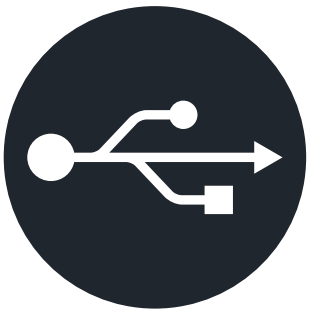
วิธีอนุญาตให้สามารถเข้าถึงไดรฟ์ USB ได้
โดยไม่ส่งผลต่อการรักษาความปลอดภัยปลายทาง

#KingstonIsWithYou #KingstonIronkey

บทนำ

ข้อมูลจำเพาะ USB 1.0 อย่างเป็นทางการได้เปิดตัวเมื่อเดือนมกราคม ปี 1996 และถือเป็นยุคใหม่ของมาตรฐานร่วม ความสะดวกสบาย รวมถึงความอเนกประสงค์สำหรับผู้จำหน่ายอุปกรณ์ต่อพ่วงและผู้ใช้ปลายทาง 27 ปีต่อมา USB ยังคงรักษาความเข้ากันได้ของอุปกรณ์รุ่นก่อนหน้าในการแก้ไขแต่ละครั้ง ทั้งนี้ USB ยังเป็นรากฐานสำคัญของอินเทอร์เฟซฮาร์ดแวร์คอมพิวเตอร์ตั้งแต่เซิร์ฟเวอร์ไปจนถึงสมาร์ทโฟนอีกด้วย



ความเรียบง่ายในการใช้งานแบบ Plug-and-Play ของ USB และความเร็วที่เพิ่มขึ้นอย่างต่อเนื่องได้ทำให้อุปกรณ์จัดเก็บข้อมูล USB แบบพกพากลายเป็นเจ้าสังเวียนที่ไม่มีใครเทียบ อย่างไรก็ตาม ความสะดวกเช่นนี้ย่อมมาพร้อมกับความเสี่ยงด้านการรักษาความปลอดภัยของข้อมูล ในโลกปัจจุบัน หากไม่มีการเลือกใช้เครื่องมือที่เหมาะสม เช่น การป้องกันปลายทางบนคอมพิวเตอร์โฮสต์และแนวทางปฏิบัติด้านการรักษาความปลอดภัยของข้อมูลที่เหมาะสม ผู้ใช้ที่ไม่ระมัดระวังในการใช้อุปกรณ์จัดเก็บข้อมูล USB แบบพกพาอาจปล่อยให้ตนเองและผู้อื่นเสี่ยงต่อการละเมิดข้อมูลที่อาจเกิดขึ้นซึ่งอาจสร้างความเสียหายให้กับผู้ใช้ปลายทาง รวมถึงหน่วยงานหรือภาครัฐทั้งหมด

นอกเหนือจากการป้องกันสภาพแวดล้อมโฮสต์แล้ว ควรรักษาความปลอดภัยให้กับไดรฟ์ USB ด้วยรหัสผ่านและการเข้ารหัสเชิงฮาร์ดแวร์ในตัวอุปกรณ์ ซึ่งเป็นวิธีป้องกันการบุกรุกที่มีประสิทธิภาพ เราจะสำรวจแนวทางปฏิบัติที่ดีที่สุดในการใช้ไดรฟ์ USB ให้ปลอดภัยมากยิ่งขึ้น พร้อมรายละเอียดเชิงลึกเกี่ยวกับไดรฟ์ USB โดยทั่วไป

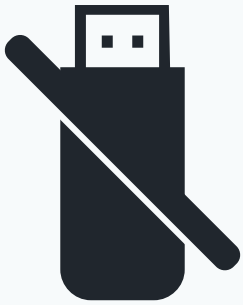
แม้ว่าแนวทางแบบผสมผสานจะเป็นทางเลือกที่เหมาะสม แต่ประสิทธิภาพของการเข้ารหัสและส่วนประกอบฮาร์ดแวร์ของไดรฟ์ USB เองคือสิ่งสำคัญที่สุด องค์ประกอบเหล่านี้มีบทบาทอย่างยิ่งตั้งแต่การเงินไปจนถึงสุขภาพ ตลอดจนอุตสาหกรรมการผลิตและการทหาร นอกจากนี้ ยังมีบทบาทด้านการทำงานทางไกลที่ไม่สามารถเข้าถึงเครือข่าย มีความสุ่มเสี่ยง หรือมีข้อจำกัดบางประการ

ไดรฟ์ USB เข้ารหัสเชิงฮาร์ดแวร์มีมาตรฐานการรับรองต่างกันไปตามระดับความปลอดภัยที่เกี่ยวข้อง การพิจารณาคุณลักษณะต่าง ๆ และทางเลือกในการปรับแต่งจะทำให้ไดรฟ์เหล่านี้สามารถนำมาใช้เป็นอุปกรณ์แบบแยกเดี่ยวที่มีความเหมาะสมภายใต้มาตรการป้องกันที่ครอบคลุมสถานการณ์ที่เปราะบางทั้งหมด

การรับรองพอร์ต: อุปกรณ์จัดเก็บข้อมูล USB จะต้องตรงตามซอฟต์แวร์การป้องกันการสูญหายของข้อมูลสำหรับการจัดการปลายทาง

นับเป็นเวลาหลายทศวรรษ การนำแอปพลิเคชันป้องกันไวรัสและมัลแวร์มาใช้เพื่อป้องกันระบบการทำงานในเบื้องต้น ซึ่งสแกนการดาวน์โหลดและอุปกรณ์ต่อพ่วงโดยอัตโนมัติ รวมถึงรายงานผลหรือจัดการข้อมูลที่น่าสงสัย การป้องกันจากซอฟต์แวร์ Next Generation Anti-Virus (NGAV) ถือเป็นพัฒนาการอีกขั้น แทนที่จะใช้ฐานข้อมูลลักษณะไวรัสที่อัปเดตอย่างต่อเนื่องเพียงอย่างเดียว NGAV ใช้ฟีเจอร์แมชชีนเลิร์นนิงและการตรวจจับพฤติกรรมที่สามารถระบุและลดจำนวนภัยคุกคามที่ไม่รู้จัก

