การเข้ารหัสซอฟต์แวร์และการปฏิบัติตามระเบียบข้อบังคับ: ทางเลือกที่ย่อมเยากว่าสำหรับป้องกันความเสี่ยงด้านความปลอดภัยที่สำคัญ

ระเบียบข้อบังคับและการปฏิบัติตามเงื่อนไข

การรักษาความปลอดภัยของข้อมูลแต่เดิมถือเป็นหน้าที่ของฝาย IT เท่านั้น แต่เนื่องจากกรณีการละเมิดข้อมูลที่เกิดขึ้นอย่างต่อเนื่อง ทำให้ภาครัฐทั่วโลกมีการกำหนดเงื่อนไขที่เข้มงวดกับธุรกิจต่าง ๆ เพื่อให้มีการเข้ารหัสและปกป้องข้อมูลระบุตัวบุคคลทั้งหมด

การเข้ารหัสข้อมูลที่ต้องได้รับการป้องกันถูกกำหนดเป็นข้อบังคับไว้อย่างชัดเจน ไม่ว่าจะเป็นมาตรฐาน HIPAA ในอุตสาหกรรมการแพทย์ มาตรฐาน GDPR ใน EMEA และ CCPA ในแคลิฟอร์เนีย หน่วยงานกำกับดูแลต่าง ๆ มีจำนวนเพิ่มมากขึ้นแบบก้าวกระโดดในช่วงกว่า 3 ปีที่ผ่านมา เนื่องด้วยข้อบังคับที่เข้มงวดมากขึ้นเหล่านี้ และจากวงเงินค่าปรับและความเสี่ยงทางกฎหมายที่มีมูลค่าสูงขึ้นเรื่อย ๆ

การเปลี่ยนแปลงที่เกิดขึ้นนี้ทำให้ฝาย IT เกิดภาระหนักในการดูแลความปลอดภัยและทำให้ค่าใช้จ่ายในการรักษาความปลอดภัยเพิ่มมากขึ้น ระหว่างสถานการณ์แพร่ระบาด COVID งบประมาณของหน่วยงานต่าง ๆ ถูกใช้ไปกับการลงทุนด้านฮาร์ดแวร์และระบบไฟร์วอลล์โดยมีเป้าหมายสำคัญคือเพื่อเข้ารหัสข้อมูล

การเข้ารหัสซอฟต์แวร์ผ่าน Microsoft BitLocker® หรือซอฟต์แวร์จัดการเครื่องปลายทางของผู้ให้บริการอย่าง Symantec, McAfee และอีกมากมายจึงเป็นที่ต้องการมากขึ้นเรื่อย ๆ ธุรกิจและผู้บริโภคหลายรายยังเลือกใช้ไดรฟ์ USB มาตรฐานร่วมกับซอฟต์แวร์ "vault" ที่จัดหาโดยผู้ให้บริการบางส่วน

การเข้ารหัสและข้อมูลทีอยู่ระหว่างนำส่ง

พนักงานและผู้ใช้ทั่วไปคาดหวังทีจะสามารถพกพาข้อมูลติดตัวไปได้ทุกที คนเหล่านีมีทางเลือกอยู่มากมาย เช่น

