Giải pháp Data Loss Prevention cho doanh nghiệp

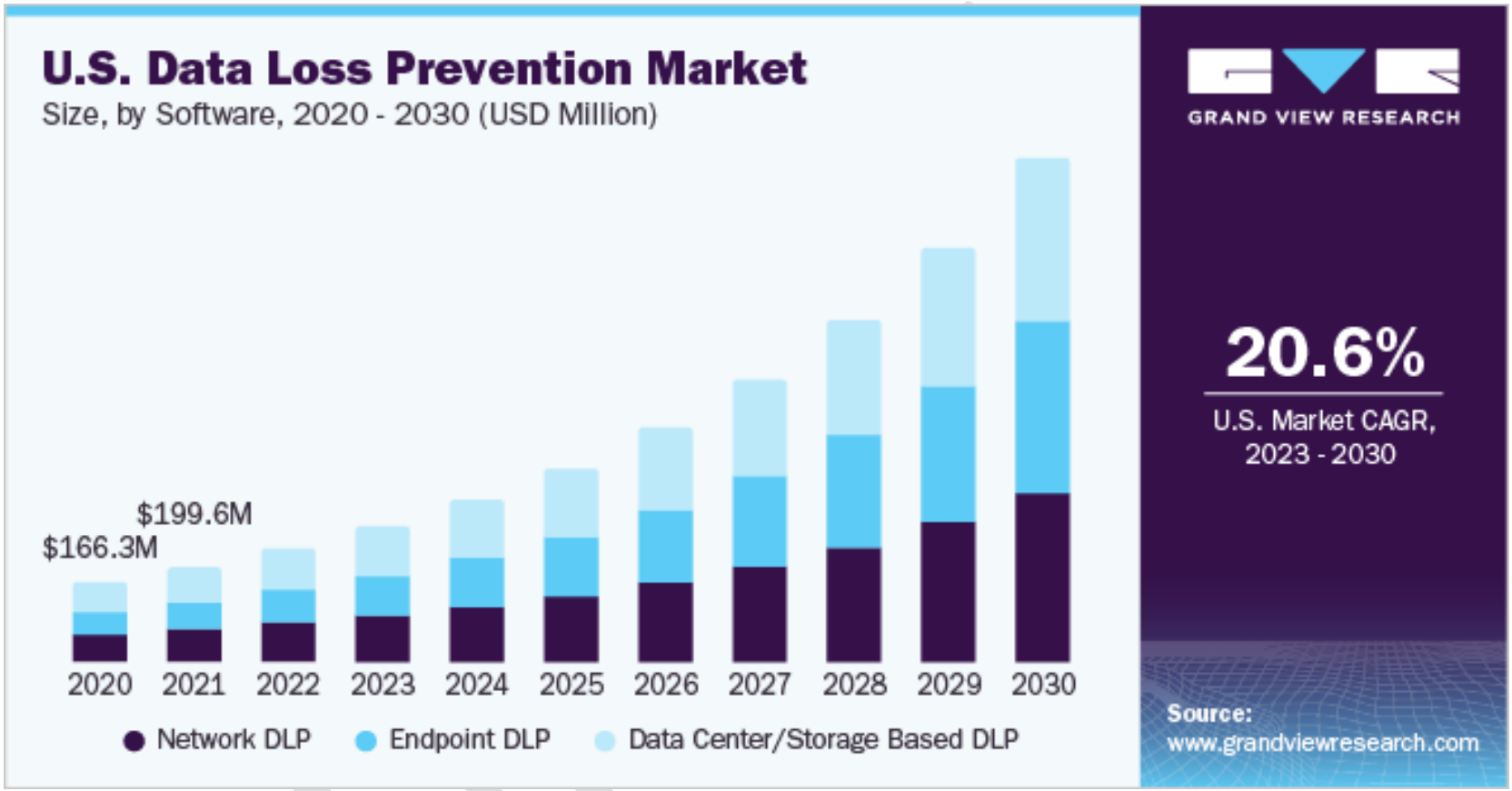
Duy NGUYEN

Mục đích của giải pháp này nhằm giảm thiểu tối đa các nguy cơ dẫn đến mất mát dữ liệu của doanh nghiệp

Đề tài cuối môn
Quản lý rui ro an toàn thông tin trong doanh nghiệp

I. Mục tiêu của đề tài

Data Loss Prevention là một trong những mối đe dọa lớn nhất trong lĩnh vực an toàn thông tin của doanh nghiệp.



Source: Internet

Source: Internet

Hiện nay, ở Việt Nam vấn đề này đang được các doanh nghiệp quan tâm. Nhận thức được sức "nóng" của vấn đề này, chúng ta hãy cùng nghiên cứu và đưa ra giải pháp để khắc phục vấn đề này.