ซึ่งไม่ใช่ฟีเจอร์รักษาความปลอดภัยเพียงอย่างเดียวในระบบของเรา และสำหรับผู้ที่คาดหวังการป้องกันประสิทธิภาพสูงจากอุปกรณ์ต่อพ่วงของผู้ใช้และอุปกรณ์อื่น ซอฟต์แวร์ป้องกันการสูญหายของข้อมูลสำหรับการจัดการปลายทาง (DLP) คือทางเลือกที่สามารถช่วยให้คุณปฏิเสธการเข้าถึงพอร์ต USB และอุปกรณ์กระจายสัญญาณอื่น ๆ



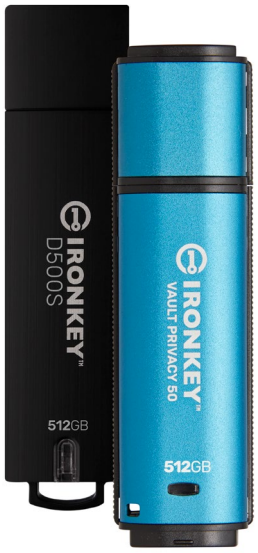
แนวทางการทำงานแบบบล็อกพอร์ตทั้งหมดเพื่อรักษาความปลอดภัยสามารถขจัดความเสี่ยงได้ อาจเป็นสิ่งที่จำเป็น แต่เนื่องจากนโยบายเช่นนี้ไม่ค่อยมีความยืดหยุ่นและมักทำให้เกิดผลลัพธ์ที่ไม่พึงประสงค์

อย่างไรก็ตาม ผู้ดูแลระบบ IT บางส่วนกลับเลือกที่จะปฏิเสธคำขอเปิดพอร์ต USB บนเครื่องของผู้ใช้ เนื่องจากการดำเนินการเช่นนี้กับปลายทางเป็นการจะอนุญาตให้สามารถเข้าถึงไฟร์วอลล์ขององค์กรได้โดยตรง มาตรการเฝ้าระวังเช่นนี้เป็นสิ่งที่เข้าใจได้ แต่เมื่อต้องเปิดใช้งานการเข้าถึงอุปกรณ์จัดเก็บข้อมูล USB การจัดสรรสิทธิ์เข้าถึงนี้ไม่จำเป็นต้องกลายเป็นภาระที่หนักหน่วงในการรักษาความปลอดภัยหากมีข้อกำหนดเบื้องต้นไว้ก่อนหน้า

ข้อกำหนดสำคัญประกอบด้วยชุดแอปพลิเคชันการจัดการปลายทางที่มีคุณสมบัติด้านการสแกนเพื่อตรวจหาภัยคุกคามผ่านโซลูชันป้องกันไวรัส/มัลแวร์ รวมถึงการเฝ้าติดตามและการจัดการส่วนกลางให้กับผู้ใช้ทั้งหมด

โดยทั่วไปแล้ว แนวทางที่ตรงไปตรงมานี้มีการนำมาใช้ในหลายกรณีผ่านโซลูชันแบบองค์รวมจากผู้จำหน่ายยอดนิยม เช่น McAfee MVision, Sophos Intercept X, Symantec Endpoint Security, Trend Micro Smart Protection และ WinMagic Secure Doc เป็นต้น

การปรับแต่งรายการอนุญาต



เมื่อกล่าวถึงการรักษาความปลอดภัยของอุปกรณ์จัดเก็บข้อมูล USB วิธีที่ใช้จะขึ้นอยู่กับระดับการป้องกันที่ต้องการ แนวทางที่มีประสิทธิภาพและไม่ยุ่งยากคือการทำรายการอนุญาตให้กับอุปกรณ์จัดเก็บข้อมูล USB ด้วยการกำหนด Vendor Identifier (VID) และ Product Identifier (PID) สิ่งหนึ่งเกี่ยวกับอุปกรณ์ต่อพ่วง USB ทุกตัวคือผู้ผลิตแต่ละรายจะกำหนด VID เฉพาะไว้ ส่วน PID จะมีการเปลี่ยนแปลงตามผลิตภัณฑ์ใหม่ทุกตัวที่มีการเปิดตัว

ในส่วนของการจัดทำรายการอนุญาต การใช้ VID ของผู้ผลิตเพียงอย่างเดียวจะไม่ครอบคลุมและปลอดภัยเพียงพอ เนื่องจากอุปกรณ์ USB ทั้งหมดที่ผลิตจะได้รับอนุญาตทั้งหมด PID จะมอบผลลัพธ์ที่ละเอียดมากขึ้นและกำหนดว่าผลิตภัณฑ์รุ่นที่เจาะจงเท่านั้นที่สามารถมอบสิทธิ์เข้าถึงระบบโฮสต์ได้

แม้ว่านี่จะเป็นแนวทางที่ได้รับการปรับปรุงให้ดียิ่งขึ้น แต่ก็ยังไม่ถือว่าสมบูรณ์แบบ อุปกรณ์จัดเก็บข้อมูล USB เป็นที่นิยมอย่างมากเนื่องจากเปิดโอกาสให้ผู้ใช้สามารถจัดหาอุปกรณ์ของตนให้ตรงตามรุ่นที่ได้รับอนุญาตให้ใช้งานได้ ภายใต้แนวคิดนี้ Kingston Technology จึงนำเสนอระบบการทำงานที่จะช่วยเพิ่มความปลอดภัยให้อุปกรณ์จัดเก็บข้อมูล USB ไปอีกขั้น

ผู้ใช้สามารถสร้างโปรไฟล์ PID แบบกำหนดเองที่จัดไว้เฉพาะสำหรับหน่วยงานตามที่กำหนดกับแฟลชไดรฟ์ USB เข้ารหัสจาก Kingston ซึ่งพร้อมให้ใช้งานผ่านโปรแกรมการปรับแต่งผลิตภัณฑ์ บริษัทที่ใช้งานอุปกรณ์ที่มีตัวบ่งชี้ผลิตภัณฑ์ที่เหมาะสมไม่เพียงได้ประโยชน์จากรายการอนุญาตที่ลดความซับซ้อนเท่านั้น แต่ยังรวมถึงการรักษาความปลอดภัยที่มีประสิทธิภาพมากขึ้นอีกด้วย เมื่อไม่มี PID แบบกำหนดเองที่ตรงกัน แม้แต่อุปกรณ์ที่มีลักษณะเหมือนกันทุกประการที่พนักงานจัดซื้อแยกต่างหากก็จะถูกปฏิเสธ

