กรุงเทพธุรกิจ
ปีที่ 25 ฉบับที่ 8511 วันพุธที่ 11 มกราคม พ.ศ.2555 หน้า 28

ภัยคุกคามไซเบอร์ ยุคหลังพีซี โจมตี..ซับซ้อนกว่าเดิม!!

นักวิเคราะห์เครือข่ายภัยคุกคามจากทั่วโลก ระบุว่า ปี 2555 นี้ จะยังคงมีอาชญากรรมเกิดขึ้นอย่างต่อเนื่อง และมีความซับซ้อนยิ่งขึ้นกว่าเดิม เนื่องมาจากการที่โลกได้เปลี่ยนผ่านจากยุคพีซีตั้งโต๊ะมาเป็นการประมวลผลแบบคลาวด์ และผ่านระบบมือถือ

ปรากฏการณ์ดังกล่าวทำให้ผู้ดูแลระบบไอทีกลายเป็นบุคคล ที่มีความสำคัญอย่างมากในการดำเนินการด้านการรักษาความปลอดภัย ภายใต้กรอบการทำงานที่เน้นข้อมูลเป็นศูนย์กลาง ซึ่งหมายถึงการปกป้องข้อมูลที่ไม่ใช่เพียงแค่การป้องกันระบบเท่านั้น

"ไรมันด์ จีนส์" ประธานเจ้าหน้าที่ฝ่ายเทคโนโลยี (ซีทีโอ) บริษัทเทรนด์ ไมโคร เปิดเผยรายงาน **"การคาดการณ์ 12 ภัยคุกคามความปลอดภัยปี 2555"** ที่ให้รายละเอียดครอบคลุม 4 ส่วน ได้แก่ แนวโน้มไอทีขนาดใหญ่ มุมมองด้านมือถือ มุมมองด้านภัยคุกคาม และการละเมิดและการรั่วไหลของข้อมูล

12 ภัยคุกคามที่คาดว่าจะพบเจอมากขึ้นปีนี้ แนวโน้มความท้าทายที่จะเกิดขึ้นที่ผู้ควบคุมระบบไอทีองค์กร ผู้ใช้คอมพิวเตอร์ รวมถึงอุปกรณ์เคลื่อนที่ต่างๆ และคอโซเชียล เน็ตเวิร์ค ไม่ควรมองข้ามมีดังต่อไปนี้

1. ความท้าทายที่แท้จริงสำหรับเจ้าของศูนย์ข้อมูล คือ การจัดการกับความซับซ้อนด้านการรักษาความปลอดภัยที่เพิ่มขึ้นอย่างมากทั้งในระบบจริง ระบบเสมือน และระบบคลาวด์ แม้ว่าการโจมตีที่ตั้งเป้าไปที่เครื่องเสมือน (VM) และบริการประมวลผลแบบคลาวด์เป็นพิเศษจะยังคงมีความเป็นไปได้สูง แต่ผู้โจมตีไม่จำเป็นต้องค้นหาตัวช่วยใดๆ เนื่องจากพวกเขาสามารถใช้เทคนิคการโจมตีทั่วไปได้กับระบบใหม่ๆ เหล่านี้

การโจมตีแพลตฟอร์มเสมือนและคลาวด์ ถือเป็นเรื่องง่ายแต่ยุ่งยากในการป้องกัน ดังนั้น ภาระทั้งหมดจึงตกอยู่ที่ผู้ดูแลระบบไอทีซึ่งจะต้องรักษาข้อมูลสำคัญของบริษัทให้ปลอดภัย เมื่อพวกเขานำเทคโนโลยีเหล่านี้เข้ามาใช้งานในองค์กร

2. เหตุการณ์ด้านการละเมิดข้อมูลและความปลอดภัยในปีนี้ จะบังคับให้บริษัทต่างๆ ทั่วโลกต้องพบกับความท้าทายที่เกี่ยวข้องกับ "ยุคแห่งการบริโภคเทคโนโลยี" หรือ ที่เรียกว่า **BYOD (Bring-Your-Own-Device: BYOD)** หรือการนำอุปกรณ์ส่วนตัวเข้ามาใช้และเชื่อมต่อกับเครือข่ายองค์กรมาถึงแล้ว และการที่ข้อมูลขององค์กรจำนวนมากได้รับการจัดเก็บ หรือเข้าถึงข้อมูลด้วยอุปกรณ์ส่วนตัวที่ไม่ได้รับการควบคุมอย่างครอบคลุมจากผู้ดูแลระบบไอที อาจส่งผลให้เกิดการสูญเสียข้อมูลเพิ่มสูงขึ้น อันมีสาเหตุมาจากการรักษาความปลอดภัยสำหรับอุปกรณ์ส่วนตัวที่ไม่เหมาะสม

[ต่อด้านหลัง]

3. ช่องโหว่ด้านความปลอดภัยจะพบได้ในแอพพลิเคชั่นมือถือที่ถูกกฎหมาย ทำให้อาชญากรไซเบอร์สามารถดึงข้อมูลออกมาได้ง่ายยิ่งขึ้น โดยปกติแล้ว ภัยคุกคามแพลตฟอร์มมือถือจะมาในรูปของโปรแกรมที่เป็นอันตราย แต่จากการพัฒนาที่เกิดขึ้นอย่างต่อเนื่อง มีการคาดการณ์ว่า อาชญากรไซเบอร์จะสามารถเจาะระบบโปรแกรมค้นหาช่องโหว่ หรือข้อผิดพลาดในการเขียนโค้ด ที่สามารถนำไปสู่การเปิดเผยข้อมูลหรือขโมยข้อมูลออกมาได้

4. การเพิ่มจำนวนของกลุ่มแฮคเกอร์จะเป็นสาเหตุของภัยคุกคามที่ใหญ่ขึ้นสำหรับองค์กรที่ต้องการปกป้องข้อมูลที่มีความสำคัญระดับสูงของตน กลุ่มออนไลน์ เช่น Anonymous และ LulzSec มีบทบาทอย่างมากในปี 2554 เนื่องจากได้ตั้งเป้าโจมตีไปที่บริษัทและรายบุคคลด้วยเหตุผลทางการเมืองต่างๆ ซึ่งดูเหมือนว่ากลุ่มวายร้ายเหล่านี้ จะมีแนวโน้มเพิ่มจำนวนมากขึ้นในปี 2555 โดยพวกเขาจะมีทักษะเพิ่มขึ้นทั้งด้านการแทรกซึมองค์กรและหลีกเลี่ยงการตรวจจับจากผู้เชี่ยวชาญด้านไอทีและหน่วยงานบังคับใช้กฎหมายต่างๆ

5. การกำเนิดของเครือข่ายสังคมออนไลน์ใหม่ทำให้ "ความเป็นส่วนตัว" ต้องถูกให้คำนิยามใหม่ ผู้ใช้เครือข่ายสังคมออนไลน์รุ่นใหม่มีทัศนคติที่แตกต่างไปจากเดิม ต่อการป้องกัน และการแบ่งปันข้อมูล โดยพวกเขามีแนวโน้มที่จะเปิดเผยข้อมูลส่วนตัวทางออนไลน์ให้แก่ผู้ชมในวงกว้างนอกเหนือจากเพื่อนของตน ในเวลานี้ บุคคลที่ตระหนักถึงความเป็นส่วนตัวจะเป็นกลุ่มคนกลุ่มน้อย จึงเป็นโอกาสที่ดีอย่างยิ่งสำหรับผู้โจมตี