Synology

ปกป้ององค์กรของคุณจากแรนซัมแวร์

การโจมตีของแรนซัมแวร์ได้รับการคาดการณ์ว่าจะทำให้องค์กรต่างๆ ต้องเสียหายมูลค่ารวมหนึ่งล้านล้าน US ในปี 2023 เพียงปีเดียว[1] แผนการปกป้องข้อมูลที่มีตัวเลือกการกู้คืนข้อมูลที่รวดเร็วเป็นสิ่งสำคัญในการลดผลกระทบของแรนซัมแวร์และรูปแบบอื่นๆ ของอาชญากรรมไซเบอร์

Date 13 ต.ค. 2023

การสำรองข้อมูล: แนวป้องกันสุดท้ายเมื่อเกิดภัยพิบัติ

เมื่อข้อมูลสูญหายจากการลบหรือการแก้ไขที่เป็นอันตราย การสำรองข้อมูลจะช่วยให้คุณกู้คืนข้อมูลสำคัญและหลีกเลี่ยงเวลาหยุดทำงานที่มีค่าใช้จ่ายได้ ใช้ประโยชน์จากโซลูชันการปกป้องข้อมูลของ Synology ในการออกแบบกลยุทธ์การสำรองข้อมูลสำหรับโครงสร้างพื้นฐานด้าน IT ทั้งหมดของคุณ

การปกป้องอย่างสมบูรณ์

ปกป้อง Endpoint รวมถึงการสำรองข้อมูลหลักเพื่อสร้างเครือข่ายความปลอดภัยหลายแห่งให้กับข้อมูลของคุณ

กู้คืนได้อย่างรวดเร็ว

ลดเวลาหยุดทำงานให้เหลือน้อยที่สุดเมื่อเกิดภัยพิบัติด้วยตัวเลือกการกู้คืนแบบทันที

พื้นที่จัดเก็บข้อมูลแบบเปลี่ยนแปลงไม่ได้

ป้องกันการเปลี่ยนแปลงข้อมูลและสแนปช็อตโดยไม่ได้รับอนุญาต

โซลูชันปลอดค่าสิทธิ์การใช้งาน

สำรองข้อมูลได้มากเท่าที่พื้นที่จัดเก็บข้อมูลสามารถเก็บได้ โดยไม่มีข้อจำกัดหรือค่าใช้จ่ายที่ซ่อนอยู่

การปกป้องจากแรนซัมแวร์แบบรวมศูนย์

รวบรวมข้อมูลสำรองจากฟลีทของเวิร์กสเตชัน, เซิร์ฟเวอร์, Virtual Machine และแอปพลิเคชันคลาวด์ ออพติไมซ์การใช้พื้นที่จัดเก็บข้อมูลและหลีกเลี่ยงปัญหาคอขวดของแบนด์วิดท์ด้วยเทคโนโลยีการขจัดข้อมูลซ้ำซ้อนและการสำรองข้อมูลส่วนเพิ่ม https://www.synology.com/dsm/solution/infrastructure

