กรมชลประทาน

กระทรวงเกษตรและสหกรณ์

โครงการศึกษาด้านสารสนเทศ

เรื่อง

นโยบาย BYOD ของกรมชลประทาน

โดย

ส่วนเทคโนโลยีสารสนเทศ
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
ประจำปีงบประมาณ ๒๕๕๘

บทสรุปสำหรับผู้บริหาร (Executive Summary)

โดย ส่วนเทคโนโลยีสารสนเทศ

๑ ชื่อเรื่อง “นโยบาย BYOD ของกรมชลประทาน”

๒ ความสำคัญของปัญหา

Bring Your Own Device หรือ BYOD คือการที่ผู้ใช้งานภายในองค์กรได้นำอุปกรณ์ส่วนตัวเข้ามาใช้งานเองภายในระบบเครือข่ายขององค์กร ซึ่งไม่เพียงแต่เครื่องคอมพิวเตอร์ประเภท Notebook หรือ Netbook เท่านั้น แต่ปัจจุบันยังมีอุปกรณ์ Smart Phone และ Tablet จำนวนมาก ทำให้ระบบเครือข่ายมีเครื่องลูกข่ายเพิ่มมากขึ้น ทำให้ ยากต่อการดูแลรักษาความปลอดภัยของระบบ เนื่องจากนโยบายรักษาความปลอดภัยสำหรับการปฏิบัติการบนเครื่องคอมพิวเตอร์ทั่วไปนั้นจะแตกต่างจากนโยบายรักษาความปลอดภัยสำหรับอุปกรณ์ Smart Phone และ Tablet โดยสิ้นเชิง จึงจำเป็นต้องกำหนดนโยบายรักษาความปลอดภัยในเรื่องนี้ใหม่ให้ชัดเจน มิฉะนั้นแล้วจะเกิดปัญหาต่อการใช้งานจริงของผู้ใช้งาน และส่งผลต่อภาพรวมของความปลอดภัยของระบบเครือข่ายองค์กรได้

๓ วัตถุประสงค์การศึกษา

ก) เพื่อศึกษาหลักการและแนวคิดในเรื่อง BYOD

ข) เพื่อเสนอแนะแนวทางการจัดทำนโยบาย BYOD แก่ผู้บริหารกรมชลประทาน

๔ กรอบแนวคิดการศึกษา

การศึกษาในเรื่อง BYOD ดำเนินการเป็นขั้นตอน ดังนี้

๑. รวบรวมข้อมูลเบื้องต้นจากเอกสารทางวิชาการ ตำรา และแหล่งข้อมูลต่างๆ ที่น่าเชื่อถือ

๒. นำข้อมูลที่ได้มาวิเคราะห์สภาพทั่วไป และประเด็นปัญหา

๓. กำหนดกรอบปัญหา และประเด็นที่ต้องดำเนินการ

๔. กำหนดข้อเสนอแนะเชิงนโยบาย และข้อเสนอแนะเชิงเทคนิค

๕ วิธีการศึกษา

การศึกษาครั้งนี้เป็นการศึกษาเอกสาร (Documentary Research) โดยอาศัยข้อมูลทุติยภูมิจากบทความต่างๆ ในเว็บไซต์ ตลอดจนเอกสารบทความ งานวิจัยต่างๆ ที่เกี่ยวข้อง เพื่อวิเคราะห์และสรุปผลการศึกษา

๖ ผลการศึกษา

ผลการศึกษาสรุปเป็นแนวทางที่กรมชลประทานควรจะต้องดำเนินการ โดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นเจ้าภาพ เพื่อดำเนินการต่างๆ ดังนี้

- จัดตั้งคณะทำงานรวบรวมข้อมูล และดำเนินการตามขั้นตอนในการจัดทำนโยบาย BYOD ตามที่เสนอไว้ในส่วนที่ ๒

- พิจารณาจัดทำและกำหนดแนวปฏิบัติสำหรับการรักษาความปลอดภัยเบื้องต้นของอุปกรณ์ BYOD โดยใช้ทรัพยากรเครือข่ายของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเท่าที่มีอยู่ปัจจุบัน
- ตรวจสอบ BYOD Solution ที่เหมาะสมกับกรมชลประทาน และจัดทำรายละเอียดและขอสนับสนุนงบประมาณในการดำเนินการ
- ดำเนินการจัดหาและติดตั้งอุปกรณ์ต่างๆ หลังจากได้รับงบประมาณ
- เสนอผู้บริหารกรมฯ เพื่อให้ความเห็นชอบและประกาศใช้ โดยให้หน่วยงานต่างๆ ถือปฏิบัติโดยเคร่งครัด

๗ ปัจจัยแห่งความสำเร็จ

การดำเนินการตามข้อเสนอแนะข้างต้นให้เป็นไปตามเป้าหมายที่กำหนดไว้ จำเป็นต้องมีปัจจัยเงื่อนไขแห่งความสำเร็จเข้ามาประกอบร่วมด้วย ดังนี้

๑ การสนับสนุนงบประมาณในการจัดหาอุปกรณ์และการพัฒนาบุคคลากร

๒ นโยบายต้องมีความต่อเนื่อง เนื่องจากนโยบาย/โครงการบางเรื่องจำเป็นต้องใช้ระยะเวลาในการปรับเปลี่ยน การสร้างการยอมรับ รวมถึงการเห็นผลอย่างเป็นรูปธรรม

๓ การจัดฝึกอบรม/สัมมนาบุคลากร เพื่อเสริมสร้างความรู้ ความเข้าใจ และภัยแฝงที่มาในขณะใช้งาน หากไม่มีนโยบายหรือแนวปฏิบัติเพื่อควบคุมที่ดีพอ

๔ จัดตั้งคณะทำงานเพื่อประสานนโยบายให้สำเร็จลุล่วงไปได้ด้วยดี

๕ ประเมินผลและปรับปรุงนโยบายเมื่อพบข้อบกพร่องทุกปี เพื่อให้มีความสมบูรณ์ต่อไป

คำนำ

ปัจจุบัน หลายๆ องค์กรในประเทศไทยกำลังประสบกับปัญหาในการบริหารจัดการทางด้านความปลอดภัยของระบบสารสนเทศ ในกรณีที่ผู้ใช้งานในองค์กรนำอุปกรณ์ส่วนตัวต่างๆ มาใช้งานเอง เช่น เครื่องคอมพิวเตอร์ Notebook, Tablet หรือ Smart Phone ต่างๆ เป็นต้น ในบางองค์กรจะมีปัญหาตั้งแต่ระดับของความไม่เพียงพอของระบบเครือข่าย ส่วนบางองค์กรมีปัญหาในเรื่องของการจัดทำนโยบายการรักษาความมั่นคงปลอดภัยเพื่อควบคุมการใช้งานอุปกรณ์ส่วนตัวต่างๆ เหล่านี้

โครงการศึกษาด้านสารสนเทศเรื่อง “นโยบาย BYOD ของกรมชลประทาน” ฉบับนี้เพื่อเสนอแนะแนวทางและขั้นตอนการจัดทำนโยบาย BYOD แก่ผู้บริหาร โดยเน้นให้เห็นถึงความสำคัญของปัญหาและปัจจัยเสี่ยงที่จะเกิดขึ้นต่อระบบสารสนเทศของกรมชลประทานหากไม่มีการควบคุมและรักษาความปลอดภัยที่ดีพอ ตลอดจนเพื่อให้เกิดประสิทธิภาพสูงสุดต่อการใช้งานอุปกรณ์ต่างๆ ในระบบสารสนเทศของกรมชลประทานที่จะมีเพิ่มมากขึ้นในทุกๆ ปี

นายสมนึก จิระศิริโสภณ
ผู้อำนวยการส่วนเทคโนโลยีสารสนเทศ
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมชลประทาน
เมษายน ๒๕๕๘

สารบัญ

ส่วนที่ ๑
ข้อมูลทั่วไป

ความเป็นมา

BYOD ย่อมาจาก Bring Your Own Device เป็นหนึ่งใน Trend เกี่ยวกับเทคโนโลยีที่กำลังจะมีบทบาทต่อการทำงานขององค์กรและหน่วยงานภาครัฐต่างๆทั่วโลก สภาพการทำงานที่เปลี่ยนแปลงไปอย่างรวดเร็วนี้ ย่อมส่งผลให้การแข่งขันในโลกไร้พรมแดนทวีความรุนแรงขึ้น และเป็นแนวทางการทำงานได้ทุกเวลาทุกสถานที่ BYOD ถือเป็นแนวคิดสำคัญที่องค์กร ต่างๆ ให้ความสำคัญมากขึ้นเรื่อยๆ องค์กรในโลกธุรกิจประมาณ ๙๐ % จะอนุญาตให้พนักงานนำอุปกรณ์พกพาส่วนตัว มาใช้งาน เช่น Notebook, Tablet หรือ Smartphone โดยใช้ทรัพยากรของ องค์กรที่มีนโยบาย การควบคุมการเข้าถึง และใช้ร่วมกับระบบเครือข่าย ระบบฐานข้อมูล, อีเมลล์, แอพพลิเคชันและบริการอื่นๆ ขององค์กรได้ ทำให้องค์กรไม่ต้องจัดหาอุปกรณ์ทำงานเหล่านี้ให้ และสามารถเชื่อมต่อเครือข่ายไร้สายขององค์กรได้อีกด้วย แต่ในขณะเดียวกันอุปกรณ์ที่นำมาใช้ก็จะต้องมีการปรับแต่งและบังคับให้มีการรักษาความปลอดภัยต่างๆ ตามที่กำหนดด้วยเช่นกัน องค์กรส่วนใหญ่จึงคิดว่านโยบาย BYOD จะช่วยเสริมประสิทธิภาพการทำงานของเจ้าหน้าที่ให้ดียิ่งขึ้นได้

วัตถุประสงค์

๑. เพื่อเพิ่มประสิทธิภาพในการทำงาน
๒. เพื่อลดค่าใช้จ่ายในการจัดซื้ออุปกรณ์และการบำรุงรักษาของหน่วยงานภาครัฐ
๓. เพื่อผสมผสานโลกของการทำงานให้เข้ากับการใช้งานส่วนตัวได้อย่างสะดวกยิ่งขึ้น

คำศัพท์เทคนิคที่ควรทราบ

การรักษาความปลอดภัยอุปกรณ์ต่างๆ ที่นำมาใช้ในองค์กร คำศัพท์เทคนิค (Keyword) ที่เรามักจะพบเห็นกันบ่อยๆ มีดังต่อไปนี้

Network Access Control – NAC

NAC คือระบบรักษาความปลอดภัยเครือข่าย โดยมุ่งเน้นไปที่การควบคุมการใช้งานเครื่องลูกข่ายและอุปกรณ์เครือข่ายทั้งหมดที่มี MAC Address และ IP Address ให้สามารถใช้งานระบบเครือข่ายได้ในระดับที่แตกต่างกันตามความปลอดภัยของอุปกรณ์นั้นๆ เช่น

- ผู้ใช้งานในองค์กรอาจจะมีสิทธิ์ในการเข้าถึงเครื่องแม่ข่าย (Server) แตกต่างกันตามแผนกของตน และผู้ใช้งานที่เป็นบุคคลภายนอกจะไม่สามารถเข้าถึงเครื่องแม่ข่ายใดๆ ได้เลย
- เครื่องลูกข่ายที่มีการติดตั้งซอฟต์แวร์และอัพเดต Anti-virus ตามที่กำหนด จะมีสิทธิ์ในการใช้งาน Protocol หรือเข้าถึงระบบงานต่างๆ ที่สูงกว่าเครื่องลูกข่ายที่ไม่ได้ติดตั้งซอฟต์แวร์ที่กำหนด หรือมี Anti-virus ที่ไม่อัพเดต

- เครื่องลูกข่ายที่มีพฤติกรรมโจมตีเครือข่าย หรือติดไวรัส จะถูกตัดสิทธิ์ในการใช้งาน Protocol ที่มีความเสี่ยง เช่น FTP ออกไป รวมถึงสามารถมีการแจ้งเตือนผู้ที่ใช้งานเครื่องลูกข่ายเหล่านั้นได้ว่ามีการติดไวรัส และสั่งเรียกให้ซอฟต์แวร์ Anti-virus ทำงานเพื่อค้นหาและกำจัด Virus ทันที

โดยทั่วไปแล้ว NAC จะสามารถตรวจสอบเครื่องลูกข่ายทั้งหมดได้ในระดับของเครือข่าย (Network) และมีการแถมซอฟต์แวร์ Agent สำหรับการตรวจสอบเครื่องลูกข่ายมาตรฐานเช่น Windows, Mac, Linux มาให้ด้วย เพื่อให้แต่ละองค์กรสามารถออกแบบนโยบายการรักษาความปลอดภัยได้อิสระ และบังคับตรวจสอบในเชิงลึกระดับ Application และ Process ที่ใช้งานได้ทันที โดย NAC จะมีบทบาทสำคัญเป็นอย่างมากในการรักษาความปลอดภัยระบบเครือข่ายทั้งแบบมีสายและไร้สายไปพร้อมๆ กัน ทำให้ระบบเครือข่ายมีความปลอดภัยมากขึ้น และผู้ใช้งานไม่สับสนจากการเจอการยืนยันตัวตนที่หลากหลายในระบบเครือข่ายแบบเดิมๆ

