BẢO MẬT MẠNG VÀ NHỮNG ĐIỀU CẦN BIẾT

Trong khi công nghệ mạng và Internet mang lại nhiều cơ hội phát triển và cạnh tranh mới cho các doanh nghiệp vừa và nhỏ (SMB) thì cũng là lúc nó làm dấy lên nhu cầu cần phải bảo vệ hệ thống máy tính trước các đe doạ về bảo mật. Theo một cuộc

Trong khi công nghệ mạng và Internet mang lại nhiều cơ hội phát triển và cạnh tranh mới cho các doanh nghiệp vừa và nhỏ (SMB) thì cũng là lúc nó làm dấy lên nhu cầu cần phải bảo vệ hệ thống máy tính trước các đe doạ về bảo mật. Theo một cuộc khảo sát được Viện Bảo mật máy tính CSI tiến hành năm 2003, có tới 78% máy tính bị tấn công qua mạng Internet (năm 2000 là 59%). Ngày nay, thậm chí cả những doanh nghiệp nhỏ nhất cũng cảm thấy họ cần phải thực hiện các hoạt động kinh doanh trực tuyến, và kéo theo đó nhiều nhân tố cần phải đảm bảo cho mô hình này. Tuy nhiên, theo Jim Browning, phó chủ tịch kiêm giám đốc nghiên cứu SMB của Gartner, hầu hết các doanh nghiệp không nhìn nhận đúng mực tầm quan trọng của bảo mật, họ thường xem nhẹ chúng trong khi đáng ra đó phải là ưu tiên hàng đầu khi tiến hành các hoạt động trực tuyến. Nếu không được bảo vệ đúng mực, mỗi phần của hệ thống mạng đều trở thành mục tiêu tấn công của tin tặc, của đối thủ cạnh tranh, hay thậm chí là cả nhân viên trong công ty. Mặc dù trong năm 2005 có tới 40% SMB thực hiện quản lý mạng bảo mật và sử dụng Internet nhiều hơn nhưng theo thống kê của Gartner, hơn một nửa trong số họ thậm chí không biết là mình bị tin tặc tấn công. Những nền tảng cơ bản Cũng như nhiều loại hình tội phạm khác, các đe doạ về mạng và tài nguyên Internet xuất phát từ cộng đồng nhỏ. Tuy nhỏ như nhân tố này lại không ngừng lớn mạnh bởi ít có chế tài nào kiềm chế nó một cách hiệu quả, chỉ cần một công cụ tấn công được phát tán lên mạng là ngay lập tức rất nhiều hệ thống máy tính trở thành mục tiêu tấn công thông qua các lỗ hổng phần mềm. Những kẻ đứng đằng sau các vụ tấn công này có thể là tin tặc, bẻ khoá phần mềm hoặc "nội gián".

- Kiểm soát truy cập: Xác nhận danh tính và quyết định có cho phép truy cập vào mạng hay không. Việc xác thực có thể thông qua mật khẩu hoặc các biện pháp phức tạp khác như sử dụng thiết bị sinh trắc (quét vân tay hoặc khuôn mặt).- Tường lửa: Giải pháp phần mềm hoặc phần cứng giúp ngăn chặn các nỗ lực xâm nhập từ bên ngoài hoặc chỉ cho phép dữ liệu hợp pháp đi vào mạng. Ngày nay, tường lửa được sử dụng rất phổ biến đối với hệ thống mạng doanh nghiệp.- Quản lý định danh: Nhận dạng người dùng và trạng thái chấp nhận hiện tại, định nghĩa và thi hành quyền truy cập tài nguyên hệ thống và mạng lưới.- Phát hiện xâm nhập: Là khả năng của phần mềm có thể phân tích hoạt động của mạng, phát hiện hành vi xâm nhập vào gửi thông báo cho người quản trị.- Ngăn chặn đe doạ: Là việc liên kết nhiều công nghệ bảo mật (tường lửa, phát hiện/bảo vệ xâm nhập) và dịch vụ mạng thông minh để giảm thiểu tác động của những đe doạ đã biết hoặc chưa được biết đến.- VPN (Virtual Private Network): Mạng riêng ảo cho phép máy tính có thể kết nối bảo mật (an toàn) tới hệ thống mạng doanh nghiệp thông qua mạng Internet. Nhờ sử dụng kết hợp thiết bị phần cứng trên mạng doanh nghiệp và phần mềm đặc biệt trên máy tính điều khiển từ xa mà DN có thể sử dụng VPN cho các văn phòng vệ tinh, các trụ sở xa trung tâm và thiết bị di động của nhân viên.