เวิร์กโหลดทางกายภาพ

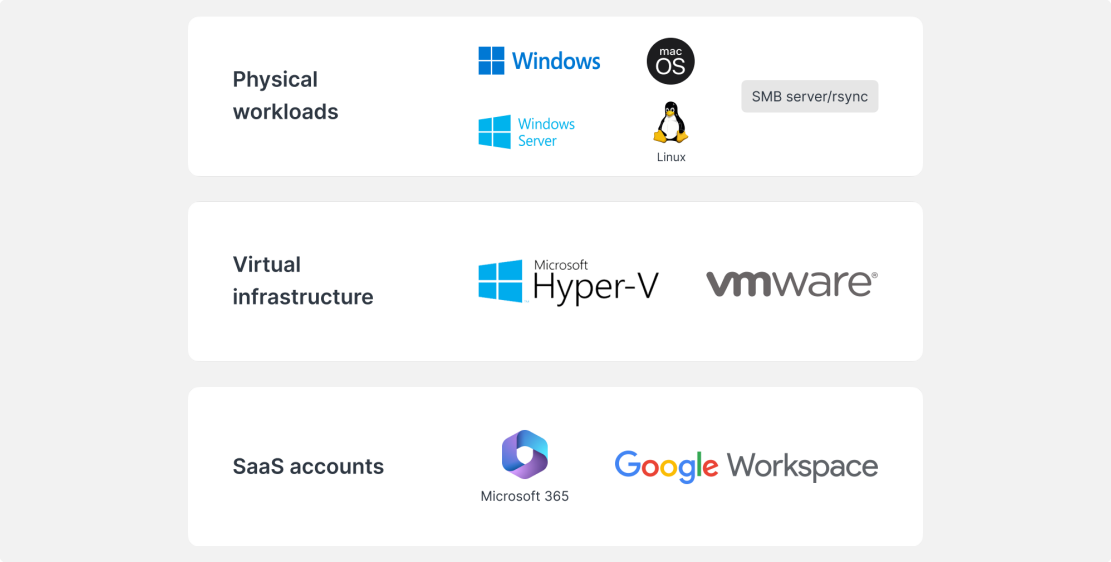
ปกป้อง Endpoint ในเหตุการณ์การโจมตีที่เป็นอันตรายด้วยการสำรองข้อมูลแบบ Bare-metal ที่ครอบคลุมและการกู้คืนระดับไฟล์ที่ยืดหยุ่น

โครงสร้างพื้นฐานของระบบ Virtualization

สำรองข้อมูล VMware® vSphere™, Microsoft® Hyper-V® VM และ LUN ด้วยเทคโนโลยีการลดข้อมูลที่มีประสิทธิภาพ

บัญชี SaaS

เปิดใช้งานการปกป้องอย่างต่อเนื่องสำหรับข้อมูลที่จัดเก็บบนคลาวด์ พร้อมการตรวจจับบัญชีที่เพิ่มใหม่โดยอัตโนมัติ



การกู้คืนที่มีประสิทธิภาพ

ลดเวลาหยุดทำงานของระบบการผลิตที่สำคัญด้วยการกู้คืนการสำรองข้อมูลจากระบบ Synology ภายในหรือนอกไซต์อย่างรวดเร็ว

RTO ใกล้ศูนย์

เมาท์อิมเมจการสำรองข้อมูลบน VMware®, Hyper-V® หรือ Synology Virtual Machine Manager เพื่อกลับมาทำงานให้เร็วที่สุดเท่าที่จะทำได้ กู้คืน VM ไปยัง Hypervisor อื่นเพื่อหลีกเลี่ยงการหยุดชะงักของบริการ

RPO ต่ำสุด

กำหนดค่าความถี่ในการสำรองข้อมูลตามความต้องการของคุณ ลดปริมาณข้อมูลที่มีโอกาสได้รับผลกระทบระหว่างการโจมตีให้น้อยที่สุด ปกป้องระบบต่างๆ ได้อย่างรวดเร็วด้วยเทคโนโลยีการสำรองข้อมูลส่วนเพิ่มและการขจัดข้อมูลซ้ำซ้อน

การทำงานที่ใช้งานง่าย

ให้พนักงานเรียกดูและดูตัวอย่างอีเมล รายชื่อติดต่อ และไฟล์จากพอร์ทัลที่สะดวกสบายก่อนการกู้คืน ให้ประสบการณ์ที่เป็นมิตรต่อผู้ใช้มากยิ่งขึ้น และลดภาระของทีม IT

เพิ่มชั้นการปกป้องพิเศษ

ปฏิบัติตามกลยุทธ์การสำรองข้อมูล 3-2-1 ด้วยการจัดเก็บข้อมูลชุดที่สามไว้นอกไซต์หรือบนคลาวด์ ปกป้องข้อมูลของคุณจากเพลิงไหม้ ภัยธรรมชาติ หรือการโจรกรรม

ไปยังเซิร์ฟเวอร์นอกไซต์

จัดเก็บการสำรองข้อมูลลงในเซิร์ฟเวอร์ Synology ในตำแหน่งสำรองเพื่อป้องกันความเสียหายทางกายภาพและสร้างสแนปช็อตแบบเปลี่ยนแปลงไม่ได้ เพื่อการป้องกันแรนซัมแวร์ให้มากขึ้น

