Matichon Online
วันที่ 19 พฤศจิกายน พ.ศ. 2551
http://www.matichon.co.th/

แนวโน้มโลก "ไอที" ปี 2552 โกลบอลเทคโนโลยี อินทิเกรเทด

คอมพิวเตอร์ เครือข่ายอินเตอร์เน็ต มีบทบาทในโลกธุรกิจยิ่งขึ้น เพราะช่วยเพิ่มประสิทธิภาพการทำงาน ลดค่าใช้จ่ายโดยรวมขององค์กรลงอย่างได้ผล ยิ่งเศรษฐกิจโลกเข้าสู่ภาวะถดถอย สิ่งที่น่าจะเห็นในอนาคตอันใกล้คือการนำระบบเทคโนโลยีสารสนเทศมาใช้แทนแรงงานคน เกิดการขยายตัวของรูปแบบการทำงานที่บ้าน โดยอาศัยการเชื่อมต่ออินเตอร์เน็ต การทำงานแบบไร้กระดาษ ตลอดจนธุรกิจอี-คอมเมิร์ซ ทวีจำนวนขึ้น

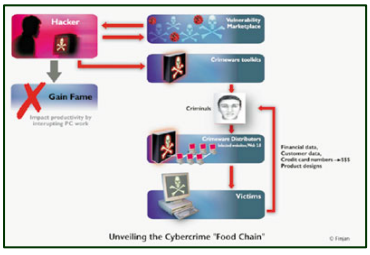
เหตุนี้แนวโน้มธุรกิจกับการวัดคุณค่าขององค์กรจึงมีแนวโน้มเปลี่ยนไป จากเดิมวัดที่ขนาดองค์กรและจำนวนพนักงาน มาเป็นวัดประสิทธิภาพบุคลากร องค์กรใหญ่จะแตกออกเป็น profit center หรือ business unit มากขึ้น จึงต้องเตรียมความพร้อม สิ่งที่ต้องตระหนักถึงและเตรียมรับมือให้พร้อม คือ

แนวโน้มเทคโนโลยีด้านความมั่นคงปลอดภัย

- เทคโนโลยี Two-Factor Authentication เป็นการระบุตัวตนในโลกอินเตอร์เน็ต ส่วนใหญ่ใช้เพียง username และ password ซึ่งเป็นจุดอ่อนที่มิจฉาชีพอาจขโมยข้อมูลและปลอมตัวเพื่อแสวงประโยชน์ได้ (Identity Threat) เทคโนโลยีจึงมีแนวโน้มอุดช่องโหว่ ด้วยการใช้ Token หรือ Smart card ID มาเสริมเพื่อเพิ่มปัจจัยในการพิสูจน์ตัวตน โดยเฉพาะกับการทำธุรกรรมทางการเงินออนไลน์ และธุรกิจอี-คอมเมิร์ซ

-เทคโนโลยี Single Sign On (SSO) เข้าระบบต่างๆ ด้วยรายชื่อเดียวเชื่อมทุกแอพพลิเคชั่นเข้าด้วยกัน จำเป็นมากในยุค Social Networking ช่วยให้เราไม่ต้องจำ username / password จำนวนมาก สำหรับอี-เมล chat, web page รวมถึงการใช้บริการ Wi-Fi / Bluetooth / WiMAX / 3G / 802.15.4 เป็นต้น

- เทคโนโลยี Cloud Computing เมื่อมีการเก็บข้อมูลและใช้งานแอพพลิเคชั่นต่างๆ มากขึ้นตามการขยายตัวของระบบงานไอที ส่งผลให้เครื่องแม่ข่ายต้องประมวลผลการทำงานขนาดใหญ่ ในเวลาอันรวดเร็ว จึงมีแนวคิดเทคโนโลยี Clustering เพื่อแชร์ทรัพยากรการประมวลผลที่ทำงานพร้อมกันหลายเครื่องได้ เรียกว่า Cloud Computing ทำให้ผู้ใช้สามารถใช้งานแอพพลิเคชั่นได้รวดเร็วยิ่งขึ้น ปราศจากข้อจำกัดทางกายภาพ เข้าสู่ยุคโลกเสมือนจริงทางคอมพิวเตอร์ (visualization) ทั้งยังช่วยลดทรัพยากรของเครื่องคอมพิวเตอร์ ถือเป็นไอทีที่เป็นมิตรกับสิ่งแวดล้อม (Green IT) อีกด้วย



