HỌC VIỆN BÁO CHÍ VÀ TUYÊN TRUYỀN
VĂN PHÒNG
*

ĐẢNG CỘNG SẢN VIỆT NAM

Hà Nội, ngày 1 tháng 10 năm 2022

BÁO CÁO
Cải tiến, nâng cấp hệ thống công nghệ thông tin tại Học viện Báo chí và Tuyên truyền

I. HIỆN TRẠNG

1. Hạ tầng kỹ thuật công nghệ thông tin

*Kênh truyền: hiện nay Học viện đang sử dụng 01 kênh internet Leased Line của Viettel (dung lượng 300MB nội địa, 15MB quốc tế) và 04 đường truyền băng thông rộng FTTH (tốc độ download/upload tối thiểu là 100Mbps).Với quy hoạch kênh truyền tạm thời như hiện nay về cơ bản đáp ứng được nhu cầu sử dụng hiện tại của Học viện.

* Hệ thống phòng máy chủ, máy chủ và thiết bị mạng:

Học viện có phòng máy chủ riêng để quản lý tập trung các máy chủ dịch vụ trong đó có:

- 01 máy chủchạy phần mềm Kế toán
- 01 máy chủ Thư viện số
- 01 máy chủ Thư viện điện tử
- 02 máy chủ để cấu hình cấp phát DHCP; cấu hình hệ thống cấp phát chứng chỉ xác thực cho hệ thống wifi.

Ngoài ra có 02 máy chủ được đặt tại tầng 2 nhà A1 chạy phần mềm Quản lý đào tạo; 01 máy chủ đặt ở tầng 3 nhà B1 phục vụ thi cấp chứng chỉ ngoại ngữ theo khung năng lực 6 bậc; 01 máy chủ đặt tại phòng thực hành trường quay ảo tầng 1 nhà B1.

Về thiết bị mạng:

Có 01 thiết bị router Cisco 2911, 01router Mirotik làm chức năng định tuyến; 01 bộ quản lý wifi tập trung Wireless controller cisco 4400; 01 chuyển mạchswitch core cisco 3750 kết nối hệ thống cáp quang tới các tòa nhà trong Học viện; 02 thiết bị chuyển mạch switch layer 3 cisco kết nối hệ thống mạng LAN nhà hành chính A1; 02 thiết bị tường lửa firewall Poloallto PA-500; ngoài ra kết nối đến các tòa nhà A2, A3, B1, B6,B8,B9 và các tầng trong tòa nhà A1 có các thiết bị chuyển mạch switch của hãng cisco, rukus, aruba, tplink...và có 01 bộ lưu điện UBS.

Thực trạng phòng máy chủ, máy chủ và các thiết bị mạng:

- Phòng máy chủ được đặt riêng biệt tại tầng 5 nhà hành chính trung tâm A1, tuy nhiên hạ tầng phòng máy chủ không đáp ứng đúng điều kiện tiêu chuẩn của một trung tâm dữ liệu (data center); phòng máy chủ không có hệ thống cửa ra vào thông minh đảm bảo an ninh; không có hệ thống camera an ninh để kiểm soát ra vào; không có hệ thống sàn nâng, thuận tiện cho việc đi dây và đảm bảo kỹ thuật; hệ thống phòng cháy chữa cháy không đảm bảo; không có nguồn điện riêng dự phòng khi mất điện lưới; không có hệ thống chống sét riêng...

- Máy chủquản trị cấp phát DHCP cho toàn bộ hệ thống mạng LAN và mạng wifi của học việnđượcsản xuất từ năm 2005và Học viện đưa vào sử dụng năm 2010, hiện nay có cấu hình thấp, tốc độ xử lý của CPU kém, dung lượng RAM thấp (IBM Server X3650M3, CPU: E5640 @2.67GHz, RAM: 8GB, 4x300GB SAS 6GB, Windown server 2008) không đáp ứng nhu cầu sử dụng ngày càng lớn của hệ thống mạng hiện nay của Học viện và nguy cơ máy hỏng đột ngột là rất cao do thời gian sử dụng đã lâu. Đối với hệ thống máy chủ dịch vụ như Quản lý đào tạo, Kế toán cũng đưa vào sử dụng lâu cấu hình máy thấp cũng không đáp ứng được nhu cầu sử dụng như hiện nay do số lượng người dùng tăng, dung lượng lưu trữ cũng phải tăng lên; hệ điều hành, các ứng dụng chạy trên máy chủ update liên tục các phiên bản mới đòi hỏi máy phải có cấu hình lớn, tốc độ xử lý cao mới cài đặt được các dịch vụ.