ไปยังคลาวด์

สำรองข้อมูลไปยังผู้ให้บริการพื้นที่จัดเก็บข้อมูลบนคลาวด์หลักทุกแห่ง ช่วยให้ข้อมูลของคุณปลอดภัยจากการเข้าถึงที่ไม่ได้รับอนุญาตผ่านการเข้ารหัส AES-256 ที่ฝั่งไคลเอนต์ https://c2.synology.com/storage/nas

ได้รับความเชื่อถือจากอุตสาหกรรมต่างๆ

"Synology [...] ทำให้เราสามารถลดค่าใช้จ่ายด้านฮาร์ดแวร์เซิร์ฟเวอร์ [...] ในขณะที่ทำให้การสำรองข้อมูล โครงสร้างพื้นฐานและเวิร์กสเตชัน การบันทึกระบบ และการจัดการไฟล์ง่ายขึ้นอย่างมาก"
https://www.synology.com/company/case_study/Investortools

"ด้วย Active Backup for Business ขณะนี้การสำรองข้อมูลทั้งหมดของเราเป็นแบบรวมศูนย์และพร้อมใช้งานตลอด 24 ชั่วโมง ซึ่งช่วยให้เราลดเวลาหยุดทำงานให้เหลือน้อยที่สุด และยังปฏิบัติตามกฎระเบียบของ FERPA ได้"
https://www.synology.com/company/case_study/University_of_Washington

"[...] Active Backup for Business มีความเร็วในการสำรองข้อมูลที่น่าอัศจรรย์ และทำงานลบข้อมูลที่ซ้ำกันได้อย่างเหลือเชื่อ — โดยใช้พื้นที่บนเซิร์ฟเวอร์ไปเพียง 28TB เท่านั้นจากทั้งหมด 58TB [...]"
https://www.synology.com/company/case_study/SHISEIDO_Taiwan_ABB

"[...] Active Backup for Business [...] ช่วยให้เราสามารถรวมศูนย์และจัดการงานสำรองข้อมูลทั้งหมดได้จากคอนโซลเดียว การกู้คืนข้อมูลที่ทำได้รวดเร็วและเชื่อถือได้ยังช่วยทำให้มั่นใจได้ถึงความต่อเนื่องทางธุรกิจ"
https://www.synology.com/company/case_study/UNESCO

คำถามที่พบบ่อย

แรนซัมแวร์คืออะไร

แรนซัมแวร์คือประเภทของมัลแวร์ที่เข้ารหัสไฟล์ของเหยื่อ จากนั้นผู้โจมตีจะเรียกค่าไถ่ในการกู้คืนการเข้าถึงข้อมูล มักจะขู่ว่าจะลบข้อมูลอย่างถาวรหากไม่มีการจ่ายค่าไถ่ การโจมตีด้วยแรมซัมแวร์อาจเป็นการก่อกวนเป็นอย่างมาก และอาจทำให้เกิดความสูญเสียทางการเงินเป็นอย่างมากสำหรับปัจเจกบุคคลและองค์กรต่างๆ การปกป้องตนเองและอุปกรณ์จากแรนซัมแวร์เป็นสิ่งสำคัญ เช่น ด้วยการทำให้ซอฟต์แวร์ทันสมัยอยู่เสมอและสำรองข้อมูลไฟล์เป็นประจำ

มีแรนซัมแวร์ประเภทใดบ้าง

มีแรนซัมแวร์อยู่หลายประเภท และมีการพัฒนาแบบใหม่ๆ ขึ้นอย่างต่อเนื่อง แรนซัมแวร์ที่พบมากที่สุดบางประเภทได้แก่:

- **แรนซัมแวร์ที่เข้ารหัส** — แรนซัมแวร์ประเภทที่พบมากที่สุดจะเข้ารหัสไฟล์ของเหยื่อเพื่อให้ไม่สามารถเข้าถึงได้หากไม่มีคีย์ถอดรหัส จากนั้นผู้โจมตีจะเรียกค่าไถ่เพื่อแลกเปลี่ยนกับคีย์
- **แรนซัมแวร์นักล็อค** — แรนซัมแวร์ประเภทที่จะล็อคเหยื่อไม่ให้เข้าคอมพิวเตอร์ของตนเองด้วยการเปลี่ยนข้อมูลรับรองการลงชื่อเข้าใช้ หรือแสดงข้อความที่ป้องกันไม่ให้เหยื่อเข้าถึงระบบของตน จากนั้นผู้โจมตีจะเรียกค่าไถ่ในการปลดล็อคคอมพิวเตอร์
- **แรนซัมแวร์ในฐานะบริการ (RaaS)** — รูปแบบธุรกิจที่ผู้โจมตีจะนำเสนอแรนซัมแวร์ให้กับปัจเจกบุคคลหรือกลุ่มอื่นๆ ที่ต้องการโจมตีผู้อื่น โดยปกติแล้วฝ่ายแรกจะให้แรนซัมแวร์และจัดการการเรียกค่าไถ่ ในขณะที่ฝ่ายหลังจะรับเปอร์เซ็นต์จากค่าไถ่
- **สแคร์แวร์** — แรนซัมแวร์ที่ออกแบบมาเพื่อหลอกให้เหยื่อกลัว เพื่อให้จ่ายค่าไถ่ โดยทั่วไปมักจะมีการแสดงคำเตือนด้านความปลอดภัยปลอม หรือข้อความที่อ้างว่าคอมพิวเตอร์ของเหยื่อติดไวรัส จากนั้นผู้โจมตีจะเรียกค่าไถ่เพื่อลบการติดไวรัสที่อ้างถึงออก

แรนซัมแวร์แพร่กระจายได้อย่างไร

โดยปกติแรนซัมแวร์จะแพร่กระจายผ่านอีเมลฟิชชิง หรือด้วยการใช้ช่องโหว่ในระบบคอมพิวเตอร์ ในการโจมตีฟิชชิง ผู้โจมตีจะส่งอีเมลที่ดูเหมือนว่าจะมีแหล่งที่มาที่ถูกกฎหมาย เช่น ธนาคาร หรือบริษัทที่มีชื่อเสียง อีเมลดังกล่าวมักจะมีลิงก์หรือไฟล์แนบที่เมื่อคลิกแล้วจะติดตั้งแรนซัมแวร์บนคอมพิวเตอร์ของเหยื่อ การใช้ช่องโหว่ของระบบก็คล้ายกัน ยกเว้นว่าผู้โจมตีจะใช้ช่องโหว่ของการรักษาความปลอดภัยของระบบในการติดตั้งแรนซัมแวร์โดยที่เหยื่อไม่ทราบ ไม่ว่าในกรณีใด เมื่อแรนซัมแวร์ได้รับการติดตั้งแล้ว มันจะแพร่กระจายไปยังคอมพิวเตอร์เครื่องอื่นๆ ในเครือข่ายเดียวกันอย่างรวดเร็ว

กระบวนการทั่วไปของการโจมตีด้วยแรนซัมแวร์คืออะไร

โดยทั่วไปกระบวนการโจมตีด้วยแรนซัมแวร์จะมีขั้นตอนดังต่อไปนี้:

1. ผู้โจมตีจะเข้าถึงคอมพิวเตอร์ของเหยื่อ ไม่ว่าจะด้วยการส่งอีเมลฟิชชิง หรือการใช้ช่องโหว่ในระบบ
2. เมื่อผู้โจมตีเข้าถึงคอมพิวเตอร์ของเหยื่อได้แล้วก็จะติดตั้งแรนซัมแวร์ในระบบ
3. จากนั้นแรนซัมแวร์จะเข้ารหัสไฟล์ของเหยื่อ เพื่อให้ผู้ใช้เข้าถึงไฟล์ไม่ได้
4. จากนั้นผู้โจมตีจะเรียกค่าไถ่จากเหยื่อ โดยปกติจะเป็นสกุลเงินดิจิตอล เช่น Bitcoin เพื่อแลกเปลี่ยนกับคีย์ถอดรหัสที่จะปลดล็อคไฟล์ที่เข้ารหัส
5. หากเหยื่อจ่ายค่าไถ่ ผู้โจมตีจะให้คีย์ถอดรหัส และเหยื่อจะเข้าถึงไฟล์ของตนเองได้อีกครั้ง อย่างไรก็ตาม ไม่มีการรับประกันว่าผู้โจมตีจะให้คีย์มาจริงๆ และแม้จะให้มา ไฟล์ของเหยื่อก็อาจเสียหาย โดยเป็นผลจากการเข้ารหัส

