Money & Banking Magazine
การเงินธนาคาร

วันที่: 18 มีนาคม 2557
แหล่งที่มา: นิตยสาร การเงินธนาคาร

คอลัมน์: News Technology

แฮกเกอร์ล็อกเป้า 4 จุดเสี่ยง จ้องฉกข้อมูล-ล้วงเงินจากบัญชี เผยปี 2557 ยุคทองภัยไซเบอร์ แฮกเกอร์ยกระดับการโจมตีผู้ใช้ ปรับการทำงานเป็นองค์กร กระหน่ำสารพัดวิธีฉกเงิน ชี้ 4 จุดสุดเสี่ยง หลังแฮกเกอร์ปรับมุมมองการโจมตี เน้นผู้ใช้เป็นหลัก

ในรอบปีที่ผ่านมา มีองค์กรธุรกิจกว่า 91% ตกเป็นเหยื่อของการโจมตีไซเบอร์อย่างน้อย 1 ครั้ง ขณะที่องค์กรอีก 9% เคยตกเป็นเหยื่อของการโจมตีแบบเจาะจงเป้าหมาย หลายๆ องค์กรยอมรับว่า ส่วนหนึ่งมาจากการเปิดให้พนักงานนำอุปกรณ์พกพาดิจิตอลเข้ามาใช้งานภายในโดยที่ไม่มีระบบการจัดการความปลอดภัยที่ดีพอ ทำให้กลายเป็นการเปิดทางให้แฮกเกอร์แฝงมัลแวร์เข้ามาภายในองค์กรเพื่อขโมยข้อมูลได้ง่ายขึ้น ด้านผลสำรวจจากไพร้ซวอเตอร์เฮาส์คูเปอร์สระบุว่า จำนวนภัยไซเบอร์ทั่วโลกได้เพิ่มจำนวนขึ้นถึง 3,741 เหตุการณ์ เติบโตขึ้นถึง 25% ในปีที่ผ่านมา และคาดว่าจะยังเติบโตอย่างต่อเนื่องไปอีกอย่างน้อย 3 ปี

เป้าหมายหลักของการโจมตีคือ “เงิน” ดังนั้น อุตสาหกรรมการเงินและธนาคารคงหลีกเลี่ยงการโจมตีทางไซเบอร์ไม่ได้ แน่นอนว่าธนาคารทั่วโลกพยายามติดตั้งระบบป้องกันภัยไซเบอร์ที่แข็งแกร่ง แต่รูปแบบการโจมตีทางไซเบอร์ไม่ใช่การเดินหน้าทุบกำแพงป้องกันเพื่อโจมตีซึ่งๆหน้า แต่ใช้วิธีแฝงตัวในสภาพแวดล้อมของธนาคารเพื่อเข้าไปล้วงเงินในระบบออกมา ดังนั้น การโจมตีของภัยไซเบอร์จะถอยระยะออกมาอีกระยะ เบนเป้าไปยังองค์ประกอบต่างๆ ที่เชื่อมต่อกับธนาคาร เช่น ผู้ให้บริการเอาต์ซอร์สหรือลูกค้าธนาคาร พยายามค้นหาช่องโหว่ก่อนจะเริ่มต้นลงมือโจมตี การเงินธนาคาร ได้สัมภาษณ์พิเศษ นายสุวิชชา มุสิจรัล วิศวกรระบบรักษาความปลอดภัย บริษัท ซอร์สไฟร์ ประเทศไทย จำกัด ถึงมุมมอง รูปแบบ และวิธีการโจรกรรมข้อมูลของแฮกเกอร์ที่จะเกิดขึ้นในปี 2557 รวมถึงการชี้ชัดไปที่ 4 จุดเสี่ยงที่จะเป็นเป้าการโจมตีหลัก

