วันที่: 29 ตุลาคม 2557
แหล่งที่มา: เว็บไซต์ Thanonline
http://www.thanonline.com/index.php?option=com_content&view=article&id=252111&catid=176&Itemid=524

PwC เผยปี 57ภัยโลกไซเบอร์พุ่ง แต่งบลงทุนเพื่อป้องกันความปลอดภัยองค์กรหดตัว

PwC เผยภัยคุกคามข้อมูลสารสนเทศและอาชญากรรมทางคอมพิวเตอร์ทั่วโลกในปี 2557เพิ่มขึ้น 48%พบมีการโจมตีทางไซเบอร์โดยเฉลี่ยถึง 117,339ครั้งต่อวัน โดยยุโรปเป็นทวีปที่เกิดภัยโลกไซเบอร์สูงสุด ชี้แม้ความกังวลด้านการรักษาความปลอดภัยของข้อมูลสารสนเทศเพิ่มขึ้น แต่พบทั่วโลกลดงบลงทุนด้านไอที สะท้อนให้เห็นว่าภาคธุรกิจยังนิ่งนอนใจกับการป้องกันภัย โดยเฉพาะอุตสาหกรรมการบิน-อวกาศและการป้องกันประเทศ ด้านไทยอาชญากรรมคอมพิวเตอร์มีแนวโน้มเพิ่มขึ้นเช่นกัน หลังคนไทยเข้าถึงอินเตอร์เน็ตมากขึ้น นางสาว วิไลพร ทวีลาภพันทอง หุ้นส่วนสายงานธุรกิจที่ปรึกษา บริษัท PwC Consulting (ประเทศไทย) เปิดเผยถึงผลสำรวจ The Global State of Information Security Survey 2015จัดทำโดย PwC ร่วมกับนิตยสาร CIO และ CSO ผ่านการสำรวจความคิดเห็นบรรดานักธุรกิจและผู้นำบริษัทไอทีชั้นนำทั่วโลกกว่า 9,700ราย ครอบคลุม 154ประเทศ โดยแบ่งเป็นผู้ถูกสำรวจจากทวีปอเมริกาเหนือ (35%) ยุโรป (34%) เอเชียแปซิฟิก (14%) อเมริกาใต้ (13%) และ ตะวันออกกลางและแอฟริกาใต้ (4%) ว่า จำนวนภัยคุกคามข้อมูลสารสนเทศและอาชญากรรมทางคอมพิวเตอร์ (Information security) ทั่วโลกในปี 2557สูงถึง 42.8ล้านรายการ เพิ่มขึ้นถึง 48%จากปี 2556และมีการโจมตีเฉลี่ย 117,339ครั้งต่อวัน หรือคิดเป็นอัตราการเติบโตเพิ่มขึ้น 66%จากปี 2552ที่เริ่มทำการสำรวจภัยคุกคามข้อมูลสารสนเทศและอาชญากรรมทางคอมพิวเตอร์เป็นครั้งแรก
“ปี 2557ที่ผ่านมาถือเป็นปีที่สร้างความกังวลที่สุดปีหนึ่งก็ว่าได้ หลังเราพบว่า ภาคธุรกิจมีการลงทุนด้านการรักษาความปลอดภัยข้อมูลลดลง สวนทางกับความถี่และความเสียหายทางการเงินที่มีแนวโน้มสูงขึ้นเรื่อยๆ” นางสาววิไลพร กล่าว

“แม้ทุกวันนี้ไซเบอร์ครามจะกลายเป็นภัยที่แทบจะไม่มีธุรกิจไหนที่ไม่รู้จัก เพราะปัจจุบันโลกเข้าถึงอินเตอร์เน็ตมากขึ้น แต่ความเสี่ยงที่ยังไม่ได้รับการแก้ไขในระยะยาว คือ การตระหนักถึงความสำคัญของการป้องกันและรับมือกับอาชญากรคอมพิวเตอร์ ที่มีรูปแบบการก่อเหตุที่หลากหลายและสร้างความเสียหายให้แก่ธุรกิจไม่ว่าเล็ก –ใหญ่มานักต่อนัก” เธอ กล่าว

