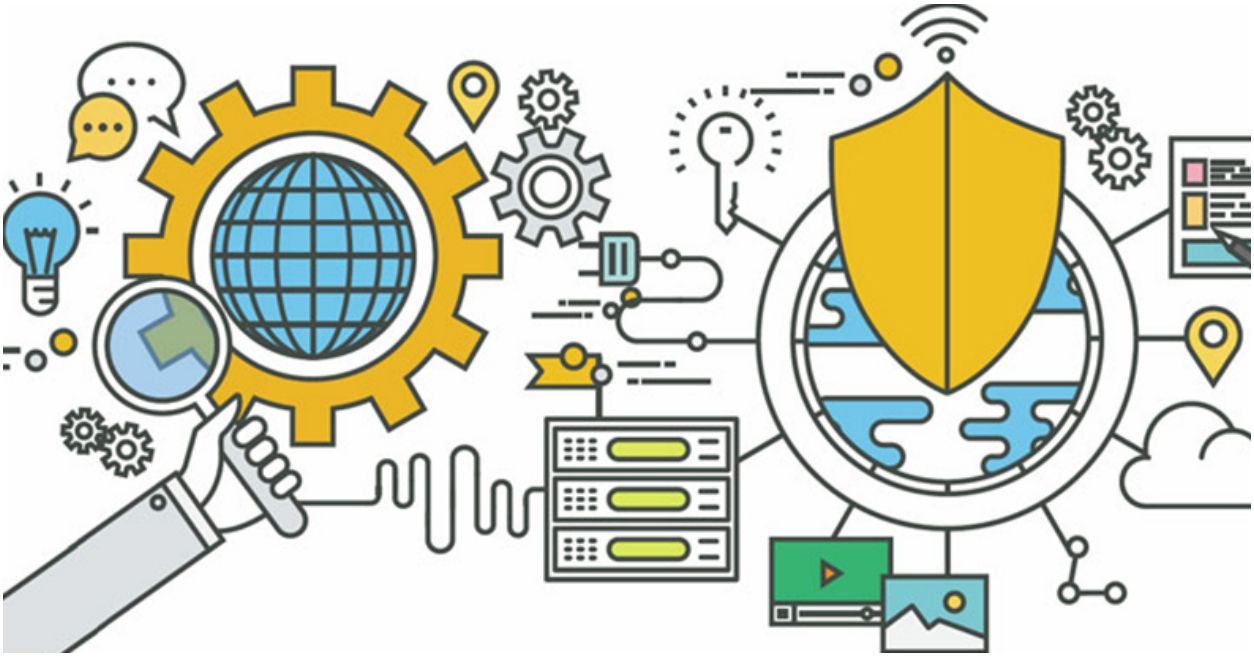
10 วิธีป้องกัน Ransomware ก่อนมันมาถึงตัว



ภัยคุกคามที่กำลังเป็นประเด็นในทุกวันนี้คงหนีไม่พ้นเรื่องของ Ransomware องค์กรต่างๆ ได้เริ่มโดนพิษร้ายของมันไปกันแล้ว บางองค์กรต้องยอมจ่ายเงินค่าไถ่เพื่อแลกกับไฟล์สำคัญที่โดนล็อกเอาไว้ตลอดจนไม่อยากที่จะเสียชื่อเสียงขององค์กรออกไปด้วย แม้ว่า ณ ตอนนี้ยังไม่มีเครื่องมือตัวไหนที่จะสามารถปลดล็อกคีย์ของ Ransomware ได้ทั้งหมดก็ตาม แต่เราก็สามารถที่จะป้องกันไม่ให้เกิดเหตุการณ์ที่จะทำให้คุณติดภัยร้ายนี้ได้ ครั้งนี้เรามี 10 วิธีการป้องกันตัวเองจากภัยคุกคามที่เรียกกันว่า Ransomware

1. วางแผนแบ็กอัพไฟล์

วางแผนและพัฒนาระบบแบ็กอัพและกู้คืนข้อมูลให้ต่อเนื่องและมีประสิทธิภาพ และเก็บข้อมูลแบบออฟไลน์เอาไว้บนอุปกรณ์แยกอีกต่างหาก

