THIẾT BỊ BẢO MẬT - CHƯA ĐỦ!

Thiết

Thiết bị bảo mật cần thiết với mọi công ty hiện đại nhưng công nghệ trong lĩnh vực này tiến triển hơi chậm so với nhu cầu. Việc thiếu hụt những giải pháp hoàn toàn mới được bù đắp bằng quảng cáo! Vậy thì giải pháp thật sự là gì, ở đâu?

Ảo tưởng an toàn

Thiết bị bảo mật ngày hôm nay đã phát triển tới điểm bão hoà công nghệ. Sự phát triển vũ bão của công nghệ cao trong môi trường này dường như chấm dứt. Vẫn chỉ là những công cụ chống virus được cải tiến, những công cụ phát hiện và ngăn chặn tấn công với khả năng nào đó được lăng xê thành "giải pháp cách mạng" mới. Sự thiếu vắng sáng tạo được bù đắp bởi chính sách phát triển những thiết bị này: nó đủ tích cực và thú vị. Thử xét một một mô hình tương tự: Nhiều tên lửa không chiến bây giờ đạt chuẩn nguyên lý "phóng rồi quên". Viên phi công chỉ có nhiệm vụ phát hiện mục tiêu, đưa nó vào tâm điểm trên radar của máy bay mình và nhấn nút đỏ phóng tên lửa đi. Mọi chuyện sau đó không còn là việc của anh ta.

Quảng cáo hiện tại cho những hệ thống và thiết bị phòng thủ thông tin cũng vậy, theo nguyên lý "mua rồi quên". Bạn hãy mua hệ thống XYZ, giải quyết vấn đề của mình rồi quên bẵng nó. Trong khi, hệ thống không phải được mua để giải quyết vấn đề cụ thể nào đó mà chỉ là phương tiện có đủ khả năng thi hành những nhiệm vụ tương tự. Người ta thường im lặng về vế sau. Người ta lờ đi vì phương tiện bảo vệ thông tin không thuộc loại phương tiện đảm bảo kết quả như nhau theo kiểu "lá chắn đảm bảo" hay ngược lại. Nhiều công ty vẫn nghĩ rằng không mua thiết bị bảo mật thì thông tin của công ty không được bảo vệ trong khi không nhà cung cấp nào dám đảm bảo 100% với người mua rằng hệ thống của khách hàng sẽ được bảo vệ ngay cả khi khách hàng đã mua cấu hình mạnh nhất.

Quảng cáo về bảo mật thường nhấn mạnh vào những điển hình chứ không đi vào đặc tính kỹ thuật của hệ thống nào đó. Các slogan quảng cáo: "Tốt hơn, nhanh hơn, đơn giản hơn!" thường xuyên xuất hiện trước những dòng liệt kê tính năng hệ thống nhưng vẫn lảng tránh các thông số kỹ thuật theo kiểu chỉ hô khẩu hiệu: "Đó là giải pháp thông minh", "Hệ thống với tầm bao phủ rộng",... Cái khó chịu nhất trong các tình huống bảo mật không ở chỗ quảng cáo và cũng không cần kể tới các trường hợp "mua rồi quên". Cái khó chịu nhất là thiết bị bảo mật tạo ảo tưởng về sự an toàn.

Chẳng hạn, ai cũng biết trong quá trình cài đặt theo mặc định, hệ thống lọc liên mạng không lọc gì hết; cũng tức là hệ thống không được bảo vệ trước bất cứ thứ gì. Chỉ quá trình cài đặt đầy hiểu biết mới có thể đạt được trạng thái mà thiết bị thực hiện đúng những chức năng "được giao". Còn đây là ví dụ với những hệ thống phức tạp và tiên tiến hơn: IPS – hệ thống ngăn chặn tấn công. Tình huống còn buồn thảm hơn. Tự thân hệ thống được mua để ứng dụng vào mạng lưới của bạn thực sự không đảm bảo bất kỳ bảo vệ nào. Cần phải cài đặt nó và không chỉ cài đặt một lần là xong. Phải thường xuyên theo dõi vận hành của hệ thống, phân tích mạch lạc những sự kiện, phản ứng tích cực với những nguy cơ mới, v.v… Những hệ thống này đều được quảng cáo là "phản ứng thông minh trước…" nhưng không có nghĩa là mình có thể quên việc cài đặt, cân chỉnh hệ thống bảo vệ.

