การใช้ไฟล์วอลล์ป้องกันเครือข่ายสารสนเทศของวิทยาลัยการทัพบก

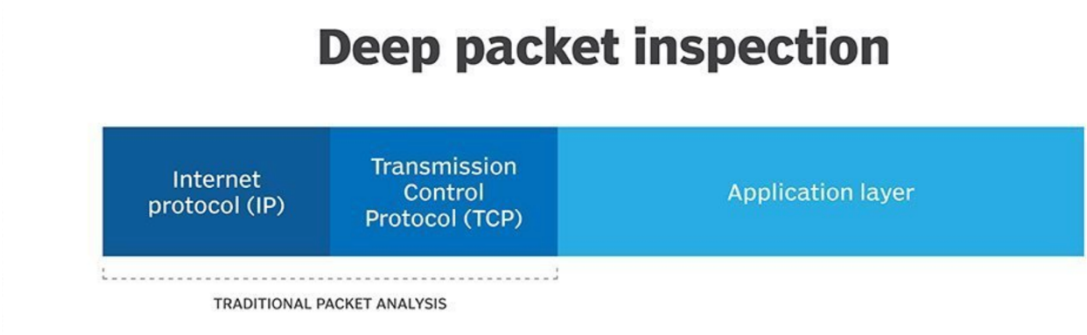
ความปลอดภัยของเครือข่ายเป็นหนึ่งในกลยุทธ์หลักและเป็นการสร้างข้อกำหนดขององค์กรแต่ละแห่งรวมไปถึงวิทยาลัยกองทัพบก เพื่อใช้รับรองความปลอดภัยในการรับส่งข้อมูลเครือข่ายทั้งหมด ความปลอดภัยของเครือข่ายนั้นจะขึ้นอยู่กับการนำฮาร์ดแวร์และซอฟต์แวร์เพื่อรักษาความปลอดภัยมาใช้งานและปฏิบัติตามกติกาอย่างเข้มงวด ซึ่งวิธีการที่จะสามารถดูแลรักษาความปลอดภัยของเครือข่ายได้อย่างดีนั้นควรจะสิ่งที่ต้องปฏิบัติดังนี้ [1] นโยบาย (Policy) การกำหนดนโยบายที่เข้มแข็งในการเข้าใช้เครือข่าย จะสร้างความปลอดภัยให้กับเครือข่ายได้อย่างมากและแน่นอนต้องแลกมาด้วยความยุ่งยากและซับซ้อนในการเข้าใช้งานแต่ละครั้งนั่นหมายถึงการสูญเสียเวลาและทรัพยากรที่มากมาย ดังนั้นจึงควรจัดการนโยบายอย่างเหมาะสมในแต่ละองค์กรหรือแต่ละแผนกในองค์กรนั้นๆ การบังคับใช้ (Enforcement) การบังคับใช้นั้นเกี่ยวข้องกับการวิเคราะห์ข้อมูลบนเครือข่ายทั้งหมดและมุ่งเน้นที่จะรักษาความลับความสมบูรณ์และความพร้อมของระบบและข้อมูลทั้งหมดในเครือข่าย โดยมีหลักการสามข้อประกอบไปด้วย ความลับ คือการป้องกันข้อมูลจากผู้ที่ไม่ได้รับอนุญาติให้เข้าถึงชั้นข้อมูลต่างๆ ความถูกต้อง คือการทำให้เชื่อมั่นว่าข้อมูลนั้นถูกต้องและอยู่ในผู้ที่ได้รับอนุญาต ความพร้อม (Availability) คือสถาณะที่พร้อมของระบบที่ผู้ได้รับอนุญาตสามารถเข้าใช้งานได้เป็นอย่างดี การบังคับตามหลักการทั้ง 3 นี้อย่างเข้มงวดในการเข้าใช้เครือข่าย จะเริ่มต้นด้วยการแบ่งข้อมูลตามโปรแกรมประยุกต์ โดยไฟล์วอลจะเป็นผู้ระบุตัวตนให้ โดยไม่คำนึงถึงพอร์ทหรือโปรโตคอล การระบุแอปพลิเคชันที่เหมาะสมจะช่วยให้สามารถมองเห็นเนื้อหาที่มีอยู่ในทราฟฟิคได้ อย่างสมบูรณ์ ด้วยเหตุนี้เองจะช่วยให้การจัดการนโยบายสามารถทำให้ง่ายขึ้นโดยการระบุแอปพลิเคชันและการแมปการใช้งานกับข้อมูลประจำตัวของผู้ใช้ในขณะที่ทำการตรวจสอบเนื้อหาตลอดเวลาเพื่อให้เป็นไปตามหลักทั้ง 3 ข้อ ของการบังคับใช้ แนวคิดของการป้องกันในเชิงลึกถือเป็นแนวทางปฏิบัติที่ดีที่สุดในการรักษาความปลอดภัยเครือข่าย โดยกำหนดให้เครือข่ายมีความปลอดภัยออกเป็นชั้นๆ(Layers) ซึ่งในชั้นเหล่านี้จะใช้การควบคุมความปลอดภัยหลากหลายประเภทเพื่อกำจัดภัยคุกคามที่พยายามเข้าสู่เครือข่ายเช่น การควบคุมการเข้าถึงการระบุตัวตน, การตรวจสอบความถูกต้อง, การตรวจจับมัลแวร์, การเข้ารหัส, การกรองประเภทของไฟล์, การกรอง URL และการกรองเนื้อหา ในชั้นเหล่านี้เอง สร้างขึ้นผ่านการติดตั้งและกำหนดค่าต่างๆของไฟร์วอลล์ และของระบบป้องกันการบุกรุก(IPS) และส่วนประกอบของโปรแกรมป้องกันไวรัส องค์ประกอบของการบังคับใช้ไฟร์วอลล์นั่นเอง กลไกการควบคุมการเข้าถึงเป็นพื้นฐานที่สำคัญของความปลอดภัยของเครือข่าย การตรวจสอบ (Audit) คือกระบวนการตรวจเช็ค