ภัยไซเบอร์พุ่งเป้าลูกค้าแบงก์ เตือนคลิกไม่คิดเสี่ยงเงินสูญ

นายสุวิชชากล่าวว่า ปัจจุบันภาคการเงินและธนาคารให้ความสำคัญกับการรักษาความปลอดภัยทางไซเบอร์อย่างมาก หลายธนาคารลงทุนติดตั้งระบบป้องกันที่แข็งแกร่ง เพื่อเสริมให้ลูกค้าเชื่อมั่นในบริการของธนาคาร ซึ่งในความเป็นจริงภาคธนาคารคือองค์กรที่มีระบบรักษาความปลอดภัยที่เข้มแข็งอันดับต้นๆ ของโลก แต่ก็ยังเกิดเหตุการณ์ที่แฮกเกอร์สวมรอยเข้ามาในระบบและล้วงข้อมูลออกไปได้ ซึ่งสิ่งที่เกิดขึ้นนั้นคือการเปลี่ยนมุมมองการโจมตี และถอยระยะโฟกัสหาช่องว่างที่จะแทรกซึมเข้าไปของแฮกเกอร์ ซึ่งหมายความว่า ธนาคารยังคงเป็นเป้าหมายหลัก แต่โฟกัสของการโจมตีไม่ใช่กำแพงเหล็กกล้าที่ล้อมธนาคาร แต่เป็นองค์ประกอบอื่นๆ ที่ต่อเชื่อมกับระบบธนาคารแทน เช่น องค์กรที่รับงานต่อจากธนาคาร (Third Party) หรือลูกค้าเจ้าของบัญชี

วิธีการของแฮกเกอร์จะเริ่มจากการศึกษาสภาพแวดล้อมการเชื่อมต่อทั้งหมดของธนาคาร ค้นหาว่าธนาคารมีการเชื่อมต่อกับองค์ประกอบใดบ้าง เช่น ใช้บริการเอาต์ซอร์สจากที่ใด และทำการวิเคราะห์หาช่องโหว่ที่จะสามารถแทรกซึมเข้าไป เมื่อเห็นโอกาสก็จะเริ่มกำหนดเป้าหมาย หากโจมตีไม่สำเร็จก็จะถอยมุมมองออกมาหาช่องโหว่อื่นต่อไป

นายสุวิชชายกกรณีศึกษาที่โด่งดังไปทั่วโลกเมื่อหลายปีก่อนว่า แฮกเกอร์ชาวจีนพยายามเจาะระบบคอมพิวเตอร์ของกระทรวงกลาโหมประเทศอเมริกา ซึ่งแน่นอนว่าไม่สามารถเข้าไปได้เพราะมีการป้องกันที่หนาแน่นมาก และยังมีการใช้ Token เพื่อสร้างรหัสยืนยันตัวตนก่อนเข้าระบบ จึงเปลี่ยนเป้าหมายไปยังบริษัทที่รับงานจากกระทรวงกลาโหมอีกทอดหนึ่งแทน (Sub-Contract) ซึ่งก็ยังไม่สามารถเจาะเข้าไปได้เพราะบริษัทเหล่านี้มีมาตรการรักษาความปลอดภัยตามที่กระทรวงกลาโหมกำหนด แฮกเกอร์รายนี้ตัดสินใจเจาะระบบของผู้ผลิต Token เพื่อขโมยข้อมูลการทำงานของ Token และสวมรอยล็อกอินเข้าระบบของกระทรวงกลาโหมได้สำเร็จ ซึ่งกรณีนี้ถูกกล่าวถึงอย่างมากในวงการรักษาความปลอดภัย

ปัจจุบัน วิธีการโจมตีลักษณะนี้เกิดขึ้นทั่วโลก เมื่อแฮกเกอร์จำกัดเป้าหมายได้แล้วก็จะหาทางหลอกล่อด้วยการโจมตีแบบ Spam Message เช่น การส่งอีเมล์ปลอมจากธนาคาร ส่งอีเมล์ปลอมว่ามีพัสดุส่งมา หรืออีเมล์หลอกคืนภาษี ซึ่งอีเมล์เหล่านี้จะมาพร้อมกับไฟล์แนบสกุล PDF ที่มีการฝังสคริปต์ให้ดาวน์โหลดมัลแวร์เข้าสู่ระบบ ผู้ใช้มักจะคาดไม่ถึงเนื่องจากวิธีการล่อลวงมีความแนบเนียนมาก และเมื่อมัลแวร์เข้าสู่ระบบได้แล้วก็จะฝังตัวหลบเลี่ยงการตรวจจับ คอยสอดส่องพฤติกรรม และหาช่องโหว่ที่สามารถเชื่อมไปยังเป้าหมายหลัก โดยในช่วง 1 เดือนแรกที่มัลแวร์ฝังตัวในเครื่อง ผู้ใช้จะไม่รู้ตัวเลยว่ากำลังถูกคุกคามอยู่ ทำให้ขาดความระมัดระวัง จากนั้นแฮกเกอร์จะรอระยะเวลาที่เหมาะสม อาจจะ 1-2 เดือน หรือนานเป็นปี เพื่อให้แน่ใจว่าจะสามารถเชื่อมโยงไปยังบัญชีธนาคารได้สำเร็จ

