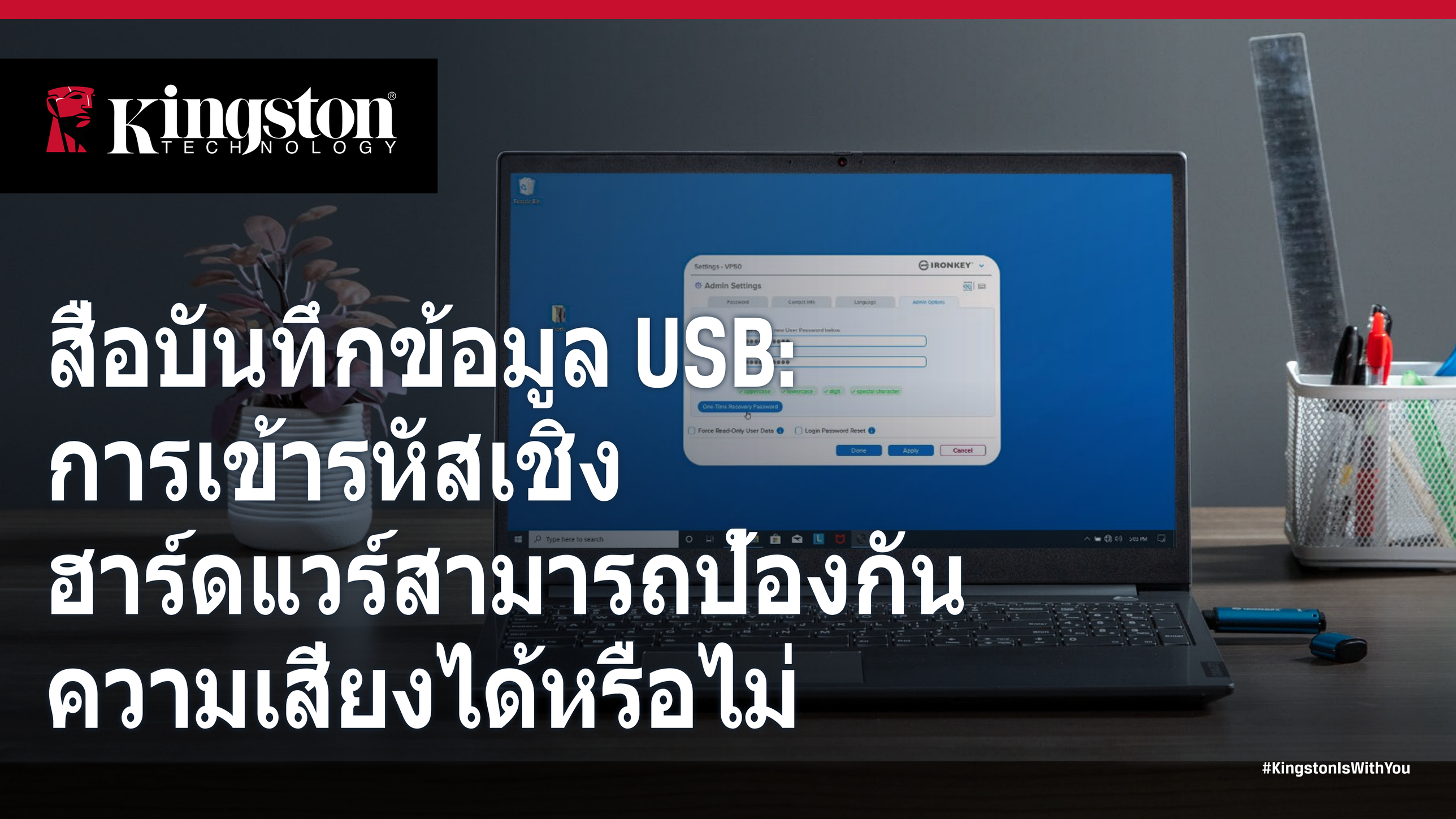
Kingston TECHNOLOGY

สือบันทึกข้อมูล USB: การเข้ารหัสเชิง ฮาร์ดแวร์สามารถป้องกัน ความเสียงได้หรือไม่



#KingstonIsWithYou

สือบันทึกข้อมูล USB: การเข้ารหัสเชิงฮาร์ดแวร์สามารถป้องกันความเสียงได้หรือไม่

บทนำและเนื้อหา

การรักษาความปลอดภัยทางไซเบอร์ถือเป็นเรืองทีกลุ่มธุรกิจต้องกังวลมากกว่าทีเคย แต่หน่วยงานหลาย ๆ แห่งกลับไม่ทราบหรือไม่ได้เตรียมพร้อมต่อภัยคุกคามด้านไซเบอร์ ในสหรัฐฯ มีธุรกิจเพียง 50% เท่านันทีจัดเตรียมแผนรักษาความปลอดภัยทางไซเบอร์ไว้ โดย 32% ในจำนวนนีไม่มีการปรับปรุงแผนการรักษาความปลอดภัยทางไซเบอร์นับตังแต่เริมสถานการณ์แพร่ระบาด COVID-19 ข้อมูลของ UpCity รายงานว่าองค์กรต่างๆ เริมเปลียนไปทำงานระยะไกลหรือแบบผสมผสานมากขึน ความถีของภัยคุกคามทางไซเบอร์เพิมจำนวนมากขึนเรือย ๆ ทัวโลก จำนวนธุรกิจต่าง ๆ ทีได้รับผลกระทบจากแรนซัมแวร์เพิมขึนจาก 37% ในปี 2020 เป็น 66% ในปี 2021[1]

ปัญหาด้านการรักษาความปลอดภัยทางไซเบอร์อาจส่งผลอย่างรุนแรงต่อธุรกิจ นอกเหนือจากค่าใช้จ่ายทางการเงินทีเกิดขึนแล้ว การสูญเสียข้อมูล ปัญหาด้านความปลอดภัยและชือเสียงยังสามารถส่งผลกระทบเชิงลบต่อองค์กรในหลาย ๆ ด้านทังในระยะสันและระยะยาว