Ví dụ, trong vùng kiểm soát xuất hiện những hành vi nghi ngờ, hệ thống phát hiện tấn công lập tức đóng và cấm mọi thứ có thể đóng và cấm. Nếu không phát hiện yếu tố này kịp thời thì hệ thống của bạn nhất thời biến thành cỗ xe cút kít, số chức năng giảm chỉ còn ở mức tối thiểu. Phản ứng của chuyên gia phải phù hợp: cần phát hiện đúng nguyên nhân xem hệ thống bị tấn công thật hay chỉ là phản ứng với các yếu tố ngẫu nhiên, cân chỉnh bằng tay với hệ thống tuỳ thuộc kết luận của việc phân tích. Những thứ này ít được nhắc đến trong các bảng hướng dẫn sử dụng thiết bị bảo mật. Sẽ là mù quáng khi mua IPS mà không hiểu biết thế nào là tấn công trên mạng. Chuyện này củng cố quan điểm: bất kỳ hệ thống nào cũng chỉ là phương tiện nằm trong tay con người và không phải là giải pháp hoàn hảo như những nhà cung cấp và quảng cáo nói.

Có một ngoại lệ thú vị trong trường hợp này: các giải pháp chống virus. Các hệ thống chống virus đã phát triển đủ cao, thực thi hầu như trọn vẹn chức năng: việc cập nhật diễn ra thường xuyên và tự động chỉ với điều kiện đồng ý với nó hay không. Thông thường khách hàng xác định chất lượng bảo vệ hoàn toàn không phụ thuộc vào số lượng virus phải diệt mà là thời hạn phản ứng trước đại dịch của virus mới chưa được biết tới. Vì thế, sản phẩm của các hãng chống virus thường na ná như nhau.

Cái nhìn hời hợt

Mong ước của người dùng: Một chạm là xong!

Vấn đề bảo vệ trước những nguy cơ từ bên trong cũng được đề cập nhiều. Cứ cho là chu vi thông tin DN đã được rào chắn, bảo vệ tốt thì tất cả thông tin trong khu vực lại là vấn đề lớn với các tổ

chức. Tuy nhiên, với những thiết bị đề xuất giải quyết những nguy cơ từ bên trong mà cũng mua sắm theo nguyên lý "mua rồi quên" thì rất nguy hiểm. Một nhà phát triển trong lĩnh vực bảo mật Nga khẳng định những nguy cơ từ bên trong là những USB và việc nhân viên sử dụng chúng bất hợp pháp là nguy cơ lớn với việc rò rỉ thông tin của mạng nội bộ DN.

Như vậy, vấn đề nguy cơ nội bộ khiến phải thảo luận là kiểm soát hay không các thiết bị ngoại vi, trong đó hàng đầu là các thanh nhớ USB? Không ai phản đối việc kiểm tra thường xuyên là thực hành bảo mật nhưng thực lòng mà nói cũng khó ngăn chặn rò rỉ thông tin. Tiếc là suy nghĩ như thế hơi phổ biến khiến cho công tác bảo mật bị biến dạng. Một số công ty, tổ chức lại cho rằng khi đã có chính sách về an toàn thông tin thì thông tin DN đã được bảo vệ từ bên trong!

Phân quyền truy nhập thông tin chỉ là bước đi đầu tiên, bắt buộc mà thôi. Tiếp theo mới là công việc khó khăn nhất – công việc với những người trực tiếp tham gia vào quá trình sản xuất thông tin của DN. Ví dụ, người nhân viên được tham gia vào một phần của kế hoạch kinh doanh lại theo kinh nghiệm luận ra được nhiều thông tin hơn thế. Cho nên, các hệ thống bảo vệ thông tin nội bộ chỉ có thể dùng để bảo vệ khỏi "người ngay" hoặc để điều tra về sự cố đã diễn ra rồi.

