ตลาดวิเคราะห์
Taladvikrao
Circulation: 100,000
Ad Rate: 625

Section: ตลาด/-
วันที่: อาทิตย์ 16 - อาทิตย์ 30 พฤศจิกายน 2557
ปีที่: 17 ฉบับที่: 380 หน้า: 26(ล่าง)
Col.Inch: 79.20 Ad Value: 49,500 PRValue (x3): 148,500 คลิป: ขาว-ดำ
หัวข้อข่าว: PwCเผยภัยโลกไซเบอร์พุ่ง ด่านงบป้องกันความปลอดภัยหด

PwCเผยภัยโลกไซเบอร์พุ่ง ด้านงบป้องกันความปลอดภัยหด

PwC เผยภัยคุกคามข้อมูลสารสนเทศและอาชญากรรมทางคอมพิวเตอร์ทั่วโลกในปีนี้ เพิ่มขึ้น 48% พบมีการโจมตีทางไซเบอร์โดยเฉลี่ย 117,339 ครั้งต่อวัน โดยยุโรปเป็นทวีปที่เกิดภัยโลกไซเบอร์สูงสุด ชี้แม้ความกังวลด้านการรักษาความปลอดภัยของข้อมูลสารสนเทศเพิ่มขึ้น แต่งบลงทุนด้านไอทีทั่วโลกลด สะท้อนถึงการนิ่งนอนใจของธุรกิจโลก

นางสาว วิไลพร ทวีลาภพันทอง หุ้นส่วนสายงานธุรกิจที่ปรึกษา บริษัท PwC Consulting (ประเทศไทย) กล่าวถึงผลสำรวจ The Global State of Information Security Survey 2015 ที่ผ่านการสำรวจความคิดเห็นบรรดานักธุรกิจและผู้นำบริษัทไอทีชั้นนำทั่วโลกกว่า 9,700 ราย ครอบคลุม 154 ประเทศว่า จำนวนภัยคุกคามข้อมูลสารสนเทศและอาชญากรรมทางคอมพิวเตอร์ ทั่วโลกในปีนี้สูงถึง 42.8 ล้านรายการ เพิ่มขึ้น 48% จากปี 2556 และมีการโจมตีเฉลี่ย 117,339 ครั้งต่อวัน หรือคิดเป็นอัตราการเติบโตเพิ่มขึ้น 66% จากปี 2552 ที่เริ่มทำการสำรวจภัยคุกคามข้อมูลสารสนเทศและอาชญากรรมทางคอมพิวเตอร์เป็นครั้งแรก

"ปีนี้ถือเป็นปีที่สร้างความกังวลที่สุดปีหนึ่งก็ว่าได้ หลังเราพบว่าภาคธุรกิจมีการลงทุนด้านการรักษาความปลอดภัยข้อมูลลดลง สวนทางกับความถี่และความเสียหายทางการเงินที่มีแนวโน้มสูงขึ้นเรื่อย ๆ"

แม้ทุกวันนี้ไซเบอร์ครามจะกลายเป็นภัยที่แทบจะไม่มีธุรกิจไหนที่ไม่รู้จัก เพราะปัจจุบันโลกเข้าถึงอินเตอร์เน็ตมากขึ้น แต่ความเสี่ยงที่ยังไม่ได้รับการแก้ไขในระยะยาว คือ ความตระหนักถึงความสำคัญของการป้องกันและรับมือกับอาชญากรคอมพิวเตอร์ที่มีรูปแบบการก่อเหตุที่หลากหลายและสร้างความเสียหายให้แก่ธุรกิจไม่ว่าเล็ก –ใหญ่มานักต่อนัก

ทั้งนี้ ภัยคุกคามข้อมูลสารสนเทศและอาชญากรรมทางคอมพิวเตอร์เพิ่มขึ้นอย่างก้าวกระโดด โดยเฉพาะในยุโรปพบว่า ภัยคุกคามข้อมูลสารสนเทศและอาชญากรรมทางคอมพิวเตอร์เพิ่มขึ้น 41% อเมริกาเหนือ 11% และในภูมิภาคเอเชียแปซิฟิก 5% ด้วยเหตุนี้เองทำให้มูลค่าความเสียหายทางการเงิน ที่เกิดจากภัยคุกคามความปลอดภัยของข้อมูลสารสนเทศทั่วโลกในปีนี้มีมูลค่าถึง 2.7 ล้านดอลลาร์สหรัฐ หรือประมาณ 87 ล้านบาท เพิ่มขึ้น 34% จากปี 2556 และมีจำนวนบริษัทที่ตกเป็นเหยื่อไซเบอร์โดยรายงานความเสียหายเป็นมูลค่าถึง 20 ล้านดอลลาร์ หรือราว 646 ล้านบาทขึ้นไปเพิ่มขึ้นเกือบเท่าตัวจากปีที่ผ่านมา