- เทคโนโลยี Information Security Compliance Law โลกไอทีเจริญเติบโตไม่หยุดนิ่ง ด้วยมาตรฐานที่หลากหลาย ระบบความปลอดภัยข้อมูลสารสนเทศจึงมีแนวโน้มจัดมาตรฐานเป็นหมวดหมู่ เพื่อความปลอดภัยข้อมูลในองค์กร โดยนำ Log ที่เกิดขึ้นจากการใช้งานมาจัดเปรียบเทียบตามมาตรฐานต่างๆ เช่น ISO27001 สำหรับความปลอดภัยในองค์กร, PCI / DSS สำหรับการทำธุรกรรมการเงิน พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อสืบหาผู้กระทำความผิด เป็นต้น

- เทคโนโลยี Wi-Fi Mesh Connection ใช้งานระบบอินเตอร์เน็ตไร้สาย ต้องเชื่อมโยงผ่าน Access Point สามารถเชื่อมต่อแบบ Mesh (ตาข่าย) เข้าถึงโลกออนไลน์ได้สะดวกขึ้น ผู้ให้บริการ Wi-Fi ก็มีแนวโน้มใช้แอพพลิเคชั่นในการเก็บบันทึกการใช้งานผู้ใช้ (Accounting Billing) และนำระบบ NIDS (Network Intrusion Detection System) มาใช้ เพื่อเฝ้าระวังการบุกรุกหลากรูปแบบ เช่น การดักข้อมูล, การ crack ค่า wireless เพื่อเข้าถึงระบบ หรือปลอมตัวเป็นบุคคลอื่นโดยมิชอบ เป็นต้น

- เทคโนโลยีป้องกันทางเกตเวย์แบบรวมศูนย์ (Unified Threat Management) แม้เทคโนโลยีนี้จะใช้กันอย่างแพร่หลายในปัจจุบัน แต่ต้องกล่าวถึงเนื่องจากธุรกิจในอนาคตมีแนวโน้มเป็นเอสเอ็มอีมากขึ้น เทคโนโลยีนี้ถือว่ามีประโยชน์กับธุรกิจขนาดเล็ก เพราะผนวกการป้องกันในรูปแบบ Firewall / Gateway เทคโนโลยีป้องกันข้อมูลขยะ (Spam) การโจมตีของ Malware/virus/worm การใช้งานเว็บไซต์ที่ไม่เหมาะสม (Content filtering) รวมอยู่ในอุปกรณ์เดียว

ต่อด้านหลัง

- เทคโนโลยีเฝ้าระวังเชิงลึก (Network Forensics) การกลายพันธุ์ของ Virus/worm computer ทำให้ยากแก่การตรวจจับด้วยเทคนิคเดิม รวมถึงพนักงานในองค์กรมีทักษะการใช้คอมพิวเตอร์สูงขึ้น ซึ่งอาจจะใช้ทักษะไปในทางที่ไม่เหมาะสม หรือเรียกได้ว่าเป็น "Insider hacker" การมีเทคโนโลยีเฝ้าระวังเชิงลึกจึงจำเป็นอย่างยิ่งในการตรวจจับสิ่งผิดปกติที่อาจเกิดขึ้นผ่านระบบเครือข่าย เพื่อใช้ในการพิสูจน์หาหลักฐานทางอิเล็กทรอนิกส์ประกอบการดำเนินคดี

- เทคโนโลยี Load Balancing Switch สำหรับ Core Network เพื่อใช้ในการป้องกันการสูญหายของข้อมูล (Data loss) โดยเฉพาะในอนาคตที่ความเร็วในการรับส่งข้อมูลบนระบบเครือข่ายจะสูงขึ้น เทคโนโลยีนี้จะช่วยกระจายโหลดไปยังอุปกรณ์ป้องกันภัยอื่นๆ ได้ เช่น Network Firewall หรือ Network Security Monitoring และอื่นๆ โดยไม่ทำให้ข้อมูลสูญหาย