แม้ว่าการใช้ PID แบบกำหนดเองจะช่วยให้ผู้ดูแลระบบ IT สามารถเชื่อมต่อกับอุปกรณ์จัดเก็บข้อมูล USB ใหม่ได้อย่าง

รวดเร็วและง่ายดาย แต่ทางเลือกที่เจาะจงกว่าคือการใช้หมายเลขประจำเครื่องของอุปกรณ์ที่มีในไดรฟ์ USB แบบเข้ารหัสของ Kingston วิธีการนี้กำหนดให้มีการลงทะเบียนซีเรียลนัมเบอร์เฉพาะของอุปกรณ์แต่ละตัวกับระบบจัดการส่วนการทำงานปลายทาง การเตรียมการเบื้องต้นจะต้องอาศัยเจ้าหน้าที่ด้าน IT ตลอดจน Kingston พร้อมจัดหาหมายเลขประจำเครื่องไว้ให้สำหรับคำสั่งซื้อแต่ละรายการ ซึ่งจะเป็นรหัสตัวอักษรและตัวเลขแบบไม่เรียงลำดับ การเลือกใช้วิธีการนี้ช่วยให้สามารถกำหนดนโยบายที่ยืดหยุ่นกว่าตามการครอบครองไดรฟ์แต่ละตัวที่มีการตรวจสอบที่มาของอุปกรณ์ได้แม่นยำ ซึ่งเป็นประโยชน์อย่างยิ่งในการตรวจพิสูจน์ทาง IT ไดรฟ์ Kingston บางตัวจะมีหมายเลขประจำเครื่องและบาร์โค้ดในกรณีสแกนผ่านระบบอิเล็กทรอนิกส์ ไดรฟ์บางตัวสามารถปรับแต่งเพื่อเพิ่มบาร์โค้ดและหมายเลขประจำเครื่องในการใช้งานทางธุรกิจ ซึ่งสามารถใช้รายการเหล่านี้เพื่อตรวจติดตามไดรฟ์ได้

ตามค่าเริ่มต้นแล้ว ระบบการจัดการปลายทางจะมอบการเข้าถึง VID/PID เพื่อการบล็อกพอร์ตหรือทำรายการอนุญาต ข้อเสนอจาก Kingston ถือเป็นทางเลือกที่หลากหลายมากกว่าโดยอาศัยประโยชน์จากองค์ประกอบต่าง ๆ เหล่านี้เพื่อให้สอดคล้องกับนโยบายและแนวทางที่คาดหวังสำหรับการใช้อุปกรณ์จัดเก็บข้อมูล USB ของผู้ใช้ การกำหนดวิธีการลงรหัสประจำตัวที่เหมาะสมทำให้แนวทางการทำงานแบบบล็อกพอร์ตทั้งหมด กลายเป็นวิธีการที่อ่อนด้อยกว่าอย่างเห็นได้ชัดและไม่มีความจำเป็นอีกต่อไป

โซลูชันที่ครอบคลุมและปลอดภัยสำหรับผู้ใช้ทางไกล

เมื่อพูดถึงการรักษาความปลอดภัย การจัดทำรายการอนุญาตให้กับอุปกรณ์สามารถจัดการปัญหาได้เพียงครึ่งหนึ่งเท่านั้น กล่าวคือเป็นการแก้ปัญหาเพียงครึ่งเดียว

ความสะดวกและเรียบง่ายของอุปกรณ์จัดเก็บข้อมูล USB ทำให้อุปกรณ์นี้กลายเป็นเครื่องมือสำคัญในธุรกิจและสถาบันต่าง ๆ ที่ความสะดวกในการพกพาคือกุญแจสำคัญในการถ่ายโอนข้อมูลแบบไร้รอยต่อ ในสภาพการใช้งานส่วนใหญ่ เพื่อให้เป็นไปตามข้อกำหนดและหลักเกณฑ์ด้าน IT ที่เหมาะสม จึงมีความจำเป็นที่จะต้องจัดหาไดรฟ์ USB เข้ารหัสให้กับพนักงานเพื่อใช้ในการทำงาน การใช้ระบบป้องกันด้วยรหัสผ่านร่วมกับการเข้ารหัสอุปกรณ์ ทำให้อุปกรณ์จัดเก็บข้อมูลแบบพกพานี้สามารถป้องกันการสืบค้นข้อมูลที่มีความละเอียดอ่อนได้ในกรณีที่อุปกรณ์สูญหาย ถูกขโมย หรืออยู่ในสถานการณ์ที่มีความเปราะบาง

ซึ่งไม่ใช่โซลูชันสำเร็จรูปที่เหมาะสมในทุกกรณีเนื่องจากเทคนิคในการเข้ารหัสจะแตกต่างกันไป ทั้งนี้คุณจะเห็นข้อแตกต่างที่สำคัญที่สุดเมื่อทำการเปรียบเทียบในโซลูชันการเข้ารหัสเชิงซอฟต์แวร์และฮาร์ดแวร์อีกด้วย ถ้าเป็นเช่นนั้นแนวทางแบบไหนดีกว่ากัน ขึ้นอยู่กับความต้องการของคุณเอง แต่คำถามที่สำคัญคือ “แบบไหนปลอดภัยกว่ากัน”

การเข้ารหัสเชิงซอฟต์แวร์ถือเป็นทางเลือกที่ประหยัดมากกว่าสำหรับส่วนปฏิบัติการขนาดเล็ก โดยจะเหมาะกับธุรกิจที่การถ่ายโอนข้อมูลไม่มีความเปราะบาง และข้อกังวลที่สำคัญอยู่ที่การควบคุมมาตรฐานเป็นสำคัญ