ซึ่งเป็นที่น่ากังวลอย่างยิ่งที่องค์กรทั่วโลกตระหนักถึงความสำคัญ


วิไลพร ทวีลาภพันทอง

ด้านความปลอดภัยของข้อมูลสารสนเทศและอาชญากรรมทางคอมพิวเตอร์ลดลง โดยผลสำรวจในปีนี้ที่พบว่า การลงทุนด้านการรักษาความปลอดภัยข้อมูล ในปี' 57 ปรับตัวลดลงลดลง 4% มาที่ 4.1 ล้านดอลลาร์ หรือประมาณ 132 ล้านบาท เมื่อเทียบกับปี 2556 ขณะที่ค่าใช้จ่ายด้านการรักษาความปลอดภัยข้อมูลในส่วนของงบด้านไอทีคงตัวอยู่ที่ 4% หรือน้อยกว่านั้น ติดต่อกันมาเป็นเวลา 5 ปี

จากผลสำรวจพบว่า ภาคอุตสาหกรรมที่ลดงบด้านการรักษาความปลอดภัยข้อมูลสารสนเทศและอาชญากรรมคอมพิวเตอร์มากที่สุด ได้แก่ อุตสาหกรรมการบินและการป้องกันประเทศ โดยลดลง 25% เทคโนโลยีลดลง 21% ค้าปลีกและสินค้าอุปโภคบริโภค ลดลง 15% ส่วนหนึ่งอาจเป็นเพราะแนวโน้มธุรกิจของบางอุตสาหกรรมมีทิศทางไม่สดใสเปรียบเทียบกับอดีต

ในทางกลับกัน อุตสาหกรรมที่มีการเพิ่มงบประมาณด้านการรักษาความปลอดภัยข้อมูลมากที่สุด ได้แก่ อุตสาหกรรมบริการด้านสุขภาพ โดยเพิ่มขึ้นถึง 66% ทั้งนี้เพื่อรักษาฐานข้อมูลส่วนบุคคล ข้อมูลทางการเงิน การแพทย์ และครอบครัวของผู้ใช้บริการ รองมาได้แก่ อุตสาหกรรมน้ำมันและก๊าซธรรมชาติ เพิ่มขึ้น 15% และอุตสาหกรรมสาธารณูปโภค เพิ่มขึ้น 9%

"ปัจจุบันการลงทุนด้านความปลอดภัยของข้อมูลสารสนเทศและอาชญากรรมทางคอมพิวเตอร์เป็นกลยุทธ์ที่สำคัญขององค์กรในระยะยาวที่ผู้บริหารทั้งไทยและเทศต้องใส่ใจ หากต้องการป้องกันความเสี่ยง รักษาความปลอดภัยของข้อมูลลับ และลดผลกระทบจากภัยบนโลกอินเตอร์เน็ตที่เมื่อเกิดขึ้นแล้ว จะส่งผลเสียมูลค่ามหาศาลต่อตัวองค์กรและพนักงาน"

ตลาดวิเคราะห์
Taladvikrao
Circulation: 100,000
Ad Rate: 625

Section: ตลาด/-
วันที่: อาทิตย์ 16 - อาทิตย์ 30 พฤศจิกายน 2557
ปีที่: 17 ฉบับที่: 380 หน้า: 26(ล่าง)
Col.Inch: 79.20 Ad Value: 49,500 PRValue (x3): 148,500 คลิป: ขาว-ดำ
หัวข้อข่าว: PwCเผยภัยโลกไซเบอร์พุ่ง ด่านงบป้องกันความปลอดภัยหด

หากพิจารณาจากขนาดขององค์กรจะพบว่า องค์กรขนาดใหญ่มีความเสี่ยงที่จะตกเป็นเป้าหมายในการก่ออาชญากรรมคอมพิวเตอร์เพิ่มขึ้น จากผลสำรวจพบว่า องค์กรที่มีรายได้ 1,000 ล้านดอลลาร์ หรือประมาณ 32,000 ล้านบาทขึ้นไป เกิดภัยคุกคามข้อมูลสารสนเทศและอาชญากรรมทางคอมพิวเตอร์เพิ่มขึ้น 44% แต่เนื่องจากองค์กรขนาดใหญ่มีมาตรการรักษาความปลอดภัยที่แน่นหนา จึงทำให้จำนวนภัยคุกคามน้อยกว่าองค์กรขนาดกลางที่มีรายได้ 100 -1,000 ล้านดอลลาร์ หรือประมาณ 3,200 - 32,000 ล้านบาทซึ่งในปีนี้เกิดภัยคุกคามเพิ่มขึ้น 64%

