bLOGGang http://www.bloggang.com **Rating:** ★★★★

บันทึกไฟล์เมื่อ: จันทร์ 17 พฤศจิกายน 2557 เวลา 13:58 **Site Value:** 50,000 **PRValue (x1):** 50,000

หัวข้อข่าว: PwC ชี้อาชญากรรมไซเบอร์ ไม่ได้หยุดแค่ไอที

BLOGGANG
WEBLOG FOR YOU AND YOUR GANG

PwC ชี้อาชญากรรมไซเบอร์ ไม่ได้หยุดแค่ไอที

PwC ชี้ภัยคุกคามเติบโตจากปีก่อนไม่ต่ำกว่า 25% โดยมุ่งสร้างความเสียหายทางด้านการเงิน พร้อมระบุองค์กรส่วนใหญ่ในไทยยังไม่เท่าทันภัยคุกคาม ยกตัวอย่างภัยคุกคามจากการดักจับข้อมูลอีเมล ก่อนส่งอีเมลหลอกให้โอนเงิน

นายวรพงษ์ สุธานนท์ หุ้นส่วนสายงานธุรกิจที่ปรึกษา บริษัท PwC Consulting (ประเทศไทย) จำกัด เปิดเผยว่า ในประเทศไทยจารกรรมทางไอทีก็เป็นอาชญากรรมที่เกิดขึ้นบ่อยมาก และไม่ได้เกิดขึ้นกับบริษัทขนาดกลางหรือขนาดเล็กเท่านั้น

แม้กระทั่งบริษัทชั้นนำขนาดใหญ่ของไทยก็เคยได้รับความเสียหายจากอาชญากรรมไซเบอร์มาแล้ว และนี่ถือว่าเป็นภัยคุกคามที่มาแรงเป็นอันดับต้นๆ จากการทำงานร่วมกับธนาคารชั้นนำหลายแห่ง

โดยที่ผ่านมา ไพร์ซวอเตอร์เฮาส์คูเปอร์ส ได้รับการติดต่อจากบริษัทแห่งหนึ่งให้สืบสวนสอบสวนการปลอมแปลงข้อมูลในจดหมายอิเล็กทรอนิกส์ (E-mail) ของบริษัทขนาดกลางแห่งหนึ่ง โดยเมื่อหลายเดือนก่อนลูกค้าของบริษัทดังกล่าวได้รับ E-mail จากทางบริษัทให้โอนเงินไปยังบัญชีธนาคาร ซึ่งเป็นบัญชีธนาคารเดิมที่เคยถูกใช้ในการหลอกลวงลูกค้าของบริษัทฯ มาแล้วเมื่อไม่กี่เดือนก่อนหน้านั้น

จากการวิเคราะห์ข้อมูลของผู้ส่งอีเมล พบว่า บัญชีดังกล่าวถูกจารกรรมจากแฮกเกอร์ในต่างประเทศ ซึ่งเมื่อแฮกเกอร์สามารถเข้าใช้งานโดยที่ไม่ต้องใส่รหัสผ่านได้แล้ว ก็สามารถดูข้อมูลจากบัญชีรายชื่อลูกค้าที่มีการติดต่อกับบริษัท และเขียนอีเมลไปยังลูกค้าให้โอนเงินเข้ามายังบัญชีธนาคารของแฮกเกอร์ได้ทันที

กรณีนี้ทีมผู้เชี่ยวชาญของ PwC ตรวจสอบพบว่า เครื่องคอมพิวเตอร์ของบริษัทติดโทรจัน ซึ่งโทรจันสามารถขโมยข้อมูลสำคัญของผู้ใช้งานต่างๆ ที่อยู่บนเครื่องคอมพิวเตอร์ ทั้งชื่อผู้ใช้ รหัสผ่าน และส่งข้อมูลเหล่านั้นกลับไปให้แฮกเกอร์

โดยแฮกเกอร์สามารถใช้ข้อมูลเหล่านี้ในการเข้าถึงอีเมล จนกระทั่งสามารถเข้าถึงรายชื่อ และข้อมูลที่มีการติดต่อกับบริษัท นอกจากนั้นแล้ว โทรจันยังเป็น keyword locker โดยจดจำด้วยว่า ผู้ใช้คอมพิวเตอร์เคย key อะไรเข้าไปในเครื่องบ้าง ซึ่งทำให้สามารถทำให้มีจารกรรมเข้าไปถึงโปรแกรมต่างๆ ที่เคยมีการใช้งานได้ด้วย เช่น webcam

