สร้างมาตรฐานความปลอดภัยสูงสุดสำหรับระบบโซล่าร์

ภัยคุกคามที่เพิ่มขึ้นต่อภาคพลังงานโลก

ในโลกที่เชื่อมโยงกันในปัจจุบัน ภาคพลังงานเป็นเป้าหมายหลักสำหรับภัยคุกคามทางไซเบอร์ที่เกิดจากแหล่งที่มาหลายแหล่ง ภัยคุกคามดังกล่าวครอบคลุมตั้งแต่แผนการที่ขับเคลื่อนด้วยการเงินที่ดำเนินการโดยอาชญากรไซเบอร์ ไปจนถึงการโจมตีที่เป็นแรงจูงใจทางการเมืองที่จัดฉากโดยรัฐชาติ เพียงในปี ค.ศ. 2023 ผู้ตกเป็นเหยื่อการแฮ็กทางไซเบอร์ทั่วโลก (จากทุกภาคส่วน) ได้จ่ายเงินจำนวนมหาศาล 1.1 พันล้านดอลลาร์สหรัฐฯ ตามหลังการโจมตีด้วยแรนซัมแวร์ - และนั่นเป็นเพียงสิ่งที่ถูกแจ้งรายงาน*

40,000

จำนวนระบบโซล่าร์เซลล์ที่ติดตั้งในบ้านและธุรกิจของเนเธอร์แลนด์ถูกรัฐบาลเนเธอร์แลนด์มองว่ามีความเสี่ยงต่อการควบคุมระยะไกล (กรกฎาคม 2022)

130,000

จำนวนระบบโซล่าร์เซลล์ของผู้ผลิตอินเวอร์เตอร์หลายรายที่ถูกรายงานว่ามีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์
(สหรัฐอเมริกา, กรกฎาคม 2023)

$200M

เป็นค่าเสียหายโดยประมาณที่ Target Corporation ได้รับหลังจากที่เครือข่ายผู้ให้บริการ HVAC ของบริษัทถูกแฮ็กในสหรัฐอเมริกาในปี ค.ศ. 2013

ระบบโซล่าร์เซลล์ที่ไม่ได้รับการรักษาความปลอดภัยก่อให้เกิดความเสี่ยงทางธุรกิจที่สำคัญ

พลังงานแสงอาทิตย์เป็นส่วนประกอบที่เติบโตอย่างรวดเร็วของการผสมผสานพลังงานระดับโลก โดยประกอบเป็นส่วนสำคัญของการผลิตพลังงานทั้งหมดสำหรับประเทศจำนวนมาก เช่น เนเธอร์แลนด์, เยอรมนี, และสหรัฐอเมริกา เป็นแหล่งพลังงานที่สำคัญที่ช่วยลดต้นทุนค่าไฟฟ้าและรับรองความต่อเนื่องทางธุรกิจสำหรับหลายบริษัท ขณะที่นำเสนอโซลูชั่นพลังงานที่ยั่งยืน ระบบโซล่าร์เซลล์ยังเปิดช่องทางใหม่สำหรับภัยคุกคามทางไซเบอร์ด้วย ที่หัวใจของแต่ละระบบคืออินเวอร์เตอร์ ซึ่งเป็นอุปกรณ์อินเทอร์เน็ตของสิ่งต่างๆ (IoT) ที่มักเชื่อมต่อกับอินเทอร์เน็ตเพื่อเปิดใช้งานการตรวจสอบและควบคุมระบบ สิ่งนี้ทำให้มีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์มากกว่าสถานีพลังงานก๊าซธรรมชาติหรือถ่านหินที่ได้รับการป้องกันอย่างดีมาก