นอกจากนี้ NAC ส่วนมากในทุกวันนี้จะมีความสามารถในการทำ BYOD พ่วงมาด้วยในตัว โดยบางยี่ห้อจะสามารถใช้งานได้ฟรีๆ ไม่มีค่าใช้จ่ายเพิ่มเติม ในขณะที่บางยี่ห้อจะต้องเป็น Option เสริม ซึ่งมีค่าใช้จ่ายเพิ่มเติม รวมถึงยังสามารถทำงานร่วมกับ MDM หลากหลายยี่ห้อได้อีกด้วย

Bring Your Own Device – BYOD

BYOD เป็นคำที่ใช้เรียกเมื่อในระบบเครือข่ายขององค์กรมีการนำอุปกรณ์ส่วนตัวเข้ามาใช้งานอย่างมีนัยยะสำคัญ ในบางองค์กรที่เมืองนอกอาจจะมีการเพิ่มเงินให้พนักงานเมื่อมีการนำ Notebook หรือ Smart Phone เข้ามาใช้งานเอง ทำให้องค์กรไม่ต้องจัดหาอุปกรณ์ทำงานเหล่านี้ให้ แต่ในขณะเดียวกันอุปกรณ์ที่นำมาใช้ก็จะต้องมีการปรับแต่งและบังคับให้มีรักษาความปลอดภัยต่างๆ ตามที่กำหนดด้วยเช่นกัน

สำหรับเมืองไทย การทำ BYOD หลักๆ คือการรักษาความปลอดภัยสำหรับอุปกรณ์ที่ผู้ใช้งานนำมาใช้เอง เช่น Notebook, Smart Phone, Tablet โดยจำกัดการใช้งานที่ระดับเครือข่าย โดยบังคับให้มีการยืนยันตัวตน และบังคับให้มีสิทธิ์ในการเข้าถึงระบบเครือข่ายน้อยกว่าการนำอุปกรณ์ขององค์กรมาใช้งาน รวมถึงในบางกรณียังมีการจำแนกประเภทของอุปกรณ์ เช่น Apple iPhone, Google Android หรือ Microsoft Windows Phone และกำหนดสิทธิ์ให้อุปกรณ์ต่างๆ มีสิทธิ์ในระดับที่แตกต่างกันอีกด้วย หรือบางกรณีก็อาจห้ามไม่ให้มีการใช้งานอุปกรณ์บางประเภทที่มีความเสี่ยงทางด้านความปลอดภัยในระดับสูงเลยก็เป็นได้

Mobile Device Management – MDM

MDM เป็นคำที่ใช้เมื่อต้องการที่จะควบคุมอุปกรณ์ Smart Phone และ Tablet ในเชิงลึก เช่น การตรวจสอบ Application ที่มีการติดตั้งและใช้งาน, การตรวจสอบการทำ Jailbreak หรือ Root, การบังคับห้ามใช้งานซอฟต์แวร์บางประเภท, การตรวจสอบสถานที่ของอุปกรณ์เหล่านั้น, การบังคับตั้งค่าการใช้งานของอุปกรณ์ให้มีความปลอดภัย, การบังคับลบข้อมูลสำคัญขององค์กร โดยทั่วไป MDM มักจะมีค่าใช้จ่ายต่ออุปกรณ์ที่มีการใช้งาน และสามารถควบคุมอุปกรณ์เหล่านั้นผ่านระบบเครือข่าย Public Internet หรือ ๓G ได้ ทำให้ MDM เหมาะสมต่อการบังคับใช้งานอุปกรณ์ Smart Phone และ Tablet ที่เป็นทรัพย์สินขององค์กรแจกให้พนักงานใช้ทำงานได้สะดวกยิ่งขึ้น ในขณะที่การบังคับใช้ MDM กับอุปกรณ์ที่พนักงานนำมาใช้เองนั้น จะทำให้องค์กรต้องเสียค่าลิขสิทธิ์ในการใช้งาน MDM ไปเป็นจำนวนมาก และไม่สามารถควบคุมจำนวนของลิขสิทธิ์เหล่านั้นได้

ข้อดี-ข้อเสียของ BYOD

ข้อดี

- **ลดค่าใช้จ่ายให้กับองค์กร (Cost Saving)** เพราะผู้ปฏิบัติงานเป็นคนนำอุปกรณ์ต่างๆ เหล่านั้นมาเอง ทำให้องค์กรไม่จำเป็นลงทุนในอุปกรณ์ บางอย่าง โดยบางองค์กรอาจใช้วิธีการเช่าเครื่องของพนักงานแทนการซื้อเครื่องให้ เพื่อลดต้นทุนในการลงทุนด้านการซื้ออุปกรณ์ต่างๆ รวมถึงซอฟแวร์บางประเภทได้เช่นเดียวกัน
- ผู้ปฏิบัติงานจะดูแลอุปกรณ์ของตัวเองเป็นอย่างดี
- **มีเทคโนโลยีใหม่ๆ อย่างต่อเนื่อง (New technology)** เมื่อเปิดโอกาสให้ ผู้ปฏิบัติงาน นำอุปกรณ์ต่างๆ มาเอง จะเปิดโอกาสให้องค์กร มีอุปกรณ์ใหม่ๆ เข้ามาใช้กับงานและธุรกิจมากขึ้น รวมถึงการแบ่งปันข้อมูลความรู้เกี่ยวกับเทคโนโลยีใหม่ๆ ระหว่างผู้ปฏิบัติงานได้ดีมากขึ้น
- **สะดวกสบาย (Convenience)** เพราะเป็นเครื่องของตัวเอง ทำให้การจัดการและดูแลอุปกรณ์ต่างๆ สะดวกมากขึ้น บางครั้งพ ผู้ปฏิบัติงาน สามารถ ลงโปรแกรมอะไรบางอย่างที่ตัวเองอยากใช้งานได้สะดวกมากขึ้น
- **สร้างความเพิ่งพอใจให้กับพนักงาน (Increase Satisfaction)** เพราะผู้ปฏิบัติงาน สามารถเลือกอุปกรณ์ต่างๆ ตามความต้องการและความเหมาะ สมของตัวเองได้
- **เพิ่มประสิทธิภาพในการทำงาน (Increase Productivity)** เพราะเนื่องจากเป็นเครื่องของตัวเอง ทำให้ผู้ปฏิบัติงานสามารถทำงานได้ทุกที่ และ สามารถกลับไปทำงานที่บ้านได้

ข้อเสีย

- **ความปลอดภัยของข้อมูลภายในองค์กร (Security)** ข้อมูลต่างๆ ของ องค์กรจะต้องอยู่ในเครื่องของผู้ปฏิบัติงาน และสามารถติดตัวไปไหนก็ได้ ดังนั้นหากเป็นข้อมูลที่เป็นความลับ อาจจะเสี่ยง ต่อการรั่วไหลของข้อมูลได้ เพราะบางครั้งผู้ปฏิบัติงานอาจจะทำอุปกรณ์เหล่านี้หายหรือลืม
- **ไวรัสและมัลแวร์ (Virus & Mallware)** เนื่องจากเป็นเครื่องส่วนตัว การดูและการจัดการอาจจะยังไม่ดี ซึ่งจะมีความเสี่ยงต่อการติดไวรัสและมัลแวร์ และเมื่อนำมาใช้กับในองค์กรอาจจะทำให้เกิด การแพร่กระจายไปยังเครื่องอื่นๆ ในองค์กรได้
- **การช่วยเหลือ (Support)** เนื่องจากเครื่องและอุปกรณ์มีความหลากหลาย อาจจะทำให้การช่วยเหลือผู้ปฏิบัติงาน กรณีอุปกรณ์ต่างๆ มีความผิดพลาดเป็นไปได้ยาก เพราะองค์กรอาจจะไม่มีบุคคลากรที่มีความรู้ความสามารถในอุปกรณ์นั้นๆ
- **การรองรับของ เน็ตเวิร์ค (Network Capacity)** เนื่องจากองค์กรต่างๆ อาจจะไม่ได้เตรียมตัวหรือรองรับจำนวนอุปกรณ์ต่างๆ ที่เพิ่มขึ้นมาจำนวนมากจาก ผู้ปฏิบัติงานได้ เช่น แต่ละคนนำ Smartphone หรือ Tablet มาเชื่อมต่อกับ เน็ตเวิร์คองค์กร อาจจะทำให้มีการใช้ Bandwidth เพิ่มมากขึ้น จนทำให้เน็ตเวิร์คขององค์กรช้าลงได้
- ผู้ปฏิบัติงาน อาจจะไม่สามารถใช้งานได้อย่างเต็มที่ และอาจจะโดนบังคับด้วยกฎต่างๆ เพื่อให้ข้อมูลมีความปลอดภัย

ความเสี่ยงกับ BYOD

- ความเสี่ยงเรื่องของความปลอดภัยของข้อมูลองค์กร อาจนำไปสู่การรั่วไหลของข้อมูล
- การดาวโหลดไฟล์ที่ไม่มีลิขสิทธิ์ที่อาจมีมัลแวร์ ซึ่งเป็นอันตรายมาติดตั้งในเครื่อง และถือเป็นความเสี่ยงอย่างยิ่งต่อความปลอดภัยของข้อมูลองค์กร เมื่อนำเครื่องนั้น ๆ มาเชื่อมต่อกับที่ทำงาน
- การติดตามและควบคุมการเข้าถึงเครือข่ายของบริษัทและเครือข่ายส่วนตัว
- ปัญหาด้าน**การรองรับของเน็ตเวิร์ค (Network Capacity)**

หน่วยงานภาครัฐที่ใช้นโยบาย BYOD

- **ธนาคารแห่งประเทศไทย**

  ชื่อโครงการ ‘BYOD@BOT’ หรือ ‘Bring Your Own Device@BOT’ เพื่อให้สอดรับกับโอกาสและเพิ่มศักยภาพในการ ใช้ประโยชน์จากความก้าวหน้าทางเทคโนโลยีและการสื่อสาร

ส่วนที่ ๒
แนวทางการจัดทำนโยบาย BYOD

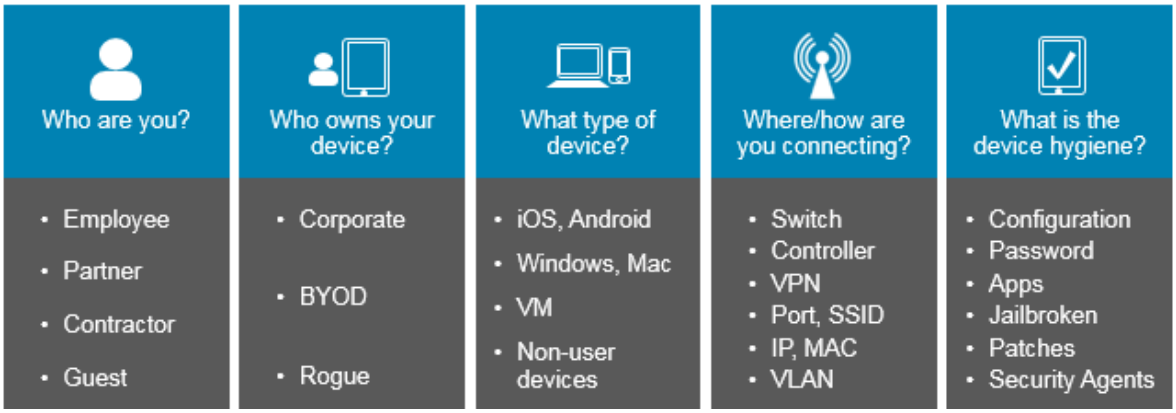
ขั้นตอนที่ต้องดำเนินการ

๑. จัดตั้งทีมงานสำหรับวางนโยบาย BYOD โดยเฉพาะ

การวางนโยบาย BYOD ที่ดีนั้นควรจะประกอบไปด้วยทีมงานที่มีความหลากหลาย ทั้งกลุ่มของทีมงาน IT ที่แตกต่างกัน เช่น ผู้ดูแลความปลอดภัย, ผู้ดูแลเครือข่าย, ผู้ดูแลเครื่องลูกข่าย และกลุ่มผู้ใช้งานจากหน่วยงานที่แตกต่างกัน รวมถึงควรจะมีผู้รับผิดชอบหลักสำหรับการวางนโยบาย BYOD โดยเฉพาะ นโยบาย BYOD ที่ดีควรจะเกิดขึ้นจากข้อตกลงร่วมกันระหว่างผู้ปฏิบัติงานและผู้บริหารจากแต่ละกลุ่มงาน พร้อมทั้งได้รับข้อมูลเสริมจากทีม HR โดยบทบาทของทีม IT ควรจะเป็นผู้ให้คำแนะนำและบังคับใช้งานระบบเครือข่ายให้เป็นไปตามนโยบายที่วางเอาไว้เท่านั้น