ทั้งนี้ ภัยคุกคามข้อมูลสารสนเทศและอาชญากรรมทางคอมพิวเตอร์เพิ่มขึ้นอย่างก้าวกระโดด โดยเฉพาะในยุโรปพบว่า ภัยคุกคามข้อมูลสารสนเทศและอาชญากรรมทางคอมพิวเตอร์เพิ่มขึ้น 41%อเมริกาเหนือ 11%และในภูมิภาคเอเชียแปซิฟิก 5%ด้วยเหตุนี้เองทำให้มูลค่าความเสียหายทางการเงิน (Financial losses) ที่เกิดจากภัยคุกคามความปลอดภัยของข้อมูลสารสนเทศทั่วโลกในปีนี้มีมูลค่าถึง 2.7ล้านดอลลาร์สหรัฐ หรือประมาณ 87ล้านบาท (อัตราแลกเปลี่ยน ณ วันที่ 27ต.ค.57ที่ 1ดอลลาร์เท่ากับ 32.32 บาท) เพิ่มขึ้น 34%จากปี 2556และมีจำนวนบริษัทที่ตกเป็นเหยื่อไซเบอร์โดยรายงานความเสียหายเป็นมูลค่าถึง 20 ล้านดอลลาร์ หรือราว 646ล้านบาทขึ้นไปเพิ่มขึ้นเกือบเท่าตัวจากปีที่ผ่านมา

น่าห่วงงบป้องกันความปลอดภัยด้านไอทีหด

นางสาววิไลพร กล่าวว่า เป็นที่น่ากังวลอย่างยิ่งที่องค์กรทั่วโลกตระหนักถึงความสำคัญด้านความปลอดภัยของข้อมูลสารสนเทศและอาชญากรรมทางคอมพิวเตอร์ลดลง โดยผลสำรวจในปีนี้ที่พบว่า การลงทุนด้านการรักษาความปลอดภัยข้อมูล (Information security budgets) ในปี 57ปรับตัวลดลง 4%มาที่ 4.1ล้านดอลลาร์ หรือประมาณ 132ล้านบาท เมื่อเทียบกับปี 2556ขณะที่ค่าใช้จ่ายด้านการรักษาความปลอดภัยข้อมูลในส่วนของงบด้านไอทีคงตัวอยู่ที่ 4%หรือน้อยกว่านั้น ติดต่อกันมาเป็นเวลา 5ปี ผลสำรวจพบว่า ภาคอุตสาหกรรมที่ลดงบด้านการรักษาความปลอดภัยข้อมูลสารสนเทศและอาชญากรรมคอมพิวเตอร์มากที่สุด ได้แก่ อุตสาหกรรมการบิน-อวกาศและการป้องกันประเทศ โดยลดลง 25%เทคโนโลยี ลดลง 21%ค้าปลีกและสินค้าอุปโภคบริโภค ลดลง 15%สาเหตุส่วนหนึ่งอาจเป็นเพราะแนวโน้มธุรกิจของบางอุตสาหกรรมมีทิศทางไม่สดใสเปรียบเทียบกับอดีต ในทางกลับกัน อุตสาหกรรมที่มีการเพิ่มงบประมาณด้านการรักษาความปลอดภัยข้อมูลมากที่สุด ได้แก่ อุตสาหกรรมบริการด้านสุขภาพ โดยเพิ่มขึ้นถึง 66%ทั้งนี้เพื่อรักษาฐานข้อมูลส่วนบุคคล ข้อมูลทางการเงิน การแพทย์ และครอบครัวของผู้ใช้บริการ รองมาได้แก่ อุตสาหกรรมน้ำมันและก๊าซธรรมชาติ เพิ่มขึ้น 15%และอุตสาหกรรมสาธารณูปโภค เพิ่มขึ้น 9%
“ปัจจุบันการลงทุนด้านความปลอดภัยของข้อมูลสารสนเทศและอาชญากรรมทางคอมพิวเตอร์ถือเป็นกลยุทธ์ที่สำคัญขององค์กรในระยะยาวที่ผู้บริหารทั้งไทยและต่างประเทศต้องใส่ใจ หากต้องการป้องกันความเสี่ยง รักษาความปลอดภัยของข้อมูลลับ และลดผลกระทบจากภัยบนโลกอินเตอร์เน็ตที่เมื่อเกิดขึ้นแล้ว จะส่งผลสียมูลค่ามหาศาลต่อตัวองค์กรและพนักงาน” นางสาววิไลพร กล่าว
ทั้งนี้ หากพิจารณาจากขนาดขององค์กรจะพบว่า องค์กรขนาดใหญ่มีความเสี่ยงที่จะตกเป็นเป้าหมายในการก่ออาชญากรรมคอมพิวเตอร์เพิ่มขึ้น จากผลสำรวจพบว่า องค์กรที่มีรายได้ 1,000ล้านดอลลาร์ หรือประมาณ 32,000ล้านบาทขึ้นไป เกิดภัยคุกคามข้อมูลสารสนเทศและอาชญากรรมทางคอมพิวเตอร์เพิ่มขึ้น 44%แต่เนื่องจากองค์กรขนาดใหญ่มีฐานทุน พร้อมทั้งมาตรการรักษาความปลอดภัยที่แน่นหนากว่า จึงทำให้จำนวนภัยคุกคามน้อยกว่าองค์กรขนาดกลางที่มีรายได้ 100-1,000ล้านดอลลาร์ หรือประมาณ 3,200-32,000ล้านบาทซึ่งในปีนี้เกิดภัยคุกคามเพิ่มขึ้น 64%