โซล่าร์ถูกใช้เพื่อจ่ายพลังงานให้กับภาระพลังงานในสถานที่เพิ่มมากขึ้น เช่น แบตเตอรี่, เครื่องชาร์จรถยนต์ไฟฟ้า, และระบบ HVAC และจะเป็นเช่นนี้มากขึ้นเรื่อยๆ เมื่อเราเปลี่ยนผ่านไปสู่ยุคของระบบการจัดการพลังงาน ระบบโซล่าร์เซลล์ที่ไม่ได้รับการรักษาความปลอดภัยไม่เพียงแต่คุกคามความต่อเนื่องทางธุรกิจเท่านั้น แต่ยังสามารถทำหน้าที่เป็นประตูที่ไม่รู้ตัวสำหรับแฮ็กเกอร์ในการเข้าถึงภาระพลังงานและแพลตฟอร์มดิจิทัลที่กว้างขึ้นขององค์กร ทำให้เกิดความเสียหายเพิ่มเติมด้านวัตถุ, การเงิน, และชื่อเสียง

* www.chainalysis.com/blog/ransomware-2024

ความเสี่ยงทางไซเบอร์ทั่วไป:

การรั่วไหลของข้อมูลและค่าปรับ

แฮ็กเกอร์สามารถใช้ประโยชน์จากระบบโซล่าร์เซลล์ที่เปราะบางเพื่อขโมยข้อมูลส่วนบุคคลที่อาศัยอยู่ในเครือข่ายภายในขององค์กร ส่งผลให้เกิดการรั่วไหลของข้อมูลที่บังคับให้เหยื่อจ่ายค่าปรับที่สูง

การควบคุมระยะไกลและการปฏิเสธการให้บริการ (Denial-of-Service หรือ DoS)

เมื่อธุรกิจตกเป็นเหยื่อของการโจมตี DoS หรือการละเมิดการควบคุมระยะไกล จะเผชิญกับการหยุดชะงักที่สำคัญ แรนซัมแวร์สามารถจับข้อมูลสำคัญเป็นตัวประกันได้ ขณะที่การควบคุมระยะไกลและการโจมตีและการละเมิด DoS อาจทำให้บริการที่สำคัญหยุดชะงักอย่างสมบูรณ์

ความเสี่ยงด้านการปฏิบัติตามกฎระเบียบ

เมื่อมีการนำกฎระเบียบทางไซเบอร์ใหม่มาใช้ เจ้าของไซต์ PV ต้องดำเนินมาตรการเชิงรุกเพื่อให้มั่นใจว่าระบบของพวกเขาจะยังคงสอดคล้องและหลีกเลี่ยงความเสี่ยงของการเรียกคืนผลิตภัณฑ์หรือค่าปรับทางการเงินหากเครือข่ายของพวกเขาถูกบุกรุก

กฎหมายและระเบียบข้อบังคับทางไซเบอร์ใหม่สำหรับระบบโซล่าร์เซลล์กำลังอยู่ในระหว่างดำเนินการ

ระบบโซล่าร์เซลล์ได้กลายเป็นโครงสร้างพื้นฐานด้านพลังงานที่สำคัญและด้วยเหตุนี้ จึงดึงดูดความสนใจอย่างจริงจังจากหน่วยงานกำกับดูแล สิ่งนี้สามารถเห็นได้แล้วใน “กระแส” ของกฎหมายและระเบียบข้อบังคับใหม่ที่กำลังจะเกิดขึ้น

UL 2941
มาตรฐานสากลเฉพาะสำหรับความปลอดภัยทางไซเบอร์ของอินเวอร์เตอร์อัจฉริยะและทรัพยากรพลังงานกระจาย (คาดว่าปี ค.ศ. 2025)

“U.S. Cyber Trust Mark” หรือเครื่องหมายความน่าเชื่อถือทางไซเบอร์ของสหรัฐอเมริกา
โปรแกรมการรับรองและการติดฉลากความปลอดภัยทางไซเบอร์ (คาดว่าปี ค.ศ. 2025)

National Association of Regulatory Utility Commissions (NARUC/NASEO)
เส้นฐานความปลอดภัยทางไซเบอร์สำหรับระบบการกระจายไฟฟ้าและ DER (กำลังดำเนินการอยู่)

IEEE P1547.10
กลุ่มงานแพลตฟอร์มเกตเวย์ Distributed Energy Resources (DER) (กำลังดำเนินการอยู่)