ช่องทางสำคัญช่องทางหนึงของภัยคุกคามทางไซเบอร์คือไดรฟ์ USB อุปกรณ์เหล่านีใช้กันอย่างแพร่หลายในหน่วยงานหลาย ๆ แห่งเนืองจากความสะดวก เพียงแค่เสียบต่อก็สามารถใช้งานได้ทันที อย่างไรก็ตาม ความสะดวกนีทำให้ไดรฟ์ USB มีความเสียงจากการถูกโจมตี แค่ไดรฟ์จัดวางผิดทีหรือถูกขโมยเพียงตัวเดียวก็อาจส่งผลกระทบอย่างร้ายแรงกับข้อมูลทีมีความอ่อนไหว ด้วยเหตุนีการเข้ารหัสจึงมีบทบาทสำคัญอย่างยิงทีจะทำให้ไดรฟ์ USB มีความปลอดภัยในการใช้งานและจะช่วยลดความเสียงทีเกียวข้องสำหรับบุคคลและหน่วยงาน ในอีบุ๊กฉบับนีเราจะนำเสนอคำตอบสำหรับคำถามทีสำคัญ ๆ ดังต่อไปนี

- ทำไมไดรฟ์ USB เข้ารหัสจึงมีความสำคัญในการป้องกันภัยคุกคามทางไซเบอร์
- หน่วยงานต่าง ๆ มีจุดเปราะบางอยู่ทีใดบ้าง
- พวกเขาสามารถทำอะไรเพือป้องกันตัวเองได้บ้าง

สือบันทึกข้อมูล USB: การเข้ารหัสเชิงฮาร์ดแวร์สามารถป้องกันความเสียงได้หรือไม่

ผู้สนับสนุน

อีบุ๊กชุดนีจัดทำขึนร่วมกับผู้เชียวชาญในกลุ่มอุตสาหกรรม IT และเทคโนโลยีเกิดใหม่ รวมทังผู้เชียวชาญด้านเทคโนโลยีของเรา

David Clarke

David ได้รับการยอมรับในฐานะอินฟลูเอนเซอร์ 10 อันดับต้น ๆ โดย Thompson Reuter's ในกลุ่ม "Top 30 most influential thought-leaders and thinkers on social media, in risk management, compliance and reg-tech in the UK" และติด 50 อันดับของ Global Experts by Kingston Technology