๒. รวบรวมข้อมูลนโยบายรักษาความปลอดภัยเดิมที่มีอยู่

จัดสร้างรายงานของนโยบายรักษาความปลอดภัยเดิมที่ใช้งานอยู่ และทำการทบทวนเพื่อทำความเข้าใจเหตุผลทางด้านความปลอดภัยและการบริหารจัดการของ IT พร้อมทั้งระบุว่าที่ผ่านมาหน่วยงานไหนที่เคยให้ความร่วมมือกับการวางนโยบายเหล่านี้มาก่อน จากนั้นจึงทำการรวบรวมข้อมูลดังต่อไปนี้ จำนวนอุปกรณ์โดยมีรายละเอียดของ Platform, OS version, ความเป็นเจ้าของอุปกรณ์เหล่านั้น เช่น เป็นขององค์กร หรือเป็นของส่วนตัวของผู้ปฏิบัติงาน, ประเมินปริมาณของข้อมูลที่มีการรับส่งผ่าน Mobile Device ทั้งหมด, Application บน Mobile Device ที่มีการใช้งาน, ความเป็นเจ้าของ Application เหล่านั้น, Security Profile ของ Application เหล่านั้น, วิธีการในการเชื่อมต่อ Mobile Device เข้ามายังระบบเครือข่ายขององค์กร เช่น ผ่านทางสัญญาณ ๓G, WiFi, Bridge เข้ากับเครื่อง PC หรือใช้ VPN เป็นต้น



๓. กำหนดและจัดลำดับความสำคัญของ Use Case ในการใช้งาน

เพื่อให้นโยบาย BYOD สามารถนำมาใช้งานได้จริง นโยบายทั้งหมดที่วางไว้จะต้องสอดคล้องกับการใช้งานหลากหลายรูปแบบบน Mobile Device ทั้งหมดในองค์กร โดยทีมงานสำหรับวางนโยบาย BYOD ควรจะต้องตอบคำถามเหล่านี้ได้อย่างชัดเจน

- อุปกรณ์ Mobile Device ต่างๆ จะถูกนำไปใช้ทำอะไรบ้าง?
- Mobile Application ใดบ้างที่จำเป็นจะต้องมีการนำไปใช้งานแบบ Offline? (เช่น บนเครื่องบิน หรือในลิฟต์โดยสาร)
- จะอนุญาตให้มีการเข้าถึงข้อมูลใดผ่านทาง Mobile Device ได้บ้าง?
- จะอนุญาตให้มีการจัดเก็บข้อมูลใดบน Mobile Device ได้บ้าง?

๔. ประเมินค่าใช้จ่าย, สิ่งที่จะได้รับกลับมา และความคุ้มค่าของโครงการ

การทำ BYOD อาจจะไม่ได้ช่วยลดค่าใช้จ่ายในทางตรง แต่ช่วยเพิ่มประสิทธิภาพในการทำงาน, ลดงานในการบริหารจัดการด้านความปลอดภัย, เพิ่มความดึงดูดในการร่วมงานจากบุคคลภายนอก โดยต้องประเมินค่าใช้จ่ายโดยรวมจาก

๔.๑. ค่าใช้จ่ายสำหรับอุปกรณ์ ซึ่งอาจจะเพิ่มขึ้นหรือลดลงตามแต่นโยบายความเป็นเจ้าของอุปกรณ์ที่กำหนด

๔.๒. ค่าใช้จ่ายสำหรับการเชื่อมต่อเครือข่าย ซึ่งองค์กรอาจจะช่วยลงทุนค่าสัญญาณโทรศัพท์หรือ ๓ G ให้

๔.๓. ค่าใช้จ่ายสำหรับลิขสิทธิ์ซอฟต์แวร์สำหรับทำงานบน Mobile Device และซอฟต์แวร์สำหรับติดตามและควบคุมการใช้งาน

๔.๔. ค่าใช้จ่ายสำหรับระบบเครือข่ายที่ต้องลงทุนเพิ่มเติม ทั้งทางด้านความปลอดภัย, การบริหารจัดการ, แบนด์วิดธ์ และการสำรองข้อมูล

๕. กำหนดนโยบาย

สำหรับองค์กรขนาดกลางและใหญ่ การออกแบบนโยบายเพียงแบบเดียวให้ครอบคลุมผู้ใช้งานทั้งองค์กรนั้นเป็นเรื่องที่แทบจะเป็นไปไม่ได้ ดังนั้นจึงควรแบ่งนโยบายแยกย่อยตามแต่ละความต้องการของผู้ใช้งานในองค์กรให้เหมาะสม เช่น สำหรับผู้ใช้งานทั่วๆ ไป ก็อาจจะเปิดให้ใช้งาน Application พื้นฐานอย่างเว็บหรืออีเมลล์ได้ แต่สำหรับทีม Sales ก็อาจจะเปิดให้ใช้งานระบบ CRM ได้เพิ่มเติมเข้าไป หรือสำหรับผู้บริหารก็อาจจะใช้งานได้ทุกอย่าง รวมถึงจำกัดประเภทของอุปกรณ์ที่สามารถนำมาใช้งานได้เพื่อลดความเสี่ยงทางด้านความปลอดภัย และแบ่งระดับของความปลอดภัยสำหรับ Mobile Device กับ Desktop/Laptop ให้ดี

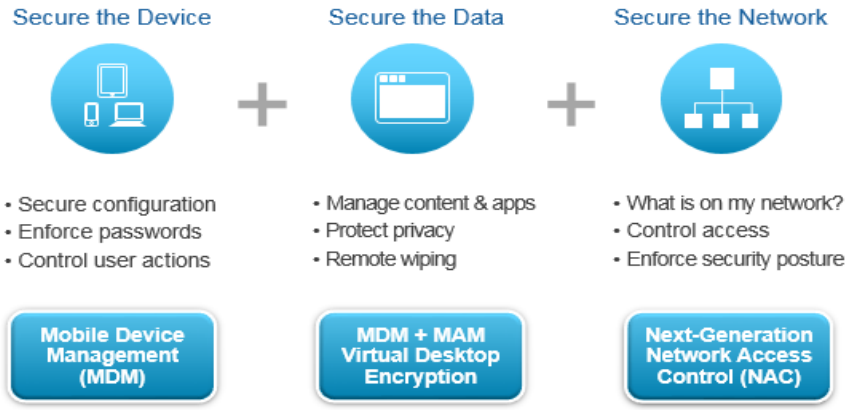
๖. เลือกวิธีการในการรักษาความปลอดภัยเครือข่าย

ส่วนนี้จะเป็นงานของทีม IT ว่าจะควบคุมระบบเครือข่ายให้สามารถทำตามนโยบายเหล่านั้นได้อย่างไรในเชิงเทคนิค เช่น จะยืนยันตัวตนอย่างไร ? จะจำกัดสิทธิ์การเข้าถึงระบบเครือข่ายอย่างไร ? จะควบคุม Application อย่างไร? โดยทั่วไปแล้ว Network Access Control (NAC) มักจะกลายเป็นตัวเลือกเพราะเป็นระบบที่มีความยืดหยุ่นสูง สามารถปรับแต่งให้เข้ากับนโยบายที่ต้องการได้ และยังบังคับใช้งานนโยบายได้อย่างอัตโนมัติ ซึ่งครอบคลุมทั้งการทำ Profiling สำหรับอุปกรณ์, ยืนยันตัวตนผู้ใช้งาน, บริหารจัดการ Guest, ทำ

Compliance และตรวจสอบการตั้งค่าต่างๆ รวมถึงทำการซ่อมแซมเครื่องลูกข่ายที่ไม่ผ่านนโยบายให้ปลอดภัยเพียงพอที่จะเข้าใช้งานเครือข่ายได้อีกด้วย

๗. เลือกวิธีการในการรักษาความปลอดภัยสำหรับข้อมูล

ถึงแม้ NAC จะช่วยรักษาความปลอดภัยในเครือข่าย แต่สำหรับอุปกรณ์ Mobile Device ที่มีการนำออกไปใช้นอกองค์กร NAC เองก็ไม่สามารถตามติดไปถึงได้ ต้องอาศัยการ Integrate ร่วมกับระบบ Mobile Device Management (MDM) เพื่อบริหารจัดการและรักษาความปลอดภัยของข้อมูลบน Mobile Device โดยเฉพาะ โดยสามารถแบ่งการจัดเก็บข้อมูลส่วนตัวและข้อมูลขององค์กรบนอุปกรณ์ต่างๆ ได้ และมีระบบ Container ช่วยป้องกันไม่ให้ข้อมูลขององค์กรถูกแชร์ออกไปผ่าน Application อื่นๆ รวมถึงสามารถทำการ Lock และล้างข้อมูลในเครื่องจากระยะไกลได้



๘. วางแผนโครงการสำหรับ BYOD

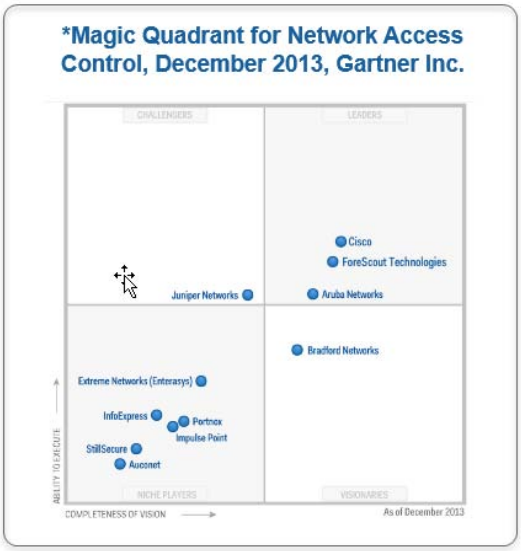
วางแผนในการติดตั้งบังคับใช้นโยบาย BYOD ในองค์กร โดยอาจจะมีการแบ่งออกเป็นหลายๆ Phase หรือบังคับติดตั้งใช้งานให้เสร็จในรวดเดียวเลยก็ได้ โดยทั่วไปแล้วนโยบายสำหรับ BYOD จะประกอบไปด้วยการควบคุมส่วนต่างๆ เหล่านี้

- การบริหารจัดการ Mobile Device จากระยะไกล
- การควบคุม Application
- การทำ Compliance และ Audit Report
- การเข้ารหัสข้อมูลและอุปกรณ์
- การรักษาความปลอดภัยในการใช้งาน Cloud Storage
- การลบข้อมูลในอุปกรณ์และลบอุปกรณ์ออกจากระบบเมื่อเลิกใช้งานอุปกรณ์นั้นแล้ว
- การยึดคืนสิทธิ์การเข้าถึงข้อมูลและเครือข่ายเมื่อผู้ปฏิบัติงานกลายเป็น Guest

๙. เลือกและประเมิน Solutions จาก Vendor รายต่างๆ

อ้างอิงจาก Gartner ซึ่งได้กล่าวไว้ว่า NAC และ MDM เป็นกุญแจสำคัญในการบังคับใช้นโยบาย BYOD ให้สำเร็จได้ เมื่อเรียก Vendor รายต่างๆ มาคุย นอกจากการพูดคุยถึงฟีเจอร์ต่างๆ แล้ว ให้ทำการประเมินให้ชัดเจนว่าการติดตั้งระบบเหล่านี้จะส่งผลกระทบอะไรต่อระบบเครือข่ายเดิมบ้าง และสามารถ

Integrate กับระบบรักษาความปลอดภัยเดิมที่มีอยู่ได้หรือไม่ ไม่ว่าจะเป็น Directories, Patch Management, Ticketing, Endpoint Protection, Vulnerability Assessment และ SIEM โดยต้องประเมินความสมดุลระหว่างค่าใช้จ่าย, ความปลอดภัย และการใช้งานจริงของผู้ใช้งาน



๑๐. เริ่ม Implement Solutions

การติดตั้งและค่อยๆ ปรับปรุงระบบเป็นหัวใจหลักในการทำให้การบังคับใช้งานนโยบาย BYOD เป็นจริงขึ้นมาได้ โดยควรเริ่มต้นจาก Pilot Project ที่แผนกใดแผนกหนึ่งก่อน เพื่อทดสอบและปรับปรุงนโยบาย BYOD ให้สามารถใช้งานได้จริง และไม่ติดขัดต่อการทำงาน จากนั้นจึงค่อยๆ เพิ่มขยายจำนวนของผู้ใช้งานต่อไปเรื่อยๆ