UK PSTI (2023)
ความปลอดภัยของผลิตภัณฑ์และโครงสร้างพื้นฐานการสื่อสารโทรคมนาคม

RED 2014/53/EU
ระเบียบอุปกรณ์วิทยุของยุโรป

Cyber Resilience Act
กฎหมายความยืดหยุ่นทางไซเบอร์ของสหภาพยุโรป สำหรับความปลอดภัยทางไซเบอร์ของ IoT และอุปกรณ์ที่เชื่อมต่อ (คาดว่าปี ค.ศ. 2026-2027)

NIS 2 Directive
ระเบียบสหภาพยุโรปเพื่อบรรลุระดับสูงของความปลอดภัยทางไซเบอร์ทั่วสหภาพยุโรป (มีผลบังคับใช้เดือนตุลาคม ค.ศ. 2024)

SolarEdge - ผู้นำระดับโลกด้านความปลอดภัยทางไซเบอร์สำหรับโซล่าร์เซลล์

ในฐานะผู้นำอุตสาหกรรมโซล่าร์เซลล์ที่มีอุปกรณ์ IoT หลายล้านเครื่องทั่วโลก SolarEdge อยู่ในตำแหน่งที่เหมาะสมในการรับรู้ถึงความเสี่ยงด้านความปลอดภัยทางไซเบอร์ที่เจ้าของสินทรัพย์โซล่าร์เซลล์เผชิญ รวมถึงภัยคุกคามต่อโครงข่ายพลังงาน

เรามีประวัติที่ยาวนานด้านความปลอดภัยของโซล่าร์เซลล์ ช่วยสร้างมาตรฐานความปลอดภัยที่สำคัญสำหรับโซล่าร์เซลล์ในสหรัฐอเมริกาและทั่วโลก และเรามุ่งหวังที่จะทำเช่นเดียวกันสำหรับความปลอดภัยทางไซเบอร์ของโซล่าร์เซลล์

เราให้ความสำคัญกับความปลอดภัยของคุณเป็นอันดับหนึ่ง

มีการลงทุนอย่างมากในการสรรหาทีมผู้เชี่ยวชาญเฉพาะด้านเพื่อนำความพยายามทางไซเบอร์ที่กำลังดำเนินการของเรา

เราช่วยกำหนดมาตรฐานความปลอดภัยทางไซเบอร์ระหว่างประเทศ

SolarEdge มีส่วนร่วมอย่างแข็งขันในคณะกรรมการทางเทคนิคต่างๆ และทำงานเพื่อให้แน่ใจว่าการออกแบบผลิตภัณฑ์ของเรามีการจัดตำแหน่งที่สอดคล้องกับระเบียบข้อบังคับที่กำลังจะเกิดขึ้น อุปกรณ์ของเราเป็นไปตามมาตรฐานของแนวทางอ้างอิงล่าสุดและมาตรฐานความปลอดภัยทางไซเบอร์ DER

ผลิตภัณฑ์ SolarEdge ได้รับการพัฒนาโดยให้ความสำคัญกับความปลอดภัยทางไซเบอร์เป็นหลัก

เราพยายามรักษาความปลอดภัยของลูกค้าอย่างต่อเนื่องจากภัยคุกคามทางไซเบอร์ที่พัฒนาอยู่ตลอดเวลา โดยการดำเนินการในทุกขั้นตอนของการออกแบบผลิตภัณฑ์ของเรา ทั่วทั้งซอฟต์แวร์และฮาร์ดแวร์ของ SolarEdge

ยกระดับความปลอดภัยทางไซเบอร์ของคุณด้วย SolarEdge

การเป็นพันธมิตรกับ SolarEdge หมายถึงคุณจะได้รับการปกป้องเพิ่มเติมตลอดอายุการใช้งานของระบบทั้งหมด วิธีการแบบแบ่งชั้นของเราในการรักษาความปลอดภัยทางไซเบอร์มีจุดมุ่งหมายเพื่อปกป้องความสมบูรณ์ของข้อมูล, การสื่อสาร, และการดำเนินงานทางธุรกิจ ตั้งแต่การเปิดใช้งานไซต์จนถึงการผลิต