Pasi Siukonen

Pasi รับหน้าทีดูแลทีมผู้เชียวชาญของส่วนงานต่าง ๆ ใน Kingston เช่น ฝ่ายประชาสัมพันธ์ การตลาด การขายภาคสนาม บริการด้านเทคนิคและฝ่ายบริการลูกค้าสำหรับผลิตภัณฑ์จาก Kingston ผลิตภัณฑ์หลัก ๆ ทีเขาดูแลคือกลุ่มแฟลชและ SSD

ความแตกต่างระหว่างไดรฟ์ทั่วไปและไดรฟ์เข้ารหัส

ในขณะที่ไดรฟ์สำหรับใช้งานทั่วไป (ไม่มีการเข้ารหัส) จะสะดวกในการเข้าถึงและใช้งานเป็นพิเศษ แต่ระบบเข้ารหัสเชิงฮาร์ดแวร์จะช่วยเพิ่มระดับการป้องกันทั้งในทางกายภาพและผ่านระบบดิจิตอลทำให้สื่อบันทึกข้อมูล USB มีความปลอดภัยมากยิ่งขึ้น ความสะดวกในการใช้งานและการเคลื่อนย้ายที่ไม่ยุ่งยากของไดรฟ์ทั่วไปแบบไม่เข้ารหัสทำให้สะดวกสำหรับทั้งผู้ใช้และผู้ไม่หวังดีที่ต้องการขโมยข้อมูลที่อ่อนไหว หรือส่งต่อมาลแวร์หรือแรนซัมแวร์เข้าไปในเครือข่ายของบริษัท และอีกมากมาย เนื่องจาก USB เป็นอุปกรณ์ที่มีความแพร่หลาย โอกาสในการคุกคามทางไซเบอร์จึงมีสูงมาก มีปัจจัยเสี่ยงที่สำคัญอยู่สองประการเกี่ยวกับไดรฟ์ที่ใช้งานทั่วไป ได้แก่

- **แรนซัมแวร์:** การโจมตีผ่าน USB เหล่านี้อาศัยการส่งมาลแวร์ไปยังเครือข่ายของบริษัทเพื่อเรียกค่าไถ่ข้อมูลของบริษัทและ/หรือระบบการทำงานต่าง ๆ โดยการเข้ารหัสข้อมูลเหล่านี้ สาเหตุส่วนใหญ่มักเกิดขึ้นจาก BadUSB ซึ่งเป็นมาลแวร์ที่มีความแพร่หลายมากที่สุด
- **ข้อมูลที่ถูกขโมย:** เพียงแค่ไดรฟ์สูญหาย ถูกขโมย หรือทิ้งไว้โดยไม่มีคนดูแลและรักษาความปลอดภัยอย่างเหมาะสมก็อาจทำให้ผู้ไม่ประสงค์ดีสามารถเข้าถึงข้อมูลที่จัดเก็บไว้ในไดร์ฟได้ง่าย ๆ ไม่ว่าจะเป็นข้อมูลลูกค้า รหัสข้อมูลต้นทางหรือข้อมูลด้านการเงินหรือผลการดำเนินงานที่อ่อนไหว

BadUSB – เป็นการใช้จุดอ่อนของไดรฟ์ USB ที่ใช้เฟิร์มแวร์ที่ไม่มีการป้องกันที่สามารถส่งโปรแกรมซอฟต์แวร์อันตรายเข้าไปแทรกแซงได้ เครื่องมือที่อันตรายเหล่านี้พบได้ทั่วไปและอาชญากรไซเบอร์สามารถนำมาใช้ได้อย่างไม่ยุ่งยาก แต่ความเข้าใจเกี่ยวกับเครื่องมือเหล่านี้กลับยังอยู่ในระดับต่ำ ทำให้การโจมตีเกิดขึ้นได้โดยง่ายเพียงแค่แทนที่เฟิร์มแวร์ของไดรฟ์ก็สามารถใช้ไดรฟ์ USB เป็นแป้นพิมพ์และตัวเรียกใช้สคริปต์ต่าง ๆ เพื่อคุกคามระบบไฟร์วอลล์ เนื่องจากภัยคุกคามทางไซเบอร์หลาย ๆ กรณีเกิดขึ้นจากคนในที่ขาดความรอบคอบหรือโดยไม่ได้เจตนา ธุรกิจต่าง ๆ จึงจะต้องเลือกใช้ไดรฟ์เข้ารหัสที่มีเฟิร์มแวร์ลงนามดิจิตอลที่มีการป้องกันเป็นอย่างดีเพื่อป้องกันภัยคุกคามและลดโอกาสที่จะเกิดผลกระทบจากผู้ไม่ประสงค์ดีเหล่านี้