เหยื่อของการโจมตีส่วนใหญ่คือผู้ใช้บริการประเภท E-Banking จะเห็นว่าทุกธนาคารเน้นมาก ในการให้ข้อมูลด้านความปลอดภัยแก่ลูกค้าอย่างสม่ำเสมอ ซึ่งถือเป็นเรื่องดีที่ช่วยให้ผู้ใช้มีความตื่นตัว แต่แฮกเกอร์ก็ยกระดับความพยายามของตัวเองพัฒนารูปแบบการโจมตีให้มีความซับซ้อน ตรวจจับได้ยากขึ้น เช่น การโจมตีแบบสวมรอยเป็นผู้ใช้ (Man in a Middle) ใช้วิธีการเฝ้าดูพฤติกรรมผู้ใช้ เก็บข้อมูลจนกว่าจะพบความเชื่อมโยง และรอคอยโอกาสที่เหมาะสมก่อนจะเริ่มการโจมตี

วิธีที่แพร่หลายในการขโมยข้อมูลผู้ใช้เวลานี้คือวิธีที่เรียกว่า DNS Poisoning หรือการวางยาพิษ ตัวอย่างเช่น เมื่อลูกค้า A พยายามจะเข้าเว็บไซต์ Bank.com คอมพิวเตอร์ของผู้ใช้จะถาม IP กับเซิร์ฟเวอร์ของผู้ให้บริการอินเทอร์เน็ตก่อนจะทำการเชื่อมต่อเข้าไปยัง Bank.com ซึ่งแฮกเกอร์ก็จะชิงส่ง IP ปลอมไปยังคอมพิวเตอร์ผู้ใช้ และหลอกให้ระบบมาเชื่อมต่อกับเซิร์ฟเวอร์ของแฮกเกอร์แทนเว็บไซต์ Bank.com จากนั้นก็จะพยายามขโมยข้อมูลบัญชีและรหัสผ่านต่างๆ ของผู้ใช้

“พฤติกรรมที่น่ากลัวและเสี่ยงต่อการถูกขโมยเงินในบัญชีอย่างมากคือการตั้งค่า DNS ด้วยตัวเอง โดยดูจากเว็บไซต์ต่างๆ ที่อ้างว่าสามารถทำให้ประสิทธิภาพของอินเทอร์เน็ตดีขึ้น ซึ่งวิธีนี้คือกลลวงผู้ใช้ โดยในช่วงแรกอาจจะตอบสนองการใช้งานได้ดี แต่พอผู้ใช้พิมพ์ URL ของธนาคารลงไป DNS นี้จะพาไปเชื่อมกับเซิร์ฟเวอร์ของแฮกเกอร์เพื่อขโมยข้อมูล”

4 จุดเสี่ยงล็อกเป้าผู้ใช้ปี 2557
แอนดรอยด์/คลาวด์ น่าห่วง

นายสุวิชชากล่าวว่า จุดเสี่ยงที่สำคัญของปี 2557 คือ “สมาร์ตโฟนและแท็บเล็ตที่ใช้ระบบปฏิบัติการแอนดรอยด์” จากการศึกษาพบว่า ในปี 2556 มัลแวร์แอนดรอยด์เติบโตขึ้นถึง 700% ขณะที่ในต่างประเทศพบว่าแฮกเกอร์โฟกัสการโจมตีไปที่ระบบปฏิบัติการแอนดรอยด์ เนื่องจากเป็นระบบปฏิบัติการที่มีผู้ใช้เยอะที่สุด นอกจากนี้ ระบบยังเปิดให้ผู้ใช้สามารถติดตั้งแอพพลิเคชั่นภายนอกได้โดยตรง ซึ่งถือเป็นการเปิดให้แฮกเกอร์ใช้โอกาสนี้แพร่กระจายแอพพลิเคชั่นที่ฝังมัลแวร์ลงไปบนสมาร์ตโฟนแอนดรอยด์ได้ง่ายขึ้น โดยเมื่อผู้ใช้ติดตั้งแอพพลิเคชั่นนี้ มัลแวร์ที่ฝังมาด้วยจะทำหน้าที่ดักข้อความ SMS ทุกชนิด และส่งต่อไปยังแฮกเกอร์

