5 ประเด็นร้อนเกี่ยวกับระบบรักษาความปลอดภัยที่กำลังท้าทาย SMB

ภัยคุกคามระบบรักษาความปลอดภัยที่เปลี่ยนแปลงอยู่ตลอดเวลาสามารถส่งผลเสียต่อการดำเนินธุรกิจได้ ดังนั้นธุรกิจขนาดกลางและขนาดย่อมจึงจำเป็นต้องหาวิธีปกป้องโครงสร้างพื้นฐานทางธุรกิจของตนเองให้รอดพ้นจากภัยคุกคามเหล่านั้น

ในยุคข้อมูลข่าวสารดังเช่นในปัจจุบัน บรรดาธุรกิจขนาดกลางและขนาดย่อม หรือ SMB (Small and Medium-sized Businesses) ต่างก็ใช้อินเทอร์เน็ต และแอพพลิเคชั่นที่เชื่อมโยงกันเป็นเครือข่ายในการเข้าถึงลูกค้ารายใหม่ๆ และเพื่อให้บริการลูกค้ารายเดิมๆ ได้ดียิ่งขึ้น ขณะเดียวกันภัยคุกคามระบบรักษาความปลอดภัย และกฎหมายใหม่ๆ ก็เป็นแรงกดดันให้ธุรกิจเหล่านี้ต้องปรับปรุงระบบเครือข่ายให้มีเสถียรภาพ และปลอดภัยยิ่งขึ้น

ผลจากการศึกษาที่ออกมาเมื่อเร็วๆ นี้ พบว่า การรักษาความปลอดภัยยังคงเป็นปัญหาหนักอกลำดับต้นๆ ของบรรดาธุรกิจขนาดกลางและขนาดย่อมอย่างต่อเนื่อง ภัยคุกคามระบบรักษาความปลอดภัยที่เปลี่ยนแปลงอยู่ตลอดเวลาทั้งที่มาจากภายนอกและภายในระบบเครือข่ายขององค์กรสามารถส่งผลเสียต่อการดำเนินธุรกิจ รวมทั้งยังมีผลกระทบต่อความสามารถในการทำกำไรและความพึงพอใจของลูกค้าอีกด้วย นอกจากนี้ ธุรกิจขนาดกลางและขนาดย่อมยังจำเป็นต้องปฏิบัติตามข้อกำหนดกฎเกณฑ์ และกฎหมายที่ถูกบัญญัติขึ้นมาเพื่อปกป้องความเป็นส่วนตัวของลูกค้าและทำให้ข้อมูลอิเล็กทรอนิกส์มีความปลอดภัย

ประเด็นที่ 1: เวิร์ม และไวรัส

เวิร์ม และไวรัสคอมพิวเตอร์ยังคงเป็นภัยคุกคามระบบรักษาความปลอดภัยที่พบเห็นโดยทั่วไปมากที่สุด โดยในหนึ่งปีธุรกิจขนาดกลางและขนาดย่อมส่วนใหญ่ก็ต้องเคยเผชิญหน้ากับไวรัสอย่างน้อยหนึ่งตัว เวิร์ม และไวรัสสามารถทำลายความต่อเนื่องในการดำเนินธุรกิจและความสามารถในการทำกำไรได้ โดยเฉพาะอย่างยิ่ง เมื่อเวิร์มและไวรัสรุ่นใหม่ๆ ได้รับการพัฒนาให้มีความชาญฉลาด และแพร่กระจายได้อย่างรวดเร็วมากขึ้นอย่างที่ไม่เคยมีมาก่อน ซึ่งหมายความว่าทั้งเวิร์ม และไวรัสอาจแพร่กระจายไปทั่วทั้งองค์กรได้ภายในเวลาไม่กี่วินาที ประกอบกับการทำความสะอาดเครื่องคอมพิวเตอร์ที่ติดเวิร์มหรือไวรัสก็ต้องใช้เวลานาน ซึ่งบ่อยครั้งอาจส่งผลให้ธุรกิจสูญเสียคำสั่งซื้อ หรือลดทอนประสิทธิภาพของฐานข้อมูล และที่สำคัญคืออาจเป็นสาเหตุให้ลูกค้าโกรธแค้นได้