แนวโน้มภัยคุกคาม

ภัยคุกคามที่น่าจะเกิดขึ้นในปี 2552 คงไม่ต่างจากปี 2551 แต่จะมีเทคนิคใหม่ เพิ่มความสลับซับซ้อนขึ้น ด้วยช่องทางการเข้าถึงข้อมูลที่หลากหลายยิ่งขึ้นยิ่งเรื่อง Personal Mobile Devices ที่ใช้มือถือเชื่อมต่ออินเตอร์เน็ต และมีการใช้ซอฟต์แวร์ต่างๆ ผ่านเว็บแอพพลิเคชั่นมากขึ้น เกิดภัยคุกคามในรูปแบบที่เรียกว่า Zombie หรือ "ผีดิบซอฟต์แวร์" จำนวนมาก รวมเรียกว่า Botnet อนาคตผีดิบพวกนี้จะมาจากมือถือด้วย ก่อให้เกิดการโจมตีในหลายรูปแบบ เช่น DDoS/DoS ทำให้เป้าหมายไม่สามารถปฏิบัติงานได้ การส่งสแปม การหลอกลวงผ่านสื่ออินเตอร์เน็ต (Phishing) การเจาะระบบ (Hack) เพื่อเข้าถึงข้อมูลชั้นความลับ วันนี้แฮกเกอร์ไม่ได้มีเป้าหมายเจาะระบบเครือข่ายธนาคารหรือผู้ให้บริการธุรกรรมออนไลน์ แต่เปลี่ยนเป้าหมายเป็นผู้ใช้งานอินเตอร์เน็ต ซึ่งเข้าถึงได้ง่ายกว่าแทน อาศัยความรู้เท่าไม่ถึงการณ์ของผู้ใช้งานทั่วไปเป็นเครื่องมือ สิ่งเหล่านี้ป้องกันได้หากรู้เท่าทันภัยคุกคามดังกล่าว...โดยเริ่มต้นจากตัวเราเอง

ทำอย่างไรให้รู้เท่าทันและไม่ตกเป็นเหยื่อภัยคุกคามสมัยใหม่ ?

1. หมั่นดูแลเครื่องคอมพิวเตอร์ เครื่องบรรจุข้อมูล (Thumb Drive) และแผ่นบันทึกข้อมูลเสมอ ให้ปลอดจากไวรัสหรือมัลแวร์ต่างๆ กำหนดรหัสผ่านเข้าใช้งานพีซี และ ธัมป์ไดร์ฟ ล็อคหน้าจอทุกครั้งเมื่อเลิกใช้งาน

2. ตั้งรหัสผ่านที่ยากแก่การคาดเดา อย่างน้อย 8 ตัวอักษร และมีอักขระพิเศษ คำที่ใช้เป็น password ไม่ควรตรงกับพจนานุกรม เลี่ยงภัยคุกคามที่เรียกว่า Brute force password จากผู้ไม่ประสงค์ดี

3. อย่าไว้วางใจเมื่อเห็นสัญญาณอินเตอร์เน็ตที่ให้บริการฟรี ไม่ว่าจะเป็นระบบไร้สาย มีสาย โปรแกรมต่างๆ ที่ให้ดาวน์โหลดฟรี เพราะมิจฉาชีพอาจให้โดยตั้งใจใช้ดักข้อมูลส่วนตัวของเรา นำไปใช้สร้างความเสียหายได้

4. อย่าไว้วางใจโปรแกรมประเภทที่มีชื่อดึงดูดใจให้ดาวน์โหลดฟรี เช่น คลิปฉาว โปรแกรม Crack Serial Number โปรแกรมเร่งความเร็ว เป็นต้น บ่อยครั้งที่มีของแถม เช่น มัลแวร์พ่วงมาด้วยเสมอ ทำให้ตกเป็นเหยื่อของมิจฉาชีพโดยไม่รู้ตัว

5. แง่บุคคล ควรหมั่นเก็บสำรองข้อมูลในสตอเรจ (Storage) ส่วนตัว อย่าให้สูญหาย กรณีเกิดเหตุฉุกเฉินขึ้นสามารถหยิบมาใช้ได้ทันท่วงที ในองค์กรควรให้ความสำคัญทำแผนสำรองข้อมูลฉุกเฉิน ทั้งการทำ Business Continuity Plan (BCP) และ Disaster Recovery Plan (DRP)

6. ใช้ชีวิตไม่ยึดติดกับสื่ออิเล็กทรอนิกส์ ที่เข้าครอบงำชีวิตคนยุคใหม่มากขึ้นไม่ถลำลึกบนโลก-สังคมเสมือน ต้องป้องกันโดยการยับยั้งชั่งใจ และสร้างสมดุลให้กับชีวิต

7. ใช้วิจารณญาณไตร่ตรองข้อมูลทางอินเตอร์เน็ต โดยตั้งสติและมองเหตุผลให้รอบด้าน เพื่อป้องกันตัวเองจากการล่อลวงผ่านทางอี-เมล เว็บไซต์

8. มีจริยธรรมในการใช้สื่ออินเตอร์เน็ต เอาใจเขามาใส่ใจเราทุกครั้ง เพื่อผลดีในระยะยาว ทั้งช่วยโอบอุ้มสังคมให้สงบสุข ปลอดภัยในการใช้สื่ออินเตอร์เน็ตต่อไป

มติชนรายวัน วันที่ 19 ธันวาคม พ.ศ. 2551 ปีที่ 31 ฉบับที่ 11241 หน้า 26

ที่มา :
http://www.matichon.co.th/matichon/view_news.php?newsid=01epe01191251&sectionid=0147&day=2008-12-19