อย่างไรก็ตามส่วนประกอบในการทำงานที่สำคัญของระบบเข้ารหัสเชิงซอฟต์แวร์ก็เป็นจุดอ่อนที่สำคัญ เนื่องจากต้องอาศัยแอปพลิเคชันที่เชื่อมประสานกับไคลเอนท์ จึงต้องอาศัยคอมพิวเตอร์ในการทำหน้าที่เข้ารหัสเป็นสำคัญ ดังนั้นเมื่อผนวกปัจจัยต่าง ๆ เข้าด้วยกันแล้ว อุปกรณ์จัดเก็บข้อมูลเข้ารหัสเชิงซอฟต์แวร์จะปลอดภัยมากแค่ไหนก็จะขึ้นอยู่กับคอมพิวเตอร์โฮสต์เป็นสำคัญ

โอกาสที่จะถูกเจาะระบบจะเพิ่มมากขึ้นเมื่อแฮคเกอร์ที่มีการเข้าถึงหน่วยความจำของคอมพิวเตอร์สามารถ “คาดเดา” คีย์เข้า/ถอดรหัสได้ นอกจากนี้ข้อมูลภายในไดรฟ์ยังอาจถูกเจาะเข้าโดยตรงผ่านการเดารหัสเนื่องจากไม่จำเป็นต้องอาศัยระบบป้องกันการเข้าถึงด้วยรหัสผ่านใด ๆ อีกต่อไป หากไฟล์ที่เข้ารหัสสามารถถูกสืบค้นหรือคัดลอกได้อยู่แล้ว

จำไว้ว่าระบบเข้ารหัสเชิงซอฟต์แวร์ต้องอาศัยการอัพเดตซอฟต์แวร์เป็นระยะ ๆ ซึ่งทำให้เกิดความยุ่งยากมากยิ่งขึ้นและเป็นภาระแก่บุคลากรด้าน IT ที่ร้ายแรงที่สุดคือการเข้ารหัสเชิงซอฟต์แวร์สามารถถูกลบออกอย่างสมบูรณ์โดยพนักงานที่ไม่พอใจและมีปัญหากับการโอนย้ายไดรฟ์ระหว่างแพลตฟอร์มต่าง ๆ ผู้ใช้ไดรฟ์สามารถคัดลอกข้อมูลในไดรฟ์เข้ารหัสไปยังคอมพิวเตอร์ ฟอร์แมตไดรฟ์ให้เป็นแบบไม่เข้ารหัส และคัดลอกข้อมูลดังกล่าวไปยังไดรฟ์อีกครั้ง เมื่อถึงตอนนี้ข้อมูลก็ไม่มีความปลอดภัยอีกต่อไป และสุ่มเสี่ยงอย่างยิ่งต่อการถูกคุกคาม ในกรณีที่ต้องการควบคุมมาตรฐานตามเงื่อนไขทางกฎหมายหรือระเบียบข้อบังคับ แนวทางนี้ถือเป็นแนวทางที่ไม่เหมาะสมอย่างยิ่ง เนื่องจากสามารถเปิดหรือปิดการทำงานการรักษาความปลอดภัยของไดรฟ์ USB ได้ตามต้องการ

การเข้ารหัสบนชิป: โซลูชันที่รวดเร็วและปลอดภัย

ในทางกลับกันไดรฟ์ USB แบบเข้ารหัสเชิงฮาร์ดแวร์จะทำงานเป็นอิสระจากคอมพิวเตอร์เนื่องจากจะมีโปรเซสเซอร์ในตัวติดตั้งไว้ในตัวไดรฟ์เพื่อจัดการการเข้ารหัส ซึ่งเป็นกระบวนการเข้ารหัสแบบต่อเนื่องพร้อมการป้องกันการโจมตีรหัสผ่านแบบ Brute Force ดังนั้นจึงไม่สามารถเข้าถึงหรือคัดลอกข้อมูลที่เข้ารหัสได้

ไดรฟ์ USB เข้ารหัสเชิงฮาร์ดแวร์ระดับองค์กรและการทหารจาก Kingston เลือกใช้การเข้ารหัส AES 256 บิตในโหมด XTS AES 256 บิตเป็นเทคนิคการเข้ารหัสที่ได้รับการรับรองในระดับสากลว่าสามารถป้องกันข้อมูลได้อย่างน่าเชื่อถือ การใช้คีย์แยกเป็นสองชุดออกจากกันระหว่างกระบวนการเข้ารหัส/ถอดรหัสเป็นวิธีการที่ใช้ในโหมด XTS ซึ่งจะเหมือนกับอุปกรณ์ถูกเข้ารหัสไว้ถึงสองชั้นซ้อน

ระหว่างใช้งาน คีย์เข้ารหัสจะมาจากระบบแจ้งตัวเลขสุ่มของชุดควบคุมไดรฟ์และต้องอาศัยรหัสผ่านของผู้ใช้เพื่อปลดล็อค การยืนยันตัวตนจะเริ่มต้นภายใต้คริปโต-ฮาร์ดแวร์ของอุปกรณ์ คีย์การเข้ารหัส และฟังก์ชันด้านความปลอดภัยที่สำคัญอื่น ๆ จะได้รับการป้องกันจากการไปใช้ประโยชน์ เช่น BadUSB, การโจมตีแบบ Cold Boot, โค้ดที่เป็นอันตราย และการโจมตีแบบ Brute Force

หนึ่งในข้อดีที่จะเห็นผลได้ทันทีจากการเข้ารหัสเชิงฮาร์ดแวร์คือประสิทธิภาพของไดรฟ์ที่จะเหนือกว่าไดรฟ์เข้ารหัสเชิงซอฟต์แวร์มาก เนื่องจากไม่มีภาระในการเข้ารหัสที่ตัวคอมพิวเตอร์โฮสต์อีกต่อไป ทุกอย่างจะเกิดขึ้นที่ตัวไดรฟ์เอง