> **“ค่าใช้จ่ายในการฟื้นฟูโครงสร้างพื้นฐานการทำงานหรือแม้แต่การจ่ายค่าไถ่ระบบอาจสูงมากกว่าการเลือกใช้ USB แบบมีระบบจัดการอย่างไม่น่าเชื่อ”**
> **- David Clarke**

ทำไมถึงต้องใช้ไดรฟ์ USB เข้ารหัส

ไดรฟ์เข้ารหัสถูกออกแบบมาโดยเฉพาะเพื่อปกป้องข้อมูลภายใน และอุปกรณ์ที่เชื่อมต่อกับไดรฟ์ ทำให้เป็นเครื่องมือที่มีค่าอย่างยิ่งสำหรับหน่วยงานที่ต้องทำงานผ่านระบบ IT ภัยคุกคามทางไซเบอร์ที่ล้ำสมัยมากขึ้นเรื่อย ๆ ทำให้คุณสมบัติการทำงานของไดรฟ์เข้ารหัสต้องพัฒนาตามไปด้วย เพื่อให้ก้าวล้ำหน้าผู้ไม่ประสงค์ดีที่ต้องการใช้ประโยชน์จากอุปกรณ์เหล่านี้ ยกตัวอย่างจาก Kingston IronKey™ ผลิตภัณฑ์ในกลุ่มเข้ารหัสเชิงฮาร์ดแวร์มาพร้อมกับคุณสมบัติการทำงานต่าง ๆ เช่น การเข้ารหัส AES 256 บิตในโหมด XTS ที่มีความปลอดภัยสูงสุด เคสมีความทนทานสูง พร้อมเฟิร์มแวร์ลงนามดิจิตอล แป้นพิมพ์เสมือนจริง โหมดการทำงาน complex หรือ passphrase และคุณสมบัติอื่น ๆ ที่มีมาอย่างต่อเนื่องตลอดเวลาที่ผ่านมาเพื่อให้ผู้ใช้ได้รับการปกป้องจากภัยคุกคามต่าง ๆ อย่างเต็มที่

เนื่องจากภัยคุกคามทางไซเบอร์มักจะถูกเข้าใจอย่างผิด ๆ ผู้ประกอบการหลายรายจึงมักเลือกใช้ไดรฟ์ทั่วไปแม้ว่าจะมีความเสี่ยงมากมาย การจัดหาที่ไม่ยุ่งยาก ราคาที่ถูกและการใช้ระบบเข้ารหัสเชิงซอฟต์แวร์กลายเป็นข้อพิจารณาที่สำคัญ นอกจากนี้องค์กรหลาย ๆ แห่งยังไม่มีกระบวนการรับรองแฟลชไดรฟ์สำหรับใช้งาน หลาย ๆ หน่วยงานไม่มีแม้แต่นโยบายหรือกระบวนการที่เหมาะสมในการควบคุมมาตรฐานด้าน IT หรือการรักษาความปลอดภัยทางไซเบอร์ เช่น ISO27001, GDPR, SOC2 และ WISP ที่กำหนดโดยภาครัฐ ซึ่งหมายถึงมีการพิจารณาปัจจัยเสี่ยงต่าง ๆ ตามความเห็นแทนที่จะพิจารณาจากข้อเท็จจริง ทำให้หน่วยงานต่าง ๆ อยู่ในภาวะเสี่ยงจากการคุกคาม