“คนใน” ตัวการสำคัญของภัยไซเบอร์คราม

ข้อมูลที่น่าสนใจที่พบจากผลสำรวจ คือ อินไซเดอร์ (Insider) หรือกลุ่มผู้ใช้ข้อมูลภายใน ถือเป็นต้นเหตุที่ทำให้เกิดอาชญากรรมคอมพิวเตอร์มากที่สุด ซึ่งในหลายกรณี เกิดจากการกระทำที่รู้เท่าไม่ถึงการ เช่น พนักงานทำการใช้ข้อมูลผ่านมือถือ หรือการถูกโจมตีแบบฟิชชิ่ง (Targeted phishing scheme) ซึ่งเป็นรูปแบบเฉพาะของอาชญากรรมไซเบอร์ โดยอาชญากรจะทำการขโมยข้อมูลผ่านการหลอกลวงทางอินเทอร์เน็ตหรืออีเมลล์ เพื่อให้ผู้ใช้งานทำการเปิดเผยข้อมูลส่วนตัว จากผลสำรวจพบว่า ภัยคุกคามด้านความปลอดภัยของข้อมูลสารสนเทศและอาชญากรรมทางคอมพิวเตอร์ที่เกิดจากพนักงานในองค์กรเพิ่มขึ้น 10%
นอกจาก พนักงานปัจจุบัน หรือ พนักงานเก่าแล้ว บุคคลที่สาม หรือผู้ที่มีแหล่งเข้าถึงข้อมูลและเครือข่ายขององค์กรอยู่เป็นประจำ ไม่ว่าจะเป็น ผู้ให้บริการรายใหม่และรายเก่า ที่ปรึกษา และผู้รับเหมา ก็ถือเป็นอาชญากรไซเบอร์ครามอันดับต้นๆเช่นกัน
“บ่อยครั้งที่เราพบว่า เมื่อมีภัยคุกคามเกิดขึ้น ผู้บริหารหลายรายกลับเลือกที่จะจัดการปัญหาเป็นการภายใน แทนที่จะจัดการดำเนินคดีหรือบังคับใช้กฎหมาย ยิ่งเป็นการเพิ่มความเสี่ยงให้แก่บริษัทอื่นๆ หากนายจ้างเหล่านั้นมีการจ้างอาชญากรพวกนี้ไปทำงานต่อ โดยรู้เท่าไม่ถึงการ” นางสาววิไลพร กล่าว
สิ่งเหล่านี้สะท้อนให้เห็นว่า ภาคธุรกิจไม่ตระหนักถึงความสำคัญในการรักษาความปลอดภัยของข้อมูลสารสนเทศและอาชญากรรมทางคอมพิวเตอร์มากเท่าที่ควร โดยขาดการสื่อสารแบบบนลงล่าง (Top-down communication) อย่างมีประสิทธิภาพ
ข้อมูลที่น่าเป็นห่วงจากผลสำรวจอีกประการ คือ การขาดการจัดอบรบหรือสัมมนาเพื่อสร้างการตระหนักถึงความสำคัญของการรักษาข้อมูลองค์กรอย่างสม่ำเสมอ โดยผู้ตอบแบบสำรวจไม่ถึงครึ่ง (49%) เท่านั้นที่ระบุว่า บริษัทของพวกเขามีการจัดตั้งคณะทำงานหรือทีมจากหลายหน่วยงานภายในองค์กร (Cross-organisational team) ร่วมกันจัดการปัญหาด้านความปลอดภัยข้อมูลเป็นประจำ ขณะที่มีเพียง 36%ที่ระบุว่า บอร์ด หรือ คณะกรรมการของบริษัทของตน มีส่วนร่วมในพิจารณานโยบายด้านความปลอดภัยอย่างจริงจัง

แนวโน้มอาชญากรรมคอมพิวเตอร์ในเอเชียและไทย

นางสาววิไลพร กล่าวต่อว่า ภูมิภาคเอเชียแปซิฟิกถือเป็นผู้นำในการดำเนินกลยุทธ์และนำมาตรการการป้องกันความปลอดภัยด้านข้อมูลในด้านต่างๆมาใช้ โดยผลสำรวจพบว่าผู้บริหารถึง 66%มีการนำกลยุทธ์การรักษาความปลอดภัยข้อมูลมาใช้ควบคู่ไปกับรูปแบบและความต้องการในการดำเนินของธุรกิจ ขณะที่ 73%กล่าวว่า ผู้บริหารระดับสูงในที่ทำงานของตนมีการสื่อสารเรื่องความสำคัญของการรักษาความปลอดภัยอย่างต่อเนื่องทั่วทั้งองค์กร