สิ่งสำคัญคือต้องทราบว่ากระบวนการนี้มีความหลากหลายเป็นอย่างมาก และไม่ใช่การโจมตีด้วยแรนซัมแวร์ทั้งหมดจะทำตามขั้นตอนเหล่านี้ทั้งหมดทุกขั้นตอน ตัวอย่างเช่น บางการโจมตีอาจจะไม่มีการเข้ารหัสเลย ในขณะที่การโจมตีอื่นๆ อาจมีการเรียกค่าไถ่หรือแบล็คเมลในรูปแบบอื่น

ฉันจะได้รับแรนซัมแวร์ได้อย่างไร

มีหลายวิธีที่คุณอาจได้รับแรนซัมแวร์ หนึ่งในวิธีที่พบมากที่สุดคือการคลิกลิงก์หรือเอกสารแนบที่เป็นอันตรายในอีเมลฟิชชิง อีเมลประเภทนี้ออกแบบมาให้ดูเป็นทางการ โดยมักจะดูเหมือนว่ามาจากบริษัทหรือองค์กรที่มีชื่อเสียง เมื่อคุณคลิกที่ลิงก์หรือเอกสารแนบ มันจะติดตั้งแรนซัมแวร์บนคอมพิวเตอร์ของคุณ อีกวิธีหนึ่งที่คุณอาจได้รับแรนซัมแวร์คือการไปที่เว็บไซต์ที่ถูกโจมตี เว็บไซต์เหล่านี้ถูกผู้โจมตีแฮกและใส่รหัสที่จะติดตั้งแรนซัมแวร์บนคอมพิวเตอร์ของคุณโดยอัตโนมัติหากคุณไปที่เว็บไซต์ คุณยังสามารถได้รับแรนซัมแวร์จากการดาวน์โหลดไฟล์ที่ติดไวรัสจากอินเทอร์เน็ต ซึ่งอาจเกิดขึ้นได้หากคุณดาวน์โหลดไฟล์จากเว็บไซต์ที่น่าสงสัยหรือหากคุณดาวน์โหลดไฟล์ที่แชร์จากผู้ที่คุณไม่รู้จัก กล่าวโดยสรุป สิ่งสำคัญคือต้องระมัดระวังเมื่อเรียกดูอินเทอร์เน็ต และหลีกเลี่ยงการคลิกที่ลิงก์ หรือดาวน์โหลดไฟล์จากแหล่งที่ไม่คุ้นเคย ซึ่งจะช่วยปกป้องคุณไม่ให้ได้รับแรนซัมอวร์และมัลแวร์ประเภทอื่นๆ

ใครคือเป้าหมายของแรนซัมแวร์

การโจมตีด้วยแรนซัมแวร์อาจมีเป้าหมายไปที่ใครก็ตามที่ใช้คอมพิวเตอร์หรืออุปกรณ์อื่นใดที่เชื่อมต่อกับอินเทอร์เน็ต อย่างไรก็ตาม บางกลุ่มจะมีแนวโน้มที่จะตกเป็นเป้าหมายมากกว่ากลุ่มอื่นๆ ตัวอย่างเช่น การโจมตีด้วยแรนซัมแวร์มักจะมีเป้าหมายที่ธุรกิจต่างๆ เนื่องจากมักจะมีข้อมูลที่มีมูลค่าและอาจจะต้องการจ่ายค่าไถ่เพื่อรับข้อมูลคืน โรงพยาบาล โรงเรียน และองค์กรอื่นๆ ที่ให้บริการสำคัญก็มักจะตกเป็นเป้าหมายด้วยเช่นกัน เนื่องจากการโจมตีด้วยแรนซัมแวร์อาจทำให้การทำงานหยุดชะงักและทำให้ชีวิตของผู้คนตกอยู่ในความเสี่ยง นอกจากนี้ปัจเจกบุคคลก็อาจตกเป็นเป้าหมายของการโจมตีด้วยแรนซัมแวร์ด้วย ในกรณีเหล่านี้ ผู้โจมตีอาจพยายามเรียกร้องเงินจากเหยื่อด้วยการขู่ว่าจะลบไฟล์ส่วนตัวหรือเผยแพร่ข้อมูลสำคัญ ยกเว้นว่าจะมีการจ่ายค่าไถ่ เป้าหมายของการโจมตีด้วยแรนซัมแวร์มักจะเลือกจากมูลค่าของข้อมูลและความต้องการที่จะจ่ายค่าไถ่เพื่อรับข้อมูลคืน