ไดรฟ์ USB เข้ารหัสเชิงฮาร์ดแวร์ เช่น Kingston IronKey D500S เป็นอุปกรณ์ป้องกันด้วยรหัสผ่านที่เข้ารหัสมาจากโรงงาน ระหว่างทำงาน เฉพาะไดรฟ์เรียกใช้งานแบบป้องกันการเขียนเท่านั้นที่จะแสดงผลในเบื้องต้น เนื่องจากจัดเก็บแอปพลิเคชันที่ใช้เพื่อตรวจรับรองรหัสผ่านไว้ และจะทำหน้าที่ปลดล็อกไดรฟ์จัดเก็บข้อมูลหลักแบบเข้ารหัส กระบวนการนี้ช่วยไม่ให้ต้องติดตั้งไดร์เวอร์หรือซอฟต์แวร์ต่าง ๆ ที่ PC โฮสต์

นอกจากนี้ ไดรฟ์ USB เข้ารหัสเชิงฮาร์ดแวร์ของ Kingston เองยังมีเฟิร์มแวร์ลงชื่อดิจิตอลที่ช่วยป้องกันการจัดการเฟิร์มแวร์ภายในตัวอุปกรณ์ ระบบการป้องกันเสริมอีกชั้นนี้ช่วยป้องกันการคุกคามต่าง ๆ เช่น BadUSB ที่จะอาศัยช่องโหว่ของเฟิร์มแวร์ของไดรฟ์ USB สถานการณ์เช่นนี้อาจนำไปสู่การเรียกใช้คำสั่งหรือรหัสข้อมูลอันตรายกับคอมพิวเตอร์โฮสต์

แน่นอนว่าแนวทางแบบบล็อคพอร์ตทั้งหมด จะช่วยจำกัดความเสี่ยงจาก BadUSB แต่ก็จะกระทำต่อผลผลิตซึ่งไม่มีความจำเป็นและเป็นวิธีการที่ล้าสมัย ตามที่ได้กล่าวไปข้างต้น ระบบการทำงานที่ปลอดภัยในสถานการณ์สามารถเกิดขึ้นได้ในสถานการณ์ที่มีการใช้อุปกรณ์จัดเก็บข้อมูลแบบพกพาหากมีกระบวนการจัดหาและการใช้งานที่ไม่ซับซ้อนกำหนดไว้ร่วมกับไดรฟ์ USB แบบเข้ารหัสเชิงฮาร์ดแวร์

การทำงานทางไกลที่ปลอดภัยและได้มาตรฐานที่กำหนด

สำหรับผู้ที่ต้องทำงานจากทางไกล ระยะทางที่ไกลจากระบบป้องกันที่ปลอดภัยของหน่วยงานทำให้ต้องมีการปรับกลยุทธ์และจัดลำดับความสำคัญด้านความปลอดภัยขึ้นใหม่

เมื่อพูดถึงแผนงานรักษาความปลอดภัยทางไกล การบล็อกพอร์ต USB จะเป็นประโยชน์กับแล็ปท็อปของพนักงานหรือไม่ โดยกำหนดให้ต้องมีการเชื่อมต่ออินเทอร์เน็ตกับเซิร์ฟเวอร์แทนหากต้องการอัปโหลดหรือเรียกดูเอกสาร ระหว่างการเดินทาง เครือข่ายเชื่อมต่ออินเทอร์เน็ตสาธารณะ เช่น จุดเชื่อมต่อ Wi-Fi ที่ไม่ปลอดภัยหรือไม่น่าเชื่อถืออาจมีความจำเป็นเพื่อการทำงาน และทำให้เกิดความเสี่ยงได้หลายอย่าง รวมทั้งการเจาะข้อมูลภายในภัยคุกคามจากการดักจับข้อมูลผ่านการแอบอ้าง แบบแทรกกลาง

การสื่อสาร (MitM) และการดักการสื่อสารผ่านเครือข่ายเป็นเพียงวิธีการแฮ็คบางส่วนที่มีความซับซ้อนที่อาชญากรคอมพิวเตอร์เลือกใช้ แม้แต่ VPN เองก็อาจมีช่องโหว่ได้

การเชื่อมต่อเครือข่ายของหน่วยงานกับอินเทอร์เน็ตเป็นอีกส่วนการทำงานปลายทางซึ่งอาจเป็นจุดเปราะบางและเป็นเป้าหมายในการเจาะระบบของผู้ไม่ประสงค์ดี การเปิดรับการเชื่อมต่อจากระยะไกลมีความเสี่ยงอยู่ในระดับหนึ่ง โดยเฉพาะหากเกี่ยวข้องกับข้อมูลที่มีความเปราะบาง

การจัดหาไดรฟ์ USB เข้ารหัสเชิงฮาร์ดแวร์ที่มีการป้องกันด้วยรหัสผ่านให้แก่ผู้ปฏิบัติงานจึงช่วยแก้ไขปัญหาช่องโหว่นี้ของระบบเครือข่ายได้ ทั้งนี้ก็จะต้องมีการตรวจสอบไดรฟ์ USB ที่เลือกใช้ ว่าผ่านเงื่อนไขในการทำงานระยะไกลที่เกี่ยวข้องหรือไม่ ไม่ใช่เรื่องง่ายในการตัดสินใจว่าจะเลือกใช้ไดรฟ์ความจุเท่าใดหรือจะต้องบันทึกหมายเลขประจำเครื่องของไดรฟ์ไว้ในระบบหรือไม่ นี่เป็นประเด็นเกี่ยวกับโครงสร้างทางกายภาพของตัวอุปกรณ์

การป้องกันการทุบทำลาย: ทางเลือกที่เชื่อถือได้

ประเด็นสำคัญในที่นี้คือไดรฟ์ USB เข้ารหัสเชิงฮาร์ดแวร์สามารถทนต่อการทุบทำลายหรือไม่ ความปลอดภัยของตัวอุปกรณ์ต่อการแทรกแซงต่าง ๆ พิจารณาได้จากมาตรฐานรับรอง เช่น FIPS 140-3 ซึ่งกำหนดระดับโครงสร้างทางกายภาพของไดรฟ์ไว้หลายระดับแยกออกจากวิธีการเข้ารหัส