ค่าต่างๆตามนโยบายความปลอดภัยที่ได้กำหนดไว้ในตอนเริ่มต้นหรือตามมาตราฐานที่กำหนดและหากไม่เป็นไปตามข้อกำหนดก็ให้ปรับปรุงและการตรวจสอบนี้ก็จะต้องกระทำอย่างสม่ำเสมอ [2]

การใช้ไฟล์วอลในการป้องกันเครือข่ายสารสนเทศ ไฟล์วอลเป็นอุปกรณ์ฮาร์ดแวร์โดยมี โอเปอเรติ้งซิสเต็มทำงานอยู่และมีแอฟพลิเคชั่นทำงานอยู่ด้านบนอีกขั้นหนึ่ง โดยใช้รักษาความปลอดภัยของเครือข่ายคอมพิวเตอร์และกำหนดสิทธิการเข้าใช้งานของผู้ใช้ โดยมีการใช้งานมาอย่างยาวนานและมีการพัฒนามาเป็นลำดับ [3]

Packet Filtering Firewalls เป็น Firewall ประเภทแรกๆที่เกิดขึ้น การทำงานแบบที่มีตำแหน่งตรวจสอบบนระบบอย่างชัดเจนคอยวิเคราะห์แพ็คเกจที่เข้ามายังระบบเช่น IP Address ต้นทางปลายทาง ชนิดของ packet และ port number โดยไม่ได้เปิดวิเคราะห์ข้างใน packet และถ้าหาก packet ที่ได้ตรวจสอบแล้วไม่ผ่านกฎเกณฑ์ที่กำหนดไว้ในตอนเริ่มต้นก็จะถูกตัดทิ้งในทันที ข้อดีของ Firewall ประเภทนี้คือไม่ต้องใช้ทรัพยากรของระบบมากนัก (non resource intensive) แต่มันก็มีข้อเสียคือสามารถเจาะผ่านไปได้ง่ายกว่าเมื่อเทียบกับ firewall ประเภทอื่นๆ โดยที่มันสามารถถูกเจาะผ่านได้โดยง่ายจึงมีการพัฒนา Circuit-level gateways firewall เป็น firewall อีกประเภทที่มีการทำงานแบบง่าย คือการส่ง TCP protocol handshake ซึ่งมีการ ตรวจสอบว่ามาจากต้นทางทีเชื่อถือได้ และต้นทางมีการกำหนดไว้ก่อนหน้านี้ (legitimate) จะเหมาะกับการใช้งานในภายในหน่วยงาน การทำงานของ firewall ประเภทนี้ในการตรวจสอบข้อมูลว่าจะให้ผ่านไปหรือไม่ เป็นไปแบบที่ไม่ละเอียดมากนัก Firewall ประเภทนี้ไม่ได้ทำการตรวจสอบภายใน packet ซึ่งหากเป็น packet ที่มาจากแหล่งที่เชื่อถือได้หรือสาขาขององค์กรเองแต่ปรากฏว่ามี malware บรรจุมาด้วยก็จะทำให้เกิดความเสียหายได้เช่นกัน หลังจากนั้นได้เกิดมี State full inspection firewall, Firewall ประเภทนี้เป็นการรวมเอาเทคโนโลยีของ firewall 2 ประเภทด้านบนเข้ามาผนวกรวมกันซึ่งจะทำให้มีการทำงานที่มีประสิทธิภาพมากขึ้น และ ได้มีการใส่การประมวลผลเข้าไปอีกทำให้มีการทำงานที่หนักเพิ่มขึ้นและทำงานได้ช้าลงกว่า Packet Filtering and State full firewall เมื่อ Hardware ได้พัฒนาขึ้นมาก เราสามารถผลิต Application level gateway firewall หรือเรียกอีกอย่างหนึ่งว่า Proxy gateway มีการทำงานในระดับ Application layer จะกรองข้อมูลระหว่างต้นทาง และเน็ตเวิร์ค โดยจะตรวจเข้าไปในระดับที่ลึกกว่าเพื่อจะดูว่ามีการฝัง malware มาใน packet ด้วยหรือไม่ แน่นอนการทำงานในลักษณะนี้เป็นการตรวจสอบที่เข้มข้นย่อมจะทำให้ระบบช้าลง ซึ่งจะต้องอาศัย Hardware ที่มีประสิทธิภาพสูงเพื่อจะให้ทำงานได้เร็วขึ้น และไม่ไปกระทบกับประสิทธิภาพโดยรวมของเครือข่ายแน่นอนมันทำให้ราคาของมันค่อนข้างสูงเมื่อเทียบกับแบบก่อนหน้านี้

Next Generation Firewall เป็น Firewall แบบใหม่ล่าสุดในแบบของ Appliance ที่มีสถาปัตยกรรมประกอบด้วย DPI , TCP Handshake , Surface Level packet inspection, บางครั้งยังมี Intrusion Prevention System (IPS) มาในตัวอีกด้วย ซึ่ง IPS จะกล่าวถัดไป การตรวจสอบ Packet เชิงลึกคือวิธีการบริหารจัดการในขั้นสูง เป็นการแยกแยะ ประเภท รูปแบบ ทิศทาง ที่ตั้งและกำหนดวิธีการ ซึ่งการคำนวณหาและวิเคราะห์แต่ใน header packet นั้นไม่สามารถทำได้ จึงจำเป็นต้องมองเข้าไปในขั้นของ Application Layer โดยที่มีการทำงานโดยจะตรวจสอบที่จุดเช็คในแบบ Real-time และตัดสินใจตามรูปแบบที่ได้กำหนดไว้ก่อนหน้าขึ้นอยู่กับ Packet ว่าบรรจุอะไรมาหากตรวจพบก็ทำงานตามกฎนั้นๆ คล้ายๆกับว่าเราเปิดซองจดหมายเพื่ออ่านเนื้อความในจดหมายนั่นเอง ซึ่งจะต้องใช้ Hardware ขนาดใหญ่และรวดเร็วมากในการจะทำภารกิจดังกล่าว การทำงานนี้เรียกว่า DPI (Deep Packet Inspection) นั่นเองทำให้ราคาของมันสูงกว่า Firewall ในทุกประเภท