ในขณะที่หลาย ๆ คนเลือกที่จะใช้ไดร์ฟใช้งานทั่วไปที่ใช้การเข้ารหัสเชิงซอฟต์แวร์ที่มีอยู่แล้ว แต่สิ่งนี้อาจเป็นความเข้าใจผิด ๆ เนื่องจากไดรฟ์เข้ารหัสเชิงซอฟต์แวร์หลายตัวสามารถแฮ็คได้ง่าย ๆ ผ่านเครื่องมือทั้งแบบฟรีหรือแบบจ่ายเงินที่หาได้ทั่วไปทางอินเทอร์เน็ต ระบบเข้ารหัสเชิงซอฟต์แวร์ยังสามารถลบได้จากไดรฟ์ผ่านการฟอร์แมตโดยผู้ใช้ได้อย่างไม่ยุ่งยาก หรือโดยการใช้ไดรฟ์กับ OS ที่ไม่รองรับ ในขณะที่ USB เข้ารหัสเชิงฮาร์ดแวร์จะไม่สามารถปลดการเข้ารหัสได้ ซึ่งเหมาะกับการใช้งานในรูปแบบนี้ และยังทนทานต่อการทุบทำลาย และยังมีเฟิร์มแวร์ลงนามดิจิตอลเพื่อให้แน่ใจว่าไดรฟ์จะมีความสมบูรณ์และเชื่อถือได้เต็มที่ การจำกัดจำนวนครั้งในการเดารหัสผ่าน (ระบบป้องกัน Brute Force) บวกกับแป้นพิมพ์เสมือนจริง (ป้องกันการบันทึกปุ่มกดหรือบันทึกหน้าจอ) เป็นคุณสมบัติการทำงานเพิ่มเติมที่พบได้ในไดรฟ์เข้ารหัส เช่น IronKey VP50 ซึ่งหมายความว่าเป็นไปตามแนวปฏิบัติที่ดีที่สุดของกลุ่มอุตสาหกรรมสำหรับป้องกันผู้ใช้ที่ไม่หวังดีในการล้วงรหัสผ่าน

> **หากไดรฟ์ IronKey ตรวจพบว่ามีการดัดแปลงเฟิร์มแวร์ ไดรฟ์จะถูกป้องกันไม่ให้ทำการบู๊ตเพื่อป้องกันความปลอดภัย - Pasi Siukonen**

ใครบ้างทีเสียง

บริษัททีไม่สามารถควบคุมการใช้งาน USB ได้ล้วนตกอยู่ในความเสียง และมักจะไม่ทราบว่าความเสียงเหล่านีมีอะไรบ้าง อย่างไรก็ตาม ยังมีปัจจัยอืน ๆ ทีอาจทำให้บริษัทบางรายเป็นเหยือทีหอมหวานมากกว่าสำหรับอาชญากรไซเบอร์

สำหรับบริษัทด้านสุขภาพและการเงิน ข้อมูลของพวกเขาไม่เพียงแต่น่าดึงดูดสำหรับอาชญากรไซเบอร์เท่านัน แต่ยังอาจส่งผลกระทบทังต่อหน่วยงานและลูกค้าได้อย่างรุนแรงจนไม่น่าเชือ ในสหราชอาณาจักร การโจมตีทางไซเบอร์ในปี 2017 ต่อ NHS ทำให้ต้องมีการยกเลิกนัดหมายกว่า 19,000 รายการ และทำให้ NHS เสียค่าใช้จ่ายมากถึง 92 ล้านปอนด์จากผลผลิตทีสูญเสีย รวมทังค่าใช้จ่ายในการกู้ข้อมูลและระบบการทำงาน สิงนีไม่เพียงแต่ทำให้ผู้ป่วยไม่สามารถรับบริการด้านสุขภาพ แต่ NHS ยังถูกวิพากษ์วิจารณ์อย่างหนักทีไม่สามารถตอบสนองสถานการณ์ได้อย่างฉับไวหรือเพียงพอแม้ว่าจะมีสัญญาณเตือนภัยคุกคามมาก่อนแล้วก็ตาม ในขณะทีหน่วยงานต่าง ๆ ควรอัพเดตระบบและหาข้อมูลให้รอบด้านเกียวกับการรักษาความปลอดภัยทางไซเบอร์ ผู้ทีต้องดูแลข้อมูลทีอ่อนไหว โดยเฉพาะข้อมูลชนิดพิเศษก็จะต้องระมัดระวังความเสียงทางไซเบอร์เช่นกัน