มาตรฐาน FIPS-197 ใช้รับรองเฉพาะองค์ประกอบในการเข้ารหัสเชิงฮาร์ดแวร์และตัวอุปกรณ์ต่าง ๆ เช่น กลุ่มผลิตภัณฑ์ IronKey Vault Privacy 50 และ Vault Privacy 80 External SSD ซึ่งเป็นผลิตภัณฑ์สำหรับองค์กรขนาดใหญ่ที่มีการกำหนดเงื่อนไขด้านความปลอดภัยไว้ในระดับต่ำกว่าเกรดใช้งานด้านการทหาร ไดรฟ์เหล่านี้มีราคาแพงน้อยกว่าแต่ก็ไม่มีระบบป้องกันความเสียหายทางกายภาพของไดรฟ์

การรับรองมาตรฐาน FIPS 140-3 ระดับที่ 3 (รอการรับรอง) เป็นวิธีการที่กำหนดไว้สำหรับอุปกรณ์ที่อาจถูกกระทบกระทั่งได้สูง โดยมีระดับการป้องกันเทียบเท่าการใช้งานด้านการทหาร Kingston จำหน่ายไดรฟ์ FIPS 140-3 ระดับที่ 3 ให้แก่องค์กรขนาดใหญ่ ภาครัฐและหน่วยงานด้านกลาโหมทั่วโลก

นอกจากนี้ยังเลือกใช้วัสดุอีพอกซีกับพื้นผิวด้านในเพื่อเคลือบวงจรของไดรฟ์ทั้งหมดเพื่อให้เกิดความปลอดภัย และยังยึดกาวส่วนประกอบภายในต่าง ๆ เข้ากับตัวเคสไว้เป็นอย่างดีเพื่อเป็นการป้องกันอีกหนึ่งชั้น ความพยายามในการเปิดเคสโลหะจะทำได้ยากมาก และอาจทำให้ชิปภายในและส่วนประกอบอื่น ๆ เสียหาย ทำให้ไดรฟ์ไม่สามารถใช้การได้ในที่สุด ด้วยการติดตั้งชั้นอีพอกซีแข็งและทึบแสง ทำให้การกระแทกกระทั้นกับส่วนประกอบที่สำคัญแทบจะเป็นไปไม่ได้เลย อุปกรณ์อย่างเช่น Kingston IronKey D500S และ S1000 ก็ใช้มาตรการรักษาความปลอดภัยนี้ด้วยเช่นกัน

ส่วนประกอบเพื่อการป้องกันเหล่านี้ไม่ได้จำกัดอยู่ที่โครงสร้างทางกายภาพเท่านั้น จะเห็นได้จาก Kingston IronKey S1000 ที่มีส่วนประกอบเพื่อการป้องกันความเสียหายเหนือขึ้นไปอีกขั้น คริปโตชิปภายในของ IronKey S1000 สามารถตรวจจับการกระแทกและสั่งปิดการใช้งานไดรฟ์ทันทีเมื่อมีเปิดอุปกรณ์ การพึ่งพาอุปกรณ์จัดเก็บข้อมูล USB เข้ารหัสเชิงฮาร์ดแวร์เพื่อสืบค้นและโอนไฟล์ข้อมูลที่อ่อนไหวถือเป็นแนวทางที่สมเหตุสมผลเพื่อให้การทำงานทางไกลมีความราบรื่นมากที่สุด และรับประกันความปลอดภัยได้อย่างเต็มประสิทธิภาพ

อย่าลืมศึกษาข้อมูลฮาร์ดแวร์และระบบรักษาความปลอดภัยของไดรฟ์ USB เพื่อพิจารณาว่าเหมาะสมกับความต้องการและการใช้งานของคุณหรือไม่ ไดรฟ์ USB แต่ละตัวจะต้องได้รับการตรวจสอบเป็นกรณีไปร่วมกับมาตรฐานรับรองที่เชื่อถือได้เพื่อช่วยในการตัดสินใจ ไม่ว่าจะให้ความสำคัญกับสิ่งใดมากกว่ากัน Kingston นำเสนอไดรฟ์ USB เข้ารหัสเชิงฮาร์ดแวร์และทางเลือกในการปรับแต่งมากมายในราคาจับต้องได้ ซึ่งตอบโจทย์การใช้งานทุกแบบ ตั้งแต่อุปกรณ์มาตรฐานทั่วไป ไปจนถึงผลิตภัณฑ์ที่มีมาตรฐานสูงสุดเพื่อการใช้งานทางทหาร

ปลอดภัยไว้ก่อน: ไม่มีเครือข่ายก็ไม่มีปัญหา

ปัจจุบันสำนักงานไม่ได้จำกัดอยู่แต่ในกรอบอีกต่อไป และการทำงานจากที่บ้านก็เริ่มเป็นกระแสอย่างจริงจัง ทำให้ช่องโหว่จากการทำงานจากที่บ้านกลายเป็นประเด็นสำคัญของผู้ประกอบการหลายราย ผู้ประกอบการเป็นจำนวนมากกำลังประสบปัญหาที่ไม่เคยพบมาก่อนและต้องการวิธีการที่ปลอดภัยในการเตรียมพร้อมสำหรับแนวโน้มในการทำงานที่เปลี่ยนไปนี้

เพื่อรองรับความต้องการเหล่านี้ของกลุ่มอุตสาหกรรมต่าง ๆ อุปกรณ์จัดเก็บข้อมูล USB เข้ารหัสเชิงฮาร์ดแวร์จึงเป็นทางเลือกที่สามารถเลือกหาได้และมีความปลอดภัยมากพอสำหรับการถ่ายโอนข้อมูลผ่านทางเครือข่ายซึ่งโดยปกติและในบางสถานการณ์อาจสุ่มเสี่ยงและมีความไม่เหมาะสม