2. ใช้ทูลที่มีประสิทธิภาพ

ใช้เครื่องมือรักษาความปลอดภัยเว็บและอีเมล์ที่สามารถวิเคราะห์เมล์, เว็บ และไฟล์ที่แฝงไปด้วยมัลแวร์ ตลอดจนบล็อกโฆษณาที่อาจจะแฝงภัยร้ายมาได้ ซึ่งเครื่องมือเหล่านี้รวมไปถึงพวก Sandbox ที่สามารถวิเคราะห์ภัยคุกคามพร้อมสร้างสภาพแวดล้อมให้ปลอดภัยได้

3. อัพเดตแพทช์ในอุปกรณ์

พยายามที่จะอัพเดตหรือแพทช์ความปลอดภัยต่างๆ อย่างต่อเนื่อง ไม่ว่าจะเป็น โอเอส, อุปกรณ์, ซอฟต์แวร์ ฯลฯ

4. อัพเดตซอฟต์แวร์ความปลอดภัย

ตรจสอบว่าพวกแอนตี้ไวรัสทั้งบนอุปกรณ์และเครือข่ายต่างๆ นั้นอัพเดตล่าสุดตลอดเวลา

5. ใช้แอพพลิเคชันที่ปลอดภัย

ถ้าเป็นไปได้ให้ใช้แอพพลิเคชันในลิสต์ที่มีความปลอดภัย และป้องกันแอพพลิเคชันที่ไม่ได้รับการรับรองการทำงาน (จากการดาวน์โหลด)

6. แบ่งเครือข่ายออกเป็นโซน

แบ่งเครือข่ายความปลอดภัยออกเป็นโซนๆ ซึ่งหากโซนใดโซนหนึ่งเกิดติดภัยร้าย มันก็จะไม่ลามไปยังส่วนอื่นอย่างง่าย (ซึ่งเราก็สามารถแก้ปัญหาเป็นส่วนๆ ได้)

7. กำหนดสิทธิ์และบังคับใช้

ทำการสร้างและบังคับใช้สิทธิ์ในการทำงาน โดยให้ระมัดระวังไม่ให้ยูสเซอร์จำนวนต่างๆ ไปมีผลกระทบหรือติดเชื้อลามไปยังพวกแอพพลิเคชันด้านธุรกิจ,ข้อมูล หรือเซอร์วิสต่างๆ ขององค์กร

8. จัดการเรื่อง BYOD

กำหนดนโยบายความปลอดภัยในส่วนของ BYOD ให้ชัดเจน จะช่วยทำให้คุณสามารถตรวจสอบและทำการบล็อกอุปกรณ์ ซึ่งอาจจะไม่ผ่านมาตรฐานด้านซีเคียวริตี้ขององค์กร (เช่น อาจจะไม่มีติดตั้งซอฟต์แวร์ป้องกันมัลแวร์, แอนตี้ไวรัสไม่อัพเดต, ระบบปฏิบัติการไม่ได้อุดแพทช์ และอื่นๆ เป็นต้น)

9. ใช้งานพวกเครื่องมือวิเคราะห์ภัยร้าย

ใช้เครื่องมือในการวิเคราะห์ภัยร้ายในแบบเชิงลึก เพื่อตรวจสอบการติดเชื้อภัยคุกคาม ไม่ว่าจะเป็น
1) ในจุดที่ภัยเข้ามา
2) ระยะเวลาที่ติดเชื่อในองค์กรของคุณว่านานเท่าใด
3) การลบพวกมันออกจากดีไวซ์ต่างๆ และ
4) วิธีการที่จะให้คุณแน่ใจว่ามันจะไม่กลับมาอีก

10. อบรมพนักงาน

ให้ความรู้แก่พนักงาน ให้พวกเขาได้เรียนรู้ถึงเรื่องความปลอดภัย และพยายามอย่าคลิกไฟล์ที่แปลกประหลาด, หรือไฟล์ที่แนบมากับอีเมล์ที่ไม่คุ้นเคย หรือไม่เข้าไปตามเว็บที่ส่งมาทางอีเมล์ ซึ่งต้องบอกว่ามนุษย์นี้แหล่ะคือต้นตอแห่งช่องโหว่ต่างๆ ที่เกิดขึ้น