แนวโน้มภัยคุกคามด้านเทคโนโลยีสารสนเทศ 2019

วิชย์ศุทธ์ เมาระพงษ์
ที่ปรึกษาโครงการสารสนเทศของหน่วยงานภาครัฐ
สังกัดสถาบันวิจัยและให้คำปรึกษา แห่งมหาวิทยาลัยธรรมศาสตร์

บทความในตอนนี้จะมีเนื้อหาต่อเนื่องจากตอน “IT Trend 2019 ปีแห่งการเปลี่ยนผ่านเทคโนโลยี” โดยผมจะกล่าวถึงแนวโน้มภัยคุกคามด้านเทคโนโลยีสารสนเทศ 2019 ที่มีการประเมินกันในระดับสากล โดย United States Cyber security Magazine รายงานจาก Aon และจากรายงาน Risk in Focus 2019 report ของ European Confederation of Institutes of Internal Auditing’s (ECIIA) รวมถึงผลกระทบต่อประเทศไทยจากบทสรุปของงานสัมมนา “Cyber Defense Initiative Conference (CDIC) 2018” ซึ่งเป็นงานสัมมนาประจำปีด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของไทย

เริ่มจากการประเมินของ United States Cyber security Magazine ซึ่งกล่าวถึงแนวโน้มความเสี่ยงด้านเทคโนโลยีสารสนเทศจากการสำรวจองค์การชั้นนำทั่วโลกโดยอ้างอิงรายงานของ CISCO องค์การด้านเทคโนโลยีเครือข่ายชั้นนำ ซึ่งมีเนื้อหาโดยสรุปดังนี้

United States Cyber security Magazine, 2019 Risks

จากรายงานความปลอดภัยทางไซเบอร์จากองค์การทั่วโลกโดย CISCO แสดงให้เห็นว่า 31% ขององค์การที่เคยประสบปัญหาโดนโจมตีทางไซเบอร์นั้น ได้รับการปรับปรุงแก้ไขเพื่อป้องกันและลดโอกาสในการที่จะโดนโจมตี ซึ่งองค์การส่วนใหญ่ให้ความสำคัญและเริ่มตื่นตัวกันมากขึ้น แต่อย่างไรก็ตามในปี 2019 ก็ยังมีภัยคุกคามทางไซเบอร์ที่ควรระวัง ซึ่งประกอบไปด้วย

■ การละเมิดสิทธิ์การเข้าถึงข้อมูลบนระบบ Cloud

การจัดเก็บข้อมูลบนระบบ Cloud กำลังเป็นที่นิยมมากขึ้นในปี 2019 องค์การหลายแห่งที่ยังใช้วิธีการจัดเก็บข้อมูลแบบเดิมไว้ที่ทรัพยากรสารสนเทศขององค์การเองก็กำลังจะถ่ายโอนข้อมูลขึ้นไปบนระบบ Cloud ซึ่งในขณะที่ทำการสำรองข้อมูล และโอนถ่ายขึ้นระบบ Cloud นั้น จะเป็นช่วงที่อาจมีการลักลอบเข้าถึงข้อมูลจากผู้

ใช้งานที่ไม่ประสงค์ดี ซึ่งใช้งานระบบ Cloud เดียวกัน เนื่องจากสามารถดักจับ และนำเอาข้อมูลสำคัญไปใช้เพื่อเข้าถึงข้อมูลที่กำลังทำการสำรอง และถ่ายโอนได้ ดังนั้น การแก้ไขปัญหาในลักษณะนี้องค์การจะต้องให้ความสำคัญในรายละเอียดมาตรการการรักษาความปลอดภัยของผู้ให้บริการระบบ Cloud เมื่อต้องเลือกผู้ให้บริการ นอกจากนี้ ต้องเพิ่มเติมความมั่นคงปลอดภัยให้กับระบบการเข้ารหัสข้อมูลขององค์การเพื่อป้องกันไม่ให้ผู้ไม่ประสงค์ดีโจมตีเข้าถึงข้อมูลขององค์การได้