* Thiết bị mạng: thiết bị định tuyến (RouterCisco 2911), thiết bị tường lửa Poloallto PA-500đang sử dụng hiện nay cấu hình của nó có thể làm việc sử lý tối đa khoảng 500 user nhưng để đạt hiệu quả thì chỉ đáp ứng khoảng 400 user tuy vậy số lượng thực tế người dùng tại Học viện rất lớn có lúc hơn 2000 user truy cập nên dẫn đến tình trạng tắc nghẽn, mạng chậm hoặc treo và không đảm bảo được an toàn an ninh mạng .

Ngoài ra các thiết bị mạng khác đều đã đã hết khấu hao, cấu hình thiết bị thấp không phù hợp với nhu cầu hiện tại, thiết bị được trang cấp mới lại ko cùng chủng loại, hang sản xuất nên hệ điều hành của thiết bị khác nhau nên khả năng tương thích kém, nhiều thiết bị đã hết giấy phép (license) nên các dịch vụ đều không được hãng sản xuất hỗ trợ (support) nên nhiều lần bị mất cấu hình hệ thống dẫn đến rất khó khăn trong việc cài đặt lại hệ thống.

* Hệ thống mạng LAN, Wifi:

Hệ thống mạng Học viện đã được hình thành trong giai đoạn 2005- 2010, đã qua nhiều lần nâng cấp, thay đổi và bổ sung.

- Mạng LAN - Tòa nhà A1

Mạng LAN - Tòa nhà A1 (11 tầng) phục vụ cán bộ, nhân viên hành chính thuộc khối Khoa, Phòng, Ban của Học viện.Các thiết bị chuyển mạch lớp truy cập (Switch Access) trong tủ kỹ thuật tại các tầng kết nối đến thiết bị chuyển mạch lõi (Switch Core Cisco SG 500X-24) đặt tại Phòng máy chủ (tầng 05 tòa nhà A1). Cổng lớp 3 (Gateway Layer 3) của các VLAN người dùng tại nhà A1 đặt trên Switch Core Cisco SG 500X-24.

- Mạng không dây các tòa nhà

Tại các tòa nhà vệ tinh và tòa nhà A1, các Switch Access Cisco 2960 PoE được kết nối quang (01 sợi) về Switch quang Cisco 3750 (đặt tại Phòng máy chủ tầng 05 nhà A1) để cung cấp kết nối cho các thiết bị Cisco Access Point.

Một số thông tin về đặc tính của hệ thống mạng không dây:

Cán bộ và sinh viên truy cập mạng không dây xác thực captive portal sử dụng tài khoản được khai báo cục bộ trên từng thiết bị wifi controller (chưa cấu

hình tích hợp domain controller để quản trị, xác thực và sử dụng mạng không dây tập trung)

Switch PoE các tòa vệ tinh đều là các Switch 2960 PoE FaEth (2 cổng quang up-link 1G). Đấu nối trục chính về Switch Quang Core 3750; cổng đấu nối đến các Access Point đều là 100Mbps; Access Point sử dụng giải pháp Cisco AIR-LAP1310G-E-K9 có cổng uplink 100 Mbps

2. Hệ thống hội nghị trực tuyến

Học viện được Học viện chính trị Quốc gia Hồ Chí Minh trang bị cho 02 hệ thống hội nghị trực tuyến Polycom, 01 hệ thống trang bị năm 2014, 01 hệ thống trang bị năm 2021, tuy nhiên cả hai hệ thống đều đang gặp phải sự cố dẫn đến hiệu quả sử dụng không như mong muốn. Hệ thống trang bị năm 2014 bị lỗi hệ thống, thường xuyên bị mất cấu hình và không lưu được cấu hình, mặt khác hệ thống này cũng đã cũ chất lượng hình ảnh camera mờ không được rõ nét. Hệ thống trang bị năm 2021 được trang bị 02 bộ camera, tuy nhiên hiện nay 01 bộ chuyển đổi tín hiệu camera đang hỏng nên chỉ sử dụng được 01 camera, hệ thống này lại lắp đặt tại hội trường lớn có không gian rộng nên việc ghi lấy khuôn hình trong các cuộc họp rất khó.

3. Hệ thống phần mềm ứng dụng

Học viện có Website riêng từ năm 2003 và đến năm 2018 đã chuyển sang sử dụng Cổng thông tin điện tử với tên miền **ajc.hcma.vn**. Đến tháng 4/2014, Học viện đã triển khai và đưa vào sử dụng hệ thống email miễn phí theo tên miền riêng **ajc.edu.vn** cho gần 400 cán bộ và 34 đơn vị trong Nhà trường dựa trên hạ tầng các thiết bị của hãng Microsoft để tận dụng thế mạnh về thiết bị mạng và các giải pháp bảo mật hệ thống của Microsoft.

