5 นวัตกรรมด้านความปลอดภัยทางไซเบอร์สำหรับ ปี 2017

“โลกไม่เคยหยุดอยู่กับที่ และในโลกของความปลอดภัยก็เช่นกัน แฮกเกอร์หลายคนเป็นคนที่ฉลาด แต่เราต้องฉลาดกว่า เร็วกว่าและมีความสร้างสรรค์มากกว่า เพื่อให้องค์กรสามารถรับมือและตอบโต้ภัยคุกคามที่เปลี่ยนแปลงรูปแบบวิธีการโจมตีอันหลากหลายได้อย่างรวดเร็ว”

จากคำกล่าวข้าง คือเหตุผลสำคัญที่ว่า ทำไมการวิจัยและพัฒนาจึงเป็นสิ่งที่สำคัญในธุรกิจความปลอดภัยบนเครือข่าย ผู้จำหน่ายโซลูชั่นต้องหาโซลูชั่นแบบเปิดและเป็นเทคโนโลยีที่สามารถรวมเอาการเชื่อมโยงเครือข่ายพร้อมกับคุณสมบัติด้านความปลอดภัยเข้าไว้ด้วยกันได้อย่างเบ็ดเสร็จ เพื่อให้บรรลุสู่เป้าหมายในการช่วยให้องค์กรมองเห็นและโต้ตอบต่อภัยคุกคามที่นับวันจะยิ่งปรับเปลี่ยนทั้งวิธีการโจมตีและรูปแบบของภัยคุกคามอยู่ตลอดเวลา นอกจากนั้นยังต้องเพิ่มความเร็วในการรับมือและปรับเปลี่ยนขนาดของระบบได้อย่างยืดหยุ่นตามการเติบโตของธุรกิจ ดังนั้นผู้จำหน่ายโซลูชันมากมายจึงหันมาพัฒนาองค์ประกอบในระบบนิเวศน์ด้วยตนเอง

ฟอร์ติเน็ตเองในปี 2016 เน้นหนักไปที่การสร้างนวัตกรรม เพื่อเป็นผู้นำในระบบนิเวศน์ของความปลอดภัยบนเครือข่าย โดยได้จดสิทธิบัตรราว 80 รายการในด้านต่างๆ อาทิ ความปลอดภัยบนคลาวด์ (CASB) เทคนิคการดักจับมัลแวร์ การป้องกันข้อมูลรั่วไหล การดักจับไวรัส การเร่งศักยภาพของฮาร์ดแวร์ บริการด้านคลาวด์ และ DDoS ฯลฯ และสำหรับปี 2017 ทางฟอร์ติเน็ตวางแผนการวิจัยและพัฒนาเพิ่มเติมอีก 5 นวัตกรรมด้วยกัน

1.เทคโนโลยี Deep learning เพื่อวิเคราะห์ภัยคุกคาม (Deep learning for attack analysis)

สำหรับ เทคโนโลยี Deep learning เป็นรูปแบบขั้นสูงของปัญญาประดิษฐ์ (Artificial intelligence: AI) เป็นกระบวนการที่ใกล้เคียงกับวิธีที่สมองมนุษย์รับรู้สิ่งต่างๆ ได้ ซึ่งมีผลกระทบกับความปลอดภัยไซเบอร์มาก โดยเฉพาะอย่างยิ่ง ในการหามัลแวร์ประเภท Zero-day malware และมัลแวร์ใหม่ หรือภัยที่มีความซับซ้อนสูงมากเป็นพิเศษ (Very sophisticated advanced persistent threats: APTs)

เมื่อแมชชีนรู้ว่าโค้ดแปลกปลอมมีหน้าตาอย่างไร แมชชีนนั้นจะสามารถระบุโค้ดที่ยังไม่รู้จักมาก่อน ว่าเป็นอันตรายหรือไม่ด้วยอัตราความแม่นยำที่สูงในความเร็วที่เกือบเป็นเรียลไทม์ ต่อจากนั้น จะประยุกต์ใช้นโยบายมาทำการลบหรือกักกันไฟล์นั้น หรือลงมือกระทำใดๆ ต่อไป ซึ่งข้อมูลใหม่นี้จะถูกแชร์กระจายไปทั่วเครือข่ายอย่างอัตโนมัติ

ในปี 2017 นี้ ฟอร์ติเน็ตจะเดินหน้าพัฒนาเทคโนโลยีที่ออกแบบมาเพื่อให้อุปกรณ์ของเราสามารถเรียนรู้ได้ฉลาดขึ้น และสามารถระบุมัลแวร์ที่ยังไม่รู้จักได้แม่นยำมากขึ้น

