ÁP DỤNG KỸ THUẬT QUẢN LÝ RỦI RO VẬT LÝ NHẰM TĂNG CƯỜNG AN NINH CHO TRUNG TÂM DỮ LIỆU VÀ TỦ MẠNG

Michael Zlatic - GĐ quản lý sản phẩm cấp cao APC

Việc gia tăng nhanh chóng nhu cầu an ninh của bất kỳ mạng công nghệ thông tin (CNTT) nào đều bao gồm rất nhiều yếu tố giúp đảm bảo sự bảo vệ tuyệt đối cho mạng, trong đó hai nhóm yếu tố rộng, đặc trưng cho các loại rủi ro: rủi ro số và rủi ro vật lý. Rủi ro số bao gồm các yếu tố như hackers, vi-rút, nghẽn mạng, những hổng hóc khác về an ninh do vô tình hoặc cố ý, sự thống nhất và lưu thông dữ liệu. Những rủi ro vật lý bao gồm các trường hợp như các điều kiện hoạt động cận tối ưu của môi trường và sự can thiệp cố tình hoặc vô ý của con người vào tự nhiên.

Những phương pháp truyền thống để đối phó với những rủi ro này như việc kiểm tra hàng tháng đã không còn phù hợp với sự thay đổi công nghệ nhanh chóng của các thiết bị hiện nay. Sự thất bại của các phương pháp truyền thống là kết quả của những quy định điều chỉnh và những tiêu chuẩn yêu cầu kiểm soát thường xuyên đối với các thiết bị này. Sự xuất hiện của các máy chủ dạng phiến (blade servers) và ảo hoá (virtualization) đang nâng cao nhu cầu năng lượng và lượng hơi nóng thải ra trong mỗi rack của thiết bị. Những qui định như Đạo luật Sarbanes-oxley và Luật Trách nhiệm trao đổi bảo hiểm y tế HIPAA tiếp tục nhấn mạnh vào tầm quan trọng của một cách tiếp cận chủ động hơn trong việc bảo vệ ổ cứng vật lý và các dữ liệu được lưu trữ trong đó. Những chuẩn qui định như của Green Grid, tổ chức toàn cầu chuyên về hiệu quả năng lượng tại các trung tâm dữ liệu và hệ sinh thái điện toán, yêu cầu sự giám sát liên tục môi trường và các thiết bị để đảm bảo hiệu quả tối ưu nhằm loại bỏ chất thải. Cần thiết lập một hệ thống tự vận hành để bảo vệ các thiết bị CNTT (IT assets) khỏi các rủi ro vật lý trong một trung tâm dữ liệu (TTDL) hoặc tủ mạng, loại bỏ tình trạng đứt đoạn hay sự cố của cấu trúc công nghệ thông tin. Với một loạt những ứng dụng được nối mạng có khả năng mở rộng, các bộ cảm biến, kiểm soát truy cập và các máy quay được thiết kế để bảo vệ các thiết bị CNTT thì các giải pháp kỹ thuật để đảm bảo an ninh có thể mở rộng khi những thiết bị CNTT thêm được đưa vào hoạt động để đáp ứng các tải máy tính gia tăng trong tương lai.

Ba thành tố chính cấu tạo nên khả năng kiểm soát môi trường và an ninh trong một TTDL hoặc tủ mạng là: môi trường, giám sát và kiểm soát truy cập.

Thứ nhất, việc đánh giá các chỉ số sức khỏe hay môi trường chủ chốt như nhiệt độ lạnh trong hàng, độ ẩm của hàng, luồng khí và sự xuất hiện của các tạp chất lưu bắt đầu miêu tả môi trường trong đó các thiết bị CNTT hiện đang vận hành.

Thứ hai, bằng cách ứng dụng hệ thống tích hợp quay video, những đoạn phim ghi lại sẽ cung cấp bằng chứng về việc những ai đã tiếp cận các thiết bị CNTT khi có sự cố xảy ra, bất kể sự cố đó do con người hay môi trường gây ra.

