การรักษาความปลอดภัยระดับเอ็นเตอร์ไพรส์ในยุคโมไบล์และคอมพิวเตอร์ระบบคลาวด์

การรักษาความปลอดภัยระดับเอ็นเตอร์ไพรส์ในยุคโมไบล์และคอมพิวเตอร์ระบบคลาวด์ โดย ปิแอร์ โนแอลหัวหน้าคณะเจ้าหน้าที่บริหารด้านรักษาความปลอดภัยและที่ปรึกษา งานด้านความปลอดภัย บริษัทMicrosoft Asia และ ผู้บรรยายในงาน CommunicAsia2016 Summit

ภายในปี 2020 จะมีผู้คนมากกว่า 4 พันล้านคนเข้าสู่โลกออนไลน์ มีอุปกรณ์มากกว่าห้าหมื่นล้านเครื่อง เชื่อมต่ออินเตอร์เน็ต รวมทั้งมีปริมาณข้อมูลมากขึ้นเป็น 50 เท่า ของที่เราเห็นในทุกวันนี้

การขยายตัวอย่างมหาศาล ของอุปกรณ์เชื่อมต่อและข้อมูลที่ไหลผ่านเน็ตเวิร์ก รวมทั้งความซับซ้อน ต่างๆ ที่มาพร้อมกับการใช้งาน ทำให้สร้างปัญหาท้าทายในทุกระดับ ไม่ว่าจะต่อตัวบุคคล บริษัทหรือประเทศต่างๆที่จะปกป้องตัวเองจากการโจมตีจากโลกไซเบอร์

ต่อไปนี้เป็นทิศทางใหม่ๆ ที่จะต้องติดตาม จับตาในปีนี้
1 มาลแวร์โมไบล์
การคุกคามด้านการรักษาความปลอดภัยจะยังคงเป็นข่าวอยู่ต่อไป และในปีนี้ เราจะเห็นอาชญากรไซเบอร์หันมาเน้นเป้าอุปกรณ์โมบาย โดยโจมตีที่ระบบปฏิบัติการที่ทำงานภายใน และมีการใช้งาน แอพพ์ที่ติดมาลแวร์ (malware)มากขึ้น

ทุกวันนี้ประเทศจีน เป็นผู้นำในด้านจำนวนผู้ใช้เครื่องโมบายของโลก และมัลแวร์ที่ จะเกิดกับ อุปกรณ์เหล่านี้จะสร้างปัญหาใหญ่ตามมา โดยจากการศึกษา ของมหาวิทยาลัยชิงฮว่า และกระทรวงวิทยาศาสตร์เทคโนโลยีของจีน พบว่า มีจำนวนแอพพ์แค่เพียงหนึ่งในสี่เท่านั้นที่มีความปลอดภัยเพียงพอ

การใช้งานระบบชำระเงินออนไลน์ที่มากขึ้นก็จะนำไปสู่ การขยายตัวของการเจาะระบบที่ต้องการ ขโมยข้อมูลจากระบบชำระเงินแบบใหม่อย่างเช่น บัตรเครดิตการ์ด EMV สมาร์ทการ์ดที่ใช้งาน RFID และระบบโมไบล์วอลเล็ตแบบต่างๆ

2 การเรียกค่าไถ่ออนไลน์และการแฮกระบบ
จากข้อมูลของบริษัท TrendMicro ซึ่งเป็นพาร์ตเนอร์ของไมโครซอฟต์ได้ชี้ให้เห็นว่าจะมีการขยายของการเรียกค่าไถ่ออนไลน์ ในปีนี้ และมีการใช้วิธีที่ซับซ้อนมากขึ้นในการขโมยข้อมูลและควบคุมอุปกรณ์ ต่างๆ ที่เข้าใช้งานเว็บ

มัลแวร์ อย่างพวก ransomware จะเป็น ประเภทที่อันตรายมากที่สุด และใช้กันมากขึ้นโดย การเข้ารหัส ข้อมูลส่วน