“เป้าหมายหลักของแฮกเกอร์วันนี้พุ่งไปที่ผู้ใช้ โดยเฉพาะผู้ใช้แอนดรอยด์ที่นิยมดาวน์โหลดแอพพลิเคชั่นฟรีจากเว็บไซต์แปลกปลอมถือเป็นการเปิดรับความเสี่ยงจากมัลแวร์ที่แฝงตัวมาโดยตรง ดังนั้น ผู้ใช้จำเป็นต้องมีการตื่นตัวและระมัดระวังในการติดตั้งโปรแกรมเสี่ยงเหล่านี้ ซึ่งหากดูในอเมริกาจะพบว่ามัลแวร์บนแอนดรอยด์มีจำนวนน้อยมาก เพราะคนอเมริกานิยมซื้อแอพพลิเคชั่นที่อยู่ใน App Store หรือ Play Store เนื่องจากผ่านการตรวจสอบจาก Apple และ Google แล้ว ซึ่งต้องทำความเข้าใจก่อนว่าบนโลกนี้ไม่อะไรที่ได้มาแบบฟรีๆ”

นายสุวิชชากล่าวว่า การโจมตีบนแอนดรอยด์นั้นแฮกเกอร์จะพยายามเก็บข้อมูลของเหยื่อจากสมาร์ตโฟนให้มากที่สุด มีการกำหนดตั้งโจทย์ในว่าต้องฝังมัลแวร์ลงในสมาร์ตโฟนทั่วโลก จากนั้นก็เฝ้าจับตาดูพฤติกรรมของเหยื่อ และสร้างเป็นฐานข้อมูลขึ้นมา เมื่อเก็บข้อมูลได้ระยะหนึ่งแฮกเกอร์จะเริ่มลงมือด้วยการตั้งแคมเปญการโจมตีที่สอดคล้องกับช่วงเวลานั้นๆ ต่อมาก็จะเลือกเป้าหมายโดยดูจากความเชื่อมโยงของพฤติกรรมเหยื่อกับฐานข้อมูล จากนั้นถึงจะเริ่มโจมตี “แฮกเกอร์ต้องการเงิน ซึ่งแหล่งเงินที่ดีที่สุดก็คือ ภาคธนาคาร อีกไม่นานเราก็จะเห็นแคมเปญการโจมตีเกี่ยวกับการหลอกคืนภาษีกลับมาอีกครั้ง โดยอาจจะใช้วิธีหลอกให้คลิกลิงก์เพื่อหลอกให้เหยื่อลงมัลแวร์ในโทรศัพท์มือถือเพื่อเก็บข้อมูลเอาไว้ ขณะที่ผู้ใช้ซึ่งคลิกลิงก์ไปก็ไม่เห็นความเปลี่ยนแปลง ซึ่งแฮกเกอร์เองก็ฉลาดพอที่จะรอและทิ้งระยะเป็นเดือน หรือปี เพื่อย้อนกลับมาโจมตีโดยที่ผู้ใช้อาจไม่ทันระวังตัว ปัจจุบันแฮกเกอร์เหล่านี้พัฒนาเป็นขบวนการข้ามชาติ อยู่ในยุโรปตะวันออกและอีกหลายๆ ประเทศร่วมมือกันทำ มีการแลกเครื่องมือซอฟต์แวร์ และวิธีการโจมตีระหว่างกัน ซึ่งการจะทลายขบวนการเหล่านี้เป็นเรื่องยากมาก แม้ว่าตำรวจจะสามารถจับกุมได้บ้าง แต่ส่วนใหญ่ก็เป็นแค่ปลายแถวเท่านั้น”