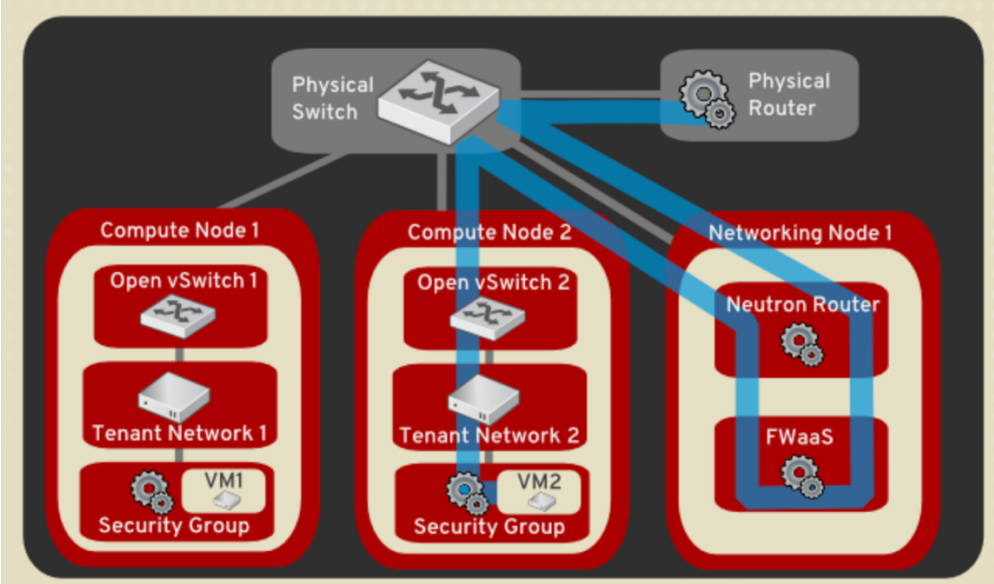
ภาพประกอบที่ 1 โครงสร้างของ Deep Packet Inspection

ต่อมาเมื่อคลาวน์พัฒนาขึ้น Firewall as a service (FWaaS) คลาวน์คอมพิวเตอร์เข้ามามีบทบาทมากขึ้น จึงเกิดการให้บริการ Firewall ในรูปแบบใหม่ขึ้น อีก 2 ประเภทคือ Firewall as a Service and Firewall Hybrid as a Service การให้บริการดังกล่าวเกิดขึ้นที่ Service Provider ทำให้เป็นการใช้บริการ Firewall แบบรวมศูนย์ซึ่งมีข้อดีกว่าแบบที่กล่าวมาใน 5 ชนิดข้างต้นคือ [4]

1) การคำนวณทราฟฟิคที่เกิดขึ้นจริงๆในแต่ละองค์กรทำได้ยากการใช้บริการ FWaaS มีความยืดหยุ่นกว่า
2) เจ้าหน้าที่ด้านความปลอดภัยขององค์กรมีน้อยและมีงานมาก การใช้งาน FWaaS จะช่วยลดการทำงานของเจ้าหน้า IT ของแต่ละองค์กรได้
3) ลดจำนวนอุปกรณ์ Firewall ของสาขาลงได้แล้วหันมาใช้ Firewall แบบรวมศูนย์ จึงเป็นทางเลือกที่น่าสนใจ

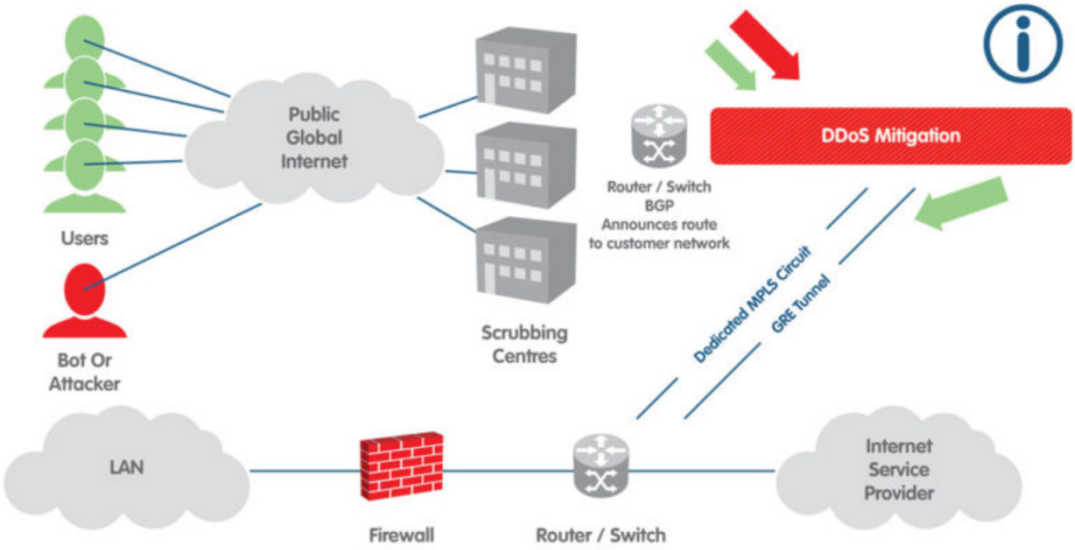
4) การ Update Service pack หรือ Firewall Signature ต่างๆ ถูกต้องและแม่นยำมากยิ่งขึ้น ลดช่องโหว่ของการถูกโจมตีลงได้

5) ลดค่าใช้จ่ายในแง่ของ Capex ลงได้ การลงทุนซื้อ Firewall ในแต่ละครั้งมีมูลค่าสูงดังนั้นการหันมาใช้ FWaaS จึงเป็นอีกทางเลือกหนึ่งที่จะช่วยลดค่าใช้จ่ายลงได้