ตัวอย่าง Solution จาก ForeScout

ผู้สนใจสามารถพิจารณาได้ในภาคผนวก ก

ทางเลือกสำหรับนโยบายรักษาความปลอดภัย BYOD

แบ่งเป็น ๒ แบบ ดังตัวอย่างต่อไปนี้

๑ นโยบายรักษาความปลอดภัย BYOD แบบทั่วไป

สำหรับการรักษาความปลอดภัย BYOD แบบทั่วไป จะมีแนวทางดังนี้

- **PC/Notebook ขององค์กร** – รักษาความปลอดภัยระดับสูงด้วย NAC พร้อมติดตั้ง Agent โดยให้สิทธิ์ในการเข้าถึงระบบงานขององค์กรได้ตามแผนกของผู้ใช้งานและใช้งาน Internet ภายนอกได้ภายหลังการยืนยันตัวตน
- **Notebook ส่วนตัว** – รักษาความปลอดภัยระดับเครือข่ายด้วย NAC โดยสามารถติดตั้ง Agent แบบชั่วคราวเพื่อตรวจสอบเชิงลึก หรือไม่ติดตั้ง Agent ก็ได้ โดยให้สิทธิ์ในการเข้าถึงระบบงานพื้นฐานของ

องค์กรและใช้งาน Internet ภายนอกได้ภายหลังการยืนยันตัวตน เช่น ระบบ Email, เว็บไซต์ภายในองค์กร หรือระบบ Chat

- **Smart Phone/Tablet ขององค์กร** – รักษาความปลอดภัยด้วย NAC พร้อม MDM Agent เพื่อตรวจสอบและควบคุมเชิงลึก และให้สิทธิ์ในการเข้าถึงระบบงานขององค์กรได้ตามแผนกของผู้ใช้งานภายหลังการยืนยันตัวตน
- **Smart Phone/Tablet ส่วนตัว** – รักษาความปลอดภัยระดับเครือข่ายด้วย NAC โดยให้สิทธิ์ในการเข้าถึงระบบงานพื้นฐานขององค์กรและใช้งาน Internet ภายนอกได้ภายหลังการยืนยันตัวตน เช่น ระบบ Email, เว็บไซต์ภายในองค์กร หรือระบบ Chat

ข้อดี

- ระบบมีความปลอดภัยสูง เพราะจำกัดสิทธิ์ของอุปกรณ์ส่วนตัวที่นำมาใช้งานแต่แรก
- เข้าใจง่าย เนื่องจากพนักงานสามารถยอมรับได้ทันทีว่าอุปกรณ์ส่วนตัวจะไม่สามารถเข้าถึงข้อมูลสำคัญขององค์กรได้ และไม่มีซอฟต์แวร์ MDM คอยรุกล้ำความเป็นส่วนตัวของพนักงาน
- ประหยัดค่าใช้จ่าย โดยมีค่าใช้จ่าย NAC ในระบบรวม และมีค่าใช้จ่าย MDM เฉพาะในส่วนของทรัพย์สินองค์กรเท่านั้น

ข้อเสีย

- พนักงานไม่สามารถนำอุปกรณ์ส่วนตัวมาใช้ทำงานได้อย่างเต็มประสิทธิภาพ

๒ นโยบายรักษาความปลอดภัย BYOD แบบเข้มงวด

สำหรับการรักษาความปลอดภัย BYOD แบบเข้มงวด จะมีแนวทางดังนี้

- **PC/Notebook ขององค์กร** – รักษาความปลอดภัยระดับสูงด้วย NAC พร้อมติดตั้ง Agent โดยให้สิทธิ์ในการเข้าถึงระบบงานขององค์กรได้ตามแผนกของผู้ใช้งานและใช้งาน Internet ภายนอกได้ภายหลังการยืนยันตัวตน
- **Notebook ส่วนตัว** – รักษาความปลอดภัยสูงด้วย NAC โดยบังคับติดตั้ง Agent แบบชั่วคราวเพื่อตรวจสอบเชิงลึก หรือไม่อนุญาตให้ใช้งาน Notebook ส่วนตัวเลยก็ได้ โดยให้สิทธิ์ในการเข้าถึงระบบงานพื้นฐานขององค์กร, ใช้งานบางระบบงานขององค์กรตามแผนกของผู้ใช้งาน และใช้งาน Internet ภายนอกได้ภายหลังการยืนยันตัวตน เช่น ระบบ Email, เว็บไซต์ภายในองค์กร หรือระบบ Chat
- **Smart Phone/Tablet ขององค์กร** – รักษาความปลอดภัยด้วย NAC พร้อม MDM Agent เพื่อตรวจสอบและควบคุมเชิงลึก และให้สิทธิ์ในการเข้าถึงระบบงานขององค์กรได้ตามแผนกของผู้ใช้งานภายหลังการยืนยันตัวตน
- **Smart Phone/Tablet ส่วนตัว** – รักษาความปลอดภัยด้วย NAC พร้อม MDM Agent เพื่อตรวจสอบและควบคุมเชิงลึก และให้สิทธิ์ในการเข้าถึงระบบงานพื้นฐานขององค์กร, ใช้งานบางระบบงานขององค์กรตามแผนกของผู้ใช้งานและใช้งาน Internet ภายนอกได้ภายหลังการยืนยันตัวตน เช่น ระบบ Email, เว็บไซต์ภายในองค์กร หรือระบบ Chat

ข้อดี

- ระบบมีความปลอดภัยสูงมาก เพราะมีการตรวจสอบอุปกรณ์ที่นำมาใช้งานอย่างเข้มงวด และจำกัดสิทธิ์การเข้าใช้งานตามความเป็นเจ้าของของอุปกรณ์เหล่านั้น
- พนักงานสามารถนำอุปกรณ์ส่วนตัวมาใช้ทำงานได้อย่างมีประสิทธิภาพมากขึ้น

ข้อเสีย

- มีค่าใช้จ่ายสูง เนื่องจากองค์กรต้องออกค่าใช้จ่ายสำหรับ MDM Agent ตามจำนวนของอุปกรณ์ส่วนตัวที่พนักงานนำมาใช้ และมีค่าใช้จ่ายเพิ่มเติมเรื่อยๆ ตามจำนวนของอุปกรณ์ที่พนักงานนำมาใช้ หรือมีการเปลี่ยนใหม่โดยไม่แจ้งผู้ดูแลระบบ
- มีการดำเนินการที่ยุ่งยาก เนื่องจากผู้ดูแลระบบต้องแบกรับภาระหน้าที่เพิ่มเติมในการแก้ปัญหาทางด้านการนำอุปกรณ์ส่วนตัวซึ่งมีความหลากหลายสูงมาใช้งาน รวมถึงการจัดการในการเพิ่มและลบอุปกรณ์ส่วนตัวออกจากระบบอีกด้วย
- ไม่มีความเป็นส่วนตัว เนื่องจากอุปกรณ์ส่วนตัวของพนักงานจะต้องติดตั้ง MDM Agent ซึ่งคอยบังคับและจำกัดสิทธิ์ในการใช้งานซอฟต์แวร์ต่างๆ ในอุปกรณ์ส่วนตัว

สรุป

แต่ละองค์กรควรจะชั่งน้ำหนักความต้องการทางด้านความปลอดภัย, ภาระหน้าที่ และค่าใช้จ่ายที่จะเกิดขึ้นให้เหมาะสมต่อความต้องการขององค์กร และเลือกกำหนดนโยบายรักษาความปลอดภัยที่เหมาะสมตามต้องการ

ส่วนที่ ๓
การเตรียมความพร้อมของกรมชลประทาน

ในส่วนของกรมชลประทานควรมอบหมายให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และหน่วยงานที่เกี่ยวข้องดำเนินการต่างๆ ดังนี้

- จัดตั้งคณะทำงานเพื่อดำเนินการตามขั้นตอนในส่วนที่ ๒ หัวข้อ ๒.๑ ดำเนินการจัดทำนโยบาย
- พิจารณาจัดทำและกำหนดแนวปฏิบัติสำหรับการรักษาความปลอดภัยเบื้องต้นของอุปกรณ์ BYOD โดยใช้ทรัพยากรเครือข่ายของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เท่าที่มีอยู่ปัจจุบัน
- ตรวจสอบ BYOD Solution ที่เหมาะสมกับกรมฯ และจัดทำรายละเอียดเพื่อเสนอขอสนับสนุนงบประมาณในการดำเนินการ เสนอต่อผู้บริหารกรมฯ
- ดำเนินการจัดหาและติดตั้งอุปกรณ์ต่างๆ หลังจากได้รับงบประมาณ
- เสนอผู้บริหารกรมฯ เพื่อให้ความเห็นชอบและประกาศใช้ โดยให้หน่วยงานต่างๆ ถือปฏิบัติโดยเคร่งครัด

ตัวอย่าง การรักษาความปลอดภัยกับ BYOD

ปัจจุบัน หาก**ผู้ปฏิบัติงาน** หลายคนได้นำอุปกรณ์ส่วนตัวมาใช้งานมากขึ้น ไม่ว่าจะเป็น Notebook ส่วนตัว, Tablet รวมถึง Smartphone ทำให้ข้อมูลต่างๆ อาจจะมีการรั่วไหลได้ง่าย และสร้า งความไม่ปลอดภัยให้กับองค์กร รวมถึงการจำกัดการใช้งาน application ที่เกี่ยวข้องกับข้อมูลสำคัญต่างๆ แล้ว จึงต้องดำเนินการต่างๆ ดังนี้

- **ลงทะเบียนอุปกรณ์ที่จะนำมาใช้** เป็นวิธีที่นิยมใช้กันมา ก เพราะจะได้ ข้อมูลประวัติต่างๆ เช่น ใครใช้อุปกรณ์ประเภทไหนจะได้แนะนำวิธีการตั้งค่า , การเข้าถึงข้อมูลและวิธีการป้องกันข้อมูลหากเกิดการสูญหาย เช่น iPad, iPhone หรือ BlackBerry สามารถสั่ง wipe ข้อมูลหรือ lock เครื่องได้ หากเป็นพวก Tablet อื่นๆ หรือ Notebook ก็อาจจะต้องหาโปรแกรมจำพวก Remote Access เพื่อสามารถเข้าถึงอุปกรณ์และจำกัดการใช้งาน หรือใช้การ Encryption เช่น Symantec Endpoint Encryption, Symantec Whole Disk Encryption หรือ PGP และ CheckPoint Full Disk Encryption
- **ใช้การระบุตัวตนก่อนการใช้งาน** เพื่อตรวจสอบว่าเป็นบุคคลที่ได้รับอนุญาตให้เข้าใช้งานได้หรือไม่ โดยปกติการทำงานจากภายนอกจะต้องผ่าน VPN ก่อน เพื่อป้องกันการดักจับข้อมูล ซึ่งอาจจะเพิ่มความปลอดภัยมากขึ้นด้วย One-Time Password (OTP) หรือ ๒-Factors Authentication ซึ่งสามารถใช้งานร่วมกับ Smartphone ได้เป็นอย่างดี ไม่ว่าจะเป็น Symantec VIP, RSA Secure ID, Vasco
- **จำกัดสิทธิการเข้าถึงข้อมูลและโปรแกรมต่างๆ** อาจจะตั้งกฎการเข้าถึงข้อมูลผ่านระบบที่ต่อเชื่อมกับอุปกรณ์ เช่น ถ้าอยู่ในระบบเครือข่ายของ กรมฯ จะสามารถใช้งานข้อมูลและแอพพลิเคชั่น ที่กำหนดให้

ได้ แต่หากมีการเรียกใช้งานจากภายนอก จะไม่สามารถเรียกใช้ข้อมูลหรือแอพพลิเคชั่นบางอย่างได้ เพื่อป้องกันข้อมูลรั่วไหล

- การล็อกหน้าจอเครื่องอยู่เสมอ การไม่นำเครื่องไป Jailbreak หรือ Root เครื่อง
- การกำหนดรุ่น หรือ Version ของระบบปฏิบัติการ (Mobile Operating System) ที่ได้รับอนุญาตให้เชื่อมต่อเครือข่ายกรมฯ
- กำหนดกลุ่มของบุคคลที่จะได้รับการอนุญาตให้ใช้อุปกรณ์เหล่านั้น

