HỆ THỐNG DỰ PHÒNG
Khâu không thể thiếu trong an toàn thông tin

ThS. Đặng Mạnh Phổ - *Giám đốc Ban Công nghệ BIDV*

Hệ thống dự phòng dưới góc nhìn an toàn thôngng tin

Để có hệ thống thông tin an toàn cần đảm bảo ít nhất ba yếu tố, đó là:

Thứ nhất, hệ thống xử lý thông tin phải được bảo vệ: Hệ thống xử lý (bao gồm các server, thiết bị mã hóa / giải mã, các bộ chuyển mạch, các hệ tích hợp phần cứng phần mềm v.v) phải được đặt trong hệ thống mạng với nhiều cấp độ bảo vệ khác nhau, được kiểm soát với các thiết bị an ninh mạng chuyên dụng như tường lửa (Firewall), Proxy, thiết bị phát hiện và ngăn chặn tấn công (IPS), mạng riêng ảo (VPN, với công dụng chính là để kiểm soát các truy cập từ xa)...

Thứ hai, hệ thống phần mềm phải được bảo vệ: Phần mềm hệ thống (hệ điều hành, cơ sở dự liệu, phần mềm trung gian...) và các phần mềm ứng dụng phải được cấu hình đảm bảo an ninh, kiểm tra định kỳ, cập nhật các bản vá mới nhất, được bảo vệ bằng các chương trình phòng chống virus/mã độc/sâu máy tính hữu hiệu...

Thứ ba, có hệ thống dự phòng.

Trong đó, yếu tố thứ ba hệ thống dự phòng là khâu không thể thiếu trong an toàn thông tin. Hệ thống dự phòng là hết sức quan trọng đối với sự an toàn của hệ thống thông tin của các doanh nghiệp và các ngành, các cơ quan, đặc biệt là hệ thống thông tin của các ngành, cơ quan quan trọng như ngân hàng, tài chính... Nhiệm vụ chính của hệ thống dự phòng là chia sẻ tài nguyên, thông tin với các hệ thống chính, chia sẻ tải và thay thế hệ thống chính khi cần thiết, đảm bảo hoạt động thông suốt của hệ thống thông tin. Hệ thống dự phòng sẽ lưu trữ và vận hành song song một hệ thống thông tin khác

cùng nội dung với hệ thống chính. Thông tin dữ liệu lưu trữ tại hệ thống dự phòng phải luôn được cập nhật, đồng bộ với thông tin dữ liệu của hệ thống chính với mục đích dự phòng cho hệ thống chính. Hệ thống dự phòng cũng phải bao gồm đầy đủ cơ sở vật chất kỹ thuật, năng lực xử lý để đảm bảo hoạt động chia sẻ và thay thế hệ thống chính khi cần thiết.Ngoài ra, hệ thống dự phòng cũng có thể được sử dụng cho mục đích đào tạo, chuyển giao công nghệ; thử nghiệm các giải pháp công nghệ mới.

Yêu cầu đối với hệ thống dự phòng

Một hệ thống dự phòng hoàn hảo phải đáp ứng các yêu cầu tối thiểu như sau:

Hệ thống dự phòng phải được đặt cách biệt với hệ thống chính và phải được bố trí với mức an toàn cao nhất. Nói chung hệ thống dự phòng phải được bố trí ở nơi đủ xa với hệ thống chính để đề phòng sự cố hoặc thảm họa có ảnh hưởng diện rộng (lũ lụt, động đất...) và phải được bố trí bảo vệ an toàn mọi mặt (cả về hành chính, vật lý, kỹ thuật...). Việc bố trí hệ thống dự phòng ở gần với hệ thống chính có thể mang lại lợi ích trước mắt là đơn giản về hạ tầng kỹ thuật và giảm chi phí đầu tư. Tuy nhiên, có thể thấy ngay là trong trường hợp này hệ thống dự phòng cũng tiềm chứa các rủi ro chẳng kém gì như hệ thống chính, ví dụ như sẽ chịu chung sự cố mất điện diện rộng, ngập lụt hay hỏa hoạn. Nhiều doanh nghiệp chọn giải pháp đặt hệ thống dự phòng ở cách xa hệ thống chính nhưng vẫn trong phạm vi quốc gia để giảm thiểu các rủi ro phù hợp với chi phí cho phép. Cũng có các tổ chức, công ty lớn xây dựng và duy trì hệ thống dự phòng xuyên quốc gia hoặc trên phạm vi toàn cầu để đạt được mức độ bảo vệ cao nhất. Hiện nay cũng đã có hình thức đi thuê và cho thuê hệ thống dự phòng.