ภาพประกอบที่ 2 แสดงภาพโครงสร้างของ Firewall ในแบบ FWaaS

Firewall Hybrid as a Service เป็นการทำงานร่วมกันของ Firewall ในแบบ Appliance Box ที่ติดตั้งในองค์กรนั้นๆร่วมกับการให้บริการจากผู้ให้บริการคลาวด์เซอวิสโพรไวเดอร์ โดยกรณีจะมี Firewall ที่ติดตั้งที่องค์กรเป็นจุดแรกในการรองรับการโจมตี จนเมื่อมีการโจมตีมากๆถึงในระดับที่ Firewall รองรับไม่ไหวจึงจะทำการส่งให้ผู้ให้บริการไปรับผิดชอบต่อไป บริการประเภทนี้มักจะมีค่าบริการที่สูงเพราะจะใช้กรณีที่ต้องการประสิทธิภาพสูงมาก (Service availability) โดยมักจะรองรับการโจมตีในแบบ Denial of Service (DoS) คือการทำให้คอมพิวเตอร์เซอร์เวอร์ไม่สามารถทำงานได้ [5]



ภาพประกอบที่ 3 ประกอบในการให้บริการแบบ Hybrid Cloud

อุปกรณ์ที่ทำหน้ารักษาความปลอดภัยในองค์กรอีกประเภทหนึ่งก็คือ Intrusion Prevention System (IPS) [6] เป็นอุปกรณ์ที่มีลักษณะของฮาร์ดแวร์ร่วมกับซอฟแวร์ที่ทำงานบนฮาร์ดแวร์ โดยเทคโนโลยีของการป้องกันผู้บุกรุกโดยการตรวจสอบข้อมูลภายในระบบคอมพิวเตอร์ เพื่อค้นหาจุดอ่อนหรือช่องโหว่ต่างๆของเครือข่ายคอมพิวเตอร์ นอกจากนี้ยังทำหน้าที่ป้องกันเครือข่ายขององค์กรได้อีกด้วย จุดอ่อนของระบบมักจะมาจากการเข้ามาแฝงตัวของไวรัส โทรจัน หรือ หนอนอินเตอร์เน็ตโดยมีเป้าหมายเพื่อหยุดยั้งการทำงานของโปรแกรมประยุกต์หรือเครื่องแม่ข่ายคอมพิวเตอร์ ถ้ามันทำงานได้สำเร็จก็จะทำให้ระบบหรือโปรแกรมหยุดทำงานหรือสร้างโอกาสในการควบคุมโปรแกรมประยุกต์ต่างๆได้

ในแผนภาพของระบบเครือข่ายคอมพิวเตอร์ในองค์กรบ่อยครั้งที่เรามักจะเห็นการติดตั้ง IPS ไว้ที่ตำแหน่งหลัง Firewall มันมักจะทำงานในลักษณะที่วางตรงกลางระหว่างต้นทางและปลายทางเพื่อที่จะทำงานในแบบอัตโนมัติได้อย่างทันเหตุการ์ณเช่นการแจ้งเตือนไปยังผู้ดูแลเครือข่าย, การทำลายไวรัส โทรจัน หรือ หนอนอินเตอร์เน็ต การห้ามทราฟฟิคที่ไม่ต้องการจากต้นทาง, การสร้างคอนเน็กชั่นใหม่อีกครั้ง IPS เมื่อการทำงานของ IPS เข้ามีส่วนร่วมกับประสิทธิภาพของเครือข่าย [7] จึงต้องพยายามหลีกเลี่ยงที่จะทำให้เกิดความล่าช้าในเครือข่าย ดังนั้นจึงทำงานให้ถูกต้องและมีความแม่นยำที่สุด IPS เองอาจจะเป็น Appliance Box เฉพาะตัวมันเองหรืออาจรวมอยู่ใน Firewall แบบ Next Generation ก็ได้ นอกจากการที่วิทยาลัยควรใช้อุปกรณ์ที่เหมาะสมแล้วยังควรปฏิบัติตามมาตราฐานด้านความปลอดภัยอีกด้วย มาตราฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ถือว่ามี

ความสำคัญอย่างยิ่งในการปกป้องทรัพยากรขององค์กร ดังนั้นการที่จะทำให้เทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัยจะต้องมีกระบวนการในการดำเนินการ ซึ่งกระบวนการเหล่านั้นได้ถูกกำหนดเอาไว้เป็นมาตรฐานที่เป็นที่ยอมรับ โดยมีองค์กรหรือสถาบันที่มีชื่อเสียงเป็นผู้กำกฎเกณฑ์และแนวทางในการปฏิบัติ ซึ่งวิทยาลัยสามารถเลือกมาตรฐานที่มีความเหมาะสมกับหน่วยงานของแต่ละองค์กรได้ [8]

สำหรับมาตรฐานการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ในระดับสากล ได้แก่ มาตรฐาน U.S. DoD, มาตรฐาน ISO27001: 2005, มาตรฐาน FIPS PUB 200, มาตราฐาน NIST 800 –14, มาตรฐาน COBIT, และ มาตรฐาน IT BPM 12 [5] โดยมาตรฐาน U.S. DoD เป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกระทรวงกลาโหมสหรัฐอเมริกา ที่ได้ระบุถึงพื้นฐานสำหรับกระบวนการประเมินความปลอดภัยของ ระบบคอมพิวเตอร์เพื่อความมีประสิทธิภาพของอุปกรณ์ตั้งแต่ขั้นตอนแรกคือกระบวนการประมูลจัดซื้อหรือจัดจ้างสำหรับหน่วยงานภาครัฐ เพื่อใช้เป็นแนวทางในการออกแบบ พัฒนา ผลิตหรือทดสอบสำหรับผู้ผลิตเทคโนโลยีหรือภาคเอกชนได้ปฏิบัติตาม เพื่อให้ได้มาตรฐานความปลอดภัยตามที่ได้กำหนดไว้ มีการกำกับคุณภาพของคนโดยมีใบรับรอง IT Certificate ทางด้าน Cyber Security ทำให้ได้เจ้าหน้าที่ ที่เหมาะสมเข้ามาทำงานด้านนี้นอกจากนี้ยังให้ความสำคัญกับหลักการประกันความมั่นคงปลอดภัยสารสนเทศ (Informational Assurance: IA) โดยมีมาตรฐานในการประเมิน และมี IT Audit team ในการกำกับควบคุมทำให้การนำนโยบายด้านไซเบอร์มาสู่การปฏิบัติมีประสิทธิภาพมากยิ่งขึ้น มาตรฐาน ISO 27001:2005 เป็นมาตรฐานที่มีแนวทางปฏิบัติที่ได้รับการยอมรับและนำไปใช้เป็นแนวทางในการรักษาความมั่นคงปลอดภัยไซเบอร์ในองค์กรทั่วโลก ในขณะที่มาตรฐาน COBIT เป็นมาตรฐานที่มีจำนวนแนวทางปฏิบัติใกล้เคียงกับ ISO 27001:2005 ยกเว้นแนวทางการป้องกันและการสร้างความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศด้านกายภาพและสิ่งแวดล้อม จากภายในและภายนอกองค์กรและมาตรฐานที่มีแนวทางปฏิบัติน้อยที่สุดได้แก่ มาตรฐาน IT BMP เนื่องจากมาตรฐานนี้เป็นการกำหนดมาตรฐานขั้นต่ำที่องค์กรควรจะปฏิบัติแนวทางในการดำเนินการพัฒนาศักยภาพทางไซเบอร์ของกระทรวงกลาโหมสู่มาตรฐานสากลนั้นจะต้องดำเนินการตามกฎหมายคือพระราชกฤษฎีกาว่าด้วย วิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.2553 ที่เกี่ยวข้องคือให้มีมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามหลักเกณฑ์ที่คณะกรรมการประกาศกำหนด