1. บริการคลาวด์: ซึงถือเป็นทางเลือกทีดี เนืองจากสามารถเข้าถึงจากอุปกรณ์ใดก็ได้ทีมีการเชือมต่ออินเทอร์เน็ต แต่ความยืดหยุ่นในการใช้งานก็มีข้อจำกัดเช่นกัน พืนทีจัดเก็บข้อมูลผ่านคลาวด์ทำให้ผู้ใช้หรือบริษัทไม่สามารถกำกับดูแลข้อมูลได้ และยังมีความเสียงทีอาจเกิดขึนได้จากการทีเซิร์ฟเวอร์คลาวด์ไม่ได้มีการล็อคป้องกันหรือมีการเข้าถึงค้างไว้
2. ไดรฟ์ USB มาตรฐาน: แม้ว่าการพกพาไดรฟ์ USB ติดตัวจะทำให้รู้สึกปลอดภัยมากกว่า แต่ความเสียงทีข้อมูลอาจรัวไหลจากการสูญหายของไดรฟ์ก็เป็นข้อพิจารณาทีสำคัญเช่นกัน เราสามารถดูตัวอย่างได้จากกรณีมากมายทีมีไดรฟ์ USB สูญหายไปพร้อม ๆ กับข้อมูลลับ หรือไดรฟ์ทีลืมไว้ในเสือผ้าเมือส่งซัก ซึงเป็นสิงทีพบเห็นได้ทัวไป
3. ไดรฟ์ USB เข้ารหัสเชิงฮาร์ดแวร์: ไดรฟ์ USB เหล่านีใช้สถาปัตยกรรมแบบพิเศษทีมีชุดควบคุมการเข้ารหัสในตัวและระบบควบคุมการใช้งาน ข้อมูลจะถูกเข้ารหัสโดยใช้การเข้ารหัส AES-256 บิตทีมีความปลอดภัยมากทีสุดในโหมด XTS ร่วมกับมาตรการป้องกันอืน ๆ เพือลดภัยคุกคามทางกายภาพและผ่านเฟิร์มแวร์ ไดรฟ์เหล่านีผลิตขึนโดยบริษัททีมีความเชียวชาญในการผลิตอุปกรณ์นิรภัย และมีราคาแพงกว่าไดรฟ์ USB มาตรฐาน เนืองจากมีความปลอดภัยของข้อมูลทีสูงกว่า ไดรฟ์มาตรฐาน FIPS 197 หรือ FIPS 140-2 Level 3 มีระดับการป้องกันและช่วยให้อุ่นใจขึนไปอีกระดับ
4. ไดรฟ์ USB มาตรฐานพร้อมการเข้ารหัสเชิงซอฟต์แวร์: เพือความปลอดภัยภายใต้ข้อกำหนด การเข้ารหัสเชิงซอฟต์แวร์ด้วย BitLocker หรือเครืองมืออืน ๆ เป็นอีกทางเลือกทีสามารถเลือกใช้ และเป็นตัวเลือกทีน่าสนใจเนืองจากมีราคาไม่แพงและใช้การเข้ารหัส AES-256 XTS เช่นกัน

ไม่น่าแปลกใจว่าทำไมธุรกิจและกลุ่มอุตสาหกรรมส่วนใหญ่ถึงเลือกใช้ตัวเลือกที 4 โดยเลือกทีจะใช้ไดรฟ์ USB มาตรฐานพร้อมการเข้ารหัสเชิงซอฟต์แวร์ สาเหตุหลัก ๆ ก็เนืองจากการเข้ารหัสเชิงซอฟต์แวร์ เช่น BitLocker หรือยูทิลิตีอืน ๆ "ไม่มีค่าใช้จ่ายเกิดขึน"

การเข้ารหัสเชิงซอฟต์แวร์ไม่ผ่านเงือนไขของข้อกำหนดทีมี

สำหรับบุคลากรด้านการรักษาความปลอดภัยในหน่วยธุรกิจ การเข้ารหัสเชิงซอฟต์แวร์มีขีดความสามารถด้านความปลอดภัยทีทัดเทียมกับไดรฟ์ USB เข้ารหัสเชิงฮาร์ดแวร์ทีมีราคาแพงกว่า แต่เป็นทางเลือกทีดีจริง ๆ หรือไม่ ข้อจำกัดด้านงบประมาณคือสิงทีทำให้ธุรกิจหลาย ๆ แห่งเลือกใช้การเข้ารหัสเชิงฮาร์ดแวร์เพือการควบคุมมาตรฐาน โดยไม่ตระหนักถึงข้อกังวลทีมีจากการเข้ารหัสเชิงฮาร์ดแวร์

แล้วไดรฟ์ USB เข้ารหัสเชิงซอฟต์แวร์มีข้อจำกัดใดบ้าง ข้อมูลทีพักเก็บไว้หรืออยู่ระหว่างนำส่งมีการเข้ารหัส AES-256 XTS หรือไม่ โดยทัวไปจะมีการเข้ารหัสไว้ แต่ปัญหาก็คือ: การเข้ารหัสเชิงซอฟต์แวร์ถือเป็น "การเข้ารหัสทียกเลิกได้"

เดียวนะ "ยกเลิกได้" เหรอ หมายความว่าผู้ใช้ไดรฟ์ USB เข้ารหัสเชิงซอฟต์แวร์สามารถปิดใช้งานการเข้ารหัสได้อย่างนันเหรอ

คำตอบคือ "ใช่" ผู้ใช้สามารถยกเลิกการเข้ารหัสเชิงซอฟต์แวร์จากไดรฟ์ USB ของตนได้ คุณอาจถามว่าจะทำอย่างนันไปทำไม ก็เพราะว่ามันทำได้ และเพราะว่าพวกเขาต้องการสืบค้นไฟล์โดยไม่ต้องคอยใส่รหัสผ่านหรืออาจเพียงแค่ลืมรหัสผ่านและต้องการใช้งานไดรฟ์ USB