Hiện tại, 100% đơn vị trong Học viện sử dụng các các phần mềm văn phòng (Microsoft Office). Một số đơn vị của Học viện đã được đầu tư phần mềm chuyên dụng như: phần mềm Quản lý đào tạo; phần mềm Kế toán; phần mềm Quản lý công văn, phần mềm lưu trữ; phần mềm Quản lý thư viện, phần

mềm Quản lý tài liệu số; phần mềm học ngoại ngữ; phần mềm chấm thi trắc nghiệm…

Các phòng máy tính thực hành cài đặt các phần mềm phục vụ học tập như Microsoft Office, Paintshop, Photoshop, Quarkpress, Adobe Premier, Adobe Audition… Hầu hết các phần mềm này là phần mềm crack (không có bản quyền).

Hiện tại tất cả các máy chủ và máy trạm ở một số đơn vị được cài đặt phần mềm diệt virus có bản quyền (Kaspersky), các máy còn lại đều được cài đặt phần mềm diệt virus miễn phí.

II. ĐÁNH GIÁ HIỆN TRẠNG HỆ THỐNG CNTT

1. Hệ thống hạ tầng kỹ thuật đảm bảo

Hệ thống phòng máy chủ là hệ thống hoạt động 24/7/365, liên tục không ngừng nghỉ trong thời gian dài, vì vậy, để hệ thống này có thể hoạt động ổn định, không có sự cố trong suốt thời gian sử dụng thì hệ thống hạ tầng kỹ thuật CNTT của Học viện cần lưu ý một số vấn đề sau:

Hệ thống nguồn dự phòng - UPS hiện đã cũ, có thiết bị UPS đã hỏng nhưng chưa được thay thế.Vấn đề này có thể dẫn đến tình trạng hệ thống ngừng hoạt động bất chợt khi nguồn điện chập chờn hoặc những sự cố mất điện xảy ra. Để bảo vệ thiết bị trong toàn hệ thống cũng như hệ thống không bị gián đoạn thì việc bổ sung, nâng cấp hệ thống UPS là yêu cầu cấp thiết.

Hệ thống điều hòa không khí liên tục luôn cần để có thể làm mát phòng máy chủ, đảm bảo nhiệt độ không bị vượt quá ngưỡng cho phép, giúp cho máy chủ và các thiết bị mạng hoạt động ổn định.Hiện tại Học viện đang sử dụng điều hòa dân dụng không phải hệ thống điều hòa chính xác, khó có thể làm giữ nhiệt độ ổn định trong phòng máy chủ.Điều này sẽ làm giảm tuổi thọ của thiết bị cũng như khả năng vận hành của thiết bị.

Hệ thống sàn nâng không có, hệ thống dây mạng bên khá rối, với hệ thống dây mạng như vậy sẽ tạo điều kiện cho côn trùng phá hoại hệ thống dây mạng,

ngoài ra, khi hệ thống dây mạng gặp trục trặc sẽ rất khó khăn trong vấn đề sửa chữa và bảo trì.

Chưa có hệ thống PCCC để bảo vệ phòng máy chủ, sẽ rất khó khăn trong việc phòng tránh và xử lý khi xảy ra những hiện tượng gây cháy.

Chưa có hệ thống chống sét đường điện cũng như đường tín hiệu dữ liệu, trong trường hợp có sét đánh trực tiếp hoặc lan truyền vào những điểm trọng yếu của hệ thống côn gngheej thông tin, thì các thiết bị trong phòng máy chủ sẽ là những điểm bị công phá đầu tiên, các thiết bị bị cháy nổ dẫn đến mất dữ liệu và gây cháy nổ..

Cần bổ sung hệ thống kiểm soát vào ra và camera giám sát phòng máy chủ để đảm bảo kiểm soát vòng ngoài của hệ thống công nghệ thông tin.

2. Hệ thống hạ tầng công nghệ thông tin

Hệ thống mạng (Mạng wan / Mạng Lan / Thiết bị mạng)

Với khoảng 500 cán bộ công nhân viên và một số lượng lớn các sinh viên (khoảng 7500 sinh viên), đồng thời thời gian đưa vào sử dụng đã lâu nên hệ thống mạng LAN và Mạng không dây của Học viện tồn tại một số vấn đề sau:

Hệ thống dây mạng kết nối đã cũ kỹ, lạc hậu (sử dụng cáp CAT5 tốc độ thấp), nhiều chỗ hư hỏng, không thể hoặc rất khó để khắc phục (nếu có thể khắc phục cũng chỉ là tạm thời).Điều này gây ra việc không đảm bảo kết nối trong thời gian dài tới.