ในอินเตอร์เน็ตมีการทำงานรูปแบบของการโจมตีเครือข่ายหลากหลายแบบการโจมตีหรือการบุกรุกเครือข่าย หมายถึง ความพยายามที่จะเข้าใช้ระบบ (Access Attack) การแก้ไขข้อมูลหรือระบบ) Modification Attack) การทำให้ระบบไม่สามารถใช้การได้) Deny of

Service Attack) และการทำให้ข้อมูลเป็นเท็จ (Repudiation Attack) ซึ่งจะกระทำโดยผู้ประสงค์ร้าย ผู้ที่ไม่มีสิทธิ์ หรืออาจเกิดจากความไม่ได้ตั้งใจของผู้ใช้เองต่อไปนี้เป็นรูปแบบต่าง ๆ ที่ผู้ไม่ประสงค์ดีพยายามที่จะบุกรุกเครือข่ายเพื่อลักลอบข้อมูลที่สำคัญหรือเข้าใช้ระบบโดยไม่ได้รับอนุญาตโดยที่มีหลากหลายรูปแบบ แพ็กเก็ตสนิฟเฟอร์ ข้อมูลที่คอมพิวเตอร์ส่งผ่านเครือข่ายนั้นจะถูกแบ่งย่อยเป็นก้อนเล็ก ๆ ที่เรียกว่า “แพ็กเก็ต (Packet)” แอพพลิเคชันหลายชนิดจะส่งข้อมูลโดยไม่เข้ารหัส) Encryption) หรือในรูปแบบเคลียร์เท็กซ์ (Clear Text) ดังนั้น ข้อมูลอาจจะถูกคัดลอกและโพรเซสโดยแอพพลิเคชันอื่นก็ได้ [9] การใช้ไอพีสปูฟฟิง (IP Spoofing) เป็นอีกรูปแบบที่นิยม หมายถึง การที่ผู้บุกรุกอยู่นอกเครือข่ายแล้วแกล้งทำเป็นว่าเป็นคอมพิวเตอร์ที่เชื่อถือได้ (Trusted) โดยอาจจะใช้ไอพีแอดเดรสเหมือนกับที่ใช้ในเครือข่าย หรืออาจจะใช้ไอพีแอดเดรสข้างนอกที่เครือข่ายเชื่อว่าเป็นคอมพิวเตอร์ที่เชื่อถือได้ หรืออนุญาตให้เข้าใช้ทรัพยากรในเครือข่ายได้ โดยปกติแล้วการโจมตีแบบไอพีสปูฟิงเป็นการเปลี่ยนแปลง หรือเพิ่มข้อมูลเข้าไปในแพ็กเก็ตที่รับส่งระหว่างไคลเอนท์และเซิร์ฟเวอร์ หรือคอมพิวเตอร์ที่สื่อสารกันในเครือข่าย การที่จะทำอย่างนี้ได้ผู้บุกรุกจะต้องปรับเราท์ติ้งเทเบิ้ลของเราท์เตอร์เพื่อให้ส่งแพ็กเก็ตไปยังเครื่องของผู้บุกรุก หรืออีกวิธีหนึ่งคือการที่ผู้บุกรุกสามารถแก้ไขให้แอพพลิเคชันส่งข้อมูลที่เป็นประโยชน์ต่อการเข้าถึงแอพพลิเคชันนั้นผ่านทางอีเมลล์ หลังจากนั้นผู้บุกรุกก็สามารถเข้าใช้แอพพลิเคชันได้โดยใช้ข้อมูลดังกล่าว[1] การโจมตีรหัสผ่าน (Password Attacks) หมายถึงการโจมตีที่ผู้บุกรุกพยายามเดารหัสผ่านของผู้ใช้คนใดคนหนึ่ง ซึ่งวิธีการเดานั้นก็มีหลายวิธี เช่น บรู๊ทฟอร์ช (Brute-Force) ,โทรจันฮอร์ส (Trojan Horse), ไอพีสปูฟิง, แพ็กเก็ตสนิฟเฟอร์ เป็นต้น การเดาแบบบรู๊ทฟอร์ช[11] หมายถึง การลองผิดลองถูกรหัสผ่านเรื่อย ๆ จนกว่าจะถูก บ่อยครั้งที่การโจมตีแบบบรู๊ทฟอร์ชใช้การพยายามล็อกอินเข้าใช้รีซอร์สของเครือข่าย โดยถ้าทำสำเร็จผู้บุกรุกก็จะมีสิทธิ์เหมือนกับเจ้าของแอ็คเคาท์นั้น ๆ ถ้าหากแอ็คเคาท์นี้มีสิทธิ์เพียงพอผู้บุกรุกอาจสร้างแอ็คเคาท์ใหม่เพื่อเป็นประตูหลัง (Back Door) และใช้สำหรับการเข้าระบบในอนาคต และ การโจมตีแบบ Man-in-the-Middle นั้นผู้โจมตีต้องสามารถเข้าถึงแพ็กเก็ตที่ส่งระหว่างเครือข่ายได้ เช่น ผู้โจมตีอาจอยู่ที่ ISP ซึ่งสามารถตรวจจับแพ็กเก็ตที่รับส่งระหว่างเครือข่ายภายในและเครือข่ายอื่น ๆ โดยผ่าน ISP การโจมตีนี้จะใช้ แพ็กเก็ตสนิฟเฟอร์เป็นเครื่องมือเพื่อขโมยข้อมูล หรือใช้เซสชั่นเพื่อแอ็กเซสเครือข่ายภายใน หรือวิเคราะห์การจราจรของเครือข่ายหรือผู้ใช้ ปัจจุบันการโจมตีแบบ DOS เป็นที่นิยมมากและทำงานได้ผล การโจมตีแบบดีไนล์ออฟเซอร์วิส หรือ DOS (Denial-of Service) หมายถึง การโจมตีเซิร์ฟเวอร์โดยการทำให้เซิร์ฟเวอร์นั้นไม่สามารถให้บริการได้ ซึ่งปกติจะทำโดยการใช้รีซอร์สของเซิร์ฟเวอร์จนหมด หรือถึงขีดจำกัดของเซิร์ฟเวอร์ ตัวอย่างเช่น เว็บเซิร์ฟเวอร์ เมล์เซอร์เวอร์ ดาต้าเบสเซอร์เวอร์

