตรวจสอบกรอบงานความปลอดภัยโดยการออกแบบของ CSA (CSA Security by Design Framework Checklist)
- แนวทางการสร้างแบบจำลองภัยคุกคามทางไซเบอร์ของ CSA (CSA Guide to Cyber Threat Modelling)
- โครงการติดฉลากความมั่นคงปลอดภัยทางไซเบอร์ของ CSA (CSA Cybersecurity Labelling Scheme)

อื่น ๆ

- ระบบที่ซับซ้อนล้มเหลวอย่างไร (How Complex Systems Fail)
- รูปลักษณ์ใหม่ในความล้มเหลวของระบบที่ซับซ้อน (The New Look in complex system failure)

เอกสารอ้างอิง

[1] https://csrc.nist.rip/publications/history/ande72.pdf

[2] https://www.cisa.gov/sbom และเอกสารอ้างอิงเพื่อการเผยแพร่รายการวัสดุซอฟต์แวร์ (SBOMs) ใน TR 03183-2 https://www.bsi.bund.de/dok/TR-03183

[3] หนังสือชื่อว่า Juran on Quality by Design แต่งโดย J.M. Juran, 1992.