สำหรับการรักษาความปลอดภัย BYOD ของอุปกรณ์ที่นำมาใช้ จะมีแนวทางดังนี้

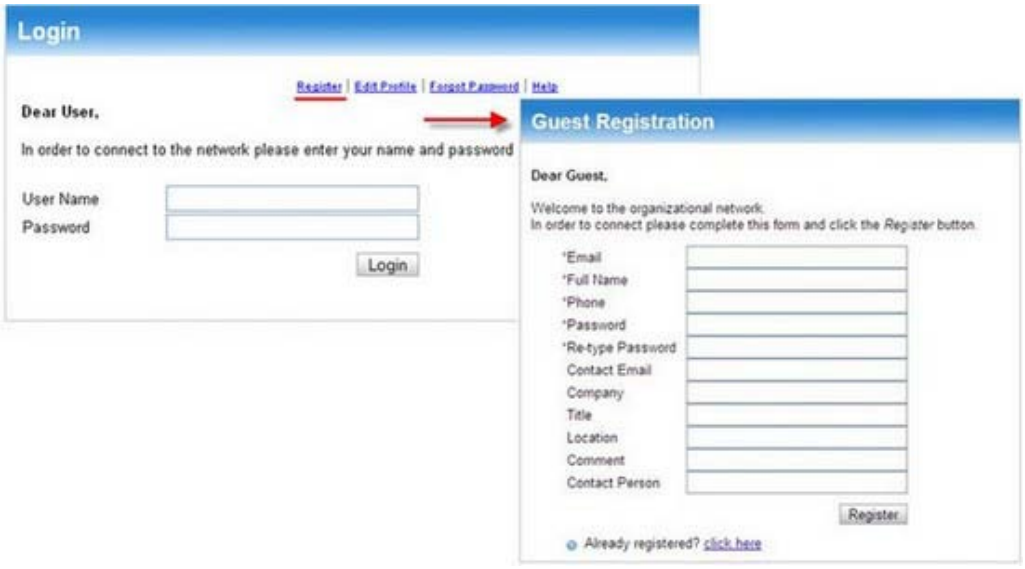
- **PC/Notebook ของกรม** – รักษาความปลอดภัยระดับสูงด้วย NAC พร้อมติดตั้ง Agent โดยให้สิทธิ์ในการเข้าถึงระบบงานของ กรมฯ ได้ตามแผนกของผู้ใช้งานและใช้งาน Internet ภายนอกได้ภายหลังการยืนยันตัวตน
- **Notebook ส่วนตัว** – รักษาความปลอดภัยสูงด้วย NAC โดยบังคับติดตั้ง Agent แบบชั่วคราวเพื่อตรวจสอบเชิงลึก หรือไม่อนุญาตให้ใช้งาน Notebook ส่วนตัวเลยก็ได้ โดยให้สิทธิ์ในการเข้าถึงระบบงานพื้นฐานของกรมฯ, ใช้งานบางระบบงานของกรมฯ ตามแผนกของผู้ใช้งาน และใช้งาน Internet ภายนอกได้ภายหลังการยืนยันตัวตน เช่น ระบบ Email, เว็บไซต์ภายในกรมฯ หรือระบบ Chat
- **Smart Phone/Tablet ของกรมฯ** – รักษาความปลอดภัยด้วย NAC พร้อม MDM Agent เพื่อตรวจสอบและควบคุมเชิงลึก และให้สิทธิ์ในการเข้าถึงระบบงานของกร มฯ ได้ตามแผนกของผู้ใช้งานภายหลังการยืนยันตัวตน
- **Smart Phone/Tablet ส่วนตัว** – รักษาความปลอดภัยด้วย NAC พร้อม MDM Agent เพื่อตรวจสอบและควบคุมเชิงลึก และให้สิทธิ์ในการเข้าถึงระบบงานพื้นฐานขององค์กร , ใช้งานบางระบบงานของกรมฯ ตามแผนกของผู้ใช้งานและใช้งาน Internet ภายนอกได้ภายหลังการยืนยันตัวตน เช่น ระบบ Email, เว็บไซต์ภายในกรมฯ หรือระบบ Chat

ภาคผนวก

ภาคผนวก ก

Solution ForeScout กับ Bring Your Own Device – BYOD

Bring Your Own Device หรือ BYOD นี้ ก็คือการที่ผู้ใช้งานภายในองค์กรมีการนำอุปกรณ์ลูกข่ายต่างๆ เข้ามาใช้งานเองภายในระบบเครือข่ายเป็นจำนวนมาก โดยเมื่อก่อนนั้นจะมีเพียงแค่ Notebook หรือ Netbook เท่านั้น แต่ปัจจุบันนี้ด้วยความแพร่หลายของอุปกรณ์ Smart Phone และ Tablet ต่างๆ ไม่ว่าจะเป็น iPhone, iPod, iPad, Android, Windows Phone และ Black Berry ทำให้ระบบเครือข่ายมีเครื่องลูกข่ายเพิ่มขึ้นมาเป็นจำนวนมาก และยากต่อการดูแลรักษาทางด้านความปลอดภัย เพราะนโยบายรักษาความปลอดภัยสำหรับระบบปฏิบัติการบน PC และ Notebook นั้น แตกต่างจากนโยบายรักษาความปลอดภัยสำหรับ Smart Phone และ Tablet โดยสิ้นเชิง ซึ่งถ้าหากเราไม่จำแนกนโยบายรักษาความปลอดภัยทั้งสองกลุ่มนี้ให้แตกต่างกัน ก็จะเกิดปัญหาต่อการใช้งานจริงของผู้ใช้งาน และส่งผลต่อภาพรวมของความปลอดภัยของระบบเครือข่ายองค์กร

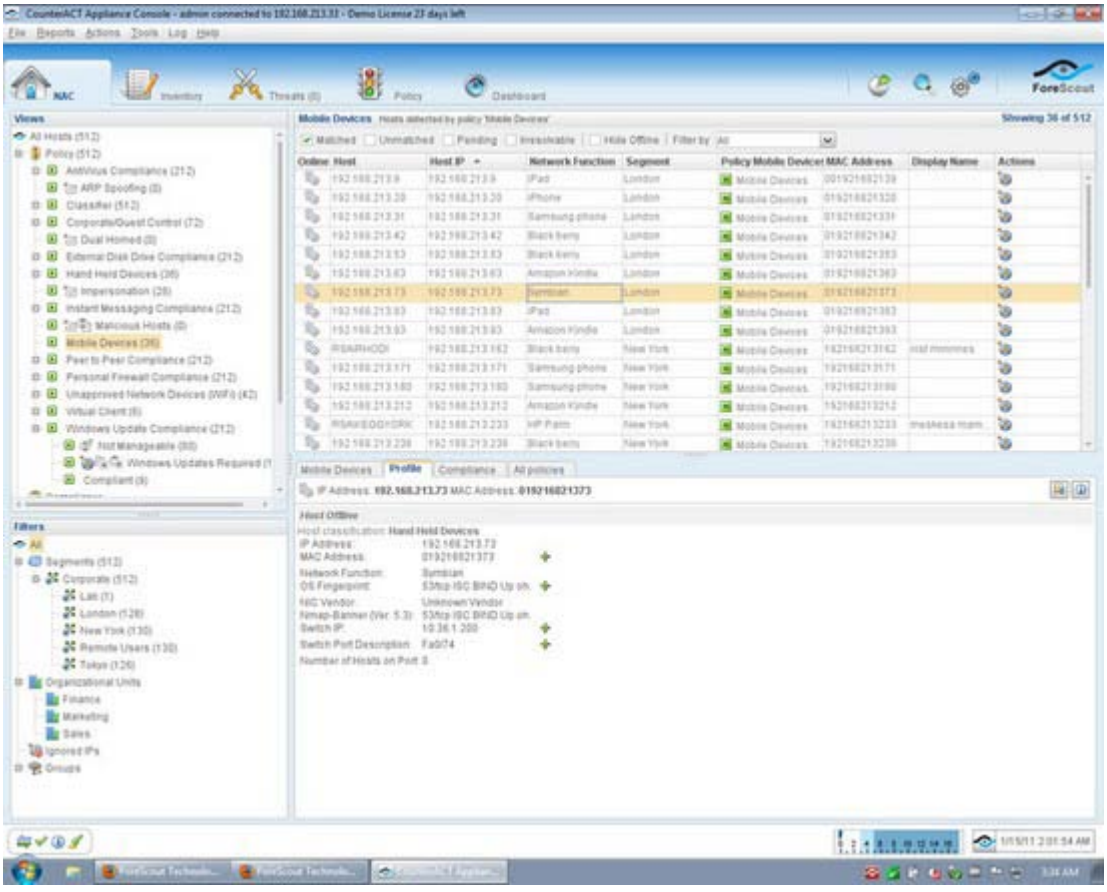


โดยเบื้องต้นของการทำ BYOD นี้ ก็คือการที่ระบบเครือข่ายสามารถรับรู้และจำแนกประเภทของอุปกรณ์ที่นำเข้ามาเชื่อมต่อในระบบเครือข่ายได้ ว่าเป็นระบบปฏิบัติการแบบ PC, Notebook หรือเป็นแบบ Smart Phone, Tablet พร้อมทั้งบังคับใช้นโยบายรักษาความปลอดภัยได้ตามต้องการ ไม่ว่าจะเป็นการลงทะเบียนผู้ใช้งาน, การยืนยันตัวตน, การกำหนดสิทธิ์การเข้าถึงเครือข่าย, การจัดเก็บ Log และการตรวจสอบและยับยั้งการโจมตีเครือข่ายจากอุปกรณ์เหล่านั้น โดยในหลายๆ องค์กรนิยมให้ผู้ที่เชื่อมต่อเครือข่ายด้วย Smart Phone และ Tablet นี้มีสิทธิ์การเข้าถึงเครือข่ายที่น้อยกว่าผู้ใช้งานจาก PC และ Notebook ขององค์กรเอง

โดยความสามารถของ ForeScout ที่สนับสนุนการทำ BYOD มีดังต่อไปนี้

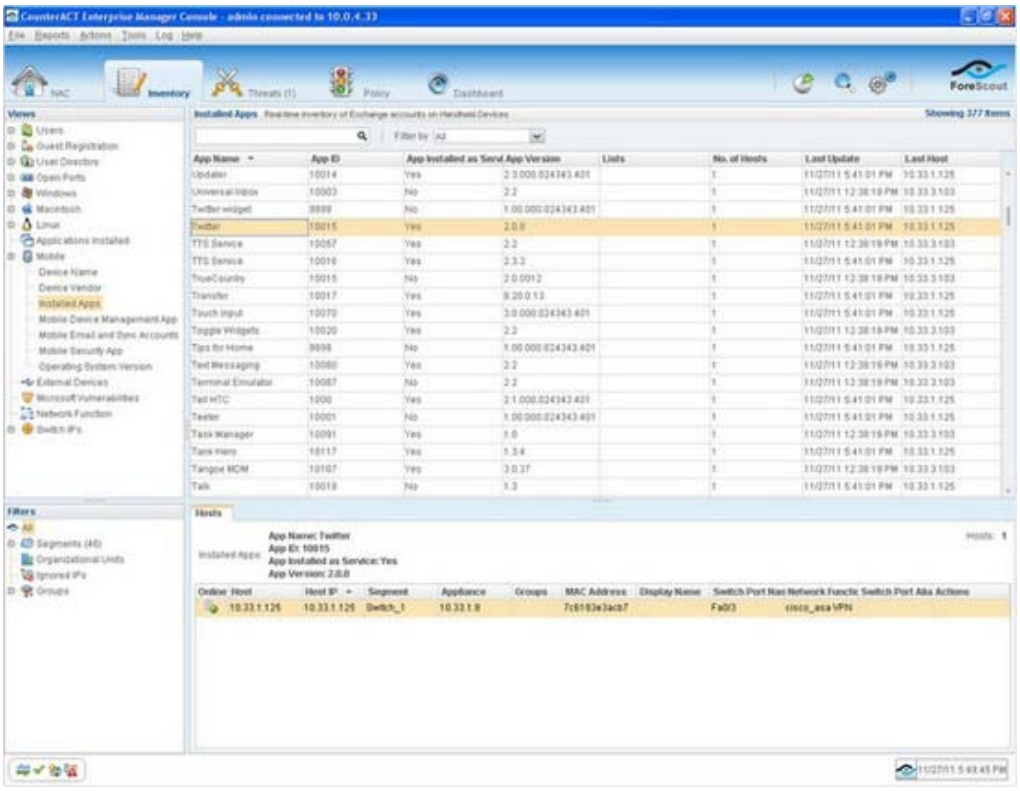
- สามารถตรวจจับอุปกรณ์ที่กำลังใช้งานระบบเครือข่ายได้แบบ Real-time พร้อมทั้งจำแนกประเภทระบบปฏิบัติการว่าเป็น Microsoft Windows, Linux, Unix, Apple iOS, Google Android, Black Berry, Nokia Symbian รวมถึง Cisco IOS ด้วย

- สามารถบังคับใช้นโยบายความปลอดภัยเช่นการยืนยันตัวตน, การกำหนดสิทธิ์ และการตรวจสอบเชิงลึกได้ตามประเภทของอุปกรณ์ที่ตรวจพบ, สถานะความปลอดภัยของอุปกรณ์ และตำแหน่งที่ตรวจพบในระบบเครือข่าย
- สามารถจำแนกอุปกรณ์ได้ตามความเป็นเจ้าของของอุปกรณ์เหล่านั้น จากการยืนยันตัวตน, การกำหนด White List, การกำหนด MAC Address และการตรวจสอบ Software ที่ติดตั้งอยู่ได้
- สามารถทำการจำกัด (Limit) และยับยั้ง (Block) การใช้งานระบบเครือข่ายของอุปกรณ์ได้ตามประเภทของการจำแนก และระดับความปลอดภัยตามนโยบายความปลอดภัยที่กำหนด
- สามารถทำการแจ้งเตือน (Notify) ผ่านทางหน้า HTTP เพื่อแจ้งข่าวสาร หรือส่งซอฟต์แวร์ใหม่ๆ ไปติดตั้งยังเครื่องลูกข่ายได้
- มีช่องทางสำหรับให้ผู้ใช้งานทำการลงทะเบียน (Registration) เพื่อให้สามารถเข้าใช้ระบบเครือข่ายได้โดยสะดวก และสามารถจัดสรรหน้าที่ในการอนุญาตการเข้าใช้งานระบบเครือข่ายของบุคคลภายนอกให้แก่คนในองค์กรที่นอกเหนือไปจากฝ่าย IT ได้
- ตรวจสอบและยับยั้งการแพร่กระจายและการโจมตีของ Worm และ Virus จากอุปกรณ์ที่เชื่อมต่อเข้ากับระบบเครือข่ายทั้งหมดโดยอัตโนมัติ โดยไม่ต้องติดตั้ง Software ที่เครื่องลูกข่าย