Các trang thiết bị được đầu tư trước đây được trang bị thuộc nhiều nguồn, dự án khác nhau và dàn trải từ năm 2010 cho đến nay nên các thiết bị hoạt động không còn ổn định, hiệu năng thiết bị giảm. Xuất hiện trạng thái quá tải của hệ thống Mạng không dây và Mạng LAN cũng như tình trạng Router Internet treo, người dùng phản ánh truy cập chậm

Một số thiết Switch Access mạng LAN các tòa nhà hiện đang sử dụng các chủng loại un-managed switch (switch Planet, TPlink) nên không có khả năng khai báo và quy hoạch VLAN đến tận lớp Access.

Băng thông mạng trong khuôn viên của Học viện không đảm bảo khi các switch access tại mạng LAN nhà A1 đang sử dụng các chủng loại un-managed switch (không thể quản lý) như: switch Planet, Tplink có tốc độ cổng 100Mbps. Cũng tương tự khi hạ tầng switch PoE kết nối mạng không dây sử dụng các switch Cisco chỉ có tốc độ cổng cao nhất là 100Mbps. Bên cạnh đó thì tại các phòng người dùng cũng sử dụng nhiều un-managed switch để mở rộng mạng LAN, điều này sẽ gây nghẽn băng thông cục bộ trên cổng switch core cũng như trên toàn hệ thống mạng LAN Campus của Học viện.

Trong quá trình vận hành khai thác, do yêu cầu thực tế nên cán bộ kỹ thuật có triển khai mở rộng mạng LAN Campus bằng phương pháp đấu nối đuôi switch mới vào các switch access tại tòa nhà, dẫn đến mở rộng broadcast domain và ảnh hưởng đến hiệu năng của switch access tòa nhà ban đầu, dẫn đến hiện tượng nghẽn băng thông tại các tòa nhà này.

Hạ tầng mạng LAN Campus, Mạng không dây thiết kế chưa theo chuẩn, rời rạc, quy hoạch VLAN hiện tại không trong sáng. Mạng không dây có thể kết nối trực tiếp với Domain Controller, không phân hoạch Security Zone là những vấn đề cần phải cải tổ.

3. Hệ thống máy chủ-lưu trữ và ứng dụng nền tảng

Máy chủ x3650 M3 được đầu tư năm 2005, hiện đã không còn được cung cấp trên thị trường, điều này đồng nghĩa với rủi ro rất lớn trong công tác vận hành khai thác hệ thống máy chủ nếu xảy ra hỏng hóc, đặc biệt khi mà hệ thống công nghệ thông tin của Học viện chưa có giải pháp Sao lưu và Phục hồi dữ liệu. Trong trường hợp không mong muốn sẽ không thể khôi phục lại dữ liệu.

Các máy chủ chưa được quy hoạch tập trung mà phân bố phân tán tại các phân khu rời rạc, ký sinh cùng vào các dải mạng LAN Campus, do vậy không thể triển khai siết chặt chính sách bảo mật.

Hiện tại dữ liệu của Học viện lưu trực tiếp trên ổ đĩa cứng của các máy chủ, điều này gây rủi ro mất mát dữ liệu khi các máy chủ được đầu tư đã lâu và ổ đĩa máy chủ thiếu cơ chế dự phòng.

Hiện tại máy chủ Domain Controller đang chạy dịch vụ Domain Controller nhưng chưa được tích hợp xác thực với mạng không dây cũng như máy tính người dùng chưa kết nối với hệ thống quản trị tập trung người dùng (join Domain) đầy đủ. Đồng thời, máy chủ Domain Controller chưa được triển khai dự phòng.

4. Hệ thống bảo mật

Người dùng truy cập mạng không dây xác thực captive portal sử dụng chung người dùng local khai báo trên wifi controller, do vậy chưa kiểm soát truy cập với từng cá thể người dùng, gây khó khăn trong việc quản trị và gây rủi ro mất an toàn thông tin hệ thống khi người dùng có thể chia sẻ và phát tán mật khẩu.

Mô hình mạng được thiết kế không theo chuẩn bảo mật an toàn thông tin khi chưa có phân vùng DMZ dành riêng cho máy chủ dịch vụ public ra Internet.

Người dùng truy cập Internet không được kiểm soát, bảo vệ.Người dùng mạng không dây kết nối trực tiếp ra internet không qua tường lửa.Trong khi người dùng mạng LAN tại nhà A1 kết nối ra Internet thông qua tường lửa Palo Alto PA500, tuy nhiên chưa có kiểm soát truy cập Internet. Tồn tại này dẫn đến mối nguy hiểm an toàn thông tin nghiêm trọng đối với hệ thống. Thực tế cho thấy, việc mất kiểm soát truy cập Internet của người dùng có thể gây ra những lỗ hổng nghiêm trọng trong hệ thống mạng, cho phép kẻ tấn công có thể thực hiện các hành vi giả mạo, ăn cắp thông tin trong mạng.