ในภาคการเงิน หน่วยงานกำกับดูแลมักมีการร้องขอข้อมูลเพื่อตรวจสอบการปฏิบัติงานและการควบคุมมาตรฐานการทำงานของบริษัทต่าง ๆ ความเสี่ยงจากข้อมูลรั่วไหลเป็นข้อพิจารณาที่สำคัญอย่างยิ่งในการใช้เครือข่ายเพื่อถ่ายโอนข้อมูลที่อ่อนไหวที่มีข้อมูลด้านการลงทุน การซื้อขายในตลาด และกิจกรรมทางธนาคารที่เป็นความลับอื่น ๆ โซลูชันที่มีประสิทธิภาพและไม่ยุ่งยากคือการนำส่งข้อมูลเหล่านี้ผ่านไดรฟ์ USB เข้ารหัสเชิงฮาร์ดแวร์

การใช้ไดรฟ์ USB ที่ปลอดภัยเพื่อโอนไฟล์ข้อมูลในกลุ่มสุขภาพหรือการแพทย์ถือเป็นเรื่องที่เกิดขึ้นในทุก ๆ วัน ทั้งนี้เพื่อความสะดวกสำหรับแพทย์และผู้เชี่ยวชาญในการวิเคราะห์ข้อมูลจากแฟ้มข้อมูล หรืออ้างอิงข้อมูลนี้กับงานวิจัย หรือนำเสนอกรณีตัวอย่างให้แก่นักศึกษาแพทย์ นอกจากนี้ยังมีประโยชน์สำหรับข้อมูลกรรมสิทธิ์ เช่น การฉายภาพทางการแพทย์ที่การสืบค้นเครือข่ายอาจมีข้อจำกัดหรือไม่ปลอดภัย การเลือกใช้ไดรฟ์ USB เข้ารหัสเชิงฮาร์ดแวร์ที่ได้มาตรฐานที่กำหนดจะช่วยให้สามารถถ่ายโอนไฟล์ข้อมูลสำหรับใช้งานในทุกที่ได้ง่าย ๆ

สิ่งที่ควรทำและไม่ควรทำ

✓ **ใช้ไดรฟ์เข้ารหัสที่ได้มาตรฐานที่กำหนด**และพิจารณาเงื่อนไขทางเทคนิคที่ต้องการเพื่อเลือกสรรไดรฟ์ที่ตรงกับการใช้งานจริง ๆ

✗ **อย่าอนุญาตให้มีการเลือกใช้อุปกรณ์ได้ตามใจหรือนโยบายการนำอุปกรณ์ส่วนตัวมาใช้ในสำนักงาน** (BYOD) – สำหรับธุรกิจแล้ว ไดรฟ์ที่สูญหายและไม่มีการเข้ารหัสถือว่าเป็นความเสียหายมหาศาลในด้านการเงินและยังอาจกระทบต่อชื่อเสียงของบริษัท

✓ **เลือกใช้ระบบจัดการส่วนการทำงานปลายทาง**และไดรฟ์ USB แบบเข้ารหัสเชิงฮาร์ดแวร์ที่รองรับการจัดทำบัญชีรายการที่เชื่อถือได้

✗ **อย่าฝากความหวังไว้กับโชคชะตา** แต่ประเมินเงื่อนไขการทำงานในพื้นที่และระยะไกลให้รอบด้าน

✓ **ให้ความรู้แก่พนักงาน** เกี่ยวกับการรักษาความปลอดภัย ทั้งนี้เพื่อประโยชน์ของคนเหล่านี้เองเพื่อช่วยกันปกป้องบริษัทจากการถูกเจาะข้อมูลที่อาจส่งผลกระทบในวงกว้าง

✗ **อย่าทำให้ระบบรักษาความปลอดภัยมีความยุ่งยาก**จนผู้ใช้ต้องพยายามเลี่ยงการใช้งานปกติและเลี่ยงไปใช้ระบบ IT อื่นที่ไม่ได้กำหนดไว้แทน นโยบายแบบครอบคลุมที่คุ้นเคยไม่ได้หมายความว่าจะเหมาะสมกับทุกสถานการณ์เสมอไป สถานที่ทำงานกำลังเปลี่ยนแปลงไปและการเลือกโซลูชันที่ถูกต้องจะทำให้สามารถพัฒนาและกำหนดนโยบายใหม่ ๆ ได้

ในสถานการณ์เช่นนี้ Kingston IronKey Keypad 200 (KP200) สามารถตอบโจทย์ได้อย่างครบถ้วน ในฐานะไดรฟ์ที่ไม่ต้องพึ่งพา OS จึงไม่มีไดรฟ์เรียกใช้งานสำหรับกรอกรหัสผ่าน แต่จะอาศัยแป้นกดตัวอักษรและตัวเลขแทนเพื่อปลดล็อคอุปกรณ์สำหรับใช้งานกับแพลตฟอร์มต่าง ๆ ไดรฟ์ USB เข้ารหัสเชิงฮาร์ดแวร์จะคล้าย ๆ กับมีดพับสวิสที่สามารถใช้ได้แม้กระทั่งในสายการผลิต ทำให้สามารถถ่ายโอนแอปพลิเคชันที่พัฒนาโดยทีมวิจัยและพัฒนาด้าน IT ไปจนถึงการใช้งานกับเครื่องจักรที่ควบคุมผ่านแพลตฟอร์มเทคโนโลยีการทำงาน (OT) สำหรับการใช้งานแบบคละแพลตฟอร์มที่ครอบคลุมถึงระบบปฏิบัติการ Linux ไดรฟ์ KP200 ถือเป็นผลิตภัณฑ์นิรภัยที่มีความยุ่งยากน้อยที่สุดที่มีจำหน่าย