ForeScout กับ Mobile Device Management – MDM

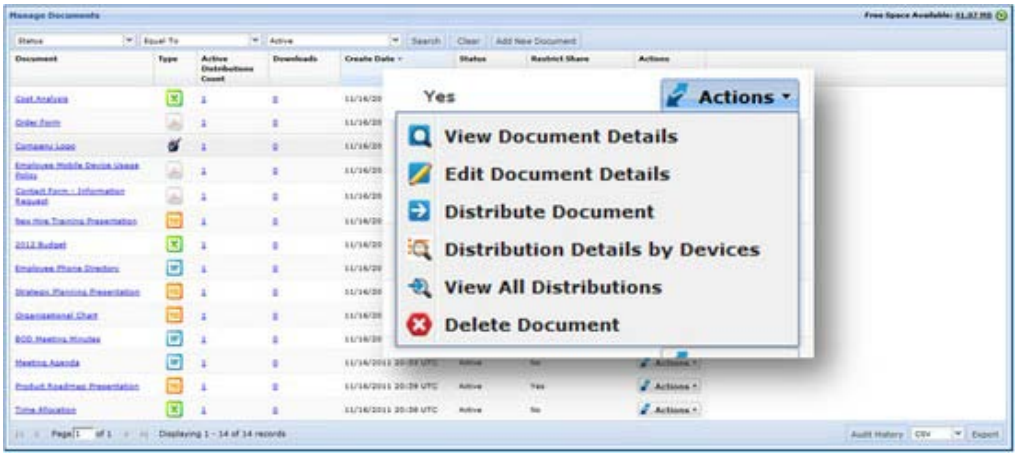
สำหรับ Mobile Device Management หรือ MDM นี้ จะเป็นแนวทางในการควบคุมอุปกรณ์ Mobile Device อย่าง Smart Phone และ Tablet ได้อย่างเบ็ดเสร็จ โดยการติดตั้งซอฟต์แวร์หรือทำการตั้งค่าเพื่อทำการควบคุมลงไปที่อุปกรณ์นั้นๆ ไม่ว่าจะเป็นการบังคับตั้ง Passcode, การบังคับห้าม Jail Break, การบังคับติดตั้ง Mobile App, การบังคับห้ามใช้ Mobile App, การบังคับเข้ารหัสอุปกรณ์, การบังคับห้ามใช้งาน Hardware บางประเภท หรือแม้แต่การบังคับลบข้อมูลในกรณีที่อุปกรณ์ Mobile Device นั้นสูญหายก็ตาม ซึ่งแนวทางของการทำ Mobile Device Management นี้จะเหมาะสมกับกรณีที่องค์กรทำการจัดซื้ออุปกรณ์ Mobile Device ให้พนักงานภายในองค์กรใช้และข้อมูลภายในอุปกรณ์ Mobile Device เหล่านั้นมีความสำคัญสูง ต่างจากกรณีของ BYOD ที่ Mobile Device เหล่านั้นเป็นของพนักงานในองค์กรเอง และไม่สะดวกต่อการติดตั้งซอฟต์แวร์เพื่อควบคุมการใช้งาน



โดยความสามารถของ ForeScout ที่สนับสนุนการทำ MDM มีดังต่อไปนี้

- ตรวจสอบ Hardware Information ได้แก่ Vendor, Model, OS Version, Installed Apps และ Serial Number
- ตรวจสอบการทำ Jail Break บน iOS และ Root บน Android
- บังคับตั้ง Password และ Passcode ได้
- บังคับทำการเข้ารหัสข้อมูลที่จัดเก็บได้
- ส่งข้อความแจ้งข่าวสารและแจ้งเตือนไปยังอุปกรณ์นั้นๆ ผ่านทาง Push Notification ได้
- ติดตั้งและอัพเดต Software ของ Mobile Device ได้
- กำหนดนโยบายความปลอดภัยและ Profile ของ Mobile Device ได้

- ทำการ Lock และ Wipe ข้อมูลทั้งหมดได้ หรือเลือกทำเฉพาะข้อมูลขององค์กรก็ได้
- ทำ Asset Management โดยจัดเก็บ Software และ Hardware Inventory ของอุปกรณ์นั้นๆ
- ให้บริการ Secure Cloud File Sharing แก่ผู้ใช้งานได้
- สร้าง App Storefront ภายในองค์กรได้
- กำหนดนโยบายการทำ Voice Roaming และ Data Roaming ได้
- กำหนด Wireless Profile และ VPN Profile ได้
- สามารถเลือกการบังคับและควบคุมเฉพาะเมื่อเชื่อมต่อภายในองค์กรได้ และสามารถควบคุมไปถึงการเชื่อมต่อเครือข่ายจากภายนอกองค์กรได้



ข้อดีของ ForeScout ที่เหนือกว่าโซลูชัน BYOD และ MDM อื่นๆ

- สามารถติดตั้งใช้งานได้ง่าย โดยไม่ต้องแก้ไขระบบเครือข่าย ต่างจาก BYOD ยี่ห้ออื่นๆ ที่ต้องแก้ไขระบบเครือข่ายทั้งหมดให้ใช้งาน ๘๐๒.๑X, SNMP, ย้าย VLAN หรือทำ ARP Spoofing ซึ่งจะทำให้ผู้ดูแลระบบเครือข่ายทำงานได้ยากขึ้น และโอกาสติดตั้งสำเร็จน้อยลงมาก
- สามารถควบคุม PC และ Mobile Device พร้อมกันได้ภายในระบบเดียว ต่างจากคู่แข่งที่มีการแยกระบบเครือข่ายมีสายออกจากไร้สายออกจากกัน
- สามารถตรวจจับและยับยั้งการโจมตีภายในระบบเครือข่ายได้ภายในตัว โดย ForeScout สามารถตรวจจับและยับยั้ง Threat ต่างๆ ภายในเครือข่ายได้ ช่วยเสริมความปลอดภัยให้ระบบเครือข่ายอีกชั้นหนึ่ง ซึ่งคู่แข่งไม่สามารถทำได้
- สามารถปรับแต่งการจำแนกประเภทอุปกรณ์ได้อย่างอิสระ โดย ForeScout อนุญาตให้ผู้ดูแลระบบทำการปรับแต่งการตรวจจับต่างๆ เหล่านี้ได้ด้วยตนเอง ทำให้สามารถปรับแต่ง ForeScout ให้ทำงานเข้ากับระบบเครือข่ายได้อย่างสมบูรณ์
- ทำการสร้าง Software Inventory และ Hardware Inventory ให้แบบ Real-time ทำให้ผู้ดูแลระบบสามารถบริหารจัดการเครื่องลูกข่ายทั้ง PC และ Mobile Device ได้อย่างสะดวกสบายยิ่งขึ้น รวมถึงสั่งติดตั้ง Software ไปยังเครื่องลูกข่ายจากศูนย์กลางได้อีกด้วย
- ตอบรับเทรนด์ Virtual Desktop Infrastructure หรือ VDI โดยสามารถควบคุมทั้งเครื่องลูกข่ายที่เป็น Physical และ Virtual ไปได้พร้อมๆ กับการควบคุม Bring Your Own Device หรือ BYOD และ Mobile Device Management หรือ MDM

ภาคผนวก ข

ปัญหา ๔ ข้อของระบบรักษาความปลอดภัยเครือข่ายองค์กรแบบเก่า และการแก้ปัญหาเหล่านั้นด้วย ForeScout CounterACT

January ๒๓, ๒๐๑๕/in Blog, ForeScout Blog /by Throughwave Thailand

ระบบบริหารจัดการทางด้านความปลอดภัยเครือข่ายองค์กรในแบบเดิมๆ เช่น Firewall, IPS, Proxy, Vulnerability Scanner หรือ Anti-virus นี้ ไม่สามารถตอบโจทย์ทางด้านการรักษาความปลอดภัยสำหรับระบบเครือข่ายองค์กรที่มีการเปลี่ยนแปลงทั้งทางด้านพฤติกรรมการใช้งาน, อุปกรณ์ที่นำมาใช้งาน และรูปแบบการโจมตีเครือข่าย ซึ่งการใช้งานระบบรักษาความปลอดภัยเพียงแบบเดิมๆ ที่มีอยู่นั้น จะนำมาซึ่งปัญหาด้วยกัน ๔ ประการ ดังนี้

๑. ไม่สามารถติดตามการเปลี่ยนแปลงที่เกิดขึ้นในระบบเครือข่ายได้

ในการบังคับให้เครื่องลูกข่ายต้องทำตามนโยบายรักษาความปลอดภัยขององค์กร หรือการติดตามการโจมตีที่เกิดขึ้นบนระบบเครือข่าย การติดตามการเปลี่ยนแปลงที่เกิดขึ้นในแบบ Real-time ถือเป็นสิ่งที่สำคัญมาก เพราะไม่เช่นนั้น หาไม่สามารถทำการจำกัดสิทธิ์ของเครื่องลูกข่ายที่ทำผิด หรือมีแนวโน้มจะทำการโจมตีระบบเครือข่าย ก็อาจนำมาซึ่งความเสียหายในระยะยาวได้

๒. ต้องใช้งาน Software Agent เพื่อติดตามข้อมูลของเครื่องลูกข่าย

ในการติดตามข้อมูลของเครื่องลูกข่ายในองค์กร ระบบส่วนมากมักบังคับให้ต้องมีการติดตั้ง Agent Software ที่เครื่องลูกข่ายก่อน ซึ่งในปัจจุบันนี้ ด้วยแนวโน้มการนำ BYOD มาใช้งานในองค์กร และการเติบโตของอุปกรณ์อื่นๆ ที่จำเป็นในการทำงาน เช่น Network Printer, NAS Appliance และอื่นๆ อีกมากมาย ก็ทำให้การบังคับลง Agent กลายเป็นข้อจำกัดที่ไม่สามารถทำได้อีกต่อไป

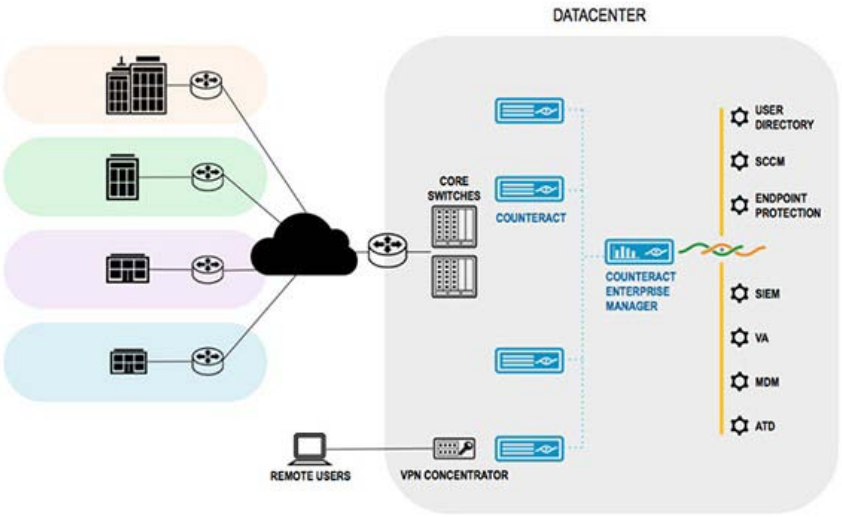
๓. การตรวจสอบช่องโหว่ในเครือข่าย ต้องทำเป็นรอบๆ เท่านั้น

การตรวจสอบช่องโหว่ในเครือข่ายผ่านระบบ Vulnerability Scanner นั้น มักทำเป็นรอบๆ และมักจะมีการเว้นช่วงของแต่ละรอบค่อนข้างยาวนาน เช่น การ Scan เพียงเดือนละครั้ง หรือปีละ ๔ ครั้ง เพียงเพื่อสร้าง Inventory หรือ Report เท่านั้น ในขณะที่การอุดช่องโหว่นั้นเป็นสิ่งที่ควรจะทำถี่ที่สุดเท่าที่จะเป็นไปได้ เพื่อลดความเสี่ยงในการถูกโจมตี

๔. ไม่สามารถจัดการแก้ไขปัญหาหรือยับยั้งการโจมตีด้วยตัวเองได้

หลายอุปกรณ์รักษาความปลอดภัย มีความสามารถเพียงแค่การตรวจจับการโจมตีหรือเหตุการณ์ผิดปกติที่เกิดขึ้น และทำการแจ้งเตือนผู้ดูแลระบบให้ไปหาวิธีการแก้ไขปัญหาเอาเองเท่านั้น โดยไม่ได้ทำการช่วยยับยั้งการโจมตีหรือปัญหาต่างๆ ที่เกิดขึ้นให้เลย