Ai có lỗi – Phải làm gì?

Để bảo vệ công ty khỏi spam, sếp sẽ cho mua thiết bị, hệ thống và ứng dụng… Việc mua thiết bị sẽ hết nhiều tiền, mua dịch vụ đảm bảo kỹ thuật (thiết bị mua được còn thường xuyên gây đình trệ công việc của toàn hệ thống), tuyển thêm nhân viên mới và huấn luyện người này vận hành hệ thống mới…, tất cả đều hết nhiều tiền. Ban lãnh đạo công ty đã chính tay mình gây nên hàng đống những vấn đề nhỏ và tiêu tốn không ít tiền nhưng vấn đề spam vẫn hầu như không giải quyết được vì tỷ lệ spam trong thư điện tử nói chung chỉ giảm chứ không hết (từ 53% giảm xuống 27% trong một trường hợp cụ thể). Cho nên, phải nghĩ xem có xứng đáng để tiêu tiền, thời gian và tiềm lực DN vào những việc như vậy hay không? Dĩ nhiên là không!

Ai có lỗi? Người "bị quảng cáo"? Nhà cung cấp? Người cho đăng quảng cáo thiết bị bảo mật? Thực sự thì điều quan trọng nằm ở chỗ phải đặt việc bảo vệ thông tin DN vào đúng vị trí của nó. Câu hỏi phải làm gì tự thân có lời giải đáp: Không vội mua thiết bị mà hãy tính kỹ kết quả đạt được với những chi phí như thế. Nếu thông tin mật của DN chỉ hiển hiện dưới dạng cơ sở dữ liệu lớn và DN không còn gì khác có giá trị đối với các đối thủ thì rõ ràng DN phải tính mua hệ thông kiểm soát sử dụng thiết bị ngoại vi và đề ra những nội quy hà khắc về sử dụng cơ sở dữ liệu. Nếu một trong những lo sợ chính của DN là tình trạng kinh doanh (dù chỉ là trong vòng mươi phút) thì DN phải tận dụng các công cụ chống virus, chống spyware, ngăn chặn tấn công, và phải thường xuyên giám sát các thiết bị ngoại vi cũng như thanh sát toàn hệ thống.

Tuy nhiên, cái giá phải trả cho những giải pháp tương tự đủ lớn. Đặc biệt khi vấn đề nào với DN cũng sống còn và DN phải giải quyết bằng chính sức mình. Công xá của các chuyên gia giỏi không nhỏ. Giá trị bỏ ra phải phù hợp với nguyên lý "hệ thống còi đèn ô tô không được đắt hơn chính cái ô tô".

Ở Nga bắt đầu thịnh hành dịch vụ bảo mật. Dĩ nhiên, người ta thường chỉ thuê bảo mật với một

phần nào tài sản thông tin DN mà thôi. Cách thức này cho phép tiếp cận vấn đề một cách chuyên nghiệp và toàn diện mà không phải huy động toàn bộ nội lực để giải quyết những vấn đề không thuộc chuyên môn hoặc để tránh phải duy trì đội ngũ chuyên gia đắt đỏ. Hơn nữa, nếu công việc được giải quyết bởi các nhà chuyên nghiệp, độ tin cậy của hệ thống gia tăng. Giá dịch vụ tương tự không cao hơn trường hợp DN tự làm, nhưng bù lại về chất lượng thì cải thiện rõ rệt. Trở ngại của dịch vụ: người ta chưa tin hoàn toàn vào các chuyên gia bên ngoài (nhỡ họ bắt tay với đối thủ thì sao…?). Chỉ khi nào DN gặp phải vấn đề, dịch vụ sẽ lại được cân nhắc.

Việt Dũng