ขณะที่ธุรกิจต่างๆ พยายามปรับปรุงคอมพิวเตอร์ของตนเองด้วยการติดตั้งแพตช์ตัวล่าสุดสำหรับระบบปฏิบัติการ และซอฟต์แวร์ต่อต้านไวรัส แต่ไวรัสใหม่ๆ ก็ยังสามารถเจาะแนวป้องกันเหล่านี้ได้อยู่ตลอดเวลา ด้วยสาเหตุที่พนักงานได้กระจายไวรัสและสปายแวร์ไปทั่วทั้งองค์กรโดยไม่เจตนา จากการเข้าเว็บไซต์มุ่งร้าย เพื่อดาวน์โหลดข้อมูลที่ไม่พึงประสงค์ หรือเปิดไฟล์ที่แนบมากับอีเมล์ แม้ว่าการโจมตีเหล่านี้จะถูกเชื้อเชิญเข้าสู่องค์กรโดยไม่เจตนา แต่ก็เป็นสาเหตุให้เกิดการสูญเสียทางการเงิน ดังนั้นระบบรักษาความปลอดภัยจะต้องสามารถตรวจจับ และกำจัดเวิร์มไวรัส และสปายแวร์จากทุกจุดในระบบเครือข่าย

ประเด็นที่ 2: การขโมยข้อมูล

เมื่อข้อมูลกลายเป็นสิ่งที่มีค่า บรรดานักเจาะระบบจึงพยายามใช้ทุกวิถีทางในการเจาะเข้าสู่เครือข่ายของธุรกิจต่างๆ เพื่อขโมยหมายเลขบัตรเครดิต หรือข้อมูลอื่นๆ ที่สามารถนำมาเปลี่ยนแปลงเป็นเงินได้ สำหรับธุรกิจขนาดกลางและขนาดย่อมนั้นมักถูกมองว่าเป็นเป้าหมายที่เจาะเข้าสู่ระบบได้ง่ายดายกว่าองค์กรขนาดใหญ่ การป้องกันบริเวณชายขอบของระบบเครือข่ายถือเป็นการเริ่มต้นที่ดี แต่ยังไม่เพียง เพราะการขโมยข้อมูลหลายๆ ครั้งมักเกิดจากบุคคลภายในองค์กรเอง เช่น พนักงาน หรือผู้รับเหมานั่นเอง

การขโมยข้อมูลสามารถสร้างความเสียหายให้กับธุรกิจขนาดกลางและขนาดย่อมได้เช่นเดียวกับองค์กรขนาดใหญ่ ด้วยเหตุที่ธุรกิจเหล่านี้ต้องอาศัยความพึงพอใจของลูกค้า และชื่อเสียงที่ดีเพื่อช่วยให้ธุรกิจเติบโต ธุรกิจต่างๆ ที่ไม่มีมาตรการป้องกันข้อมูลที่ดีพอก็อาจเผชิญปัญหาภาพลักษณ์ทางด้านลบต่อสาธารณะชน ค่าปรับจากภาครัฐ หรือแม้แต่ถูกฟ้องร้อง ตัวอย่างเช่น กฎหมายคุ้มครองผู้บริโภคที่บัญญัติขึ้นในมลรัฐแคลิฟอร์เนียกำหนดให้ธุรกิจต่างๆ ที่สงสัยว่ามีผู้ไม่ได้รับอนุญาตเข้ามาดูข้อมูลลูกค้าจะต้องแจ้งให้ลูกค้าทั้งหมดของพวกเขารับทราบ ยุทธศาสตร์ด้านการรักษาความปลอดภัยต่างๆ จะต้องป้องกันการขโมยข้อมูลอิเล็กทรอนิกส์ที่มีความสำคัญจากทั้งภายในและภายนอกองค์กรได้