นอกจากนี้ การใช้บริการพื้นที่จัดเก็บข้อมูลบน Cloud นั้น มีความเสี่ยงต่อการถูกละเมิดสิทธิ์เริ่มตั้งแต่ขั้นตอนเข้าใช้งาน ซึ่งปัญหาสำคัญคือยังไม่มีกระบวนการลงทะเบียนที่ปลอดภัย การสมัครเข้าใช้บริการทำได้ง่ายไม่มีความยุ่งยากซับซ้อน ตัวอย่างเช่น แค่มีบัตรเครดิต และระบุข้อมูลสำคัญในการสมัคร เมื่อได้รับการอนุมัติก็สามารถใช้งาน Cloud ได้ทันที ซึ่งในทางกลับกันความเรียบง่ายดังกล่าว กลับทำให้ระบบ Cloud เสี่ยงต่อการสร้างข้อมูลหลอกลวงโดยผู้ไม่ประสงค์ดี (Phishing) และการโจมตีที่เป็นอันตรายอื่นๆ ซึ่งผู้ให้บริการ Cloud จะต้องทบทวน และพัฒนากระบวนการตรวจสอบและลงทะเบียนที่มีความสะดวก และรัดกุมมากขึ้น นอกจากนี้ควรมีวิธีการติดตามธุรกรรมบัตรเครดิต การประเมินการรับส่งข้อมูลเครือข่ายอย่างละเอียด ซึ่งเป็นสิ่งสำคัญในการกำจัดการเข้าถึง และใช้งานได้

■ ส่วนเชื่อมต่อกับ application (API หรือ Application Program Interface) ที่ไม่ปลอดภัย

ในเรื่องของส่วนเชื่อมต่อกับ application ที่ไม่ปลอดภัย ซึ่งก็เช่นเดียวกันกับประเด็นของการถูกละเมิดสิทธิ์การเข้าถึงข้อมูลบนระบบ Cloud นั่นคือก็เป็นเรื่องของมาตรการการรักษาความปลอดภัยของผู้ให้บริการระบบ Cloud เนื่องจากช่องโหว่ของส่วนเชื่อมต่อกับ application หรือเรียกย่อๆ กันว่า API นั้น เกิดจากขาดการรักษาความปลอดภัยที่เข้มงวด เริ่มตั้งแต่การพิสูจน์ตัวตนผู้ใช้งานจนถึงการเข้ารหัสข้อมูล โดย API จะใช้เพื่อกำหนดขอบเขตในการเรียกใช้งานข้อมูลจาก application โดยจะอนุญาตให้ application นั้นๆ เรียกใช้งานข้อมูลเฉพาะส่วนที่จำเป็นเท่านั้น ซึ่งตัว API ก็จะถูกติดตั้ง และให้บริการผ่าน Cloud เช่นกัน ในฐานะของผู้ใช้บริการ องค์การควรต้องให้ความสำคัญกับมาตรการรักษาความปลอดภัยที่ผู้ให้บริการ Cloud กำหนดไว้ นอกจากนี้กระบวนการเข้ารหัส และการรับรองความถูกต้องในสิทธิ์การเข้าถึงจะต้องมีความเข้มงวด และรัดกุม

■ การโจมตีของ Malware

การโจมตีของ Malware เป็นอีกหนึ่งความเสี่ยงที่ต้องระวัง การโจมตีของ Malware อาทิ การ download ติดตั้งและใช้งาน software ฟรีที่ไม่ได้ตรวจสอบเรื่องความปลอดภัยโดยผู้ใช้งานอนุญาตให้ติดตั้งหรือการอนุญาตให้เข้าถึงข้อมูล พื้นที่จัดเก็บข้อมูล การแบ่งปันไฟล์ผ่าน software ประเภท Bit-torrent ฯลฯ โดยที่ไม่มีการใช้งานโปรแกรมรักษาความปลอดภัยทาง internet ปัญหานี้จะต้องแก้ไขที่กลไกการรักษาความปลอดภัย และการปฏิบัติตามกฎระเบียบการใช้งานที่เข้มงวด

■ การถูกเจาะระบบ (HACK)

ความเสี่ยงจากการถูกเจาะระบบยังไม่มีแนวโน้มที่จะลดลง ดังนั้นองค์การควรจะใช้มาตรการรักษาความปลอดภัยเพื่อลดภัยคุกคามดังกล่าว โดยเฉพาะเมื่อนำเอาเทคโนโลยี Internet of Things เข้ามาทดแทนการทำงานเดิมในหลายๆ ส่วน ซึ่งส่งผลให้จุดอ่อนถูกสร้างขึ้นในระบบ เนื่องจากอาจจะการเกิดการแชร์หรือส่งผ่านข้อมูลส่วนตัวหรือแม้กระทั่งรหัสผ่านในการเข้าถึงระบบโดยไม่ได้มีการเข้ารหัส นอกจากนี้หากในมุมของผู้ให้บริการควรต้องมีข้อจำกัดในการแบ่งปันข้อมูลระหว่าง application หรืออุปกรณ์ หรือใช้มาตรการพิเศษเพื่อขออนุญาตติดตามกิจกรรมที่เกิดขึ้นจากการทำงานของบุคลากรเพื่อให้แน่ใจว่าจะไม่เกิดกิจกรรมที่ไม่ได้รับอนุญาตขึ้นซึ่งส่งผลให้เกิดความเสี่ยง

อ่านต่อฉบับหน้า