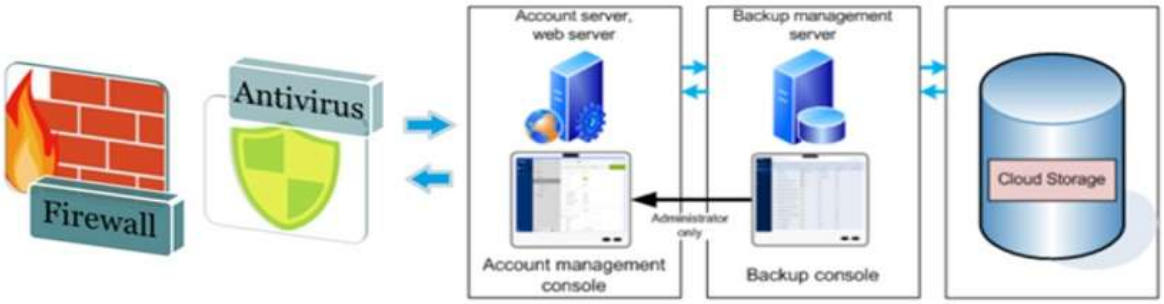
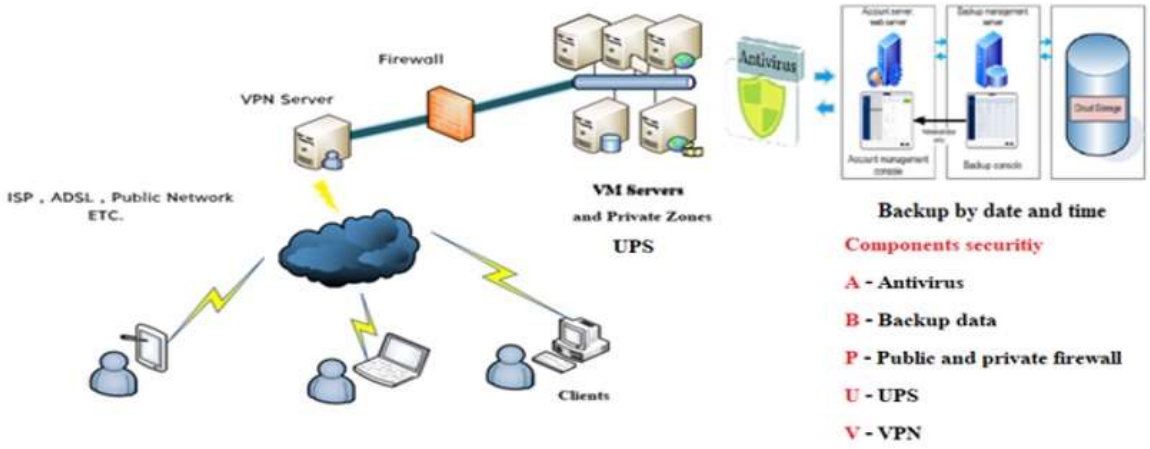
องค์ประกอบสำคัญในการดำเนินการสำรองข้อมูล by TaskS

การดำเนินการสำรองข้อมูล สิ่งสำคัญ ได้แก่ การกำหนดนโยบายการสำรองข้อมูล ต้องมีความปลอดภัยของข้อมูล โดยข้อมูลที่จะสำรองต้องถูกการป้องกันด้วย VPN, Firewall, UPS, Antivirus และเพื่อไม่ให้เกิดการสำรองข้อมูลที่เป็นไวรัส จึงต้องมีการตรวจสอบก่อนเสมอว่าไม่ติดไวรัส จึงจะสำรองข้อมูล หรือการสำรองข้อมูลอัตโนมัติต้องตั้งชื่อวันและเวลาในการป้องกันความเสียหายโดยการกำหนดช่วงวันและเวลา ที่สามารถย้อนวันและเวลาของข้อมูลไม่เสียหายได้ ตัวอย่างในการออกแบบองค์ประกอบสำคัญของการสำรองข้อมูล ตามรูปภาพ ดังนี้



Backup by date and time

การจัดการระบบเครือข่าย



1) การควบคุมระบบการสื่อสาร (Communication control) คือ การป้องกันการเข้าถึงระบบการสื่อสารของเครือข่าย โดยการทำ Virtual Private Network: VPN ซอฟต์แวร์ที่ถูกสร้างขึ้นมาเพื่อปกป้องความเป็นส่วนตัวออนไลน์ การปิดกั้นการเข้าถึงเนื้อหาเพื่อเข้าถึงเนื้อหา และควรกำหนดโซน (Zone) เพื่อแยกกลุ่มสะดวกต่อการตรวจสอบและติดตาม