นายสุวิชชากล่าวว่า จุดเสี่ยงต่อมาที่แฮกเกอร์เน้นมากขึ้นคือ “บริการคลาวด์เซอร์วิส” ซึ่งมีรูปแบบการใช้งานแบบจ่ายเมื่อใช้จริงหรือ as a service ที่ได้รับความนิยมจากองค์กรมากมายเนื่องจากช่วยประหยัดค่าใช้จ่าย ช่วยให้องค์กรไม่จำเป็นต้องลงทุนเยอะ ซึ่งในมุมของการทำงานจริงถือว่าช่วยตอบโจทย์ได้อย่างมาก แต่ในมุมของการรักษาความปลอดภัยนั้น บริการลักษณะนี้อาจกลายเป็นการเปิดช่องโหว่ให้แฮกเกอร์หาทางเจาะเข้ามาในระบบได้

“ธนาคารแห่งหนึ่งในสิงค์โปร์ที่ใช้โซลูชั่นคลาวด์พริ้นติ้ง ซึ่งโซลูชั่นนี้จะเปิดให้พนักงานธนาคารสามารถสั่งพิมพ์เอกสารผ่านระบบคลาวด์ เครื่องพิมพ์ที่ใช้งานในโซลูชั่นนี้จำเป็นจะต้องมีฮาร์ดดิสก์ในตัว เพื่อที่จะคอยเก็บข้อมูลเอกสารต่างๆ เอาไว้ ซึ่งแฮกเกอร์รายหนึ่งสามารถค้นหาช่องโหว่ในจุดนี้ได้สำเร็จ จึงแฮกเข้าไปที่เซิร์ฟเวอร์ของผู้ให้บริการงานพิมพ์ จากนั้นจึงเจาะเข้าไปที่ฮาร์ดดิสก์ของเครื่องพิมพ์จนสามารถขโมยข้อมูลลูกค้าออกมาได้ถึง 600 ราย” กรณีนี้คือ ตัวอย่างที่สะท้อนให้เห็นว่าแม้ธนาคารจะมีระบบป้องกันที่แข็งแกร่ง แต่องค์กรอื่นๆ ที่เชื่อมต่อกับธนาคารนั้นยังมีช่องโหว่อยู่ ดังนั้น ธนาคารจำเป็นจะต้องคำนึงว่า เมื่อข้อมูลได้ไหลออกไปจากระบบแล้ว ต้องมีการรักษาความปลอดภัยที่เข้มแข็งมากพอ แม้ว่าในความเป็นจริงผู้ให้บริการคลาวด์ระดับโลกหลายรายจะมีการป้องกันระดับเวิลด์คลาส แต่ช่องว่างระหว่างการส่งข้อมูลสู่ระบบคลาวด์ก็ยังคงเป็นประเด็นที่น่ากังวล แม้ว่าจะมีการเข้ารหัสความปลอดภัยข้อมูลที่หนาแน่น แต่ก็มีความเป็นไปได้ที่จะถูกดักข้อมูลระหว่างส่งออกไปได้เช่นกัน

นายสุวิชชากล่าวอีกว่า วิธีการเจาะเข้าระบบที่แพร่หลายในเวลานี้คือการอาศัยไฟล์ Dropper ซึ่งไฟล์ประเภทนี้ไม่ใช่มัลแวร์ และไม่มีพฤติกรรมในการโจมตีระบบ แต่ทำหน้าที่เก็บข้อมูล และเปิดทางให้มัลแวร์จากภายนอกเข้ามาในระบบได้ง่ายขึ้น เมื่อสามารถดาวน์โหลดไฟล์มัลแวร์ต่างๆได้ครบตามต้องการแล้วถึงจะเริ่มโจมตี โดยจะทำแบบช้าๆ มีการปรับกลยุทธ์เพื่อให้ได้มาซึ่งผลลัพธ์ที่ต้องการ (Target Persistent Attack) โดยที่แฮกเกอร์พร้อมจะนั่งเฝ้าเก็บข้อมูล แล้วค่อยโจมตีเมื่อมีโอกาสประสบความสำเร็จสูง