จะยกเลิกการเข้ารหัสเชิงซอฟต์แวร์จากไดรฟ์ USB เข้ารหัสได้อย่างไร

สำหรับผู้ใช้ทีไม่ต้องการวุ่นวายกับการกรอกรหัสผ่านทียุ่งยากเพือสืบค้นข้อมูล ขันตอนสามารถทำได้ง่าย ๆ ดังนี

1. เสียบไดรฟ์เข้ารหัสเชิงซอฟต์แวร์เข้ากับคอมพิวเตอร์
2. ฟอร์แมตไดรฟ์
3. หลังจากฟอร์แมตไดรฟ์แล้ว การเข้ารหัสทังหมดก็จะถูกยกเลิกไปด้วย
4. คัดลอกไฟล์ทีมีข้อมูลลับไปยังไดรฟ์เพือให้สามารถเข้าถึงได้โดยง่าย

นีเป็นขันตอนง่าย ๆ ทีผู้ใช้ทำได้ผ่านคอมพิวเตอร์โดยมีข้อจำกัดใด ๆ - ฝาย IT อาจมีการล็อคคำสังฟอร์แมตไว้ทีคอมพิวเตอร์ของบริษัท แต่ก็สามารถเลือกทำผ่านคอมพิวเตอร์อืนทีไม่ใช่ของบริษัทได้

เพือปฏิบัติตามข้อกำหนด ความสะดวกในการยกเลิกฟังก์ชันเข้ารหัสข้อมูลทำให้ไดรฟ์ของบริษัทไม่มีการเข้ารหัสอีกต่อไป อีกทังข้อมูลเข้ารหัสเดิมในไดรฟ์ก็จะหายไปอย่างถาวรเมือมีการยกเลิกการเข้ารหัสตามวิธีการข้างต้น (คีย์เข้ารหัสจะเชือมโยงอยู่กับข้อมูล) ข้อมูลทีถูกคัดลอกไปยังอุปกรณ์หลังจากยกเลิกการเข้ารหัสจะถือเป็นข้อมูลทีไม่ปลอดภัยและอาจไม่ผ่านเกณฑ์มาตรฐานและถือเป็นการละเมิดข้อบังคับของ HIPAA, GDPR, CCPA และมาตรฐานอืน ๆ อีกมากมาย

ผลจากการทีไดรฟ์ทีไม่มีการเข้ารหัสสูญหาย

หากไดรฟ์ USB ของบริษัทสูญหายและถูกเก็บได้ แม้ว่าบริษัทจะไม่ทราบแต่รับรู้ในภายหลังผ่านทางโซเชียลมีเดีย ก็จะมีเงือนไขควบคุมพิเศษทีบริษัทต้องดำเนินการ เช่น

1. การดำเนินการตรวจสอบเพือพิจารณาว่าข้อมูลใดบ้างทีมีการสูญหาย
2. การพิจารณาว่ามีการละเมิดกฎหมายข้อใดหรือไม่ โดยปรึกษาร่วมกันกับฝ่ายกฎหมาย
3. การประเมินสถานการณ์ว่าจะต้องแจ้งให้ลูกค้าทราบหรือไม่

นีคือสถานการณ์ทีการสูญหายของไดรฟ์เพียงตัวเดียวก็อาจทำให้เกิดความเสียหายทางการเงินได้อย่างไม่น่าเชือ เนืองจากค่าใช้จ่ายในการดำเนินคดีทางกฎหมายทีสูง กระบวนการควบคุมมาตรฐานนีจึงอาจทำให้หน่วยงานทีเกียวข้องต้องสินเปลืองเงินเป็นจำนวนมาก และอาจยังต้องเสียค่าปรับ และถูกดำเนินคดีโดยลูกค้าหรือบุคคลอืน ๆ อีกทังยังทำให้เสือมเสียชือเสียง

หากมีการเลือกใช้การเข้ารหัสเชิงซอฟต์แวร์เนืองจากปัจจัยด้านต้นทุน ความเสียงเหล่านีและผลกระทบทางการเงินทีร้ายแรงทีอาจเกิดขึนคือสิงทีหลาย ๆ คนมองข้าม