ปัญหาทั้ง ๔ ข้อดังกล่าวนี้จะทำให้การโจมตีระบบเครือข่ายรูปแบบใหม่ๆ หรือการบังคับใช้นโยบายรักษาความปลอดภัยบนเครือข่ายองค์กรที่เต็มไปด้วยข้อจำกัด รวมถึงค่าใช้จ่ายของระบบเครือข่ายในระยะยาวก็จะยิ่งบานปลายต่อไปเรื่อยๆ ForeScout จึงได้มุ่งเน้นที่จะแก้ไขปัญหาเหล่านี้ ให้ทุกๆ องค์กรสามารถวางนโยบายรักษาความปลอดภัยได้อย่างอิสระตามต้องการ และสามารถรับมือกับการโจมตีรูปแบบใหม่ๆ เช่น Advanced Persistent Threat หรือ Targeted Attack ได้อย่างมีประสิทธิภาพยิ่งขึ้น ด้วย Solution จาก ForeScout CounterACT ดังต่อไปนี้



๑. ForeScout CounterACT ใช้หลายๆ วิธีรวมกัน ในการตรวจสอบเครื่องลูกข่าย และการเปลี่ยนแปลงในแบบ Real-Time

ด้วยการใช้เทคนิคที่หลากหลายในการตรวจสอบระบบเครือข่าย ทำให้ ForeScout สามารถแสดงข้อมูลเชิงลึก และการเปลี่ยนแปลงทั้งหมดของเครื่องลูกข่ายได้อย่างมีประสิทธิภาพ ในแบบ Real-time

๒. ForeScout CounterACT ไม่จำเป็นต้องพึ่งพา Software Agent เสมอไป

ด้วยการรองรับการตรวจสอบเครื่องลูกข่ายโดยไม่ต้องใช้งาน Software Agent ทำให้ ForeScout CounterACT สามารถตอบโจทย์ของการรับมือ BYOD และอุปกรณ์ต่างๆ ที่ต้องใช้ในการทำงานภายในองค์กรได้อย่างครอบคลุม

๓. ForeScout CounterACT จะช่วยยกระดับความสามารถ และความคุ้มค่าของระบบเครือข่ายที่มีอยู่เดิมให้เพิ่มขึ้น

ด้วยความสามารถในการแลกเปลี่ยนข้อมูลทางด้านความปลอดภัยต่างๆ ร่วมกับอุปกรณ์เครือข่ายและอุปกรณ์รักษาความปลอดภัยหลากหลายยี่ห้อ รวมถึงการตรวจสอบ Traffic ภายในระบบเครือข่ายด้วยตัวเอง และยังสามารถสั่งการอุปกรณ์เครือข่ายให้ปรับเปลี่ยน Configuration ของตัวเองเพื่อรับมือกับสถานการณ์ที่กำลังเกิดขึ้นได้โดยอัตโนมัติ ทำให้ระบบเครือข่ายมีความปลอดภัยเพิ่มขึ้นในทุกส่วน

๔. ForeScout CounterACT มีความสามารถในการยับยั้งการโจมตีได้หลากหลายวิธีการ

ด้วยความสามารถในการกำหนดเงื่อนไขของนโยบายรักษาความปลอดภัย และการยับยั้งการโจมตีได้อย่างอิสระ ทำให้ ForeScout CounterACT มีความยืดหยุ่นในการใช้งานสูง และสามารถโต้ตอบต่อเหตุการณ์ต่างๆ ที่เกิดขึ้นในระบบเครือข่ายได้หลากหลายวิธีการ ไม่ว่าจะเป็นการแจ้งเตือนผู้ใช้งาน, การจำกัดสิทธิ์ผู้ใช้งาน, การแก้ไข ACL/Rule ของอุปกรณ์เครือข่าย, การ Block Application และ USB หรือแม้แต่การยับยั้ง Zero Day Threats ต่างๆ ได้อีกด้วย

ภาคผนวก ค
ข้อมูลจาก ThaiCERT

ตารางที่ ๑ ประเภทของภัยคุกคามที่ได้รับแจ้งผ่านระบบอัตโนมัติ

Botnet	ภัยคุกคามด้านสารสนเทศที่เกิดกับกลุ่มของเครื่องคอมพิวเตอร์ที่มีโปรแกรมไม่พึงประสงค์ติดตั้งอยู่ ซึ่งโปรแกรมไม่พึงประสงค์นี้จะทำการรับคำสั่งจากผู้ควบคุมผ่านเครือข่ายอินเทอร์เน็ต โดยอาจเป็นคำสั่งที่ให้ทำการโจมตีระบบเครือข่าย ส่งสแปม หรือโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์นั้น เป็นต้น
Open DNS Resolver	ภัยคุกคามด้านสารสนเทศที่เกิดจากการตั้งค่าของเครื่องให้บริการ DNS อย่างไม่เหมาะสม อาจถูกใช้เป็นส่วนหนึ่งในการโจมตีระบบต่าง ๆ ในลักษณะ DDoS ได้
Spam	ภัยคุกคามด้านสารสนเทศที่เกิดจากผู้ไม่หวังดีทำการส่งจดหมายอิเล็กทรอนิกส์ออกไปยังผู้รับจำนวนมาก โดยผู้ที่ได้รับจดหมายอิเล็กทรอนิกส์เหล่านั้นไม่ได้มีความประสงค์ที่จะได้รับข้อมูลนั้นมาก่อน ส่วนมากเป็นการโฆษณาสินค้าและบริการ ทำให้เกิดความเดือดร้อนรำคาญแก่ผู้รับ
Scanning	ภัยคุกคามด้านสารสนเทศที่เกิดจากการที่ผู้ไม่หวังดี ทำการตรวจสอบข้อมูลเบื้องต้นของระบบปฏิบัติการหรือบริการบนเครื่องแม่ข่าย โดยใช้วิธีส่งข้อมูลไปสู่ระบบที่เป็นเป้าหมายผ่านระบบเครือข่าย แล้วรวบรวมผลลัพธ์จากการตอบสนองจากระบบที่เป็นเป้าหมายนั้น ข้อมูลที่ได้จากการสแกนมักจะใช้เป็นข้อมูลในการเจาะหรือบุกรุกเข้าระบบต่อไป
Open Proxy Server	ภัยคุกคามด้านสารสนเทศที่เกิดจากการตั้งค่าบริการ Web Proxy ไม่เหมาะสม โดยยินยอมให้ผู้ใช้งานทั่วไปเรียกใช้งานเพื่อเข้าถึงบริการเว็บในเครือข่ายอินเทอร์เน็ตได้โดยไม่มีระบบยืนยันตัวตน (Authentication) ซึ่งอาจทำให้ผู้ไม่หวังดีใช้เป็นช่องทางในการกระทำความผิดหรือใช้โจมตีระบบอื่น ๆ ได้ Web Defacement ภัยคุกคามด้านสารสนเทศที่เกิดจากการเจาะระบบได้สำเร็จแล้วทำการเปลี่ยนแปลงข้อมูลบนหน้าเว็บไซต์ โดยมีจุดประสงค์ของการกระทำเพื่อสร้างความอับอาย ทำให้หน่วยงานเจ้าของเว็บไซต์ หรือผู้เกี่ยวข้องเสื่อมเสียชื่อเสียง
Malware URL	ภัยคุกคามด้านสารสนเทศที่เกิดจากเว็บไซต์ที่ใช้เพื่อเผยแพร่ Malware ส่วนมากจะเกิดจากการที่ผู้ไม่หวังดีบุกรุกเข้าไปยังเว็บไซต์ของผู้อื่นและใช้พื้นที่ของเว็บไซต์นั้นในการเผยแพร่ Malware และหลอกลวงให้ผู้อื่นเข้าถึงหรือดาวน์โหลด Malware นี้
Phishing	ภัยคุกคามด้านสารสนเทศในลักษณะการฉ้อฉล ฉ้อโกง หรือหลอกลวงเพื่อผลประโยชน์ ส่วนใหญ่มีวัตถุประสงค์ในการขโมยข้อมูลสำคัญของผู้ใช้งาน เช่น บัญชีผู้ใช้ รหัสผ่าน หรือข้อมูลสำคัญทางธุรกรรมอิเล็กทรอนิกส์ เป็นต้น ผู้โจมตีใช้วิธีการล่อลวงให้ผู้ใช้งานเข้าถึงบริการที่ทำปลอมขึ้นและทำให้ผู้ใช้งานเข้าใจผิดว่ากำลังใช้งานกับระบบของผู้ให้บริการจริงอยู่
Brute Force	ภัยคุกคามด้านสารสนเทศในลักษณะการโจมตีหรือเจาะระบบเป้าหมายด้วยวิธีการสุ่มข้อมูลตามอัลกอริทึมที่ผู้โจมตีคิดค้น เพื่อให้ได้ข้อมูลสำคัญหรือข้อมูลลับของระบบเป้าหมาย เช่น การสุ่มบัญชีชื่อผู้ใช้งานและรหัสผ่านเพื่อเข้าสู่ระบบ

DDoS	ภัยคุกคามด้านสารสนเทศในลักษณะการโจมตีสภาพความพร้อมใช้งานของระบบ โดยมีลักษณะการโจมตีมาจากหลายที่โดยแต่ละที่โจมตีเป้าหมายเดียวกันภายในช่วงเวลาเดียวกัน เพื่อทำให้บริการต่าง ๆ ของระบบไม่สามารถให้บริการได้ตามปกติ มีผลกระทบตั้งแต่เกิดความล่าช้าในการตอบสนองของบริการจนกระทั่งระบบไม่สามารถให้บริการต่อไปได้

ตารางที่ ๒ คำอธิบายประเภทของภัยคุกคามแบบต่าง ๆ

ประเภท	**คำอธิบาย**
เนื้อหาที่เป็นภัย (Abusive Content)	ภัยคุกคามด้านสารสนเทศ ที่เกิดจากการใช้/เผยแพร่ข้อมูลที่ไม่เป็นจริงหรือไม่เหมาะสม (Abusive Content) เพื่อทำลายความน่าเชื่อถือ เพื่อก่อให้เกิดความไม่สงบ หรือข้อมูลที่ไม่ถูกต้องตามกฎหมาย เช่น ลามก อนาจาร หมิ่นประมาท และรวมถึงการโฆษณาขายสินค้าต่าง ๆ ทางอีเมล์ที่ผู้รับไม่ได้มีความประสงค์จะรับข้อมูลโฆษณานั้น ๆ (Spam)
โปรแกรมไม่พึงประสงค์(Malicious Code)	ภัยคุกคามด้านสารสนเทศ ที่เกิดจากโปรแกรมหรือชุดคำสั่งที่พัฒนาขึ้นด้วยความประสงค์ร้าย (Malicious Code) เพื่อทำให้เกิดความขัดข้องหรือเสียหายกับระบบที่โปรแกรมหรือซอฟต์แวร์ไม่พึงประสงค์นี้ติดตั้งอยู่ โดยปกติโปรแกรมหรือซอฟต์แวร์ไม่พึงประสงค์ประเภทนี้ต้องอาศัยผู้ใช้งานเป็นผู้เปิดก่อน จึงจะสามารถติดตั้งตัวเองหรือทำงานได้ เช่น Virus, Worm, Trojan หรือ Spyware ต่าง ๆ
ความพยายามรวบรวมข้อมูลของระบบ (Information Gathering)	ภัยคุกคามด้านสารสนเทศ ที่เกิดจากความพยายามของผู้ไม่หวังดีในการรวบรวมข้อมูลจุดอ่อนของระบบ (Scanning) ด้วยการเรียกใช้บริการต่าง ๆ ที่อาจจะเปิดไว้บนระบบ เช่น ข้อมูลเกี่ยวกับระบบปฏิบัติการ ระบบซอฟต์แวร์ที่ติดตั้งหรือใช้งาน ข้อมูลบัญชีชื่อผู้ใช้งาน (User Account) ที่มีอยู่บนระบบ เป็นต้น รวมถึงการเก็บรวบรวมหรือตรวจสอบข้อมูลจราจรบนระบบเครือข่าย (Sniffing) และการล่อลวงหรือใช้เล่ห์กลต่าง ๆ เพื่อให้ผู้ใช้งานเปิดเผยข้อมูลที่มีความสำคัญของระบบ (Social Engineering)
ความพยายามจะบุกรุกเข้าระบบ (Intrusion Attempts)	ภัยคุกคามด้านสารสนเทศที่เกิดจากความพยายามจะบุกรุก/เจาะเข้าระบบ (Intrusions Attempts) ผ่านจุดอ่อนหรือช่องโหว่ที่เป็นที่รู้จักในสาธารณะ (CVE- Common Vulnerabilities and Exposures) หรือผ่านจุดอ่อนหรือช่องโหวใหม่ที่ยังไม่เคยพบมาก่อน เพื่อให้ได้เข้าครอบครองหรือทำให้เกิดความขัดข้องกับบริการต่าง ๆ ของระบบ รวมถึงความพยายามจะบุกรุก/เจาะระบบผ่านช่องทางการตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่าน (Login) ด้วยวิธีการสุ่ม/เดาข้อมูล หรือทดสอบรหัสผ่านทุกค่า (Brute Force)
การบุกรุกหรือเจาะระบบได้สำเร็จ (Intrusions)	ภัยคุกคามด้านสารสนเทศที่เกิดกับระบบที่ถูกบุกรุก/เจาะเข้าระบบได้ส □ำเร็จ (Intrusions) และระบบถูกครอบครองโดยผู้ที่ไม่ได้รับอนุญาต
การโจมตีสภาพ	ภัยคุกคามด้านสารสนเทศที่เกิดจากการโจมตีสภาพความพร้อมใช้งานของ