และเอฟทีพีเซิร์ฟเวอร์ การโจมตีจะทำได้โดยการเปิดการเชื่อมต่อ) Connection) กับเซิร์ฟเวอร์จนถึงขีดจำกัดของเซิร์ฟเวอร์ ทำให้ผู้ใช้คนอื่น ๆ ไม่สามารถเข้ามาใช้บริการได้ ทำให้เว็บหรือบริการต่างๆล่มนั่นเอง[11] ไวรัสอีกแบบหนึ่งคือ โทรจันฮอร์ส เวิร์ม และไวรัส คำว่า “โทรจันฮอร์ส (Trojan Horse)” นี้เป็นคำที่มาจากสงครามโทรจัน ระหว่างทรอย (Troy) และกรีก (Greek) ซึ่งเปรียบถึงม้าโครงไม้ที่ชาวกรีกสร้างทิ้งไว้แล้วซ่อนทหารไว้ข้างในแล้วถอนทัพกลับ พอชาวโทรจันออกมาดูเห็นม้าโครงไม้ทิ้งไว้ และคิดว่าเป็นของขวัญที่กรีซทิ้งไว้ให้ จึงนำกลับเข้าเมืองไปด้วย พอตกดึกทหารกรีกที่ซ่อนอยู่ในม้าโครงไม้ก็ออกมาและเปิดประตูให้กับทหารกรีกเข้าไปทำลายเมืองทรอย สำหรับในความหมายของคอมพิวเตอร์แล้ว โทรจันฮอร์ส หมายถึงโปรแกรมที่ทำลายระบบคอมพิวเตอร์โดยแฝงมากับโปรแกรมอื่นๆ เช่น เกม สกรีนเซฟเวอร์ เป็นต้น[12]

วิธีการที่ผู้ไม่ประสงค์ดีจะเข้ามาเจาะระบบเครือข่ายก็คือการสแกนพอร์ทที่เปิดอยู่ พอร์ทต่างๆที่เปิดอยู่ทำหน้าที่รับส่งข้อมูลตามความจำเป็นและตามมาตราฐานที่กำหนดตามหลักสากล การสแกนพอร์ททำให้ทราบได้ว่ามีพอร์ทใดเปิดอยู่ รวมไปถึงการแสดงให้เห็นว่ามีอุปกรณ์ใดในการักษาความปลอดภัย ดังนั้นจึงเป็นเครื่องมือยอดนิยมของผู้โจมตีระบบ พอร์ทตั้งแต่ 0-1023 เป็นพอร์ทที่กำหนดไว้เป็นมาตรฐาน โดยองค์กร Internet Assigned Numbers Authority (IANA)

โดยการจะใช้พอร์ทใดขึ้นอยู่กับการบริการที่จะใช้ ตามตารางด้านล่างเป็นตัวอย่างพอร์ทที่นิยมใช้ดังนี้

• Port 20 (udp) – File Transfer Protocol (FTP) for data transfer
• Port 22 (tcp) – Secure Shell (SSH) protocol for secure logins, ftp, and port forwarding
• Port 23 (tcp) – Telnet protocol for unencrypted text commutations
• Port 53 (udp) – Domain Name System (DNS) translates names of all computers on internet to IP addresses
• Port 80 (tcp) – World Wide Web HTTP
• Port 8080 (tcp) – World Wide Web Secure HTTPs

ตารางที่ 1 แสดงพอร์ทที่ใช้บ่อยของคอมพิวเตอร์

พอร์ตแตกต่างกันไปตามบริการที่นำเสนอ โดยมีหมายเลขตั้งแต่ 0 ถึง 65535 แต่ก็มีการใช้ช่วงบางช่วงที่บ่อยกว่า มีเครื่องมือที่ผู้ใช้เจาะระบบในเบื้องต้นนิยมใช้ได้แก่ โปรแกรมวนิลา(Vanilla) เป็นโปรแกรมพื้นฐานที่ใช้สแกนพอร์ททั้ง 65536 ในครั้ง