ความเสี่ยงของการจ่ายค่าไถ่ให้แรนซัมแวร์คืออะไร

การจ่ายค่าไถ่ให้กับผู้โจมตีด้วยแรนซัมแวร์อาจดูเหมือนเป็นวิธีที่ง่ายที่สุดในการรับไฟล์ของคุณคืน แต่อาจเป็นการตัดสินใจที่เสี่ยงมาก มีความเสี่ยงหลายอย่างที่เกี่ยวข้องกับการจ่ายค่าไถ่ รวมถึง:

- ไม่มีการรับประกันว่าผู้โจมตีจะให้คีย์ถอดรหัสมาจริงๆ ในหลายกรณี เหยื่อที่จ่ายค่าไถ่ไม่เคยได้รับคีย์และยังคงเข้าถึงไฟล์ของตนเองไม่ได้
- การจ่ายค่าไถ่อาจส่งเสริมผู้โจมตีให้โจมตีต่อไป หากผู้โจมตีทราบว่าเหยื่อต้องการจ่ายค่าไถ่ พวกเขาอาจมีแนวโน้มที่จะโจมตีมากขึ้นในอนาคต
- การจ่ายค่าไถ่อาจทำให้คุณเป็นเป้าหมายสำหรับการโจมตีในอนาคต หากผู้โจมตีทราบว่าคุณต้องการจ่ายค่าไถ่ คุณอาจมีแนวโน้มที่จะเป็นเป้าหมายในอนาคต
- การจ่ายค่าไถ่อาจผิดกฎหมาย ในบางกรณี การจ่ายค่าไถ่ให้กับองค์กรอาชญากรรมอาจถูกพิจารณาว่าเป็นรูปแบบหนึ่งของการให้ทุนกับการก่อการร้ายหรือกิจกรรมที่ผิดกฎหมายอื่นใด

ในขณะที่การจ่ายค่าไถ่ให้กับผู้โจมตีด้วยแรนซัมแวร์อาจดูเหมือนเป็นวิธีที่ง่ายที่สุดในการรับไฟล์ของคุณ แต่ที่จริงแล้วอาจเป็นการตัดสินใจที่เสี่ยงมาก การพิจารณาถึงความเสี่ยงอย่างรอบคอบก่อนตัดสินใจคือสิ่งสำคัญ

ราคาของแรนซัมแวร์มีเท่าใด

ราคาของการโจมตีแบบแรนซัมแวร์อาจแตกต่างกันเป็นอย่างมากโดยขึ้นอยู่กับปัจจัยต่างๆ เช่น ประเภทของแรนซัมแวร์ที่ใช้ จำนวนไฟล์ที่เข้ารหัส และผลของการโจมตี ในบางกรณี ราคาของการโจมตีด้วยแรนซัมแวร์อาจจะต่ำ เมื่อผู้โจมตีเรียกร้องค่าไถ่ไม่กี่ร้อยดอลลาร์ ในกรณีอื่นๆ ราคาอาจสูงกว่ามาก เมื่อผู้โจมตีเรียกค่าไถ่หลายพันดอลลาร์หรือมากกว่านั้นเพื่อกู้คืนการเข้าถึงไฟล์ของเหยื่อ นอกเหนือจากราคาโดยตรงที่เกี่ยวข้องกับการจ่ายค่าไถ่แล้ว การโจมตีด้วยแรนซัมแวร์ยังอาจมีค่าใช้จ่ายโดยอ้อมจำนวนมากอีกด้วย ตัวอย่างเช่น การโจมตีด้วยแรนซัมแวร์อาจทำให้เกิดเวลาหยุดทำงานและการสูญเสีย Productivity ซึ่งอาจส่งผลให้สูญเสียรายได้ นอกจากนี้ยังอาจทำให้บริษัทสูญเสียชื่อเสียงและความเชื่อมั่นของลูกค้า ซึ่งอาจส่งผลกระทบทางลบต่อธุรกิจเป็นระยะยาว บ่อยครั้งที่ค่าใช้จ่ายโดยอ้อมเหล่านี้สูงกว่าค่าไถ่มาก