แม้ว่าแนวโน้มการลงทุนด้านความปลอดภัยข้อมูลสารสนเทศและอาชญากรรมทางคอมพิวเตอร์ของภูมิภาคจะเพิ่มสูงในช่วงหลายปีที่ผ่านมา แต่ในปีล่าสุด กลับมีทิศทางปรับตัวลดลงถึง 13% สวนทางกลับมูลค่าความเสียหายทางการเงินที่เกิดจากภัยคุกคามความปลอดภัยของข้อมูลสารสนเทศที่เพิ่มขึ้นถึง 22% สะท้อนให้เห็นถึงความไม่ต่อเนื่องของการบริหารจัดการความเสี่ยงที่อาจเกิดจากภัยคุกคามข้อมูลสารสนเทศและอาชญากรรมทางคอมพิวเตอร์

สำหรับประเทศไทย มีแนวโน้มที่จะเกิดอาชญากรรมทางคอมพิวเตอร์เพิ่มขึ้นเช่นกัน เนื่องจากอัตราการเข้าถึงอินเตอร์เน็ตของคนไทยเพิ่มขึ้นทุกปี ประกอบกับการใช้งานผ่านอินเทอร์เน็ตต่าง ๆ นั้นสามารถทำได้จากโทรศัพท์มือถือหรือแท็บเล็ต ทำให้การเข้าอินเตอร์เน็ตเป็นเรื่องง่าย ยอดผู้ใช้บริการ Facebook ของไทยที่เพิ่มขึ้นทุกปี โดยปัจจุบันอยู่ที่ประมาณ 28 ล้านคน ติดอันดับที่ 9 ของโลกจากการจัดอันดับของเว็บไซต์จัดอันดับสถิติโซเชี่ยลเน็ตเวิร์ค ZocialRank

จากข้อมูลของกองบัญชาการปราบปรามอาชญากรรมที่เกี่ยวกับเทคโนโลยี (บอท.) พบว่า ในปี 2556 มีการฉ้อโกง ซื้อ-ขายสินค้าผ่านอินเทอร์เน็ตมากที่สุดจำนวนกว่า 250 คดี รองลงมา เป็นการหมิ่นประมาทด้วยการโฆษณาจำนวน 100 คดี มีมูลค่าการเสียหายกว่า 100 ล้านบาท

ทั้งนี้ สิ่งที่น่าเป็นห่วงคือ แนวโน้มอาชญากรรมทางคอมพิวเตอร์ในไทยที่เพิ่มขึ้น กลับสวนทางกับความพร้อมในการรับมือภัยจากโลกไซเบอร์ เพราะมาตรการรักษาปลอดภัยที่มีนั้น อาจไม่ทันสมัย หรือเพียงพอต่อการก่ออาชญากรรมที่พัฒนารูปแบบไปอย่างรวดเร็ว นอกจากนี้ โซลูชั่นที่ใช้งานกันอย่างแพร่หลาย ก็อาจกลายเป็นบ่อเกิดของภัยคุกคามเสียเอง ทั้งจากการใช้งานผู้ให้บริการภายนอก แอพพลิเคชั่นมือถือ การเข้ารหัสข้อมูล และการจัดการข้อมูลขนาดใหญ่ขององค์กร ดังนั้น ภาคธุรกิจและหน่วยงานของรัฐฯต้องหันมาให้ความสำคัญและแนวทางรับมือภัยคุกคามความปลอดภัยอย่างจริงจัง

"ยิ่งธุรกิจไทยนำบริการออนไลน์มาให้บริการแก่ผู้บริโภคมากเท่าไหร่ ยิ่งจำเป็นต้องลงทุนเพื่อป้องกันความปลอดภัยด้านข้อมูลสารสนเทศของผู้ใช้บริการมากขึ้นเท่านั้น ผู้บริหารต้องปรับกระบวนทัศน์และกลยุทธ์ให้มีความสามารถในการปรับตัวเพื่อรองรับกับการเปลี่ยนแปลง และผลกระทบที่อาจเกิดขึ้นจากภัยคุกคามไซเบอร์ในรูปแบบใหม่ ๆ ที่เกิดขึ้นแทบทุกวัน"