ยิงบริษัทมีมูลค่า (พิจารณาจากรายได้) มากเท่าไร ผลตอบแทนสำหรับผู้ไม่ประสงค์ดีก็จะยิงมากเท่านัน ด้วยเหตุนีความเสียงทีจะถูกคุกคามทางไซเบอร์ก็มากขึนตามไปด้วย แต่สิงนีไม่ได้หมายความว่าหน่วยงานขนาดเล็กไม่ควรกังวลเรืองความปลอดภัยทางไซเบอร์ องค์กรขนาดใหญ่ต่าง ๆ อาจเป็นเป้าหมายทีหอมหวานสำหรับการโจมตี แต่ก็มักมีการจัดสรรทรัพยากรและบุคลากรโดยเฉพาะเพือจัดการกับภัยคุกคามทางไซเบอร์เช่นกัน ในทางกลับกัน SMB หลาย ๆ แห่งอาจไม่ได้มีทีมงานรักษาความปลอดภัยทางไซเบอร์ และมีการงดเว้นสำหรับผู้บริหารระดับสูงในการใช้ USB ได้ตามใจชอบ ทำให้มีความเสียงผลต่อร้ายแรงทีอาจเกิดขึนตามมา ผลการศึกษาบางแห่งพบว่าธุรกิจขนาดเล็กและขนาดกลางกลับเป็นเป้าหมายสำคัญของการโจมตีทางไซเบอร์

ความเสียงจะยิงสูงขึนสำหรับผู้บริหารระดับสูง เนืองจากบุคคลเหล่านีมักสามารถระบุตัวได้ง่าย ๆ และมักได้รับสิทธิพิเศษในองค์กร ทำให้การควบคุมทางไซเบอร์ เช่น การจัดการอุปกรณ์ USB ไม่ได้ถูกบังคับใช้ คนเหล่านีจึงกลายเป็นเหยืออันโอชะของอาชญากรไซเบอร์ ไดรฟ์เข้ารหัสเชิงฮาร์ดแวร์จึงเกิดขึนร่วมกับมาตรการทีชัดเจนด้านการรักษาความปลอดภัยทางไซเบอร์และแนวทางหรือกระบวนการทีเหมาะสมต่าง ๆ ทีจะช่วยลดความเสียงและสามารถป้องกันภัยคุกคาม

> กรณีการเจาะระบบทีพบส่วนใหญ่เมือเร็ว ๆ นีเกิดขึนจากการอาศัยคนวงใน ไม่ว่าจะรู้ตัวหรือไม่รู้ตัวก็ตาม - David Clarke

ใครบ้างทีเสียง

> **หน่วยงานหลาย ๆ แห่งยังไม่พยายามเพียงพอในการตอบโต้กับภัยคุกคามทางไซเบอร์ - David Clarke**

ห่วงโซ่อุปทานคืออีกจุดเปราะบางสำหรับหน่วยงานต่าง ๆ การโจมตีผ่านห่วงโซ่อุปทานเป็นสิ่งที่เกิดขึ้นบ่อยครั้งมาก ในปี 2013 Target บริษัทค้าปลีกสัญชาติสหรัฐฯ ประสบปัญหาการถูกล้วงข้อมูลครั้งใหญ่ที่สุดในประวัติศาสตร์ของวงการค้าปลีก ทำให้ข้อมูลบัตรเดบิตและเครดิตของลูกค้ากว่า 40 ล้านรายรั่วไหล แม้ว่า Target จะให้ความสำคัญด้านการรักษาความปลอดภัยทางไซเบอร์อย่างมาก แต่การติดตั้งระบบรักษาความปลอดภัยที่ครอบคลุมเพียง 6 เดือนก่อนหน้าถูกคุกคามก็ไม่สามารถป้องกันสถานการณ์ข้อมูลรั่วไหลที่เกิดขึ้นเนื่องจากซัพพลายเออร์ของ Target เอง ทำให้ผู้ไม่ประสงค์ดีสามารถเจาะเครือข่ายข้อมูลหลักของ Target ผ่านซัพพลายเออร์เหล่านี้ มีการฟ้องร้องถึง 90 คดีกับ Target ทำให้บริษัทเสียเงินถึง 61 ล้านเหรียญสหรัฐฯ จากเหตุละเมิดที่เกิดขึ้นแม้ว่าบริษัทจะไม่ได้เป็นสาเหตุโดยตรงของการคุกคามดังกล่าว จุดอ่อนในห่วงโซ่อุปทานด้านการรักษาความปลอดภัยทางไซเบอร์นี้มากเพียงพอที่จะทำให้เกิดความเสียหายทั้งในด้านการเงินและชื่อเสียง