บุคคลสำคัญของเหยื่อ เช่น ภาพหรือ บันทึกการสนทนา และเรียกค่าไถ่เป็นเงินออนไลน์ หากอยากได้ข้อมูลคืน

3 การหลอกกู้พาสเวิร์ด ในแบบSpear phishing และ smishing
Spear phishing ก็คือ กลลวงทางอีเมล์ ที่เล็งเป้าหมายไปที่ องค์กรใดองค์กรหนึ่ง เพื่อมองหาทางเจาะเข้าระบบ ข้อมูลลับ และมักจะไม่ได้เกิดขึ้นโดยบังเอิญแต่จะลงมือโดยคนที่หวังผลทางการเงิน ข้อมูลความลับทางการค้าและข้อมูลทางทหาร

ในปัจจุบัน การทำฟิชชิ่ง ไม่จำกัดอยู่แค่อีเมลแล้ว ยังมีการใช้งาน ฟิชชิ่ง กับ SMS (smishing) จะพบเห็นมากขึ้น โดยแฮกเกอร์ที่สร้างระบบกู้รหัสผ่านปลอม โดยเมื่อแฮกเกอร์ได้ที่อยู่อีเมลและเบอร์โทรศัพท์มือถือ ก็สามารถสร้างระบบกู้รหัสปลอม เพื่อหลอกเอาพาสเวิร์ด

คิดใหม่ทำใหม่เรื่องการรักษาความปลอดภัยไซเบอร์

เมื่อปลายปีก่อน สัตยา นาเดลลา CEO ของบริษัทไมโครซอฟท์ได้ ชี้ให้เห็นว่า โลกดิจิตอลที่เราอยู่ในปัจจุบันจำเป็นจะต้องมีแนวคิดใหม่ในการปกป้องตรวจสอบและตอบสนองต่อภัยคุกคามทางด้านการรักษาความปลอดภัยออนไลน์ โดยบริษัทต่างๆจะต้อง เปลี่ยนจา แนวคิดแค่ ป้องกันและกู้ระบบ แบบเดิม มาเป็น การปกป้องแบบองค์รวม ที่ตรวจสอบและตอบสนองต่อ ภัยคุกคามในแบบเรียลไทม์และมีระบบอัจฉริยะที่สามารถคาดการณ์ป้องกันล่วงหน้า

แนวคิดในปัจจุบันของการรักษาความปลอดภัยไซเบอร์ก็คือเน้น การรวบรวมข้อมูลเชิงลึก เพื่อ ดักล่วงหน้าต่อภัยคุกคาม ตัวอย่างเช่น ransomware ที่เรียกค่าไถ่จะมีเป้าหมาย และรูปแบบการใช้งานที่ ชัดเจนและมีการเปลี่ยนแปลงรูปแบบไปอย่างรวดเร็ว ดังนั้นจะก้าวให้ทันต้อง ใช้งานระบบคลาวด์มาเพื่อวิเคราะห์ข้อมูล ล่วงหน้าในการสกัดภัยคุกคาม

ขณะเดียวกัน บริษัทต่างๆก็จะต้องเน้นความรักษาความปลอดภัยหลักๆ ของตน โดยใช้ระบบสมัยใหม่การพิสูจน์ไอดีที่ครอบคลุม ตลอดจนโซลูชั่นการรักษาความปลอดภัยและบริหารต่างๆ และหันมาใช้ ฟีเจอร์ใช้งานผ่านระบบคลาวด์และต้องให้การศึกษาและความรู้ต่อบุคลากรในองค์กร

อนาคตยังมีแง่ดี เพราะในอนาคตมีแนวโน้มที่บริษัทต่างๆ และหน่วยงานภาครัฐหันมาร่วมมือมากขึ้นเพื่อรับมือภัยคุกคามไซเบอร์ต่อไป