อุปกรณ์จัดเก็บข้อมูล USB เข้ารหัสเชิงฮาร์ดแวร์มีบทบาทสำคัญด้านการบังคับใช้กฎหมายเช่นกัน โดยช่วยในการปกป้องและดูแลความปลอดภัยในการถ่ายโอนไฟล์ข้อมูล ภาพและหลักฐานอื่น ๆ สำหรับเจ้าหน้าที่ภาคสนาม ทีมสอบสวนและทีมตรวจพิสูจน์ Kingston ยังมีคุณสมบัติเพิ่มเติมเนื่องจากสามารถมอบให้ไดรฟ์ที่มีหมายเลขประจำเครื่องภายในไว้ที่เคสด้านนอกร่วมกับบาร์โค้ด การจัดสรรและจัดทำแคตาล็อกไดรฟ์จึงไม่ยุ่งยากและติดตามได้ง่าย ทำให้เกิดความสะดวกไม่แตกต่างจากการบันทึกซีเรียลนัมเบอร์ด้วยตัวเอง และมีความรวดเร็วเทียบเท่ากับการสแกนบาร์โค้ด การตรวจสอบและจัดการวัสดุอุปกรณ์คงคลังจึงง่ายกว่าเดิม นี่เป็นคุณสมบัติเด่นที่จัดมาให้สำเร็จใน Kingston IronKey D500S, D500SM และ S1000B/E นอกจากนี้ยังมีจัดไว้ให้สำหรับรุ่นเข้ารหัสเชิงฮาร์ดแวร์ตัวอื่น ๆ ภายใต้แผนงานปรับแต่งผลิตภัณฑ์เฉพาะจาก Kingston

ระบบรักษาความปลอดภัยและสื่อบันทึกข้อมูลเพื่อการพกพา: เทคโนโลยีใหม่

ระบบป้องกันด้วยรหัสผ่าน การเข้ารหัสเชิงฮาร์ดแวร์ ระบบป้องกันการทุบทำลาย ระบบจัดทำบัญชีส่วนการทำงานปลายทางที่เชื่อถือได้ มาตรฐานการป้องกัน FIPS 140-3 ระดับที่ 3 (รอการรับรอง) หรือระบบการเข้าสู่ระบบอย่างรวดเร็ว ถือเป็นคุณสมบัติการทำงานสำเร็จรูปจากไดรฟ์ Kingston USB ที่สามารถเรียกใช้งานได้ในทันที

ระบบรักษาความปลอดภัยที่แข็งแกร่งนี้ทำให้มั่นใจว่าไดรฟ์ USB และข้อมูลภายในโฮสต์จะปลอดภัยเต็มที่ แม้ว่าในทางเทคนิคแล้วคุณสมบัติการทำงานจะน่าประทับใจมาก แต่การสุ่มเลือกผลิตภัณฑ์โดยไม่ศึกษาข้อมูลให้ดีอาจทำให้ไม่สามารถตอบโจทย์การใช้งานที่ตรงกับเงื่อนไขการทำงานของหน่วยงาน

Kingston คือผู้ผลิตอิสระที่นำเสนอผลิตภัณฑ์ที่หลากหลายตามความต้องการเฉพาะด้านของลูกค้า โครงการปรับแต่งผลิตภัณฑ์จาก Kingston คือทางเลือกที่จัดไว้ให้เพื่อตอบสนองความต้องการเพื่อให้ลูกค้าเกิดความพึงพอใจในระดับสูงสุด

การปรับแต่งระบบความปลอดภัยที่ไม่ใช่แค่การจัด USB PID เฉพาะเพื่อจัดทำเป็นบัญชีรายชื่อที่เชื่อถือได้เพียงอย่างเดียว โปรไฟล์รักษาความปลอดภัยในการเรียกใช้ระบบการทำงานยังสามารถปรับแต่งได้โดยใช้ค่าสำเร็จสิบห้ารูปแบบ ไม่ว่าจะเป็นการพิจารณาจากรายชื่อผู้ติดต่อและรายละเอียดบริษัท ไปจนถึงการบอกใบ้รหัสผ่านและการกำหนดจำนวนการกรอกรหัสผ่านสูงสุดที่อนุญาต ทั้งนี้ ผู้ใช้สามารถเลือกนำเสนอแบรนด์ร่วม (co-logo) พร้อมกำหนดสีไดรฟ์ที่ระบุได้ตามต้องการ โดยจะต้องมียอดสั่งซื้ออย่างน้อยห้าสิบชุด เพื่อให้การใช้งานอุปกรณ์แบบเฉพาะตัวของคุณทำได้แบบไม่ยุ่งยาก

หากไม่มีระบบจัดการส่วนการทำงานปลายทางที่เหมาะสมเพื่อดูแลความปลอดภัยของสื่อบันทึกข้อมูล USB เรามีระบบการจัดการจัดไว้ให้สำหรับหน่วยงานที่ต้องการจัดการไดรฟ์ Kingston ในหน่วยงานของตน รวมทั้งบริการรีเซ็ตรหัสผ่านจากระยะไกล

ความแพร่หลายของ USB และการใช้งานที่สะดวกทำให้ผลิตภัณฑ์ประเภทนี้สามารถคงอยู่มาได้ยาวนานกว่าเทคโนโลยีหลาย ๆ ตัว และสำหรับงานหลายประเภท ความสะดวกของ USB กลายเป็นความจำเป็นที่จะขาดไปเสียไม่ได้ ไดรฟ์ USB ที่มีการป้องกันและพร้อมใช้งานในทันทีคือผลิตภัณฑ์ที่ตอบโจทย์การใช้งานได้อย่างรวดเร็ว

จะกังวลเกี่ยวกับการเจาะข้อมูลเครือข่ายเนื่องจากการทำงานทางไกลอยู่ทำไม อุปกรณ์จัดเก็บข้อมูล USB เข้ารหัสเชิงฮาร์ดแวร์ IronKey จาก Kingston คือคำตอบที่อยู่ในมือของคุณ

เรียนรู้เพิ่มเติมเกี่ยวกับแนวทางช่วยเหลือต่าง ๆ จาก Kingston ได้ที่ kingston.com/ironkey หรือสอบถามข้อมูลแบบเจาะจงได้กับผู้เชี่ยวชาญผลิตภัณฑ์ USB เข้ารหัสของเรา

#KingstonIsWithYou #KingstonIronkey

เอกสารนี้อาจมีการเปลี่ยนแปลงเนื้อหาโดยไม่ต้องแจ้งให้ทราบล่วงหน้า
©2023 Kingston Technology Far East Corp. (Asia Headquarters), No. 1-5, Li-Hsin Rd. 1, Science Park, Hsin Chu, Taiwan
สงวนลิขสิทธิ์ เครื่องหมายการค้าและเครื่องหมายการค้าจดทะเบียนทั้งหมด ถือเป็นกรรมสิทธิ์ของผู้เป็นเจ้าของ