นีคืออีกหนึงในความเสียงทีเกิดขึนจากการอนุญาตให้ใช้ไดรฟ์ USB แบบไม่เข้ารหัสในเครือข่ายของบริษัท ซึงโดยปกติจะเรียกเป็น "BadUSB" BadUSB คือมัลแวร์ประเภทหนึงทีถูกใช้โดยผู้ไม่ประสงค์ดีเพือเจาะไฟร์วอลล์ของบริษัทและเผยแพร่มัลแวร์ไปยังระบบป้องกันทางไซเบอร์ของบริษัทผ่านอุปกรณ์จัดเก็บข้อมูล USB

BadUSB

เมือเสียบไดรฟ์ USB เข้ากับคอมพิวเตอร์ ชุดควบคุมของชิปเซ็ตของคอมพิวเตอร์จะเริมทำการทักทายกับชุดควบคุมของไดรฟ์ USB ผ่านทางเฟิร์มแวร์ การทักทายดังกล่าวจะเกิดขึนก่อนระบบปฏิบัติการไม่ว่าจะเป็น Microsoft/macOS/Linux จะทราบว่ามีการเชือมต่อเกิดขึน ไดรฟ์ USB ทุกตัวจะมีเฟิร์มแวร์ทีทำงานเมือไดรฟ์เสียบต่อเข้าทีพอร์ต USB

ผู้ไม่ประสงค์ดีรู้ดีว่าตนเองสามารถปล่อยมาลแวร์ได้ผ่านกลไกการทักทายนีโดยการแทนทีเฟิร์มแวร์ทีทำงานในไดรฟ์ USB เป็นเฟิร์มแวร์อืนทีอันตรายและจะทำหน้าทีปล่อยมัลแวร์เข้าไปยังระบบคอมพิวเตอร์เป้าหมายขณะทีมีการสือสารกับไดรฟ์ USB ไดรฟ์ USB มาตรฐานไม่มีระบบรักษาความปลอดภัยในเฟิร์มแวร์ภายในทีสังการโดยชุดควบคุม ดังนัน BadUSB จึงอาจปรากฏในรูปแบบไดรฟ์ USB ทีน่าเชือถือและพร้อมทีจะเจาะไฟร์วอลล์และระบบป้องกันต่าง ๆ ในโลกไซเบอร์

บริษัทหลายแห่งพยายามทีจะแบนการใช้ไดรฟ์ USB กับระบบของตน หรือถึงขนาดทีมีการอุดอีพอกซีไว้ทีพอร์ต USB เลยทีเดียว อย่างไรก็ตาม อาจมีพนักงานบางกลุ่มทีมีความจำเป็นต้องถ่ายโอนข้อมูลโดยใช้ไดรฟ์ USB เช่น ผู้บริหารทีต้องการนำข้อมูลไปด้วยสำหรับการทำงาน หรือประสานงานกับทีปรึกษาทางกฎหมายหรือด้านการเงินจากภายนอกทีไม่ได้อยู่ในระบบคลาวด์ของบริษัท หรือผู้รับเหมาของบริษัททีต้องการข้อมูลเพือทำงานแต่ไม่สามารถใช้ฐานข้อมูลของบริษัทได้ หรือนักวิเคราะห์ด้านการเงินทีรีบร้อนสรุปรายงานประจำเดือนและจะต้องนำข้อมูลไปทำงานต่อทีบ้าน

ผลการวิเคราะห์ก่อนหน้านีระบุว่าการใช้ไดรฟ์ USB มาตรฐานร่วมกับระบบเข้ารหัสเชิงซอฟต์แวร์นันมีความเสียงอย่างยิง ในเบืองต้น ผลิตภัณฑ์ทีราคาถูกอาจเป็นอันตรายคุกคามและทำให้สินเปลืองค่าใช้จ่ายมากกว่าได้อย่างไม่น่าเชือ ค่าใช้จ่ายในการปรึกษาทนายเพียง 2-3 ชัวโมงเกียวกับการรัวไหลของข้อมูลทีอาจเกิดขึนก็ทำให้การลดค่าใช้จ่ายจากการเลือกใช้ผลิตภัณฑ์ราคาถูกหมดประโยชน์ไปอย่างสินเชิง

ไดรฟ์ USB เข้ารหัสเชิงฮาร์ดแวร์ถือเป็นตัวเลือกทีดีทีสุดเพือให้เป็นไปตามข้อกำหนดทีเกียวข้อง

อะไรทีทำให้ไดรฟ์ USB เข้ารหัสเชิงฮาร์ดแวร์เป็นตัวเลือกทีดีทีสุดในการปฏิบัติตามข้อบังคับเหล่านี:

1. ไดรฟ์ USB เข้ารหัสเชิงฮาร์ดแวร์มีการเข้ารหัสทีไม่สามารถยกเลิกได้: ผู้ใช้ไม่สามารถปิดฟังก์ชันการเข้ารหัส รีเซ็ตฟังก์ชันรหัสผ่าน (การกำหนดความยาวขันต่ำ ความซับซ้อนของรหัส) หรือปิดฟังก์ชันนับจำนวนครังในการกรอกรหัสผ่านใหม่ การทำงานดังกล่าวจะแตกต่างจากการเข้ารหัสเชิงซอฟต์แวร์ซึงไม่สามารถป้องกันการเดารหัสผ่านแบบต่อเนืองโดยใช้การเดาคำตามพจนานุกรมผ่านฮาร์ดแวร์ โดยระบบการทำงานเชิงฮาร์ดแวร์จะจำกัดการกรอกรหัสผ่านซำ และล็อคข้อมูลทันทีเมือมีการกรอกรหัสผ่านผิดพลาด 10 ครังหรือน้อยกว่านีตามทีกำหนดไว้ ซึงจะมีความปลอดภัยกว่ามากในยุคทีคอมพิวเตอร์ในปัจจุบันมีประสิทธิภาพสูงมาก
2. ไดรฟ์เข้ารหัสเชิงฮาร์ดแวร์ใช้ชุดควบคุมการเข้ารหัสระดับพรีเมียมร่วมกับระบบรักษาความปลอดภัยอืน ๆ: แม้ว่าเราไม่นิยมทีจะเปิดเผยวิธีการตอบโต้สถานการณ์ด้านความปลอดภัย แต่ก็มีมาตรการตอบโต้ทีคุณสามารถใช้เพือป้องกัน BadUSB ได้เช่นกัน ทีโรงงานขณะโหลดเฟิร์มแวร์ไปยังไดรฟ์เข้ารหัสเชิงฮาร์ดแวร์เท่านัน เฟิร์มแวร์จะมีการลงลายมือชือและโหลดข้อมูลผ่านระบบดิจิตอล ซึงหมายความว่าเมือเสียบไดรฟ์ USB เข้ารหัส ชุดควบคุมการเข้ารหัสจะเริมจากตรวจสอบความสมบูรณ์ของเฟิร์มแวร์ผ่านลายมือชือดิจิตอล และจะโหลดก็ต่อเมือผ่านการยืนยันทีกำหนด ความพยายามในการแทนทีเฟิร์มแวร์จะเป็นการล็อคไดรฟ์ทำให้ไม่สามารถใช้งานได้และไม่เกิดอันตรายใด ๆ ตามมา
3. ไดรฟ์ USB เข้ารหัสเชิงฮาร์ดแวร์สามารถกำหนด Product ID (PID) ได้เฉพาะสำหรับหน่วยงานทีใช้งาน: ไดรฟ์ระดับพรีเมียมเหล่านีอาจมีรหัสดิจิตอลทีตังโปรแกรมไว้ โดยหากเสียบไดรฟ์กับไฟร์วอลล์ภายในหรือภายนอกของบริษัทก็จะสามารถระบุรหัสประจำตัวไดร์ฟได้ว่าเป็นไดร์ฟของบริษัท เช่น หากพนักงานทำไดรฟ์ของบริษัทหายและซือไดรฟ์รุ่นเดียวกันมาแทน ไดรฟ์ทีจัดซือใหม่จะไม่ผ่านการตรวจสอบของเครือข่ายบริษัท การปรับแต่งดังกล่าวนีถือเป็นระบบป้องกันอีกขันสำหรับการใช้งานไดรฟ์ USB
4. ไดรฟ์เข้ารหัสเชิงฮาร์ดแวร์สามารถช่วยให้หน่วยงานประหยัดค่าใช้จ่ายลงได้อย่างรวดเร็ว: เพียงแค่ระดับความเสียงทีลดลงหรือหายไปก็ทำให้การคืนทุนรวดเร็วมากอย่างไม่น่าเชือแล้ว

Kingston คือผู้ผลิตไดรฟ์ USB เข้ารหัสรายใหญ่ทีสุดในโลก และมีไดรฟ์หลากหลายรุ่นทีมีคุณสมบัติการใช้งานและช่วงราคาต่าง ๆ กัน ติดต่อ Kingston ได้โดยตรงเพือสอบถามว่าเราสามารถช่วยคุณในการปฏิบัติตามเงือนไขทีกำหนดผ่านไดรฟ์ USB เข้ารหัสเพือการใช้งานในกลุ่มผู้บริหาร พนักงาน ผู้รับเหมาและผู้ใช้อืน ๆ ได้อย่างไร