Daily News Online

วันที่ 12 กุมภาพันธ์ พ.ศ. 2552
http://www.dailynews.co.th/

20 ช่องโหว่ที่ผู้ใช้คอมพ์ต้องระวัง

ในโอกาสครบ 20 ปี บริษัท เทรนด์ ไมโคร ได้จัดทำรายงานสรุป 20 อันดับช่องโหว่ความปลอดภัยในโลกดิจิทัลปัจจุบัน พร้อมเสนอแนวทางการป้องกันภัยคุกคามข้อมูล

20 อันดับช่องโหว่ความปลอดภัยในโลกดิจิทัลปัจจุบัน

1. เว็บเบราว์เซอร์ที่มีช่องโหว่หรือไม่ได้ติดตั้งโปรแกรมซ่อมแซม 2. ระบบปฏิบัติการที่มีช่องโหว่หรือไม่ได้ติดตั้งโปรแกรมซ่อมแซม 3. เว็บไซต์/เว็บเพจ หรือจาวาสคริปต์ที่มีช่องโหว่หรือไม่ได้ติดตั้งโปรแกรมซ่อมแซม 4. ซอฟต์แวร์สำรองข้อมูล 5. ซอฟต์แวร์ฐานข้อมูล 6. อีเมล ไคลเอ้นต์ 7. สิทธิใช้งาน ของผู้ใช้ที่มีมากเกินความจำเป็น 8. โปรแกรม สนทนาออนไลน์ 9. เซิร์ฟเวอร์บริหารจัดการ 10. โปรแกรมเพื่อความบันเทิง (ฟังเพลง, ดูหนัง) 11. ซอฟต์แวร์สำนักงาน 12. โปรแกรมแบบเพียร์ทูเพียร์ 13. ซอฟต์แวร์ด้านความปลอดภัย 14. ชุมชนเครือข่ายสังคมออนไลน์ 15. อุปกรณ์ที่ไม่ได้รับอนุญาต 16. แล็ปท็อปที่ไม่ได้เข้ารหัสลับ 17. สื่อที่ใช้บันทึกข้อมูลที่ไม่ได้เข้ารหัสลับ 18. ระบบปฏิบัติการยูนิกซ์ (Unix) 19. บริการ VoIP 20. เซิร์ฟเวอร์ และแอพพลิเคชั่นโทรศัพท์ผ่านอินเทอร์เน็ต

แนวทางการป้องกันภัยคุกคามข้อมูล

1. เปิดใช้งานและปรับปรุงซอฟต์แวร์รักษาความปลอดภัยให้ทันสมัยเสมอ โดยเฉพาะถ้าใช้งานแล็ปท็อปที่ต้องเชื่อมต่อกับเครือข่ายที่ไม่มีการป้องกันใด ๆ ในบริเวณสนามบิน ร้านกาแฟ และสถานที่ต่าง ๆ
2. ติดตั้งผลิตภัณฑ์และโซลูชั่นที่ปกป้องผู้ใช้งานในทุกกรณีไม่ว่าจะท่องอินเทอร์เน็ตหรือดาวน์โหลดไฟล์ลงในคอมพิวเตอร์โดยตรง
3. ตรวจสอบให้แน่ใจว่าซอฟต์แวร์ป้องกันภัยบนเว็บครอบคลุมการป้องกันอีเมล รวมถึงเครือข่ายแบบเพียร์ทูเพียร์ และแอพ พลิเคชั่นการประมวลผลที่ใช้ทั้งหมด และ สามารถแจ้งเตือนเกี่ยวกับปริมาณการส่งผ่าน ข้อมูลทั้งเข้าและออกจากคอมพิวเตอร์ของผู้ใช้งานในเวลาจริง
4. ปรับใช้เทคโนโลยีล่าสุด เช่น การป้องกันโดยเทคโนโลยีการตรวจสอบชื่อเสียง และประวัติเว็บไซต์ (Web Reputation) ซึ่งสามารถวัดระดับความปลอดภัย และความน่าเชื่อถือของเว็บไซต์ก่อนที่คุณจะเข้าเยี่ยมชมได้ ควรใช้เทคโนโลยีการตรวจสอบประวัติเว็บร่วมกับเทคโนโลยีการกรองยูอาร์แอล (URL) และการสแกนเนื้อหา
5. ใช้เว็บเบราว์เซอร์รุ่นล่าสุดและติดตั้งโปรแกรมปรับปรุงความปลอดภัยเมื่อพร้อมใช้งาน
6. ใช้เว็บเบราว์เซอร์ที่มีปลั๊กอินป้องกันสคริปต์
7. ตรวจสอบกับผู้ให้บริการอินเทอร์เน็ตว่าเครือข่ายของผู้ให้บริการใช้การป้องกันชนิดใด
8. ถ้าใช้ระบบปฏิบัติการไมโครซอฟต์ วินโดว์ ให้เปิดใช้งานคุณลักษณะ "ปรับปรุงอัตโนมัติ" (Automatic Update) และติดตั้งโปรแกรมปรับปรุงใหม่ ๆ ทันทีที่พร้อมใช้งาน
9. ติดตั้ง ปรับปรุง และดูแลไฟร์วอลล์ รวมทั้งซอฟต์แวร์ป้องกันการบุกรุกเสมอ ซึ่งครอบคลุมการป้องกันมัลแวร์หรือสปายแวร์ด้วย
10. ตรวจสอบให้แน่ใจว่าโซลูชั่น ซอฟต์แวร์รักษาความปลอดภัยที่ใช้งานอยู่เป็นรุ่นล่าสุด

ผู้ใช้งานคอมพิวเตอร์และอินเทอร์เน็ตที่สนใจอยากทราบข้อมูลเกี่ยวกับภัยคุกคาม ใหม่ ๆ ที่เกิดขึ้นคลิกไปได้ที่ http://blog.trendmicro.com/

ที่มา : http://www.dailynews.co.th/web/html/popup_news/Default.aspx?Newsid=190648&NewsType=1&Template=1