2. บิ๊กดาต้าสำหรับรายงานสหสัมพันธ์ (Big data for log correlation)

ไอทีได้เข้ามามีบทบาทสำคัญในชีวิตและธุรกิจของเราอย่างลึกซึ้ง ซึ่งนำไปสู่ภาวะการเกิด รวบรวม เก็บข้อมูลจากทั่วโลกมากมาย จึงทำให้มีข้อมูลขนาดใหญ่เติบโตขึ้นอย่างรวดเร็ว ฟอร์ติเน็ตตั้งเป้าจะใช้เทคโนโลยีด้านการบริหารอีเวนท์และข้อมูลด้านความปลอดภัย (Security Information & Event Management: SIEM) ในปีนี้ และจะเพิ่มประสิทธิภาพการทำงานของโซลูชั่นนี้ เพื่อเพิ่มความแม่นยำของทีม FortiGuard ในการตรวจสอบภัยไซเบอร์ได้ลึกมากขึ้น

3.สร้างคอนเทนเนอร์ให้แข็งแกร่ง (Strengthening container security)

ในปีนี้ พบว่าการรันแอพพลิเคชั่นในคอนเทนเนอร์ (Container) ที่สร้างสภาพแวดล้อมเฉพาะให้ซอฟต์แวร์ทำงานได้โดยไม่รบกวนกับซอฟต์แวร์ตัวอื่นบนระบบปฏิบัติการเดียวกันและจัดไว้แทนที่จะใช้ในเครื่องเสมือน (Virtual machines: VMs) นั้นมีผลกระทบที่สำคัญมาก ทั้งนี้ โซลูชั่น เช่น Docker ซึ่งเป็นโปรเจ็กและแพลตฟอร์มแบบโอเพ่นซอร์ส ที่เอื้ออำนวยให้ผู้ใช้งานสามารถรวบรวม แจกจ่าย และบริหารแอปพลิเคชั่น Linux ภายในได้นั้นกำลังเป็นที่กล่าวถึงอย่างมาก

ไมเคิล ซี ผู้ก่อตั้ง ประธานและประธานบริหารด้านเทคโนโลยี, ฟอร์ติเน็ต

การใช้ซอฟต์แวร์ Docker มีประโยชน์มากมาย อาทิ ง่ายกว่า ตั้งค่าได้เร็วกว่า เริ่มต้นใช้งานได้เร็วกว่า แต่อาจยังมีข้อด้อยด้านความปลอดภัยอยู่ เช่น ช่องโหว่ Kernel exploits ไม่เหมือน VM ที่ Kernel จะถูกแชร์ในคอนเทนเนอร์และโฮสต์ทั้งหมด ซึ่งจะเป็นการขยายช่องโหว่ใน Kernel ได้กว้างมากขึ้นอาจถึงขั้นที่จะต้องปิดโฮสต์และแอพพลิเคชั่นที่เกี่ยวข้องทั้งหมด หรือภัยประเภท Denial-of-service attacks คอนเทนเนอร์จะแชร์ทรัพยากรของ Kernel ทั้งหมด ดังนั้น ถ้าคอนเทนเนอร์หนึ่งควบคุมการเข้าใช้ทรัพยากรใด อาจทำให้เกิดการปฏิเสธการให้บริการ (DoS) ในคอนเทนเนอร์อื่นในโฮสต์ได้

ข้อด้อยอีกประการก็คือ การทะลุเข้าคอนเทนเนอร์ โดยผู้ที่รุกรานที่เข้ามาในคอนเทนเนอร์ได้นั้นจะไม่สามารถเข้าในคอนเทนเนอร์อื่นๆ หรือบนโฮสต์ได้ แต่ใน Docker ผู้ใช้งานโดยดีฟอลท์จะไม่ใช่กลุ่ม Name-spaced ดังนั้น หากสามารถทะลุเข้ามาในคอนเทนเนอร์ได้ จะมีสิทธิ์เช่นเดียวกับในคอนเทนเนอร์กระทำการบนโฮสต์ได้ ซึ่งนี่อาจจะเป็นการโจมตีเพื่อยกระดับสิทธิ์ของตนเองให้สูงขึ้นได้มาก (เช่น พวก root user) นอกจากนี้ คอนเทนเนอร์ที่จะเชื่อมโยงไปสู่ดาต้าเบสหรือบริการ และมักจะขอ API keyหรือชื่อผู้ใช้งานและรหัสผ่าน ซึ่งเป็นปัญหาในโครงสร้างประเภทที่คอนเทนเนอร์จะหยุดและเริ่มทำงานใหม่อยู่บ่อยๆ รวมถึงโครงสร้าง VMs ด้วยเช่นกัน ดังนั้นการวิจัยของฟอร์ติเน็ตจะให้ความสำคัญแก่เรื่องในข้างต้นเป็นอย่างมาก เนื่องจากมีแนวโน้มการใช้เทคโนโลยีคอนเทนเนอร์มากขึ้น