การลัดขั้นตอนต่าง ๆ ของพนักงานเองก็อาจเป็นปัญหาทำให้เกิดช่องโหว่ขึ้น แม้ว่าการลัดขั้นตอนเหล่านี้จะทำให้พนักงานทำงานของตนเองได้สะดวกขึ้น แต่ก็เป็นการละเว้นกระบวนการด้านความปลอดภัยขั้นพื้นฐานหลาย ๆ อย่าง เช่น การจัดการรหัสผ่าน แม้ว่าแนวทางจาก NCSC และ CISA จะไม่ได้ซับซ้อนอะไร แต่ก็ยังอาจเป็นปัญหาในการนำไปใช้จริง โดยเฉพาะสำหรับทีมงานที่ไม่คุ้นเคยกับระบบ IT และมาตรการรักษาความปลอดภัยทางไซเบอร์ แม้ว่าการมีทีมงานรักษาความปลอดภัยทางไซเบอร์จะเป็นประโยชน์ การจัดหาเครื่องมือที่เหมาะสม เช่น ไดรฟ์เข้ารหัสเชิงฮาร์ดแวร์ก็สามารถช่วยลดความเสี่ยงจากการลัดขั้นตอนในการทำงานของพนักงานลงได้เช่นกัน

> **ไดรฟ์ USB เข้ารหัสเชิงฮาร์ดแวร์สามารถใช้งานและปรับใช้กับนโยบายรักษาความปลอดภัยทางไซเบอร์ในปัจจุบันได้โดยง่าย เนื่องจากรองรับอินเทอร์เฟซที่หลากหลาย (ทั้งระบบกราฟิก ปุ่มกด ทัชสกรีน) ไปจนถึงความสามารถในการทำงานกับระบบปฏิบัติการต่าง ๆ ไดรฟ์ยังมีจำหน่ายหลากหลายความจุตามความต้องการขององค์กรแต่ละแห่ง - Pasi Siukonen**

หน่วยงานต่าง ๆ จะลดความเสี่ยงทางไซเบอร์ได้อย่างไร

ในมุมมองของหน่วยงาน มีหลายสิ่งที่สามารถทำได้เพื่อรักษาความปลอดภัยของอุปกรณ์ปลายทางและปกป้องข้อมูล หากไม่มีแผนงาน GRC (การกำกับดูแล บริหารความเสี่ยงและควบคุมมาตรฐาน) การรักษาความปลอดภัยทางไซเบอร์ก็จะเกิดปัญหา ดังนั้นคุณจะต้องทำความคุ้นเคยและปฏิบัติตามกระบวนการต่อไปนี้ซึ่งถือเป็นเรื่องสำคัญอย่างยิ่งสำหรับธุรกิจต่าง ๆ ในการปกป้องตัวเอง การมีซอฟต์แวร์รักษาความปลอดภัยของอุปกรณ์ปลายทางที่มีประสิทธิภาพยังสามารถช่วยจัดการกับภัยคุกคามทางไซเบอร์ได้หลาย ๆ อย่าง และยังทำให้สามารถแก้ไขช่องโหว่ด้านความปลอดภัยได้ตามสถานการณ์

> **การตัดสินใจใช้นโยบายการเข้ารหัสแบบบังคับใช้ถือเป็นข้อพิจารณาที่สำคัญไม่แพ้กันหรือมากยิ่งกว่าด้านการจัดการความเสี่ยงเมื่อเทียบกับประเด็นการเลือกว่าจะจัดทำชุดข้อมูลสำรองหรือไม่ - Pasi Siukonen**