Cặp thiết bị Tường lửa Palo Alto PA500 là thiết bị duy nhất bảo vệ hệ thống công nghệ thông tin nhưng có hiệu năng thấp (băng thông tường lửa 250 Mbps) do vậy không đáp ứng đủ nhiệm vụ bảo vệ truy cập web cho toàn bộ hệ thống mạng Campus (bao gồm LAN và Mạng không dây). Thực tế hiện nay cặp thiết bị Palo Alto PA500 chỉ bảo vệ kết nối tại tòa nhà A1.

5. Hệ thống khác

Bên cạnh những yếu điểm trên, hạ tầng công nghệ thông tin của Học viện còn tồn tại một số vấn đề như sau:

Chưa có hệ thống giám sát mạng

Chưa có giải pháp Sao lưu và Phục hồi dữ liệu

Các máy chủ hiện tại vẫn cài đặt OS trên máy chủ vật lý mà chưa triển khai giải pháp ảo hóa để đạt được tối ưu hóa trong sử dụng tài nguyên máy chủ và tăng cường bảo đảm an toàn dữ liệu khi 01 máy chủ vật lý bị hỏng.

Nguồn nhân lực quản lý hệ thống hạ tầng kỹ thuật công nghệ thông tin

Hiện nay, Bộ phận phụ trách các thiết bị hạ tầng kỹ thuật công nghệ thông tin còn mỏng, chưa đáp ứng về số lượng và chất lượng để vận hành một hệ thống lớn hơn, hoàn chỉnh hơn.

Trên đây là Báo cáo về hiện trạng hệ thốngcông nghệ thông tin ở Học viện Báo chí và Tuyên truyền hiện nay, mong trong thời gian tớiHọc viện sẽ được đầu tư trang cấp một hệ thống công nghệ thông tin đồng bộ, hiện đại đảm bảo phục vụ tốt các mặt công tác tiến tới tin học hóa, hiện đại hóa Nhà trường./.

III. GIẢI PHÁP CẢI TIẾN, NÂNG CẤP HỆ THỐNG

1. Hệ thống hạ tầng kỹ thuật đảm bảo

1.1 Mục tiêu

Để đáp ứng yêu cầu phát triển Học viện cần nâng cấp đồng bộ giữa Hệ thống hạ tầng kỹ thuật đảm bảo (no-IT) và Hệ thống CNTT. Hệ thống hạ tầng kỹ thuật đảm bảo cần chắc chắn, hiệu quả và an toàn để bảo đảm cho hệ thống CNTT được hoạt động thông suốt, an toàn về cháy nổ, hạn chế tối đa thiệt hại *khi hệ thống bị sét đánh trực tiếp hoặc lan truyền...*

1.2 Giải pháp

1.2.1 UPS

Khác với tủ điện, việc nâng công suất UPS bằng cách lắp đặt thêm các UPS khá dễ dàng và nhanh chóng mà không cần phải dừng hoạt động của hệ thống. Do vậy, để phù hợp với kinh phí đầu tư ban đầu, đề xuất việc trang bị UPS theo tính chất cần đến đâu đầu tư đến đó.

1.2.2 Điều hòa tập trung

Phòng máy chủ yêu cầu một môi trường ổn định, chính xác, để tối ưu hoá hoạt động của các thiết bị CNTT có tính nhạy cảm cao. Sự thay đổi đột ngột của nhiệt độ và độ ẩm có thể dẫn đến sập toàn bộ hệ thống và có thể khiến cho cơ quan chủ quản phải chịu một chi phí khổng lồ cho các chi phí sửa chữ thiết bị, cài đặt lại phần mềm, … và các tổn thất gián tiếp khác do bị dừng hệ thống.

1.2.3 Phòng máy chủ - sàn nâng và các yêu cầu khác

Phòng máy chủ là phòng quan trọng nhất trong hệ thống CNTT của một đơn vị như Học viện, sử dụng để đặt thiết bị máy chủ chạy các ứng dụng, các phần mềm lõi, xử lý dữ liệu tự động và các thiết bị mạng. Phòng này có yêu cầu đặc trưng về độ ổn định nguồn điện cũng như nhiệt độ môi trường làm việc. Kết hợp các khu lưu trữ dữ liệu: Sử dụng để đặt các thiết bị lưu trữ và sao lưu dữ liệu.

1.2.4 Tủ rack phòng máy chủ và tại các điểm trọng yếu khác

Tủ rack tương đương các tiêu chuẩn chính như: ETS 300 019, IEC 297-3, IEC 529, IEC 917, MIL-STD 801E, UL test 1244, VDE 0 100 T 540

Độ sâu tối thiểu 1000mm để phù hợp với xu hướng thiết bị hiện nay - thiết bị mỏng hơn, dài hơn - không gian mở rộng phía sau của tủ tạo nhiều không gian hơn để quản lý dây cáp, dễ dàng thao tác lắp đặt, bảo dưỡng, bảo hành.