ข้อเท็จจริงดังกล่าวสอดคล้องกับผลสำรวจล่าสุดของบริษัท PwC Consulting (ประเทศไทย) ที่ระบุว่า จำนวนภัยคุกคามข้อมูลสารสนเทศและไซเบอร์ครามทั่วโลกในปีที่ผ่านมามีจำนวนเพิ่มขึ้นเป็น 3,741 เหตุการณ์ หรือเติบโต 25% จากปีก่อน ในขณะที่ความเสียหายทางการเงิน (Financial losses) ที่เกิดจากภัยคุกคามข้อมูลองค์กรก็เติบโตในทิศทางเดียวกัน โดยปรับตัวเพิ่มขึ้น 18% โดยเฉลี่ยในช่วงเดียวกันของปีก่อน

นายวรพงษ์ กล่าวต่อว่า ผลการสำรวจความคิดเห็นของบริษัทต่างๆ ที่ทำธุรกิจในประเทศไทยว่า บริษัทส่วนใหญ่ยังไม่ตระหนักถึงภัยของไซเบอร์คราม โดยมีเพียง 39 % ของผู้ตอบแบบสอบถามเท่านั้นที่รับรู้ว่ามีภัยคุกคามรูปแบบนี้อยู่

ทั้งนี้ 1 ใน 5 ขององค์กรที่ตอบแบบสอบถามในครั้งนี้ประเมินว่าความเสียหายที่เกิดจากไซเบอร์ครามอยู่ในวงเงินสูงถึง 5 หมื่นเหรียญสหรัฐฯ หรือประมาณ 1.6 ล้านบาท อย่างไรก็ตาม ภัยคุกคามที่เกี่ยวข้องกับไอทีในประเทศไทยส่วนใหญ่เป็นกรณีที่มีความซับซ้อนและตรวจสอบความเสียหายได้ยาก

ดังนั้น มีความเป็นไปได้สูงที่ว่า มูลค่าความเสียหายที่เกิดจากอาชญากรรมในโลกไซเบอร์ที่เกิดขึ้นจริงจะสูงกว่าตัวเลขที่มีการประเมินกันไว้มาก

"จากกรณีตัวอย่าง โทรจันที่เราตรวจพบเป็นโทรจันที่ออกมานานแล้ว ซึ่งสะท้อนให้เห็นว่า คนไทยไม่เฉลียวใจเพราะใช้โปรแกรม anti-virus ปลอม ซึ่งไม่สามารถตรวจพบ (detect) โทรจันดังกล่าวได้

ทุกวันนี้อาชญากรไซเบอร์ก่อเหตุกันง่ายมาก คนกลุ่มนี้แสวงหาโอกาสจากบริษัทหรือองค์กรต่างๆ ที่ขาดความระมัดระวังเรื่อง IT Security ซึ่งเมื่อเขาเข้าถึงเครื่องคอมพิวเตอร์ของเราแล้ว ก็เท่ากับว่า เขายึดเครื่องเราไปทั้งเครื่องโดยที่ไม่ต้องเสียเวลาเดินทางนั่งเครื่องบิน แล้วใช้มีดใช้ปืนมาจี้เพื่อปล้นทรัพย์ไปจากเรา"

ทั้งนี้ ยังให้ความมั่นใจว่าเรื่องนี้เกิดขึ้นกับบริษัทที่ใช้ซอฟต์แวร์เถื่อน แล้วไม่มีโปรแกรม anti-virus ซึ่งถ้าบริษัทยอมลงทุนติดตั้งซอฟต์แวร์ที่ถูกกฎหมาย มีโปรแกรมสแกนไวรัสที่อัปเดตและมีประสิทธิภาพจริงๆ โทรจันตัวนี้ก็โดนตรวจพบนานแล้ว

อย่างไรก็ตามหากเกิดเหตุเช่นนี้ขึ้นกับบริษัทไหน ต้องมีหน่วยงานผู้เชี่ยวชาญไปสืบค้นข้อเท็จจริงว่า เกิดขึ้นได้อย่างไร แล้วหาทางกำจัดอย่างถูกต้องและเหมาะสม เพราะถ้าไม่รู้สาเหตุที่แท้จริงแล้ว จะก็ไม่สามารถหาทางกำจัดไปได้

Company Relate Link :
PwC