อาการของแรนซัมแวร์มีอะไรบ้าง

อาการของแรนซัมแวร์อาจแตกต่างกันไปตามประเภทของแรนซัมแวร์ที่ใช้ อย่างไรก็ตาม อาการที่พบได้ทั่วไปมีดังนี้:

- ไฟล์ของคุณถูกเข้ารหัสและเข้าถึงไม่ได้
- คุณได้รับข้อความจากผู้โจมตี เรียกร้องให้ชำระค่าไถ่เพื่อแลกเปลี่ยนกับคีย์ถอดรหัส
- คุณเห็นโปรแกรมหรือการประมวลผลที่ไม่คุ้นเคยบนคอมพิวเตอร์ของคุณ
- คอมพิวเตอร์ของคุณทำงานช้าหรือไม่ตอบสนอง
- คอมพิวเตอร์ของคุณแสดงข้อความแสดงข้อผิดพลาดหรือหน้าต่างป๊อปอัพที่ไม่ปกติ

หากคุณสงสัยว่าคอมพิวเตอร์ของคุณติดแรนซัมแวร์ สิ่งสำคัญคือการดำเนินการโดยเร็ว ยกเลิกการเชื่อมต่อคอมพิวเตอร์ของคุณจากอินเทอร์เน็ตเพื่อป้องกันไม่ให้แรนซัมแวร์แพร่กระจาย

วิธีป้องกันการโจมตีจากแรนซัมแวร์เป็นอย่างไร

มีหลายขั้นตอนที่คุณสามารถทำเพื่อป้องกันการโจมตีด้วยแรนซัมแวร์ ได้แก่:

- ใช้ซอฟต์แวร์ป้องกันไวรัสหรือรักษาความปลอดภัยที่เชื่อถือได้ และอัปเดตอยู่เสมอ ซึ่งจะช่วยปกป้องคอมพิวเตอร์ของคุณจากแรนซัมแวร์และมัลแวร์ประเภทอื่นๆ
- ระมัดระวังเมื่อเปิดเอกสารแนบหรือลิงก์ในอีเมล แรนซัมแวร์มักจะถูกส่งผ่านอีเมลฟิชชิง ดังนั้นสิ่งสำคัญคือต้องระวังเกี่ยวกับสิ่งที่คุณคลิก
- อัปเดตระบบปฏิบัติการและซอฟต์แวร์อื่นๆ อยู่เสมอ การอัปเดตซอฟต์แวร์มักจะมีแพตช์ด้านความปลอดภัยซึ่งจะช่วยปกป้องคอมพิวเตอร์ของคุณจากแรนซัมแวร์และภัยคุกคามอื่นๆ ได้
- สำรองข้อมูลไฟล์ของคุณเป็นประจำ การทำเช่นนี้จะช่วยปกป้องข้อมูลของคุณหากคอมพิวเตอร์ของคุณติดแรนซัมแวร์ ตรวจสอบว่ามีการใช้หนึ่งในกลยุทธ์การสำรองข้อมูลที่แนะนำ เช่น กลยุทธ์การสำรองข้อมูล 3-2-1
- ระวังถึงความเสี่ยงของแรนซัมแวร์และให้การศึกษาผู้อื่นในองค์กรของคุณเกี่ยวกับภัยคุกคามเหล่านี้ ซึ่งจะช่วยป้องกันการโจมตีด้วยแรนซัมแวร์และช่วยให้ตรวจจับและตอบสนองได้ง่ายขึ้นหากถูกโจมตี