ความพร้อมใช้งานของระบบ (Availability)	ระบบ เพื่อทำให้บริการต่าง ๆ ของระบบไม่สามารถให้บริการได้ตามปกติ มีผลกระทบตั้งแต่เกิดความล่าช้าในการตอบสนองของบริการจนกระทั่งระบบไม่สามารถให้บริการต่อไปได้ อาจจะเกิดจากการโจมตีที่บริการของระบบโดยตรง เช่น การโจมตีประเภท DoS (Denial of Service) แบบต่าง ๆ หรือการโจมตีโครงสร้างพื้นฐานที่สนับสนุนการให้บริการของระบบ เช่น อาคารสถานที่ ระบบไฟฟ้า ระบบปรับอากาศ
ฉ้อโกงหรือหลอกลวงเพื่อผลประโยชน์ (Fraud)	ภัยคุกคามด้านสารสนเทศที่เกิดจากการฉ้อฉล ฉ้อโกง หรือการหลอกลวงเพื่อผลประโยชน์ (Fraud) สามารถเกิดได้ในหลายลักษณะ เช่น การลักลอบใช้งานระบบหรือทรัพยากรทางสารสนเทศที่ไม่ได้รับอนุญาตเพื่อแสวงหาผลประโยชน์ของตนเอง หรือการขายสินค้าหรือซอฟต์แวร์ที่ละเมิดลิขสิทธิ์

ตารางที่ ๓ อภิธานศัพท์และคำย่อ

คำศัพท์	**ความหมาย**
Port Scanning	การตรวจสอบข้อมูลเบื้องต้นของระบบปฏิบัติการหรือบริการบนเครื่องแม่ข่าย โดยการส่งข้อมูลไปสู่ระบบที่เป็นเป้าหมายแล้วรวบรวมผลการตอบสนอง ข้อมูลที่ได้จากการสแกนมักถูกใช้เป็นข้อมูลในการเจาะหรือบุกรุกเข้าระบบต่อไป
Social Engineering	เทคนิคการหลอกลวงโดยใช้หลักการพื้นฐานทางจิตวิทยาเพื่อให้เหยื่อเปิดเผยข้อมูล เช่น การโทรศัพท์โดยแอบอ้างเป็นบุคคลอื่นเพื่อหลอกให้เปิดเผยรหัสผ่าน
Trojan	มัลแวร์ที่อยู่ในรูปของโปรแกรมทั่วไป แต่มีจุดประสงค์แอบแฝงเพื่อทำอันตรายต่อระบบ เช่น ขโมยข้อมูลบัญชีผู้ใช้ เป็นต้น โปรแกรมที่เป็นโทรจันนั้นจะหลอกล่อให้ผู้ใช้คิดว่าตัวมันเองปลอดภัย และให้ผู้ใช้เป็นคนนำโปรแกรมเข้ามาติดตั้งอยู่ในระบบเอง
Worm	มัลแวร์ที่สามารถแพร่กระจายไปยังเครื่องคอมพิวเตอร์อื่น ๆ ในเครือข่ายหรือข้ามเครือข่ายโดยไม่ผ่านการใช้งานของผู้ใช้
Malware URL	การเผยแพร่โปรแกรมไม่พึงประสงค์ผ่านเครื่องแม่ข่าย โดยโปรแกรมไม่พึงประสงค์จะทำงานเมื่อผู้ใช้เปิดเข้าไปใน URL ที่เป็นที่อยู่ของโปรแกรมไม่พึงประสงค์ มีผลทำให้เบราว์เซอร์ถูกควบคุมการทำงานให้เป็นไปตามความต้องการของผู้เขียนมัลแวร์ เช่น ขโมยข้อมูล แสดงหน้าต่างโฆษณาหรือดาวน์โหลดโปรแกรมไม่พึงประสงค์อื่น ๆ ตามมา เป็นต้น
Domain Name	ชื่อที่ตั้งขึ้นเพื่อใช้แทนการเรียกหมายเลขไอพี (IP Address) เพื่อให้เป็นที่รู้จักและจดจำได้ง่ายขึ้น
Vulnerability Assessment	กระบวนการตรวจสอบหาช่องโหว่ของระบบสารสนเทศที่อาจเป็นจุดอ่อนให้ผู้ไม่หวังเจาะระบบเข้ามาได้ และประเมินความสำคัญและผลกระทบของช่องโหว่นั้น
Penetration Testing	ขั้นตอนถัดจากการตรวจสอบและประเมินช่องโหว่ของระบบสารสนเทศ โดยทำการบุกรุกเจาะระบบสารสนเทศจริงโดยอาศัยวิธีการทางเทคนิค,

	การหลอกลวงแบบโซเชียลเอนจิเนียริง หรือแม้กระทั่งบุกรุกทางกายภาพเข้าไปขโมยข้อมูลก็ถือเป็นการทดสอบเจาะระบบ
Digital Forensics	การเก็บหลักฐาน การค้นหา การวิเคราะห์ และการนำเสนอหลักฐานทางดิจิทัลที่อยู่ในอุปกรณ์คอมพิวเตอร์และอิเล็กทรอนิกส์ เช่น ไฟล์ที่อยู่ในคอมพิวเตอร์ อุปกรณ์อิเล็กทรอนิกส์ โทรศัพท์มือถือ รวมถึงหลักฐานดิจิทัลที่สร้างจากระบบคอมพิวเตอร์ เป็นต้น ซึ่งข้อมูลเหล่านี้สามารถนำไปใช้ระบุผู้กระทำผิดและใช้เป็นหลักฐานในการดำเนินคดีได้
Computer Security Incident Response Team (CSIRT)	หน่วยงานที่มีหน้าที่ประสานงานและจัดการภัยคุกคามที่เกิดกับระบบสารสนเทศในขอบเขตเครือข่ายที่กำหนด เช่น ซีเซิร์ตระดับองค์กรที่จัดการภัยคุกคามระบบสารสนเทศภายในองค์กร หรือ ซีเซิร์ตระดับประเทศที่สามารถประสานงานไปยังซีเซิร์ตในระดับประเทศด้วยกันหรือหน่วยงานที่เกี่ยวข้องเพื่อจัดการภัยคุกคามทางสารสนเทศ
One Time Password (OTP)	รหัสผ่านที่สามารถใช้ได้เพียงครั้งเดียวในการเข้าสู่ระบบ ซึ่งมีความแตกต่างจากรหัสผ่านทั่วไป (Static Password) คือสามารถป้องกันภัยคุกคามเกี่ยวกับการกรอกรหัสผ่านซ้ำ (Replay Attack) กล่าวคือ หากผู้ประสงค์ร้ายทำการจดจำรหัสผ่านเดิมที่ผู้ใช้งานเคยเข้าสู่ระบบ เพื่อจะนำกลับมาใช้ซ้ำ จะไม่สามารถกระทำได้เนื่องจากรหัสผ่านจะมีการเปลี่ยนไปในแต่ละครั้งที่เข้าสู่ระบบ แต่อย่างไรก็ตามการใช้งานรหัสผ่าน OTP มีข้อเสียคือผู้ใช้งานอาจจดจำรหัสผ่านดังกล่าวได้ยาก ดังนั้นจึงมักพบเห็นการใช้รหัสผ่านแบบ OTP ร่วมกับเทคโนโลยีอื่น ทั้งนี้ เทคโนโลยีที่ใช้ในการสร้างรหัสผ่านแบบ OTP ได้แก่ การคำนวณจากเวลา การคำนวณจากรหัสผ่านเดิม หรือค่าสุ่มอื่น ๆ เป็นต้น
Content Management System (CMS)	ระบบซอฟต์แวร์คอมพิวเตอร์ที่ใช้เพื่อจัดระเบียบเอกสารหรือเนื้อหาสาระ โดยส่วนมากนำมาช่วยในการสร้างและบริหารเว็บไซต์แบบสำเร็จรูป โดยในการใช้งาน CMS นั้นผู้ใช้งานแทบไม่ต้องมีความรู้ในด้านการเขียนโปรแกรมก็สามารถสร้างเว็บไซต์ได้
Corporate	เครือข่ายที่ให้บริการอินเทอร์เน็ตกับหน่วยงาน หรือองค์กรที่มีหมายเลขไอพี (IP Address) คงที่ โดยทั่วไปจะมีระบบเครือข่ายและสารสนเทศภายในจำนวนมาก และมีผู้ดูแลระบบประจำหน่วยงาน
Broadband	เครือข่ายที่ให้บริการอินเทอร์เน็ตกับผู้ใช้ทั่วไป มีการระบุหมายเลขไอพี (IP Address) กับเครื่องที่เป็นลักษณะไดนามิกไอพี (Dynamic IP) ซึ่งหมายเลขไอพี (IP Address) จะเปลี่ยนแปลงไปได้ตามเงื่อนไขที่ผู้ให้บริการกำหนด ผู้ใช้เครือข่ายแบบนี้ส่วนมากจะเป็นผู้ใช้บริการตามบ้าน หรือสำนักงานขนาดเล็กที่มีผู้ใช้บริการจำนวนน้อย

แหล่งอ้างอิงข้อมูล

๑. นางสาวรจนา ล้ำเลิศ. (ม.ป.ป.). **“BYOD เรื่องใกล้ตัวในองค์กร”** เข้าถึงได้จาก: https://www.etda.or.th/file_storage/uploaded/Etda_Website/article/๒๐๑๒๐๙๑๙-Article-a-๐๑.pdf (วันที่ค้นข้อมูล: ๓๐ มกราคม ๒๕๕๘)

๒. คุณสมชาย สุระมณี. (ม.ป.ป.). **“BYOD - Bring Your Own Device”** เข้าถึงได้จาก: http://www.csloxinfo.com/enews/eNews_vol๑๒thai.pdf (วันที่ค้นข้อมูล: ๓๐ มกราคม ๒๕๕๘)

๓. “BYOD@BOT เปิดโลกการทำงานยุคใหม่ แบบไร้ขีดจำกัด” (ม.ป.ป.). เข้าถึงได้จาก: http://www.bot.or.th/Thai/AboutBOT/Phrasiam/Documents/Phrasiam_๑_๒๕๕๖/No.๑๙_DigitalLife.pdf (วันที่ค้นข้อมูล: ๓๐ มกราคม ๒๕๕๘)

๔. suramanee. (๒๐๑๒). **“BYOD - Bring Your Own Device”** เข้าถึงได้จาก: https://suramanee.wordpress.com/๒๐๑๒/๑๑/๐๙/b-y-o-d-bring-your-own-device/ (วันที่ค้นข้อมูล: ๓๐ มกราคม ๒๕๕๘)

๕. Throughwave Staff. (๒๐๑๔) **“๑๐ เทคนิค เพื่อการทำนโยบาย BYOD ให้ได้ผล”** เข้าถึงได้จาก: http://www.throughwave.co.th/๒๐๑๔/๑๐/๐๓/๑๐-byod-mdm-techniques/ (วันที่ค้นข้อมูล: ๓๐ มกราคม ๒๕๕๘)

๖. Throughwave Thailand. (๒๐๑๓) **“แนวทางการออกแบบนโยบายรักษาความปลอดภัย BYOD ด้วย Network Access Control”** เข้าถึงได้จาก: http://www.throughwave.co.th/๒๐๑๓/๐๕/๐๘/secure-byod-with-nac-forescout/ (วันที่ค้นข้อมูล: ๓๐ มกราคม ๒๕๕๘)

คณะผู้จัดทำ

๑. หัวหน้าทีม ผู้จัดทำ รวบรวมแก้ไข เพิ่มเติมข้อมูล และจัดพิมพ์รูปเล่ม
- นายสมนึก จิระศิริโสภณ ผู้อำนวยการส่วนเทคโนโลยีสารสนเทศ

๒. ที่ปรึกษา กลุ่มนักศึกษาผู้ค้นหาข้อมูล
- นางไขแสง วิภาโตทัย หัวหน้ากลุ่มงานสารสนเทศภูมิศาสตร์

๓. ผู้ช่วยค้นหาข้อมูล
- น.ส.ภาวินี สุวรรณโยธี นักศึกษา มหาวิทยาลัยราชภัฏสวนสุนันทา