1.2.5 Hệ thống Phòng cháy Chữa cháy (PCCC) cho Phòng máy chủ

Trong các phòng máy chủ, khi có sự cố cháy nổ thường thấy có hai loại đám cháy thường xảy ra đó là cháy âm ỉ và bùng cháy.

Khi các thiết bị điện có vỏ nhựa hoặc các loại dây cáp bị quá nhiệt, sẽ xảy ra hiện tượng cháy âm ỉ.

Khi các thiết bị quá nhiệt và không thể kiểm soát được, sẽ xảy ra đám cháy bùng phá. Đám cháy này có đặc điểm là lan truyền rất nhanh.

Cả hai đám cháy này đều rất nguy hiểm và có thể bùng phát nhanh dẫn đến gây thiệt hại cho người và thiết bị nếu không được xử lý kịp thời.

Với các Phòng Máy chủ luôn hoạt động ngày đêm, chúng ta không thể trực liên tục 24/24 được, vì vậy để đảm bảo an toàn trong việc phòng cháy chữa cháy, nên lựa chọn hệ thống phòng cháy chữa cháy tự động để đề phòng là tốt nhất.

1.2.6 Hệ thống chống, cắt và lọc sét

Một trong những nguyên nhân gây ra sự hư hỏng các thiết bị điện tử nhạy cảm, các thiết bị mạng máy tính nhưng vẫn chưa được chú ý và quan tâm đến chính là Sét. Thành phố Hà Nội nói chung nằm trong vùng có mật độ ngày dông trong năm khá cao, do đó chịu nhiều những thiệt hại bởi những xung sét cảm ứng gây ra. Đặc biệt những xung sét này thường xuất hiện trên đường điện nguồn, đường điện thoại, đường truyền dữ liệu, đường tín hiệu .v.v., chúng có thể gây cháy, làm hư hỏng các hệ thống điện, điện thoại, máy tính, gây hư hỏng các mao mạch điện tử, các bộ vi xử lý.v.v., đồng thời gây nên thiệt hại đáng kể do gián đoạn liên lạc, ảnh hưởng dây chuyền đến toàn bộ các hoạt động liên quan.

Vì vậy vấn đề đảm bảo sự an toàn, hoạt động ổn định của hệ thống mạng máy tính tránh những thiệt hại, ảnh hưởng do dòng sét lan truyền gây ra là vô cùng quan trọng và cần thiết.

1.2.7 Hệ thống kiểm soát vào ra và Camera giám sát

Sử dụng hệ thống thống kiểm soát vào ra bằng thẻ quản lý ra vào với độ chính xác cao, nâng cao tính hiệu quả trong quản lý, hạn chế ngăn ngừa các trường hợp ra vào không đúng thời gian, không đúng nhiệm vụ.

1.2.8 Hệ thống cửa chống cháy phòng Server

Cửa chống cháy hay còn gọi là cửa ngăn cháy được sử dụng làm các loại cửa như: Cửa thoát hiểm, cửa kỹ thuật cho các tòa nhà, các Data Center hoặc các phòng Server của các doanh nghiệp.

Trong hệ thống PCCC cho phòng Server, việc bảo vệ, dập tắt các đám cháy phát sinh từ trong phòng Server là điều cần thiết, tuy vậy, việc bảo vệ phòng Server khỏi các đám cháy lan truyền từ ngoài vào cũng cần thiết không kém. Vì vậy, với giải pháp PCCC và cửa chống cháy sẽ đảm bảo an toàn nhất cho các thiết trong phòng Server.

1.2.9 Ưu điểm của hệ thống sau khi cải tiến, nâng cấp hoặc triển khai mới

Với những bổ sung, nâng cấp cho hệ thống phòng máy chủ, hệ thống máy chủ và các thiết bị sẽ được bảo vệ toàn diện giúp cho việc hoạt động, vận hành ổn định, tăng tuổi thọ của các thiết bị trong phòng máy chủ.

Với hệ thống UPS sẽ đảm bảo hệ thống phòng máy chủ không bị gián đoạn trong thời gian làm việc, đảm bảo cho các máy chủ không bị dừng, tắt đột ngột. Người quản trị có thể chủ động trong việc tắt hệ thống đúng quy trình khi xảy ra những sự cố mất điện.

Hệ thống điều hòa đảm bảo tuổi thọ cho thiết bị, tránh các nguy cơ hỏng hóc thiết bị do tác động của nhiệt độ, giữ cho thiết bị hoạt động ổn định, không sai lệch.