แม้ว่าแนวโน้มการลงทุนด้านความปลอดภัยข้อมูลสารสนเทศและอาชญากรรมทางคอมพิวเตอร์ของภูมิภาคจะเพิ่มสูงขึ้นในช่วงหลายปีที่ผ่านมา แต่ในปีล่าสุด กลับมีทิศทางปรับตัวลดลงถึง 13%สวนทางกลับมูลค่าความเสียหายทางการเงินที่เกิดจากภัยคุกคามความปลอดภัยของข้อมูลสารสนเทศที่เพิ่มขึ้น 22%สะท้อนให้เห็นถึงความไม่ต่อเนื่องของการบริหารจัดการความเสี่ยงที่อาจเกิดจากภัยคุกคามข้อมูลสารสนเทศและอาชญากรรมทางคอมพิวเตอร์

สำหรับประเทศไทย มีแนวโน้มที่จะเกิดอาชญากรรมทางคอมพิวเตอร์เพิ่มขึ้นเช่นกัน เนื่องจากอัตราการเข้าถึงอินเตอร์เน็ตของคนไทยเพิ่มขึ้นทุกปี ประกอบกับการใช้งานผ่านอินเทอร์เน็ตต่างๆ นั้นสามารถทำได้จากโทรศัพท์มือถือหรือแท็บเล็ต ทำให้การเข้าเน็ตเป็นเรื่องง่าย ดูได้จากยอดผู้ใช้บริการ Facebook ของไทยที่เพิ่มขึ้นทุกปี โดยปัจจุบันอยู่ที่ประมาณ 28ล้านคน ติดอันดับที่ 9 ของโลกจากการจัดอันดับของเว็บไซต์จัดอันดับสถิติโซเชี่ยลเน็ตเวิร์ก ZocialRank นอกจากนี้ ข้อมูลของกองบัญชาการปราบปรามอาชญากรรมที่เกี่ยวกับเทคโนโลยี (ปอท.) พบว่า ในปี 2556มีการฉ้อโกง ซื้อ-ขายสินค้าผ่านอินเทอร์เน็ตมากที่สุดจำนวนกว่า 250คดี รองลงมา เป็นการหมิ่นประมาทด้วยการโฆษณาจำนวน 100คดี มีมูลค่าการเสียหายกว่า 100ล้านบาท

ทั้งนี้ สิ่งที่ต้องจับตาในระยะต่อไปคือ แนวโน้มอาชญากรรมทางคอมพิวเตอร์ในไทยที่เพิ่มขึ้น ที่กลับสวนทางกับความพร้อมในการรับมือภัยจากโลกไซเบอร์ เพราะมาตรการรักษาปลอดภัยที่มีนั้น อาจไม่ทันสมัย หรือเพียงพอต่อการก่ออาชญากรรมที่พัฒนารูปแบบไปอย่างรวดเร็ว นอกจากนี้ โซลูชั่นที่ใช้งานกันอย่างแพร่หลาย ก็อาจกลายเป็นบ่อเกิดของภัยคุกคามเสียเอง ทั้งจากการใช้งานผู้ให้บริการภายนอก แอพพลิเคชั่นมือถือ การเข้ารหัสข้อมูล และการจัดการข้อมูลขนาดใหญ่ขององค์กร ดังนั้น ภาคธุรกิจและหน่วยงานของรัฐฯต้องหันมาให้ความสำคัญและแนวทางรับมือภัยคุกคามความปลอดภัยอย่างจริงจัง

“ยิ่งธุรกิจไทยนำบริการออนไลน์มาให้บริการแก่ผู้บริโภคมากเท่าไหร่ ยิ่งจำเป็นต้องลงทุนเพื่อป้องกันความปลอดภัยด้านข้อมูลสารสนเทศของผู้ใช้บริการมากขึ้นเท่านั้น ผู้บริหารต้องปรับกระบวนทัศน์และกลยุทธ์ให้มีความสามารถในการปรับตัวเพื่อรองรับกับการเปลี่ยนแปลง และผลกระทบที่อาจเกิดขึ้นจากภัยคุกคามไซเบอร์ในรูปแบบใหม่ๆ ที่เกิดขึ้นแทบทุกวัน” นางสาววิไลพรกล่าวทิ้งท้าย