Để nghiên cứu và làm tốt đề tài này. Các bạn cần chuẩn bị tốt những kiến thức sau :

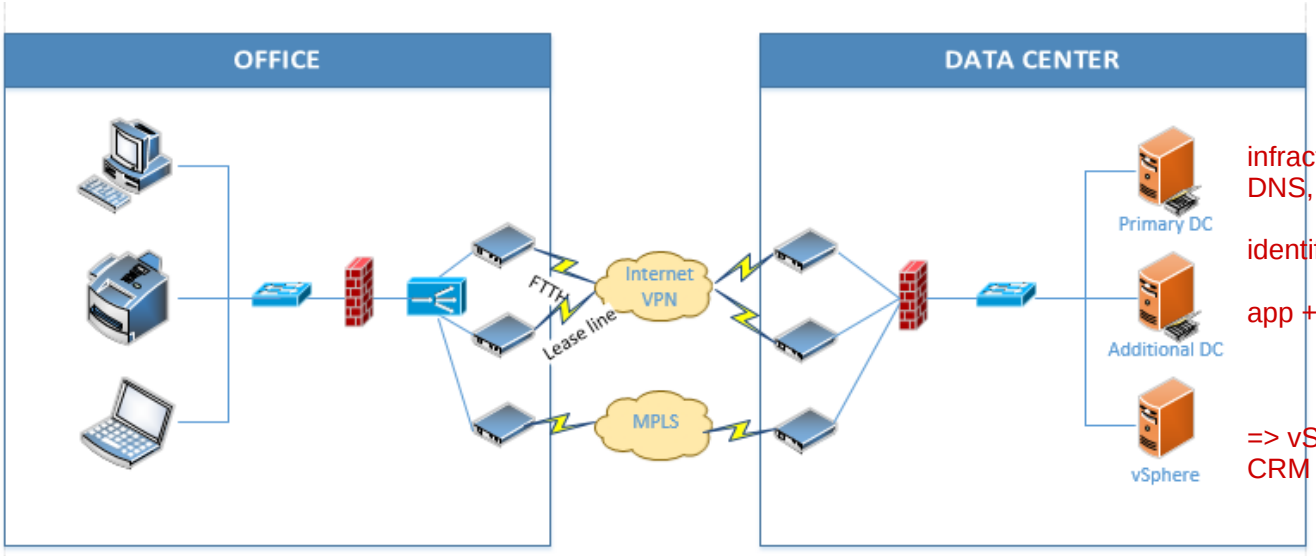
- Chuẩn ISO27001 và ISO27002
- Bảo mật mạng
- Bảo mật application

II. Hiện trạng hệ thống mạng của doanh nghiệp

Hiện tại doanh nghiệp có khoảng 100 người dùng. Thông tin chi tiết các dịch vụ chạy trong hệ thống xem hình bên dưới.

Những thông tin chi tiết về hệ thống:

- Quản trị theo mô hình Domain
- Router Cisco tích hợp firewall
- Thiết bị cân bằng tải kết nối internet
- Không có phần mềm antivirus, firewall chuyên dụng cũng như các chính sách bảo mật khác.
- Chưa có chính sách vận hành hệ thống
- Chưa có chính sách về vấn đề an toàn thông tin trong hệ thống
- Chưa có chính sách sao lưu và phục hồi dữ liệu
- Tất cả các máy chủ đặt tại Data Center



infractructure service: DHCP, DNS, mail, file

identify: domain controller

app + data

=> vSphere: DHCP, file, HR, CRM [server]

III. Yêu cầu

1. Phân tích những điểm yếu trong mô hình mạng hiện tại (tối thiểu phân tích 10 rủi ro liên quan tới ATTT).
2. Phân tích những rủi ro liên quan tới mất mát dữ liệu
    a. Attacker (5 rủi ro)
    b. Nhân viên (5 rủi ro)

    ➔ Phương pháp và công cụ assessment.

    ➔ Bảng Risk Score của hệ thống hiện tại.
3. Thiết kế lại hệ thống – mạng với tính bảo mật tốt nhất có thể (hướng tới giải pháp chống thất thoát dữ liệu)
    a. Vẽ mô hình tổng thể
    b. Vẽ mô hình chi tiết cho từng phần (Web Security, Email Security, IDS/IPS Security,…)
    c. Thuyết minh giải pháp cho từng phần (mỗi giải pháp thuyết minh 2 trang)

    ➔ Bảng Risk Score của hệ thống mới.

1.router tich hop fw de bi dos/ddos
2.không có AV
3.ko có FW chuyên dung
4.ko có chinh sach van hành
5.ko có chinh sach ve ATTT chung
6.ko có chinh sach sao luu và phuc hoi
7.
8.
9.
10.

4. Xây dựng chính sách để phối hợp với các công nghệ được sử dụng trong hệ thống để giảm thiểu tối đa khả năng mất mất dữ liệu trong hệ thống (20 chính sách).