Hệ thống sàn nâng đảm bảo các vấn đề về hệ thống dây, giúp che lấp và bảo vệ hệ thống dây, nâng cao tính thẩm mỹ cũng như tránh cho dây bị ảnh hưởng bởi các tác động của môi trường, các tác động từ côn trùng …

Hệ thống PCCC đảm bảo phòng và chống kịp thời trong những trường hợp có thể gây cháy, đảm bảo có thể phản ứng nhanh nhất có thể với những nguy cơ xảy ra hỏa hoạn.

Hệ thống chống sét đảm bảo cho thiết bị hoạt động an toàn trong những khi thời tiết xấu.

2. Hệ thống hạ tầng công nghệ thông tin

2.1 Mục tiêu

Đáp ứng yêu cầu phát triển trong hoạt động đào tạo, giảng dạy và nghiên cứu khoa học của Học viện, hệ thống công nghệ thông tin cũng cần phải có những thay đổi, thích nghi với nhịp độ phát triển của khoa học công nghệ, trở thành công cụ đắc lực bổ trợ cho các hoạt động đào tạo giảng dạy.

2.2 Giải pháp

2.2.1 Hệ thống mạng (Mạng wan / Mạng Lan / Thiết bị mạng)

Qua khảo sát hiện trạng và đánh giá những tồn tại của hệ thống mạng CNTT tại Học viện cần đầu tư những hạng mục dưới đây để nâng cấp và bổ sung tính năng, hiệu năng:

- Loại bỏ thiết bị Router, thiết bị switch quang C3750 và hệ thống các switch PoE để truy cậpMạng không dây hiện đã xuống cấp và lạc hậu

Tận dụng lại cặp thiết bị tường lửa Palo Alto PA500 để bảo vệ cho phân vùng Server Farm.

- Tận dụng lại cặp switchCisco SG500X24 tại nhà A1 để sử dụng là thiết bị switch gom kết nối (Agg switch) cho các phân vùng DMZ và Server Farm

- Tận dụng lại một số hạ tầng cáp mạng sẵn có (cáp quang, cáp đồng). Tuy nhiên đối với một số hạ tầng cáp mạng sử dụng cáp Cat5 thì triển khai thay mới cáp Cat6 có tốc độ và độ bền cao hơn.

- Triển khai bổ sung một số tuyến cáp quang liên tòa để cấu hình dự phòng đường link cho các switch PoE để truy cập mạng không dây.

- Đầu tư mới 01 kết nối Internet FTTH. Đồng thời đầu tư 01 cặp thiết bị cân bằng tải đường link (Link Balancer) để cấu hình dự phòng đường link cho hệ thống mạng Học viện.

- Đầu tư mới 01 cặp thiết bị switch quang kết nối mạng không dây từ các tòa nhà về để thay thế cho thiết bị Cisco 3750G hiện tại do băng thông hạn chế.

- Đầu tư mới toàn bộ hệ thống switch access mạng LAN tại tòa nhà A1.

- Đầu tư mới toàn bộ hệ thống switch PoE kết nối đến các access point tại các tòa nhà vệ tinh.

- Đầu tư bổ sung hoặc thay thế một số vị trí Access Point

2.2.2 Giải pháp cân bằng tải đường link (Link Balancer)

Link Balancer là giải pháp giúp hệ thống phân phối tài nguyên hiệu quả hơn theo từng mục đích sử dụng. Giải pháp đáp ứng nhu cầu luôn trực tuyến của Học viện, giảm thiểu tình trạng quá tải đường truyền cũng như gián đoạn dịch vụ của Học viện. Những ưu điểm mà giải pháp Link Balancer mang lại cho hệ thống.

2.2.3 Hệ thống bảo mật cho hạ tầng công nghệ thông tin

Giải pháp tường lửa thế hệ mới (UTM)

Thiết bị sử dụng trong hệ thống phải được xây dựng với kiến trúc module, cho phép nâng cấp, mở rộng các khả năng bảo vệ hệ thống một cách dễ dàng. Đồng thời thiết bị phải hỗ trợ các cổng kết nối ảo, ví dụ như IEEE 802.1q VLAN trunking, để sử dụng khi cần phân chia hệ thống thành nhiều vùng mạng.

2.2.4 Giải pháp phòng chống virus tập trung

Lớp phòng chống virus sử dụng phần mềm diệt virus, cài đặt trên các máy chủ, máy tính trạm của cán bộ nhân viên Học viện nhằm bảo vệ máy tính trước các nguy cơ do virus gây ra.

Lớp phòng chống virus sử dụng mô hình quản lý tập trung. Theo đó, tại Học viện sẽ cài đặt bộ quản trị tập trung cho phần mềm diệt virus. Bộ quản trị tập trung này có chức năng quản lý, giám sát, can thiệp đến phần mềm diệt virus cài đặt trên máy trạm nhằm đảm bảo toàn bộ hệ thống được bảo vệ an toàn và thống nhất.