Thứ ba, các hệ thống điện tử giúp giới hạn việc tiếp cận vào các rack dựa trên ứng dụng thẻ cảm ứng của mỗi người sử dụng. Nếu không được phép truy cập thì quá trình truy cập sẽ bị từ chối và ngay lập tức một file ghi nhớ sẽ được thiết lập và lưu trữ cho việc tra cứu sau này. Cảnh báo sớm về những nhân tố môi trường hay con người có thể giúp ngăn chặn những sự cố hoặc hư hỏng thiết bị nhờ hệ thống chủ động thông báo cho các bên có thẩm quyền về một sự kiện sẽ xảy ra trong tương lai gần hoặc vừa xảy ra. Lưu trữ trung đến dài hạn quyết định xu hướng của mỗi chỉ số: các xu hướng hàng ngày, hàng tuần hoặc theo chu kỳ có thể dễ dàng được xác định và các biện pháp sửa chữa được đặt đúng chỗ nhằm ngăn chặn tình trạng các thiết bị CNTT có thể hoạt động ngoài tầm kiểm soát mà nhà sản xuất cho phép.

TTDL và các ứng dụng tủ mạng đòi hỏi những cách tiếp cận đặc biệt khác nhau tới việc kiểm soát an ninh và môi trường. Trong một TTDL, các rack luôn luôn được gắn liền với những bảng đặc ở phía trên, bên trái, bên phải trong khi mặt trước và phần sau được làm từ các lưới kim loại cứng cho phép khí lạnh có thể đi vào các thiết bị CNTT từ phía trước và khí nóng sẽ thoát ra từ phía sau. Mỗi rack tạo thành một môi trường nhỏ (micro-environment) để giải thoát khí từ các thiết bị CNTT và đây cũng chính là nhân tố ảnh hưởng tới tuổi thọ của thiết bị, đặc biệt là nếu thiết bị không được duy trì ở những môi trường tối ưu. Theo Viện Nghiên cứu toàn cầu về trung tâm dữ liệu Uptime của Mỹ (Uptime Institute), với mỗi 15oF trên 75oF mà các thiết bị CNTT được sử dụng như trên, tuổi thọ của thiết bị CNTT có thể bị giảm xuống với hệ số là 2. Điều này đúng với các tủ mạng nhỏ tuy nhiên đối với các TTDL thì ứng dụng này có khác đôi chút. Trong nhiều trường hợp, tủ mạng chứa hai hoặc bốn rack phía sau và có thể mở ra môi trường ở trong phòng. Kiểm soát truy cập vào thiết bị được duy trì cho cửa đến phòng. Môi trường của một phòng được xem là đồng nhất khi không có những dòng khí khác biệt. Các giải pháp cho những loại ứng dụng này bao gồm kiểm soát ở cấp độ phòng hơn là kiểm soát ở từng rack cụ thể cũng như đối với các rack khép kín.

Một biến số môi trường dễ hiểu nhất là nhiệt độ. Nếu nhiệt độ không được duy trì ở mức độ tối ưu thì có thể sớm dẫn đến những sự cố xảy ra đối với các thiết bị CNTT. Xem xét phân tích hiệu quả của một TTDL sau đây. Dựa trên sự di chuyển năng lượng từ lúc đi vào các lớp vật lý tới ổ cứng máy tính, tới các chip và cuối cùng là tới các thiết bị ứng dụng. Ở mỗi bước, phần lớn năng lượng được chuyển thành khí nóng. Cụ thể, trong khi chỉ 0.001% là được sử dụng một cách hữu ích thì 99.999% năng lượng còn lại bị chuyển thành khí nóng, do vậy vấn đề tại sao nhiệt độ luôn gia tăng là một việc hiển nhiên. Năm 2005, Viện Uptime đã nhận thấy rằng 10% các rack hoạt động ở nhiệt độ quá nóng và không đáp ứng được những tiêu chuẩn của ngành về khả năng hoạt động và mức độ tin cậy công nghệ tối đa. Ngoài ra,