เดียว โดยมีหลักการโดยการส่ง Syn-Flag และรอรับ Syn-Ack ถ้าหากมีพอร์ทใดเปิดอยู่ก็จะได้รับ Syn-Ack และทำการส่ง Ack-Flag กลับไปเพื่อทำ TCP handshake เป็นการทำงานที่มีความเที่ยงตรงสูงทำให้สามารถใช้ในการเจาะระบบต่อไป แต่การทำลักษณะนี้เป็นการทำงานแบบสมบูรณ์จะถูกบันทึกโดยไฟล์วอลล์ได้ง่าย[13], โปรแกรม SYN Scan จะทำงานโดย ส่ง Syn แล้วรอ Syn-Ack เท่านั้น โดยไม่ส่งอะไรกลับไป ทำให้ไม่ถูกบันทึกลงในไฟล์วอลล์[14], โปรแกรมถัดไป FTP Bounce Scan เป็นอีกโปรแกรมที่ได้รับความนิยม อนุญาตให้ส่งตำแหน่งปลอมของผู้ส่งโดยการตีกลับแพ็กเก็ตผ่าน FTP Server โดยที่ผู้ส่งจะไม่สามารถตรวจสอบได้ เป็นต้น ยังมีเครื่องมืออีกหลายชนิดที่ผู้ไม่ประสงค์ดีใช้เป็นเครื่องมือ อีกตัวอย่างหนึ่งคือการใช้ URL Scan เพื่อทราบช่องโหว่ของระบบจากการทดลอง จากการ ทดลอง SCAN www.awc.ac.th ได้พบว่าการวิเคราะห์ www.awc.ac.th ลักษณะของ Web Server ของวิทยาลัยการทัพบก URL: htttp://www.awc.ac.th , IP Address: 182.52.236.169, Web Server: Apache web server, OS: FreeBSD, Coding Software: PHP 5.6.20 ผลการตรวจสอบ URL : http://www.awc.ac.th
ด้วย URL Scan https://observatory.mozilla.org/analyze/awc.ac.th
ผลลัพธ์ ได้คะแนน 25/100

Test Scores

Test	Pass	Score	Reason	Info
Content Security Policy	✗	-25	Content Security Policy (CSP) header not implemented	ⓘ
Cookies	–	0	No cookies detected	ⓘ
Cross-origin Resource Sharing	✓	0	Content is not visible via cross-origin resource sharing (CORS) files or headers	ⓘ
HTTP Public Key Pinning	–	0	HTTP Public Key Pinning (HPKP) header not implemented (optional)	ⓘ
HTTP Strict Transport Security	✗	-20	HTTP Strict Transport Security (HSTS) header not implemented	ⓘ
Redirection	✗	-5	Initial redirection from HTTP to HTTPS is to a different host, preventing HSTS	ⓘ
Referrer Policy	–	0	Referrer-Policy header not implemented (optional)	ⓘ
Subresource Integrity	–	0	Subresource Integrity (SRI) not implemented, but all scripts are loaded from a similar origin	ⓘ
X-Content-Type-Options	✗	-5	X-Content-Type-Options header not implemented	ⓘ
X-Frame-Options	✗	-20	X-Frame-Options (XFO) header not implemented	ⓘ
X-XSS-Protection	✗	-10	X-XSS-Protection header not implemented	ⓘ

ซึ่งพบว่ามีจุดอ่อนห-ลากหลายที่ควรแก้ไขเพื่อให้ไม่ให้ถูกโจมตีได้โดยง่ายดังตารางสามารถวิเคราะห์ได้ดังนี้ Content Security Policy คือการป้องกันการแทรกโค้ด [15] ในหัวข้อนี้มีคะแนนน้อยมาก ดังนั้นจึงควรแก้ไข , HTTP Strict Transport Security คือการระบุให้

การส่งข้อมูลที่ต้องเป็นแบบ HTTPs เท่านั้น และมีการระบุเวลาของ caching [16)]เป็นอีกข้อที่ต้องได้รับการแก้ไข , X Frame Options เป็นการกำหนดนโยบายว่าจะให้เว็บอื่นแสดงผลเว็บเราภายใน frame ได้หรือไม่ซึ่งหากไม่กำหนดนโยบายจะเกิดช่องโหว่การโจมตีได้ [17] , X-XSS Protection คือมาตราฐานความปลอดภัยในการป้องกันการที่ hacker สามารถอ่านค่าคุกกี้ได้ [18] ความปลอดภัยทางสารสนเทศ (Information and cyber security) เราจะเห็นได้ว่าความมั่นคงปลอดภัยของข้อมูลในทางการทหารนั้นสำคัญมาก สำหรับทหารเองจึงต้องมีความรู้ในเรื่องนี้และยังนำความรู้สามารถนำไปใช้ต่อยอดในเรื่องภัยความมั่นคงได้อีกด้วย เจ้าหน้าที่หรือผู้ดูแลระบบเครือข่ายคอมพิวเตอร์จำเป็นต้องมีความรู้ที่ทันสมัยและผู้ที่เข้าศึกษาอบรมในวิทยาลัยการทัพบกควรมีความรู้ในด้านนี้พอสมควรเนื่องจากจะต้องไปเป็นผู้บังคับบัญชาต่อไปในอนาคต และต่อไปจะรบกันทางไซเบอร์ (Cyber Security) การทำสงครามขึ้นมาอยู่บน ไซเบอร์แล้วทั้งสิ้นมีความจำเป็นอย่างยิ่งที่จะต้องเข้ามาศึกษาหาความรู้ทางด้านนี้อย่างเข้มข้น

