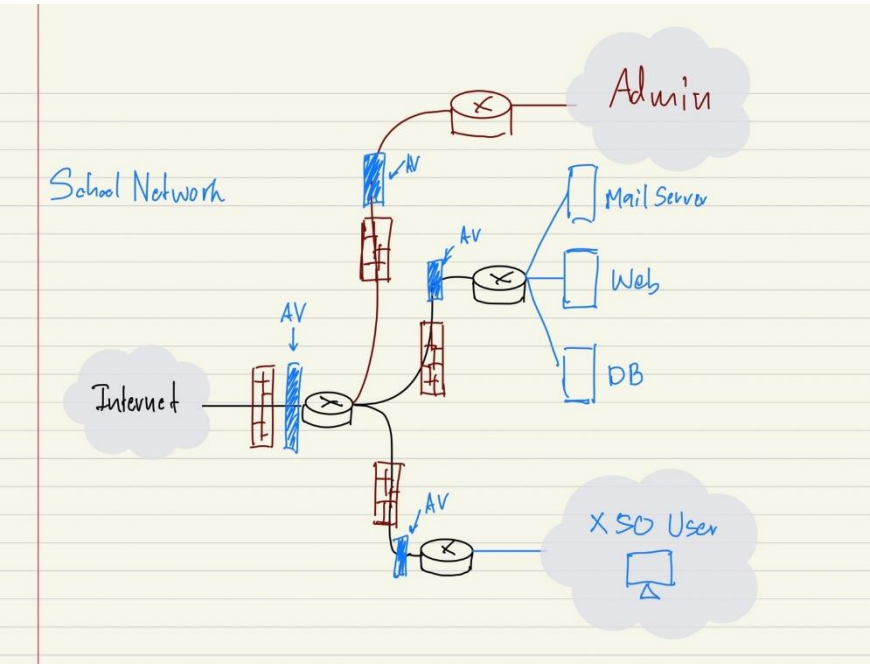
Activity IRP 62010465 นรวิชญ์ อยู่บัว



รายละเอียดของระบบ

1 Web Server สามารถแลกเปลี่ยนข้อมูลกับ Database Server ได้

2 Mail Server สามารถให้บุคลากรทั่วไปใช้งานได้และรับ email จากบุคคลภายนอกได้

3 บุคคลภายนอกและบุคลากรทั่วไปสามารถใช้งาน Web Site ของโรงเรียนได้

4 บุคลากรทั่วไปในโรงเรียนสามารถใช้ Internet ได้

5 Admin ของระบบสามารถติดต่อกับ DataBase Sever และทุกๆ Device ในเครื่อค่ายได้โดยตรง

บุคลากร

- System Admin 1 : CCNA , CCNP
- System Admin 2 : CCNA , CCNP
- Network Engineer : CCNA, CCNP

เหตุฉุกเฉิน 1

- **DDOS**
- **การเตรียมการก่อนเกิด**

ซื้อ Server สำรอง

ซื้อ Application Proxy

ตรวจสอบ Sever สำรองทุกๆ 1 เดือน

Back up ข้อมูลย้อนหลังทุกๆ 1 เดือน

ตรวจสอบการทำงานของ Application Proxy ทุกๆ 1 อาทิตย์

เตรียมความพร้อมบุคลากรทุกๆ 1 เดือน

- **การดำเนินงานเมื่อตรวจพบเหตุฉุกเฉิน**

ตรวจสอบว่าเกิดการเหตุขึ้นจริงๆ

ดูสถานะ load ของ Application Proxy

เมื่อ load ของ Application Proxy อยู่ใน critical state จำกัดการเชื่อมต่อกับต้นทาง-

เตรียม Backup Server ให้พร้อม

- **การดำเนินงานหลังจัดการเหตุฉุกเฉิน**

เขียนสรุป Report ทั้งหมดของเหตุการ

นำเสนอ Report ในที่ประชุม

นำข้อผิดพลาดมาปรับปรุง IRP ใหม่

<u>เหตุฉุกเฉิน 2</u>

- **Ransomware**
- **การเตรียมการก่อนเกิด**

ซื้อ Anti-virus

ซื้อ Server สำรอง

ตรวจสอบ Sever สำรองทุกๆ 1 เดือน

Back up ข้อมูลย้อนหลังทุกๆ 1 เดือน

ต่อสัญญา Anti-virus ทุกๆ 1 ปี

ตรวจสอบประสิทธิภาพของ Antivirus ทุกๆ 1 เดือน

ใช้งาน Multi Factor Authentication

เตรียมความพร้อมบุคลากรทุกๆ 1 เดือน

- **การดำเนินงานเมื่อตรวจพบเหตุฉุกเฉิน**

ตรวจสอบว่าเกิดการเหตุขึ้นจริงๆ

สังเกต pop-ups แปลกๆ หรือ file เข้ารหัส

ตรวจสอบ Firewall log

ตรวจสอบการใช้ load ของอุปกรณ์ทุกชนิด

ทำการตัดการเชื่อมต่อกับเครือค่ายที่น่าสงสัย

เตรียม Backup Server ให้พร้อม

- **การดำเนินงานหลังจัดการเหตุฉุกเฉิน**

  เขียนสรุป Report ทั้งหมดของเหตุการ

  นำเสนอ Report ในที่ประชุม

  นำข้อผิดพลาดมาปรับปรุง IRP ใหม่

<u>เหตุฉุกเฉิน 3</u>

- **Phishing**
- **การเตรียมการก่อนเกิด**

  เตรียมความพร้อมบุคลากรทุกๆ 1 เดือน

  ใช้งาน DomainKeys Identified

  ใช้งาน Sender Policy Framework

  ใช้งาน Domain-based Message Authentication, Reporting & Conformance

  ใช้งาน Email Sandboxing

  ใช้งาน Multi Factor Authentication

  ตรวจสอบระบบทั้ง 5 ด้านบนว่าพร้อมเสมอทุกๆ 1 เดือน
- **การดำเนินงานเมื่อตรวจพบเหตุฉุกเฉิน**

  ตรวจสอบว่าเกิดการเหตุขึ้นจริงๆ

  ตรวจสอบ email ที่น่าสงสัย

  จำกัด email ที่น่าสงสัยไม่ให้ user ทั่วไปเข้าถึงได้
- **การดำเนินงานหลังจัดการเหตุฉุกเฉิน**

  เขียนสรุป Report ทั้งหมดของเหตุการ

  นำเสนอ Report ในที่ประชุม

  นำข้อผิดพลาดมาปรับปรุง IRP ใหม่