sau khi đã tính đến những xu hướng gần đây như ảo hóa, máy chủ dạng phiến, hội tụ thoại và dữ liệu thì thậm chí người ta còn thống kê được rằng hơn 10% các hàng rack hoạt động ở nhiệt độ nóng quá mức cho phép. Theo đánh giá của Tập đoàn Cisco, mức năng lượng tiêu thụ bởi một tủ mạng trung bình đã tăng vọt (theo cấp số 10) trong 10 năm qua. Giả sử hầu hết năng lượng chuyển thành khí nóng thì nhu cầu kiểm soát môi trường của các thiết bị công nghệ sẽ càng trở nên bức thiết. Do đó, nhu cầu về tính hiệu quả cao hơn và kỹ thuật kiểm soát toàn bộ ngày càng lớn hơn. Nếu không đảm bảo rằng các thiết bị đang hoạt động theo đúng những chỉ số kỹ thuật của nhà sản xuất thì tuổi thọ của thiết bị sẽ bị rút ngắn đáng kể.

Trong khi các nhân tố về môi trường đang được xem là bước đầu tiên cho các công ty trong quá trình giám sát nguy cơ vật lý, ngày càng có nhiều chuyên gia về phòng mạng nhỏ và trung tâm dữ liệu chú trọng tới bảo mật với việc tuân thủ theo đúng các quy định và giảm thiểu sự cố. Theo thông tin từ viện nghiên cứu Uptime, hơn 60% sự cố do con người gây ra, từ việc vận hành, xây dựng và thiết kế các hạng mục liên quan. Những nhân tố khác quyết định đến an ninh là những quy định như của Sarbanes-Oxley và HIPAA khiến việc quản lý khả năng truy cập vật lý ở cấp độ tủ rack trở nên ngày càng quan trọng hơn. Rất nhiều công ty giảm khả năng truy cập tới các không gian CNTT và tiến hành giám sát toàn bộ các thiết bị của họ để đạt được hiệu quả bảo mật mong muốn. Tuy vậy việc kết hợp chức năng điều khiển truy cập và giám sát với các công cụ cảnh báo và phân tích cũng rất quan trọng. Nó cho phép các sự cố hay các lỗ hổng về an ninh có thể nhanh chóng được theo dõi, tìm tới nguyên nhân của sự cố.

Cứ tưởng tượng rằng mỗi ngày trong cuộc sống, con người được vây bọc bởi rất nhiều các hệ thống tự động làm việc để bảo vệ cuộc sống và tài sản của con người, tạo ra một loạt các lưu trữ về những sự kiện trong toàn bộ quá trình như:

- Hệ thống chống hỏa hoạn để bảo vệ cuộc sống và tài sản của con người.
- Hệ thống kiểm soát truy cập giúp ngăn chặn sự xâm nhập trái phép qua cửa vào.
- Giám sát video tạo ra một loạt kiểm duyệt bằng hình ảnh của các sự kiện
- Hệ thống Điều hòa thông gió HVAC duy trì một môi trường có lợi cho sức khỏe của cộng đồng trong một công trình.
- Các nhân viên bảo vệ đảm bảo anh ninh tại các địa điểm cũng như khu vực cấm xâm nhập
- Bơm xả nước luôn đảm bảo ở mức nước thấp bảo vệ các tòa nhà khỏi ngập nước

Nhưng câu hỏi vẫn còn tồn tại là, những giải pháp nào bảo vệ thiết bị CNTT chống lại các nguy cơ vật lý có thể gây ra sự cố hoặc sự hủy hoại đối với hạ tầng CNTT? Giống như các hệ thống bảo vệ cuộc sống và tài sản, các thiết bị CNTT phải có đủ sức chịu được mức độ bảo vệ hay chịu được mức phá hoại có thể xảy ra của những hệ thống không được bảo vệ ■