2) การควบคุมระบบไฟร์วอลล์ (Firewall control) คือ ซอฟต์แวร์หรือฮาร์ดแวร์ในระบบเครือข่าย หน้าที่ของไฟร์วอลล์ คือ เป็นตัวกรองข้อมูลสื่อสาร โดยการกำหนดกฎระเบียบมาบังคับใช้ โดยเฉพาะเรื่องของการควบคุมดูแลระบบเครือข่าย ควรกำหนดการแบ่งกลุ่มให้ชัดเจนในการควบคุมที่มีการใช้ไฟร์วอลล์ร่วมกัน (Public firewall) และไฟร์วอลล์ส่วนบุคคล (Private firewall) เพื่อสามารถหาความผิดพลาดของการระบบและตรวจสอบช่องโหว่ได้ง่าย และนำไปสู่สาเหตุของการโจรกรรมข้อมูลทางคอมพิวเตอร์ได้

3) การควบคุมไวรัส (Antivirus control) คือ โปรแกรมที่สร้างขึ้นเพื่อคอยตรวจจับ ป้องกัน และกำจัดโปรแกรมคุกคามทางคอมพิวเตอร์หรือมัลแวร์ โดยสามารถกำหนดการควบคุมไวรัสที่มีการใช้ร่วมกัน(Public antivirus) และส่วนบุคคล (Private Antivirus) โปรแกรมป้องกันไวรัสแบ่งได้เป็น 2 กลุ่มใหญ่ คือ

3.1) แอนติไวรัส (Anti-Virus) เป็นโปรแกรมโปรแกรมป้องกันไวรัสทั่ว ๆ ไป จะค้นหาและทำลายไวรัสในคอมพิวเตอร์ของเรา

3.2) แอนติสปายแวร์ (Anti-Spyware) เป็นโปรแกรมป้องกันการโจรกรรมข้อมูล จากไวรัสสปายแวร์ และจากแฮ็กเกอร์ รวมถึงการกำจัด Adsware ซึ่งเป็นป๊อปอัพโฆษณา

4) การเปิดใช้งานบริการพอร์ต (Service ports) ที่เชื่อมต่อตามความจำเป็น พร้อมทั้งมีวิธีการเพื่อระบุถึงอุปกรณ์ที่เชื่อมต่อ (Authenticate) อย่างชัดเจน และที่สำคัญควรหลีกเลี่ยงการใช้ หมายเลขพอร์ตที่มีการกำหนดมาให้ เช่น ฐานข้อมูล MariaDB and MySQL มีการกำหนดหมายเลขพอร์ต 3306 ควรเปลี่ยนเป็นหมายเลขพอร์ตที่ไม่ใช้งาน 3808 เป็นต้น

5) การควบคุมการสำรองข้อมูล (Backup data control) คือ ฮาร์ดแวร์หรือซอฟต์แวร์ ทำหน้าที่สำรองข้อมูลที่สามารถกำหนดการสำรองข้อมูลตามวันและเวลาที่กำหนด

6) การบันทึกแฟ้มร่องรอยของเครือข่าย (Log file network) คือ การจัดเก็บหลักฐาน (Logs) เพื่อติดตามตรวจสอบการทำงานที่เกี่ยวข้องหรืออาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ โดยใช้เทคโนโลยี Security Information and Event Management: SIEM จะช่วยองค์กรในการเก็บรวบรวมข้อมูล Logs จากอุปกรณ์รักษาความปลอดภัยทางไซเบอร์ ซึ่งผู้ที่เกี่ยวข้องในการดูแลระบบไซเบอร์ขององค์กรไม่ว่าจะเป็น System Administrator or Server Administrator (ผู้ดูแลระบบหรือ ผู้ดูแลเซิร์ฟเวอร์) Security Administrator (ผู้ดูแลด้านความปลอดภัย) Security Analyst (นักวิเคราะห์ด้านความปลอดภัย) Auditor (ผู้ตรวจสอบ) Management Team (ผู้บริหารองค์กร)

ภาพจาก https://blog.eccouncil.org/what-is-security-incident-and-event-management-siem/components-and-capabilities-of-siem/