Có cơ sở vật chất kỹ thuật độc lập, tách biệt với hệ thống chính. Cụ thể, hệ thống dự phòng cần có đường điện và hệ thống điện (bao gồm trạm biến áp, UPS, máy phát điện, ATS...) tách biệt; có hệ thống đường truyền và mạng riêng biệt; có đủ cơ sở phòng máy, phòng làm việc, kho tàng... Khi xây dựng hệ thống dự phòng cũng cần lưu tâm đến vấn đề bảo đảm các điều kiện làm việc của cán bộ vận hành thường xuyên cũng như trong trường hợp chuyển sang sử dụng hệ thống dự phòng thay thế cho hệ thống chính.

Hệ thống dự phòng phải có đủ năng lực kỹ thuật sẵn sàng đảm nhận toàn bộ vai trò cua hệ thống chính trong trường hợp hệ thống chính bị sự cố ngừng hoạt động và đáp ứng yêu cầu về thời gian vận hành tối thiểu tại

hệ thống dự phòng. Chẳng hạn, trong trường hợp hệ thống chính bị phá hủy hoàn toàn thì phải thiết lập một hệ thống xử lý mới và khoảng thời gian vận hành tại hệ thống dự phòng sẽ không bị giới hạn.

Phải đảm bảo tại hệ thống dự phòng thường xuyên sao lưu và cập nhật được thông tin dữ liệu hoạt động cua hệ thống chính, đáp ứng yêu cầu mục tiêu điểm khôi phục (RPO). Ở đây mục tiêu điểm khôi phục (RPO- Recovery Point Objective) là tổn thất tính theo thời gian. Ví dụ RPO = 10 phút có nghĩa là khoảng tổn thất là 10 phút (mất dữ liệu/hệ thống trong 10 phút). Chỉ tiêu này thường mang ý nghĩa tổn thất chấp nhận được trong trường hợp có thảm hoạ xảy ra đối với hệ thống chính và đặc biệt quan trọng đối với các hệ thống thông tin xử lý giao dịch trực tuyến (online) và theo thời gian thực (real-time) vì sẽ liên quan đến các giao dịch, đặc biệt là các giao dịch tài chính bị mất trong khoảng thời gian đó. Nói chung, RPO được xác định tùy thuộc vào tính chất và mục tiêu hoạt động của hệ thống thông tin. Thực tế cho thấy muốn có RPO nhỏ (tổn thất ít trong trường hợp có sự cố đối với hệ thống chính phải chuyển sang sử dụng hệ thống dự phòng) thì phải đầu tư thích đáng vào việc xây dựng và duy trì hệ thống dự phòng.

Phải đảm bảo tính sẵn sàng hoạt động của hệ thống dự phòng trên phương diện như là hệ thống chính thứ hai, trong đó đặc biệt quan trọng là thời gian đưa hệ thống dự phòng vào hoạt động thay thế hoàn toàn cho hệ thống chính phải đáp ứng yêu cầu về thời gian khôi phục (RTO - Recovery Time Objective), đây là thời gian cần thiết để khôi phục (trên hệ thống dự phòng) đối với các ứng dụng và hệ thống chủ chốt của doanh nghiệp. Chẳng hạn đối với một doanh nghiệp RTO có thể là 4 giờ (nửa ngày làm việc) nhưng đối với doanh nghiệp khác có thể là 8 giờ (1 ngày làm việc). Ngoài ra cũng cần quan tâm đến tính sẵn sàng của các dịch vụ viễn thông nhằm đảm bảo công tác truyền thông giữa các bộ phận liên quan và người sử dụng.