p18-19_Market_Top5.pmd 18 2/6/2551, 16:22

ประเด็นที่ 3: ความพร้อมในการดำเนินธุรกิจ

เวิร์ม และไวรัสคอมพิวเตอร์ไม่ได้เป็นเพียงภัยคุกคามสองประเภทที่มีผลต่อความสามารถในการดำเนินธุรกิจเท่านั้น เพราะการโจมตีเพื่อให้ระบบปฏิเสธการให้บริการ หรือ DoS (Denial-of-Service) ก็สามารถปิดเว็บไซต์ และปิดการค้าขายผ่านระบบอิเล็กทรอนิกส์ได้เช่นเดียวกัน ด้วยการส่งทราฟฟิกขนาดใหญ่ไปยังส่วนประกอบของระบบเครือข่ายที่มีความสำคัญ และทำให้ระบบล้มเหลว หรือทำให้ไม่สามารถประมวลผลทราฟฟิกที่ถูกต้องได้ ผลของการโจมตีก่อให้เกิดหายนะต่างๆ ตามมา อาทิ ข้อมูล หรือคำสั่งซื้อสูญหาย และคำร้องขอของลูกค้าไม่ได้รับการตอบสนอง ถ้าการโจมตีเหล่านี้กลายเป็นเรื่องที่ถูกเผยแพร่สู่สาธารณะ เครดิตขององค์กรจะถูกทำลาย การที่คนส่วนใหญ่มักมองว่า DoS มักจะมุ่งไปที่การโจมตีธนาคารใหญ่ๆ และองค์กรธุรกิจระดับแนวหน้ามากกว่าธุรกิจขนาดกลางและขนาดย่อม ดังนั้นพวกเขาจึงมีการเตรียมพร้อมรับมือการโจมตีในลักษณะนี้น้อยกว่าองค์กรขนาดใหญ่

บ่อยครั้งที่องค์กรต่างๆ ให้ความสนใจแต่เรื่องของการอุดช่องโหว่ของระบบรักษาความปลอดภัยที่เกิดขึ้น แต่ไม่ได้เข้มงวดกับพฤติกรรมการใช้งานระบบแบบผิดประเภทของผู้ใช้ ซึ่งอาจสร้างความเสียหายให้กับองค์กรได้เช่นเดียวกัน ตัวอย่างเช่น การขโมยใช้ทรัพยากรของระบบในการแบ่งปันไฟล์เพลง ภาพยนตร์ หรือซอฟต์แวร์ผิดกฎหมาย นอกจากจะส่งผลให้คอมพิวเตอร์ หรือระบบเครือข่ายเหล่านั้นตอบสนองลูกค้าช้าลงแล้ว การเข้าไปเป็นผู้มีส่วนร่วมในการแบ่งปันไฟล์ผิดกฎหมายของผู้ใช้ภายในองค์กรโดยไม่เจตนาอาจทำให้องค์กรถูกฟ้องร้องได้ด้วย

ประเด็นที่ 4: สิ่งที่คาดไม่ถึง

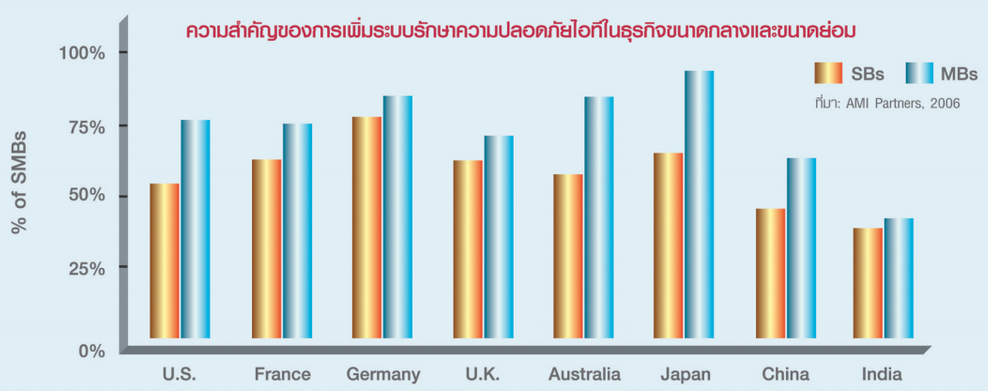
ความก้าวหน้าในการประมวลผล และการติดต่อสื่อสารมักมาพร้อมกับวิธีการใหม่ๆ ในการแสวงหาประโยชน์จากเทคโนโลยี และความเสียหายเสมอ ฮาร์ดแวร์ หรือซอฟต์แวร์ใหม่ที่ออกมาจะนำมาซึ่งโอกาสใหม่ๆ เช่น การเชื่อมต่อเครือข่ายแบบ peer-to-peer และการรับส่งข้อความแบบฉับพลัน (instant messaging–IM) แม้ว่าจะทำให้การทำงานมีประสิทธิภาพมากขึ้นก็ตาม แต่ก็มีผู้ไม่หวังดีใช้เทคโนโลยีใหม่ๆ เหล่านี้เป็นช่องทางการโจมตีระบบไอที และระบบเครือข่ายขององค์กรเช่นเดียวกัน