* Tin tặc (hacker): Phần lớn là những người am hiểu về bảo mật và các nguyên lý vận hành mạng Internet và máy tính. Trước đây, mục đích của tin tặc khi đột nhập vào máy tính thường mang màu sắc phi lợi nhuận, chỉ để chứng tỏ tay nghề hay khoe "thành tích". Ngày nay, mục đích này đã dần biến mất và thay vào đó là các động cơ lớn hơn: tiền, thù hằn cá nhân, chính trị... Khái niệm và quan niệm về hacker cũng rất đa dạng, tuy nhiên, có thể chia tin tặc thành 3 dạng: mũ trắng, mũ đen và mũ xám. Hacker "mũ trắng" thường là các chuyên gia bảo mật, những người vì sự an toàn chung của cộng đồng trong cuộc chiến chống lại hacker "mũ đen". "Mũ xám" là cụm từ mới ám chỉ những tin tặc "nửa trắng nửa đen" (vừa chính lại vừa tà), những nhân tố có thể thay đổi theo hoàn cảnh). * Bẻ khoá (cracker): Cũng rất nguy hiểm và gây thiệt hại lớn đối với doanh nghiệp. Những công việc "ưu thích" của loại người này là bẻ khoá phần mềm, sửa đổi trang Web, đánh cắp thông tin thẻ tín dụng, phá huỷ dữ liệu * Nội gián: Đó chính là nhân viên trong công ty, những người muốn có được thông tin cá nhân của người khác để thoả mãn tính tò mò hoặc phục vụ cho mục đích khác. Những đe doạ bảo mật thường thấy là tấn công mạng, tấn công tâm lý (social engineering), virus, sâu và phần mềm gián điệp. Những phi vụ tấn công mạng phức tạp có động cơ chính trị hoặc tài chính thường chỉ nhắm tới một công ty hoặc hệ thống máy tính cụ thể. Mục đích không nằm ngoài ý định sửa đổi cơ sở dữ liệu, đánh cắp tài khoản hoặc thông tin cá nhân, cài đặt các chương trình do thám để cho phép kẻ đột nhập có thể khởi phát các cuộc tấn công từ chính hệ thống máy tính nạn nhân. Tấn công mạng có 3 phương thức cơ bản: * Tấn công do thám: Là phương pháp tấn công thu thập thông tin để khởi phát cuộc tấn công thực sự sau này vào mạng lưới. * Tấn công truy nhập: Là phương pháp lợi dụng điểm yếu của mạng (thường là lỗi hoặc lỗ hổng bảo mật). * Tấn công từ chối dịch vụ: Là phương pháp tấn công mạnh tay nhất hiện nay bằng cách gửi một số lượng lớn truy vấn thông tin tới máy chủ, gây ra hiện tượng quá tải, khiến máy tính không thể (hoặc khó có thể) truy cập từ bên ngoài. Quản trị hệ thống cần phải đánh giá đúng mực mức độ của các cuộc tấn công để từ đó đề ra biện pháp chống trả và bảo vệ hợp lý.

- Virus: Là một chương trình có thể tìm kiếm các chương trình khác trên thiết bị mạng và lây nhiễm vào chúng bằng cách copy vào đó một phiên bản của virus. Khi những chương trình này được thực thi, virus đính kèm cũng được kích hoạt theo để bắt đầu chu trình lây nhiễm tiếp theo. Không giống sâu, virus không thể lây nhiễm vào máy tính mà không có sự trợ giúp nào đó (sự tương tác của người dùng).- Sâu: Chương trình có thể tự phát tán và lây nhiễm qua mạng với tốc độ rất nhanh.- Trojan Horse (Ngựa Trojan): Được lấy tên từ một thành ngữ, đây là cụm từ chỉ một chương trình nguy hiểm được che giấu trong một vỏ bọc nào đó (chẳng hạn như một chương trình game), giúp kẻ chủ mưu có thể phát lệnh điều khiển hệ thống từ xa.