ชี้ BYOD เสี่ยง Walk in Worm

แฮกเกอร์สบโอกาสเจาะอินฟราฯ

นายสุวิชชากล่าวว่า จุดเสี่ยงที่ 3 ซึ่งคาดว่าจะเป็นประเด็นมากในปี 2557 คือ การทำงานแบบ "Bring Your Own Device" หรือ BYOD ที่เปิดให้พนักงานสามารถนำอุปกรณ์พกพาดิจิตอลอย่างสมาร์ตโฟนและแท็บเล็ตเข้ามาใช้งานในองค์กรได้ หากว่าองค์กรไม่มีการป้องกันและกำหนดการใช้งานของอุปกรณ์ที่เข้ามาภายในองค์กรได้ดีพอ ก็จะทำให้เกิดการโจมตีที่เรียกว่า "Walk in Worm" ที่ครั้งหนึ่งเคยระบาดหนักมาแล้วจากโปรแกรม Autorun บน Flash Drive วิธีนี้เป็นวิธีที่สะดวกและง่ายที่สุด สามารถฝ่าด่านการป้องกันที่หนาแน่นเข้าไปโจมตีจากภายใน ซึ่งการโจมตีแบบนี้จะกลับมาอีกครั้งบนแท็บเล็ตและสมาร์ตโฟน

"walk in worm คือศัพท์เฉพาะที่เรียกการโจมตีประเภทนี้ จากเมื่อก่อนที่มัลแวร์หรือหนอนคอมพิวเตอร์จะมาทางอินเทอร์เน็ต แต่ปัจจุบันผู้ใช้กลายเป็นคนที่นำมัลแวร์เหล่านั้นไปกระจายสู่ระบบด้วยตัวเอง ผ่านอุปกรณ์พกพาอย่างสมาร์ตโฟน แม้ว่าด้านนอกองค์กรจะตั้งกำแพงแข็งแกร่งเพื่อป้องกันภัยคุกคาม แต่การโจมตีในปัจจุบันนั้นเปลี่ยนรูปแบบมาเป็นการโจมตีจากภายในแทน ซึ่งส่วนใหญ่จะเกิดขึ้นโดยที่องค์กรไม่เคยรู้ตัวเลยว่ากำลังถูกโจมตี" เมื่อพนักงานนำโทรศัพท์มือถือเข้าไปเชื่อมต่อกับเน็ตเวิร์กภายในองค์กร มัลแวร์ก็สามารถที่จะสแกนเน็ตเวิร์กเพื่อหาช่องว่างในการโจมตีองค์กรด้วย นอกจากนี้ ยังมีความเสี่ยงจากการนำสมาร์ตโฟนเชื่อมต่อกับคอมพิวเตอร์ เพราะเมื่อมัลแวร์สามารถฝังตัวลงในแอนดรอยด์แล้ว พบว่ามีการเชื่อมต่อกับคอมพิวเตอร์ มัลแวร์ก็สามารถที่จะแพร่กระจายเข้าไปในคอมพิวเตอร์สำนักงาน และแพร่กระจายไปยังเครื่องอื่นๆ ต่อได้อีก ส่งผลให้แฮกเกอร์มีตัวเลือกและวิธีการโจมตีที่หลากหลายมาก

แม้ว่าในการทำงานจริงแล้ว คอนเซ็ปต์ BYOD มีประโยชน์ต่อการทำงานมาก แต่หากไม่มีระบบที่ป้องกันและจำกัดการใช้งานอุปกรณ์เหล่านี้ได้ดีพอ ก็จะเป็นการเปิดช่องโหว่ให้แฮกเกอร์เข้ามาโจมตีได้ ซึ่งเป้าหมายหลักที่แฮกเกอร์ควบคุมได้ง่ายที่สุดก็คือตัวพนักงาน จะเห็นว่าหลายองค์กรที่รู้ตัวว่ายังไม่มีระบบป้องกันที่แข็งแกร่งพอก็จะมีนโยบายห้ามใช้งานอุปกรณ์ส่วนตัวเด็ดขาดเพื่อเป็นการตัดความเสี่ยง หรือหากมีการลงทุนระบบป้องกัน พนักงานก็จะต้องลงทะเบียนอุปกรณ์เข้ากับระบบก่อนเข้ามาใช้งานก่อน