ปัจจุบัน โทรศัพท์ตกเป็นเป้าหมายที่ไวรัสมุ่งโจมตีบ่อยครั้งขึ้น ด้วยเหตุที่เราไม่สามารถทำนายได้ว่าจะมีอะไรเกิดขึ้นในอนาคต ดังนั้นวิธีป้องกันที่ดีที่สุดวิธีหนึ่งก็คือต้องสามารถปรับเปลี่ยนระบบรักษาความปลอดภัยเพื่อรับมือกับภัยคุกคามที่จะเกิดขึ้นในอนาคตได้ และมีเสียค่าใช้จ่ายอย่างสมเหตุสมผล

ประเด็นที่ 5: กฎหมายด้านการรักษาความปลอดภัย

หากไม่นับเรื่องภัยคุกคามระบบรักษาความปลอดภัยข้างต้น ข้อกำหนดทางกฎหมาย และข้อกำหนดกฎเกณฑ์ใหม่ๆ ที่ธุรกิจขนาดกลาง และขนาดย่อมใช้ป้องกันความเป็นส่วนตัว และความถูกต้องสมบูรณ์ของข้อมูลก็เป็นสิ่งที่พวกเขาต้องตระหนักถึง ดังนั้นธุรกิจทุกประเภทต้องรักษาโครงสร้างพื้นฐานทางธุรกิจและไอทีให้มีความปลอดภัยด้วยงบประมาณที่มีอยู่อย่างจำกัด นอกจากนี้ธุรกิจขนาดกลางและขนาดย่อมโดยทั่วไปต่างต้องการโซลูชั่นที่เรียบง่าย เหมาะสม และมีราคาที่สามารถซื้อหามาใช้งานได้ now

การเพิ่มระบบรักษาความปลอดภัยไอทียังคงเป็นประเด็นหลักที่ธุรกิจขนาดกลางและขนาดย่อมให้ความสำคัญ



- ข้อมูลจากบริษัทวิเคราะห์ทางการตลาด Access Markets International (AMI) Partners พบว่าธุรกิจขนาดกลางและขนาดย่อมทั่วโลกได้ประมาณตัวเลขค่าใช้จ่ายเกี่ยวกับระบบรักษาความปลอดภัยไอทีและโครงสร้างพื้นฐานต่อปีไว้ที่ 1.4 พันล้านดอลลาร์ อันเป็นผลมาจากภัยคุกคามระบบอิเล็กทรอนิกส์ที่มีปริมาณเพิ่มขึ้นอย่างต่อเนื่อง นอกจากนี้ค่าใช้จ่ายด้านนี้ยังมีแนวโน้มจะเพิ่มขึ้นเป็นตัวเลขสองหลักในอีก 2-3 ปีข้างหน้าด้วย
- แม้ว่าธุรกิจขนาดกลางและขนาดย่อมจะเติบโตอย่างรวดเร็ว แต่ค่าใช้จ่ายด้านการรักษาความปลอดภัยในช่วง 1-2 ปีที่ผ่านมากลับไม่ได้เพิ่มขึ้นมากนัก AMI ประมาณการณ์ว่ามีธุรกิจขนาดกลางและขนาดย่อมเกือบ 13 ล้านรายทั่วโลกที่ไม่มีแม้กระทั่งโปรแกรมต่อต้านไวรัสบนเครื่องพีซีของตนเอง ข้อมูลเหล่านี้เป็นผลมาจากการสำรวจธุรกิจขนาดกลางและขนาดย่อมที่ AMI จัดทำขึ้นในกว่า 20 ประเทศซึ่งเป็นตัวแทนของตลาดที่กำลังพัฒนา และตลาดเกิดใหม่

p18-19_Market_Top5.pmd 19 2/6/2551, 16:22