บทสรุป

วิทยาการทางด้านเทคโนโลยีสารสนเทศ มีการพัฒนาอย่างต่อเนื่องและมีพัฒนาการที่รวดเร็วมากซึ่งนำมาซึ่งประโยชน์มหาศาลหากนำไปใช้ในทางที่ถูกและในทางกลับกันหากผู้ประสงค์ร้ายสามารถเข้ามายังเครือข่ายได้ย่อมนำซึ่งความเสียหายอย่างมหาศาล ดังนั้นจำเป็นที่ทุกๆหน่วยงานที่เก็บรักษามีข้อมูลอันมีความสำคัญ จำเป็นต้องมีการศึกษาและทำความรู้ความเข้าใจและนำหลักการที่เหมาะสมมาปรับใช้ให้เหมาะสมกับแต่ละหน่วยงานเพื่อปกป้องรักษาข้อมูลเหล่านั้นไว้อย่างดีที่สุดโดยมีการป้องกันทั้งทางระบบและทางวินัยเพื่อไม่ให้เกิดการย่อหย่อนหรือเกิดด้วยความประมาท วิทยาลัยการทัพบกเองเป็นองค์กรที่มีความสำคัญและมีข้อมูลที่สำคัญมาก จึงมีความจำเป็นต้องมีระบบป้องกันที่เหมาะสมและมีการนำมาตราการ์ณต่างๆมาใช้ รวมถึงนำมาตราฐานสากลที่เหมาะสมมากำกับดูแลเพื่อให้ได้มาตรฐานและได้รับความปลอดภัยจากผู้ที่ประสงค์ร้ายไม่สามารถเข้ามายังระบบได้โดยง่าย เพราะในโลกของอินเตอร์เน็ตนั้นเชื่อมโยงกันทั้งโลก ดังนั้น จึงเป็นไปได้ว่าอาจจะถูกผู้ไม่ประสงค์ดีพยายามเข้ามายังระบบได้ ซึ่งเป็นเรื่องที่เสี่ยงและอันตรายมาก ภายใต้ข้อจำกัดที่มีมากมายทั้งทางงบประมาณและความรู้ความสามารถของบุคลากร ซึ่งต้องยอมรับว่าในประเทศเองก็มีบุคลากรด้านความปลอดภัยทางไซเบอร์น้อยมาก ดังนั้นอาจจำเป็นจะต้องหาหน่วยงานกลางเข้ามาเพื่อรับผิดชอบความสมบูรณ์ ความปลอดภัยของข้อมูลและไม่เกิดการซ้ำซ้อนของข้อมูลอีกด้วยและยังทำให้เกิดการนำข้อมูลมาใช้ได้อย่างสะดวกและมีประสิทธิภาพด้วย การนำข้อมูลไปใช้เช่น Data Analytic หรือ การทำ Big Data การใช้ AI มาทำงานอีกด้วยซึ่งสิ่งต่างๆเหล่านี้ต้องอาศัยข้อมูลเป็นสำคัญ

เอกสารอ้างอิง

[1] What is network security? เข้าถึงเมื่อ พ.ศ. 2562 https://www.paloaltonetworks.com/cyberpedia/what-is-network-security [ออนไลน์] 2562.

[2] 4 Easy step How to conduct IT Security เข้าถึงเมื่อ พ.ศ. 2562 https://www.smartdatacollective.com/4-easy-steps-conduct-security-audit-company/ [ออนไลน์] 2562

[3] What type of Firewall? เข้าถึงเมื่อ พ.ศ. 2562 https://www.compuquip.com/blog/the-different-types-of-firewall-architectures [ออนไลน์] 2562

[4] ประโยชน์ของไฟล์วอลล์ ประเภทคลาวน์. https://www.catonetworks.com/glossary-use-cases/firewall-as-a-service-fwaas/ ออนไลน์2561 [] .

[5] การโจมตีแบบ DOS https://en.wikipedia.org/wiki/Denial-of-service_attack .ออนไลน์256 [1].

[6] IPS คืออะไร เข้าถึงเมื่อ พ.ศ. 2562 https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips.256 [ออนไลน์] 2 .

[7] การทำงานของ Hybrid Cloud. https://www.redhat.com/en/topics/cloud-computing/what-is-hybrid-cloud .2561 [ออนไลน์]

[8] การรักษาความปลอดภัยทางไซเบอร์. เข้าถึงเมื่อ พ.ศ. 2562 https://www.tcithaijo.org/index.php/ndsijournal/article/view/39369. [ออนไลน์] 2561.

[9] Packet Sniffer เข้าถึงเมื่อ พ.ศ. 2562 http://code32bit.blogspot.com/2014/01/sniffer.html ออนไลน์] 256]2.

[10] IP Spoffing เข้าถึงเมื่อ พ.ศ. 2562 http://peelovely.blogspot.com/2009/01/spoofing.html [ออนไลน์] 2562.

[11] Denial of Service Attack เข้าถึงเมื่อ พ.ศ. 2562 https://en.wikipedia.org/wiki/Denial-of-service_attack ออนไลน์25 [

[12] การโจมตีระบบเครือข่ายคอมพิวเตอร์ เข้าถึงเมื่อ พ.ศ. 2562 https://suphap277.wordpress.com/assignment/assignment4/assignment ออนไลน์ [2562]

[13] เทคนิคต่างๆ ของ Port Scan เข้าถึงเมื่อ พ.ศ. 2562 http://www.tnetsecurity.com/content_audit/scan_port.php]

[14] Syn Scaning เข้าถึงเมื่อ พ.ศ. 2562 https://searchnetworking.techtarget.com/definition/SYN-scanning
[ออนไลน์] 2562.

[15] Cross Site Script Attack เข้าถึงเมื่อ พ.ศ. 2562 https://www.babelcoder.com/blog/posts/ storing-access-token-localstorage-vs-cookies#XSS-ออนไลน์256 [2].

[16] Script Transport Security เข้าถึงเมื่อ พ.ศ. 2562 https://www.jodbush.com/http-strict-transport-security/ ออนไลน์2256

[17] I-Frame เข้าถึงเมื่อ พ.ศ. 2562 http://webneena.blogspot.com/2016/05/frame.html ออนไลน์256 [2].

[18] Cookie Protection Using HTTP header เข้าถึงเมื่อ พ.ศ. 2562 https://hackfacebookhackwifi.wordpress.com/tag/ ออนไลน์ 2562

ประวัติย่อผู้วิจัย

ยศ ชื่อ นาย โอภาส กัลยาณพจน์

วัน เดือน ปีเกิด 31 ตุลาคม 2515

ประวัติการศึกษา

ปี 2538	อิเล็คทรอนิคส์และคอมพิวเตอร์ ครุศาสตร์บัณฑิต วิชาเอกคอมพิวเตอร์ มหาวิทยาลัยพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ปี 2547	วิทยาการคอมพิวเตอร์ วิทยาศาสตรมหาบัณฑิต มหาวิทยาลัยรังสิต

ประวัติการทำงาน

ปี 2539 - 2544	วิศวกรประจำ บริษัท พานาโซนิคซิวเซล (ประเทศไทย) จำกัด
ปี 2544 - ปัจจุบัน	กรรมการผู้จัดการ บริษัท เน็ตไบร์ท จำกัด

ตำแหน่งปัจจุบัน

ปี 2544 - ปัจจุบัน กรรมการผู้จัดการ บริษัท เน็ตไบร์ท จำกัด