Tích hợp các công nghệ IP và công nghệ quang nâng cao hiệu năng mạng và giảm chi phí vận hành

Ngọc Cường

Nokia Siemens Networks và Juniper Networks, đang cùng hợp tác trong lĩnh phát triển các giải pháp IP qua DWDM (IP over DWDM) tối ưu hóa chi phí 10G, 40G và 100G, tích hợp quản lý và sử dụng chung bảng điều khiển GMPLS. Mục tiêu của 'mối nhân duyên' này nhằm cho ra đời Giải pháp IP-Quang tích hợp - Một giải pháp tiết kiệm chi phí và có độ linh hoạt cao trong việc mở rộng hệ thống mạng của họ nhằm quản lý số lượng các ứng dụng dữ liệu, thoại và đa phương tiện ngày càng gia tăng.

Cuộc nhân duyên này sẽ cho ra đời nền tảng công nghệ mới gồm công nghệ định tuyến IP của Juniper được kết hợp với công nghệ truyền dữ liệu ghép kênh theo bước sóng cao (Wavelength Division Multiplexing - WDM) của Nokia, cùng với các hệ thống quản lý hoạt động của cả hai công nghệ này. Việc có cả hai thế giới dưới một mái nhà quản lý mạng cũng đồng nghĩa với việc cần đảm bảo chất lượng cao nhất có thể trong cả hai yếu tố là sự đơn giản và tính hiệu quả. Theo ông Uwe Fischer, đại diện của Nokia Siemens Networks thì: Khi các nhà khai thác hợp nhất các môi trường IP và DWDM của họ để bảo đảm tăng cường hiệu quả về chi phí, giải pháp mới này sẽ giúp phá bỏ những rào cản giữa các lớp quang và điện.

Khi những xu thế như video, ảo hóa và điện toán đám mây tiếp tục định hướng nhu cầu về năng lực mạng lõi, các nhà khai thác sẽ tìm kiếm những phương thức để mở rộng hệ thống mạng của họ một cách hiệu quả và tiết kiệm chi phí. Việc kết hợp các công nghệ truyền dẫn quang và IP se giúp tăng cường hiệu quả của hệ thống mạng.

Việc triển khai đưa quang học DWDM vào các thẻ giao diện dòng bộ định tuyến sẽ giúp tăng hiệu quả của hệ thống mạng nhờ việc làm giảm bớt nhu cầu về các hệ thống tiếp sóng dự trữ, nhưng có thể làm nảy sinh những thách thức về quản lý hệ thống mạng bởi vì các hệ thống mạng quang và IP theo truyền thống là được quản lý hoàn toàn độc lập với nhau. Để giải quyết những mối lo ngại này, Nokia Siemens Networks và Juniper đang nghiên cứu và phát triển một giải pháp sáng tạo có thể quản lý toàn bộ kết nối bộ định tuyến-tới-quang như là một thực thể đơn nhất. Sử dụng các Bộ định tuyến Lõi dòng T-series của Juniper, các giao diện DWDM quang tích hợp bộ định tuyến sẽ hoàn toàn tương thích với nền tảng WDM hiT7300 của Nokia Siemens Networks và được quản lý bởi Hệ thống Quản Lý Mạng Truyền Dẫn (TNMS) cấp độ nhà khai thác của công ty.

Sử dụng phần mềm hoạch định mạng TransNet, giải pháp chung này sẽ nâng cao hiệu quả tổng thể trong hệ thống mạng. Bên cạnh đó, nhà khai thác sẽ có thể cung cấp dịch vụ một cách nhanh chóng hơn khi chỉ có duy nhất giao diện DWDM là cần phải được cài đặt và cấu hình, độ tin cậy cũng được tăng cường nhờ khả năng phát hiện lỗi kết nối sớm, cải thiện việc xử lý sự cố và đơn giản hóa một cách tổng thể.