เพื่อรักษาความปลอดภัยของการเชื่อมต่อระบบ ฟังก์ชั่นการทำงาน และข้อมูลลูกค้า SolarEdge ปฏิบัติตามหลักการ Cyber Informed Engineering (CIE) โดยฝังกลไกความปลอดภัยของข้อมูลลงในผลิตภัณฑ์ของเราตั้งแต่ขั้นตอนการออกแบบเริ่มต้น เราปรับตัวและปรับปรุงโซลูชั่นของเราอย่างต่อเนื่องเพื่อให้สอดคล้องกับความต้องการที่พัฒนาและมาตรฐานด้านกฎระเบียบ

เราให้ความสำคัญกับความต้องการของทีมรักษาความปลอดภัยของลูกค้าของเรา โดยการออกแบบผลิตภัณฑ์ของเราไม่เพียงแต่ให้ปลอดภัยเท่านั้น แต่ยังเพื่อให้มั่นใจถึงความมองเห็นและการควบคุมสูงสุดสำหรับผู้ใช้ของเรา

เครือข่ายย่อยด้านพลังงานถูกสร้างขึ้นเพื่อรวมเข้ากับเครือข่าย IT และ OT ขององค์กรของคุณอย่างปลอดภัย

ข้อมูลผู้ใช้และข้อมูลการใช้พลังงานถูกถ่ายโอนและจัดเก็บอย่างปลอดภัย มั่นใจถึงความเป็นส่วนตัวของข้อมูลสูงสุดและการป้องกันจากภัยคุกคามทางไซเบอร์

อินเวอร์เตอร์ของ SolarEdge เป็นหัวใจของระบบโซล่าร์เซลล์และร่วมกับอุปกรณ์ SolarEdge อื่นๆ ได้รับการออกแบบเพื่อป้องกันและตรวจจับการโจมตีทางไซเบอร์ทั่วทั้งระบบโซล่าร์เซลล์

เช่นเดียวกับความปลอดภัยของโซล่าร์เซลล์ เราไม่อาจมองข้ามความปลอดภัยทางไซเบอร์ของระบบโซล่าร์เซลล์ได้

ลดความเสี่ยงทางไซเบอร์ของคุณโดยเลือกเป็นพันธมิตรกับ SolarEdge มั่นใจว่าธุรกิจของคุณจะยังคงปลอดภัยและยืดหยุ่นต่อภัยคุกคามที่พัฒนาอยู่ตลอดเวลา

เกี่ยวกับ SolarEdge

SolarEdge Technologies เป็นผู้นำระดับโลกด้านเทคโนโลยีพลังงานหมุนเวียน นำวิศวกรรมชั้นนำและนวัตกรรมมาประยุกต์ใช้เพื่อมอบโซลูชั่นพลังงานแสงอาทิตย์แบบ PV สำหรับภาคที่อยู่อาศัย, เชิงพาณิชย์, และสาธารณูปโภค SolarEdge นำเสนอแนวทางที่เหมาะสมที่สุดในการผลิต กักเก็บ จัดการ และใช้พลังงาน บริษัทพัฒนาและผลิตอินเวอร์เตอร์พลังงานแสงอาทิตย์ (PV) และ Power Optimizer โซลูชั่นการจัดการและเพิ่มประสิทธิภาพพลังงาน ระบบกักเก็บพลังงาน และบริการด้านระบบจำหน่ายไฟฟ้า เทคโนโลยี DC-optimized ของ SolarEdge ถูกติดตั้งในบ้านเรือนหลายล้านหลังคาเรือนในกว่า 140 ประเทศ และบริษัทในกลุ่ม Fortune 100 มากกว่า 50% มีเทคโนโลยี SolarEdge อยู่บนหลังคา SolarEdge กำลังเร่งการเปลี่ยนผ่านไปสู่เครือข่ายพลังงานแบบกระจายที่ยั่งยืน ซึ่งจะช่วยเพิ่มประสิทธิภาพการใช้พลังงานทุกที่

 Rv: 2024/10/V1/THA