4.ความปลอดภัยแก่อุปกรณ์ปลายทางเสมือนของลูกค้า(Securing vCPE)

ในปัจจุบัน ความต้องการของธุรกิจเปลี่ยนรวดเร็วมาก องค์กรจึงต้องการความยืดหยุ่น ความไวในการปรับเปลี่ยนสาขาของตนเอง จึงนิยมใช้อุปกรณ์ปลายทางเสมือน (Virtual customer premise equipment: vCPE) มากขึ้น และนี่เป็นวิธีที่ผู้ให้บริการแบบ Manage Service จะให้บริการของตนแก่ลูกค้าองค์กรได้เร็วและเป็นแบบ On-Demandได้ด้วย ซึ่งรวมถึงบริการ Firewall และ VPN

นอกจากนี้ ในด้านการยกระดับ Network Function Virtualization (NFV) ฟอร์ติเน็ตมีความก้าวหน้าในการรวมบริการด้านความปลอดภัยและการเชื่อมโยงเครือข่ายในระดับสูงในอุปกรณ์เดียวกันเป็นที่เรียบร้อยแล้ว นั่นคืออุปกรณ์FortiHypervisor ซึ่งจะสามารถลดจำนวน CPE ในขณะที่จะให้บริการแบบออนดีมานด์ในอุปกรณ์เดียวได้ ซึ่งแน่นอนว่า ฟอร์ติเน็ตยังคงเดินหน้าพัฒนาคุณภาพการใช้บริการของลูกค้าในปีนี้ต่อไป

5. ช่วยองค์กรยกระดับSD-WAN (Helping enterprises leverage SD-WAN)

องค์กรมีความต้องการใช้เทคโนโลยี Cloud-based WAN ที่อยู่บนคลาวด์มากขึ้น ส่งผลให้เครือข่ายประเภท Software Defined Wide Area Networks (SD-WANs)มีความจำเป็นมากขึ้น แน่นอนว่า SD-WAN มีศักยภาพในการพัฒนาความปลอดภัยเครือข่ายได้หลายวิธี อาทิ สร้างการเชื่อมต่อที่มีความปลอดภัย สามารถทำให้ทราฟฟิคถูกเข้ารหัสได้ง่าย สามารถแบ่งเครือข่ายเพื่อทำการจำกัดการแพร่กระจายให้อยู่ในวงแคบและจัดการได้ นอกจากนี้ในการจัดวางอุปกรณ์ยังสามารถช่วยเพิ่มการมองเห็นภัยคุกคามในจุดที่ทราฟฟิคจะเข้ามายังเครือข่าย SD-WAN ช่วยให้องค์กรเห็นภัยคุกคามได้เร็วขึ้น ดังนั้นในปีนี้ ฟอร์ติเน็ตจะพัฒนา SD-WAN เพื่อประโยชน์สำหรับกลุ่มลูกค้าองค์กร

จากวิสัยทัศน์และการพัฒนาทางเทคโนโลยีของซีเคียวริตี้แฟบริค (Security Fabric) ผืนผ้าด้านความปลอดภัยของฟอร์ติเน็ต เราจึงมีศักยภาพในการรับมือกับภัยคุกคามที่เกิดขึ้นหลายรูปแบบในข้างต้น และสามารถช่วยสนับสนุนองค์กรให้ก้าวเข้าสู่ยุค Digital Transformation เราจะเดินหน้าพัฒนาผืนผ้าแห่งความปลอดภัยนี้ให้ครอบคลุมบริเวณที่กว้างมากขึ้น พร้อมกับมุ่งมั่นทำความเข้าใจว่าองค์กรจะสร้างวิธีปฏิบัติด้านความปลอดภัยที่ดีที่สุดในอุตสาหกรรมของตนเองได้อย่างไร