ในระดับบุคคล ฮาร์ดแวร์เข้ารหัสจะสามารถลดช่องโหว่จากภัยคุกคามทางไซเบอร์ลงได้อย่างมาก เมื่อพิจารณาจากความแพร่หลายและมาตรการทำงานทางไกลสลับกับที่ทำงานที่ยังคงเป็นไปอย่างต่อเนื่องและจำนวนภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้นในปีที่ผ่านมา การกำกับดูแลให้พนักงานทุกระดับมีการจัดการ โอนและอ่านข้อมูลของบริษัทอย่างปลอดภัยจึงเป็นประเด็นที่สำคัญมากขึ้น USB เข้ารหัสเชิงฮาร์ดแวร์ทำให้ผู้ใช้ยังคงสามารถโอนข้อมูลผ่านแฟลชไดรฟ์ที่ใช้งานได้อย่างสะดวก และยังช่วยลดปัจจัยเสี่ยงต่าง ๆ ที่จะเกิดขึ้นจากแฟลชไดรฟ์ ในขณะที่ไดรฟ์ใช้งานทั่วไปที่ขาดการกำกับดูแลหรือถูกขโมยอาจทำให้ข้อมูลสูญหาย กระทบต่อชื่อเสียงและเกิดปัญหาอีกมากมาย ไดรฟ์เข้ารหัสเชิงฮาร์ดแวร์จึงถูกออกแบบมาเพื่อปกป้องข้อมูลที่อ่อนไหวจากการคุกคามต่าง ๆ อาชญากรไซเบอร์มีการพัฒนาแนวทางใหม่ ๆ ในการคุกคาม ไดรฟ์เข้ารหัสจึงมีการพัฒนาอย่างต่อเนื่องเพื่อจัดการกับความท้าทายต่าง ๆ เหล่านี้

นอกจากนี้ค่าใช้จ่ายที่เกิดขึ้นจากภัยคุกคามทางไซเบอร์ยังอาจสูงอย่างไม่คาดคิด ในขณะที่การเลือกใช้ไดรฟ์เข้ารหัสในระดับองค์กรอาจต้องมีการกำหนดกระบวนการรับรองและเตรียมอุปกรณ์เข้ามาเกี่ยวข้อง แต่วิธีการนี้ก็จะสามารถช่วยบริษัทประหยัดค่าใช้จ่ายลดลงได้อย่างมาก ทั้งจากการขู่กรรโชก หรือรายได้ที่อาจสูญเสียเนื่องจากชื่อเสียงที่เสียหายในระยะยาว เฉพาะค่าใช้จ่ายในการดำเนินคดีเพียงอย่างเดียวก็อาจมากพอสำหรับการจัดซื้อไดรฟ์ USB เข้ารหัสเชิงฮาร์ดแวร์

> **ปณิธานในระยะยาวในการจัดหาไดรฟ์ USB เข้ารหัสที่เชื่อถือได้จาก Kingston ทำให้หน่วยงานต่าง ๆ สามารถตอบสนองเงื่อนไขด้านการรักษาความปลอดภัยทางไซเบอร์ของตน ร่วมกับระบบเข้ารหัสเชิงฮาร์ดแวร์มาตรฐานอุตสาหกรรม นโยบายควบคุมสำหรับอุปกรณ์ปลายทางและแผนการจัดการอุปกรณ์ - Pasi Siukonen**

สรุป

ที Kingston เราไม่เคยหยุดทีจะพัฒนาระบบรักษาความปลอดภัยทางไซเบอร์เพือให้แน่ใจว่าไดรฟ์ USB IronKey เข้ารหัสของเราจะมีความทันสมัยตามข้อกำหนดล่าสุดและและตรงตามความต้องการด้านการรักษาความปลอดภัยทางไซเบอร์ของหน่วยงานไม่ว่าจะขนาดใหญ่หรือเล็ก ในขณะทีการรักษาความปลอดภัยทางไซเบอร์กลายเป็นสิงทีทัวโลกให้ความกังวลมากขึนเรือย ๆ เรามีความมันใจว่าด้วยเครืองมือและองค์ความรู้ทีเหมาะสมหน่วยงานต่าง ๆ ก็จะสามารถจัดการกับความท้าทายต่าง ๆ พร้อม ๆ กับการปกป้องตัวเองพนักงานและลูกค้าของตนเองได้อย่างเต็มที

เกียวกับ Kingston

ประสบการณ์กว่า 35 ปีทำให้ Kingston มีองค์ความรู้ในการพิจารณาและแก้ไขปัญหาในการเคลือนย้ายข้อมูลของคุณ ทำให้เกิดความสะดวกกับแรงงานของคุณในการทำงานได้อย่างปลอดภัยโดยไม่กระทบต่อหน่วยงานของคุณ

#KingstonIsWithYou

1. https://www.techtarget.com/searchsecurity/news/252516423/Sophos-66-of-organizations-hit-by-ransomware-in-2021