"ทั่วโลกยกให้ปี 2557 เป็นปีทองของการโจมตี เนื่องจากการใช้งานอุปกรณ์พกพาที่เพิ่มขึ้นหลายเท่าตัว ขณะที่อุปกรณ์อื่นๆก็พยายามเพิ่มคุณสมบัติการเชื่อมต่อกับอินเทอร์เน็ตลงไป เช่น นาฬิกา แว่นตา จึงเกิดแนวโน้มที่เรียกว่า Internet of everything นอกจากนี้ยังมีการนำอุปกรณ์เหล่านี้เข้าไปใช้ในองค์กรด้วย ซึ่งต้องยอมรับว่าระบบรักษาความปลอดภัยบนอุปกรณ์ที่เกิดขึ้นใหม่เหล่านี้ยังไม่แข็งแกร่งมากพอเมื่อเทียบกับคอมพิวเตอร์พีซีที่มีการต่อสู้กับภัยไซเบอร์มากกว่า 10 ปี ซึ่งหากคิดในมุมของแฮกเกอร์แล้ว ยิ่งมีอุปกรณ์เชื่อมต่ออินเทอร์เน็ตมากขึ้นเท่าไหร่ ยิ่งเป็นการขยายช่องทางในการโจมตีให้มากขึ้นเท่านั้น"

นายสุวิชชากล่าวว่า จุดเสี่ยงที่ 4 ซึ่งน่าสนใจในปี 2557 คือ "การโจมตีในอุตสาหกรรมโครงสร้างพื้นฐาน" เช่น ระบบสาธารณูปโภค ไฟฟ้า ประปาต่างๆ ซึ่งที่ผ่านมา ระบบสาธารณูปโภคเหล่านี้ไม่เคยใช้การเชื่อมต่อผ่านอินเทอร์เน็ตมาก่อน แต่ปัจจุบันระบบสาธารณูปโภคเหล่านี้เริ่มเปิดให้มีการเชื่อมต่อผ่านอินเทอร์เน็ต เช่น ในหลายประเทศที่มีนโยบายสนับสนุนให้ประชาชนติด Solar Roof เพื่อผลิตไฟฟ้าพลังงานแสงอาทิตย์และจำหน่ายคืนให้กับการไฟฟ้า ช่องทางในการส่งข้อมูลกลับไปที่การไฟฟ้านั้นใช้ช่องทางอินเทอร์เน็ต ตรงนี้ถือเป็นโอกาสให้แฮกเกอร์ใช้ช่องทางนี้ในการเจาะเข้าไปโจมตีได้

ในอดีตการจะเจาะระบบควบคุมการจ่ายไฟฟ้านั้นถือเป็นเรื่องยากมาก แต่ปัจจุบันแฮกเกอร์มีทุน สามารถที่จะส่งคนไปเรียนรู้ระบบการจ่ายไฟฟ้า หรือหาเครื่องมือมาทดลองใช้งานได้ พัฒนาการที่ก้าวกระโดดของแฮกเกอร์นั้นทำให้หน่วยงานสาธารณูปโภคต่างๆ ที่มีการเชื่อมต่อกับอินเทอร์เน็ตจำเป็นต้องมีระบบความปลอดภัยที่สูงขึ้นเพื่อป้องกันภัยคุกคามใหม่ๆ ที่อาจเกิดขึ้นได้ในอนาคต

“แฮกเกอร์อาจจะเริ่มจากวิธีง่ายๆ ด้วยการค้นหาข้อมูลจากกูเกิลว่ามีประเทศใดที่ทำ Smart Grid บ้าง จากนั้นก็เลือกประเทศเป้าหมายที่จะโจมตี ซึ่งหากว่าแฮกเกอร์ทำได้สำเร็จ วิธีที่ง่ายที่สุดคือ การเข้าไปที่ระบบควบคุมและสั่งให้ตัดการจ่ายไฟฟ้าก่อนจะยื่นข้อเสนอเป็นเงินค่าไถ่ สำหรับในประเทศไทยซึ่งกำลังก้าวเข้าสู่ยุค Smart Grid นั้น การไฟฟ้าแห่งประเทศไทยมีแผนรับมือภัยไซเบอร์เหล่านี้อยู่แล้ว”