วิธีที่ดีที่สุดในการป้องกันการโจมตีด้วยแรนซัมแวร์คือการตื่นตัวอยู่เสมอ และใช้ขั้นตอนต่างๆ ในการปกป้องคอมพิวเตอร์และข้อมูลของคุณ ซึ่งจะช่วยลดความเสี่ยงของการโจมตีด้วยแรนซัมแวร์ และทำให้กู้คืนได้ง่ายหากเกิดขึ้น

Synology จะปกป้องฉันจากแรนซัมแวร์ได้อย่างไร

การดำเนินการป้องกันคือสิ่งสำคัญในการป้องกันจากการตกเป็นเหยื่อของแรนซัมแวร์ ใช้โซลูชัน Synology เหล่านี้เพิ่มเติมจากซอฟต์แวร์ป้องกันไวรัสที่คุณเลือก:

- **ป้องกันการเข้าถึง** — ลดการแพร่กระจายของแรนซัมแวร์โดยการตั้งค่าไฟล์ แอปพลิเคชัน และสิทธิ์การเข้าถึง และกำหนดค่าข้อมูลรับรองการลงชื่อเข้าใช้ที่ปลอดภัยโดยใช้ Secure SignIn และ C2 Password
- **ปกป้องอุปกรณ์** — ระบบที่ล้าสมัยจะมีความเสี่ยงมากกว่า อัปเดต NAS ทั้งหมดของคุณพร้อมกันด้วย Synology Central Management System (CMS) และปกป้องอุปกรณ์อื่นๆ ที่ใช้นโยบายกลุ่มใน Synology Directory Server และ C2 Identity
- **หลีกเลี่ยงไฟล์ที่น่าสงสัย** — อีเมลสแปมและฟิชชิงที่มีไฟล์ที่น่าสงสัยคือวิธีแพร่กระจายแรนซัมแวร์ที่พบได้ทั่วไป Synology MailPlus ให้การปกป้องจากมัลแวร์และการป้องกันจากสแปมที่แข็งแกร่ง
- **ตรวจสอบช่องโหว่** — ใช้ Synology Security Advisor ในการสแกนหามัลแวร์ ช่องโหว่ และกิจกรรมการลงชื่อเข้าใช้ที่ผิดปกติเป็นประจำ ขอแนะนำให้ใช้งานเพื่อปรับปรุงความปลอดภัย NAS ของคุณ https://www.synology.com/dsm/overview/security

วิธีอื่นๆ ในการปกป้องข้อมูลของคุณ

จัดการฟลีทของคุณ

ใช้ประโยชน์จากฟีเจอร์ที่ครอบคลุมเพื่อจัดการสิทธิ์การเข้าถึงข้อมูล สถานะซอฟต์แวร์ สถานภาพของระบบ และอื่นๆ จากศูนย์กลาง
https://www.synology.com/dsm/overview/administration

ตรวจสอบระบบทั้งหมดของคุณ

ระบบกิจกรรมการลงชื่อเข้าใช้ที่น่าสงสัย จัดการอัปเดต และตรวจสอบสถานภาพของอุปกรณ์ ไม่ว่าอุปกรณ์ของคุณจะอยู่ที่ใด
https://www.synology.com/dsm/feature/active-insight

ปกป้องข้อมูลของคุณ

ทำตามกฎการสำรองข้อมูล 3-2-1 เพื่อปกป้องข้อมูลของคุณจากการแก้ไขหรือการลบที่ไม่ได้ตั้งใจและเป็นอันตราย
https://www.synology.com/dsm/solution/data_backup

เริ่มต้น

ติดต่อเรา

ติดต่อฝ่ายขายในภูมิภาคสำหรับข้อมูลเพิ่มเติม
https://www.synology.com/form/inquiry/sales

แหล่งจำหน่าย

ค้นหาคู่ค้า Synology ในภูมิภาคของคุณ
https://www.synology.com/wheretobuy

หมายเหตุ:

1. eSentire, 2022 Official Cybercrime Report
   https://www.esentire.com/resources/library/2022-official-cybercrime-report

ปกป้ององค์กรของคุณจากแรนซัมแวร์

https://www.synology.com/th-th/dsm/solution/ransomware

เว็บไซต์ Synology

https://www.synology.com/

ติดต่อเรา

https://www.synology.com/company/contact_us