Phương pháp "social engineering" thường được sử dụng để đánh cắp thông tin nhạy cảm của doanh nghiệp. Đây là phương pháp tấn công ít tốn sức lực nhất như lại rất hiệu quả trong nhiều trường hợp. Đôi khi chỉ cần một cú điện thoại là kẻ tấn công có thể lấy được thứ mình muốn, chẳng hạn như hỏi thông tin mật khẩu để nâng cấp hệ thống từ bộ phận hỗ trợ kỹ thuật. Virus, Trojan, sâu và các mối đe doạ khác có thể kết hợp cùng nhau để tạo ra nguy cơ lớn đối với sự an toàn của một doanh nghiệp. Những đe doạ này thường tấn công vào một mục tiêu định trước, được tung lên mạng và tìm kiếm lỗ hổng trong hệ thống máy tính nạn nhân để xâm nhập. Virus và Trojan thường đòi hỏi sự tương tác của người dùng mới có thể lây nhiễm, trong khi sâu máy tính lại không cần; chúng có khả năng tự phát tán qua e-mail để lây nhiễm tới những hệ thống máy tính "kém an toàn" chỉ trong vài giờ, hoặc thậm chí là vài phút. Theo thống kê của hãng bảo mật phần mềm PestPartrol, số lượng đe doạ bảo mật đã tăng từ 27.000 (2000) lên 60.500 trong năm 2003. * Giải pháp Để giảm thiểu thiệt hại từ các vụ tấn công lợi dụng lỗ hổng bảo mật, doanh nghiệp cần phải thực hiện nghiêm túc quy trình phát hiện -> giải quyết triệt để hoặc ngăn chặn tối đa lỗ hổng. Thường bước đầu tiên cần thực hiện là thảo ra một chính sách bảo mật và thông báo rộng rãi tới các nhân viên trong công ty. Chính sách này cần quy định rõ quyền và nghĩa vụ từng người khi tiếp xúc với tài nguyên kỹ thuật doanh nghiệp. Khi đã có chính sách và quy định rõ ràng, bước tiếp theo cần kết hợp các biện pháp nghiệm vụ để giảm thiểu hoặc thậm chí xoá bỏ rất nhiều "cơn đau đầu" về bảo mật hiện nay. Những biện pháp này có thể bao gồm việc triển khai kỹ thuật để phát hiện và ngăn chặn các hành vi lạm dụng và phá hoại; đào tạo nhân viên và áp dụng triệt để, thông suốt chính sách bảo mật đề ra. * Tác động Bảo mật Internet có thể ảnh hưởng trực tiếp tới doanh thu và tình hình kinh doanh của doanh nghiệp. Một cuộc khảo sát của CSI và Đội chống xâm nhập máy tính FBI năm 2003 cho thấy, trong số 75% doanh nghiệp được khảo sát đều cho rằng họ phải gánh chịu thiệt hại về tài chính từ sự cố bảo mật; 47% doanh nghiệp cho biết có thể đánh giá chính xác thiệt hại bảo mật; và 23% cho biết thất thu khoảng 10 triệu USD mỗi năm do các hành vi đột nhập tấn công. Một thiệt hại khác rất khó đánh giá nhưng lại cực kỳ quan trọng đối với SMB, đó là khoảng thời gian trục trặc về hệ thống (downtime) và thiệt hại sản phẩm do phản ứng chậm chạm đối với sự cố bảo mật. Trong rất nhiều trường hợp, doanh nghiệp phải tạm thời gỡ bỏ các máy chủ quan trọng, hệ thống desktop và dây chuyền liên quan tới sự cố bảo mật. Tuy phải đối mặt với những thiệt hại tiềm tàng nhưng rất nhiều doanh nghiệp nhỏ vẫn chưa chú trọng tới nguy cơ này. * Một số công việc cần làm Đe doạ bảo mật và việc triển khai công nghệ để giảm thiểu chúng luôn có quan hệ mật thiết với nhau. Để bảo mật thành công đòi hỏi phải có bước tiếp cận và quy trình xử lý xuyên suốt: - Tiến hành đánh giá định kỳ về chính sách bảo mật- Triển khai công nghệ bảo mật để cung cấp các kết nối an toàn, ngăn chặn các nguy cơ và quản lý việc nhận dạng, đánh giá... ở những thời điểm và bộ phận hợp lý.- Sửa chữa và bảo vệ các điểm đầu cuối, máy chủ và desktop trước những đe doạ đã được nhận dạng hoặc chưa được nhận dạng. Cần ý thức rằng trên thực tế không có một công nghệ bảo mật đơn lẻ nào là hoàn hảo, mà cần kết hợp nhiều biện pháp và công nghệ khác nhau. Có rất nhiều bước bảo mật cơ bản không đòi hỏi nhiều tiền hoặc nỗ lực bỏ ra. SMB có thể thực hiện cá bước đơn giản và dễ áp dụng để cải thiện môi trường bảo mật của doanh nghiệp mình. SMB tuy có thể là mục tiêu nhỏ nhưng không phải vì thế họ ít bị tấn công mà ngược lại doanh nghiệp loại này cần phải bảo vệ mình trước các nguy cơ bằng cách triển khai những hoạt động ngăn chặn, thông dụng và dễ triển khai.Còn nữa...