2.2.5 Giải pháp sao lưu – phục hồi dữ liệu

Các tổ chức, Học viện đã và đang thấy được sự tăng trưởng về dữ liệu của họ theo cấp luỹ thừa trong một vài năm trở lại đây. Cũng chính vì vậy mà vấn đề bảo mật dữ liệu đang trở thành một trong những vấn đề rất phức tạp và cần phải đáp ứng nhiều nhu cầu khác nhau đang ngày một tăng. Rõ ràng sự bảo vệ dữ liệu là một mối quan tâm chủ yếu đối với các Học viện ở đủ mọi loại hình kích cỡ, nên nó cần một sự đầu tư đáng kể (phụ thuộc vào kích cỡ của tổ chức, Học viện).

2.2.6 Giám sát mạng

Hiện Học viện có nhiều tòa nhà, các tòa nhà được kết nối với nhau bởi một hệ thống mạng phức tạp và có nhiều thiết bị, vì vậy nhu cầu có một giải pháp giám sát mạng toàn diện là khá cần thiết nhằm quản lý kết nối hệ thống, thiết bị mạng, quản lý lỗi và những công cụ hỗ trợ nhằm đảm bảo hệ thống mạng luôn đạt được hiệu suất cao nhất. Thông qua giao diện mạng vùng biên, phần mềm giám sát mạng đem đến cái nhìn thống nhất về hoạt động của hàng ngàn điểm và giao diện trong hệ thống mạng. Thông qua một giao diện web duy nhất,

có thể giám sát thời gian thực các tham số năng lực hoạt động của bất cứ thiết bị nào đã được kích hoạt SNMP, bao gồm router, switch, tường lửa và máy chủ. Những tham số thường được giám sát bao gồm việc sử dụng băng thông, mất gói tin, độ trễ, lỗi, loại bỏ gói tin, và chất lượng dịch vụ.

IV. KẾ HOẠCH TRIỂN KHAI

STT	Hạng mục	Từ tháng 01-5 Năm 2023	Từ tháng 6-12 năm 2023	Từ tháng 01-05 Năm 2024
1	- Khảo sát xây dựng đề án (Tổng thể và phân kỳ triển khai dự án)			
2	- Lập, trình và phê duyệt đề án. - Trình thẩm định và phê duyệt dự án đầu tư. - Trình thẩm định và phê duyệt Thiết kế, Tổng dự toán, HSMT.			
3	- Tổ chức đấu thầu lựa chọn nhà thầu giai đoạn 1, thương thảo hợp đồng, ký hợp đồng			
4	Triển khai thực hiện hợp đồng			
5	Nghiệm thu thanh lý hợp đồng			

V. KẾT LUẬN

Báo cáo này đã đề xuất các cải tiến quan trọng cho hệ thống CNTT trong Học viện. Việc triển khai những cải tiến này sẽ cải thiện hiệu suất, bảo mật và khả năng mở rộng của hệ thống, từ đó đáp ứng được yêu cầu và mục tiêu phát triển của Học viện.

Để thành công trong việc cải tiến hệ thống CNTT, đề nghị các bước tiếp theo:

1. Xác định nguồn lực: Xác định nguồn lực cần thiết cho việc triển khai các cải tiến, bao gồm ngân sách, nhân lực và thời gian. Điều này sẽ giúp đảm bảo rằng có đủ tài nguyên để triển khai kế hoạch.
2. Lập kế hoạch chi tiết: Xác định các bước cụ thể và mục tiêu cho từng cải tiến. Điều này bao gồm xác định các công việc cần thực hiện, lập lịch triển khai, phân công trách nhiệm và xác định các chỉ số thành công để đánh giá tiến độ.
3. Triển khai từng giai đoạn: Thực hiện triển khai theo kế hoạch đã lập, tuân thủ lịch trình và phân công công việc cho các thành viên trong nhóm. Đảm bảo có cơ chế theo dõi và báo cáo tiến độ để giám sát quá trình triển khai.

4. Đánh giá hiệu quả: Theo dõi và đánh giá hiệu quả của từng cải tiến sau khi triển khai. Điều này giúp xác định liệu các cải tiến đã đạt được mục tiêu và mang lại lợi ích cho tổ chức hay chưa. Nếu cần, điều chỉnh kế hoạch và phương pháp triển khai để tối ưu hóa kết quả.
5. Đảm bảo bền vững: Sau khi triển khai các cải tiến, đảm bảo có các chính sách và quy trình bền vững để duy trì hiệu quả của hệ thống CNTT. Điều này bao gồm việc tiếp tục đào tạo nhân viên, cập nhật công nghệ mới và thực hiện kiểm tra định kỳ để đảm bảo rằng hệ thống luôn hoạt động ổn định và an toàn.

VĂN PHÒNG

Vũ Quốc Cường