Phải đảm bảo yêu cầu về thời gian để quay về trạng thái hoạt động bình thường, tức là chuyển hoạt động trên hệ thống dự phòng về hệ thống chính. ở đây cũng liên quan đến RTO và nói chung phải bảo đảm tính khả chuyển hai chiều đối với hoạt động giữa hệ thống chính và hệ thống dự phòng.

Xây dựng hệ thống dự phòng khi còn chưa muộn

Người Việt Nam có câu: "Mất bò mới lo làm chuồng, người Trung Quốc thì nói: "Mất dê mới lo làm chuồng ("Vong dương bổ lao), người Anh có câu: "Sống ngựa mới lo khóa chặt cửa (lock the stable door after the horse has bolted). Tất cả các thành ngữ này đều mang hàm ý: Do không chịu phòng ngừa hậu họa, không sửa chữa sai sót kịp thời nên phải gánh chịu tổn thất.

Như trên đã nêu, hệ thống dự phòng là khâu không thể thiếu trong an toàn thông tin và là hết sức quan trọng đối với sự an toàn của hệ thống thông tin của các doanh nghiệp, tổ chức. Tuy nhiên, trong thực tế việc xây dựng và duy trì hệ thống dự phòng không phải lúc nào cũng được các đơn vị, tổ chức quan tâm đúng mức. Điều này cũng có lý do của nó. Chẳng hạn, có ý kiến cho rằng hệ thống dự phòng chỉ đơn giản là dùng để khôi phục lại thông tin dữ liệu sau khi sự cố hoặc thảm họa xảy ra, và như vậy có vẻ như hệ thống dự phòng là một sự lãng phí, một kiểu bảo hiểm quá xa xỉ. Không doanh nghiệp nào muốn đầu tư một hệ thống dự phòng một tài sản đắt tiền nhưng nhàn rỗi, năm thì mười họa mới sử dụng đến khi có sự cố. Tất nhiên, đây là một cách nhìn phiến diện. Để trả lời cho vấn đề này cần xác định rõ rằng hệ thống dự phòng được sử dụng với nhiều mục đích khác nhau, trong đó mục đích dự phòng để thay thế hệ thống chính khi cần thiết là chính yếu, ngoài ra còn có mục đích chia xẻ tải với hệ thống chính để tạo ra sự cân bằng tải chung, chống sự ách tắc, nghẽn cổ chai trong xử lý thông tin; hệ thống dự phòng có thể sử dụng để sao lưu và sửa chữa các lỗi ứng dụng khi mà các lỗi này không thể sửa trên hệ thống chính do yêu cầu vận hành liên tục; hệ thống dự phòng cũng có thể phục vụ các mục đích thử nghiệm ứng dụng mới, đào tạo và chuyển giao công nghệ... Nói cách khác, hệ thống dự phòng được khai thác song song với hệ thống chính và điềunày góp phần nâng cao hiệu suất làm việc và khả năng cạnh tranh của doanh nghiệp.

Cần nhìn nhận hệ thống dự phòng là giải pháp bảo vệ hữu hiệu nhằm đảm bảo kinh doanh liên tục đồng thời đem lại những khả năng mới, đẩy nhanh thời gian tiếp cận thị trường thông qua các ứng dụng mới và giảm chi phí tổng thể. Cần xem xét việc xây dựng và duy trì hệ thống dự phòng trong chiến lược phát triển cua doanh nghiệp, tổ chức, gắn với lợi ích lâu dài, gắn với hoạt động an toàn, ổn định của hệ thống thông tin nói riêng và của bản thân doanh nghiệp, tổ chức nói chung.

Hãy xây dựng và duy trì hệ thống dự phòng kịp thời, đừng để mất bò mới lo làm chuồng ■

Tài liệu tham khảo:

Disaster and Recovery Planning Networks, Telecommunications, and Data Communications. Regis J. Bates, Jr. McGraw-Hill, Inc.

Disaster and Recovery Planning: A Guide for Facility Managers. 2nd Edition. Joseph F. Gustin. THE FAIRMONT PRESS, INC. & MARCEL DEKKER, INC.

Xây dựng trung tâm dự phòng và phục hồi thảm họa Nguyễn Đức Anh Website NHNNVN