GIẢM THIỂU RỦI RO TỪ CÁC CUỘC TẤN CÔNG BẢO MẬT

Tăng cường kiểm soát chặt chẽ việc cài đặt phần mềm của nhân viên sẽ giúp các công ty cải thiện tình hình an ninh mạng. Phần lớn các sự cố về an ninh mạng đều có chung một nguyên nhân: người dùng cuối (end-user) cài đặt hoặc chạy các chương tr

Tăng cường kiểm soát chặt chẽ việc cài đặt phần mềm của nhân viên sẽ giúp các công ty cải thiện tình hình an ninh mạng. Phần lớn các sự cố về an ninh mạng đều có chung một nguyên nhân: người dùng cuối (end-user) cài đặt hoặc chạy các chương trình không được quản lý hoặc không được phê chuẩn bởi các chuyên viên quản trị mạng (admin). Hầu hết các cuộc tấn công vào an ninh mạng xảy ra do người sử dụng vô tình cài đặt các malware (malware là các phần mềm làm hỏng chức năng chương trình ứng dụng, cố gắng ẩn nấp, trốn tránh không bị phát hiện bởi các chương trình chống spyware, virus và các tiện ích hệ thống), trong đó, có nhiều chương trình có bản chất rất nguy hiểm và sẽ bị tấn công ngay sau khi cài đặt như như virus, sâu máy tính (worm), Trojan, và phần mềm gián điệp (spyware). Trong khi đó, có nhiều chương trình khác lúc đầu rất hữu ích nhưng sau đó lại tạo điều kiện cho các hình thức tấn công bảo mật khác xuất hiện. Có thể nói bất kỳ một hành động cài đặt phần mềm nào, cho dù đó là Skype, Java, RealPlayer, Firefox, QuickTime, iTunes, hay thậm chí phần mềm diệt vius, đều làm gia tăng nguy cơ bị tấn công. Chẳng hạn nếu công ty cho phép các nhân viên cài đặt các công cụ Flash của Macromedia, hệ thống máy tính có thể bị tấn công bởi các mã điều khiển Flash độc hại. Hay cài đặt các thanh công cụ tìm kiếm nhanh hay tìm kiếm từ desktop của Google, thông tin mật trong máy cũng có nguy cơ bị truy lục. Ngay cả khi công ty cho phép các nhân viên dùng các đĩa CD cá nhân trên máy tính của công ty, nguy cơ thâm nhập của các chương trình malware cũng rất cao. Chính vì vậy, điều mà các công ty cần làm để giảm thiểu những điểm yếu về an ninh mạng là: Kiểm soát các phầm mềm mà nhân viên cài đặt và ứng dụng; nhận biết được những cài đặt tiện ích (add-in) nào của trình duyệt web đang chạy trên máy và ActiveX controls nào được cài đặt (ActiveX controls là các hệ thống tiêu chuẩn dùng để xây dựng các thành phần (component) trong môi trường Windows); Chuyên viên CNTT phải kiểm soát ở mức cao nhất và tiến hành việc cấp phép cài đặt. Dĩ nhiên, các biện pháp này thường được cho là tốn kém về thời gian và tiền bạc, nhưng thực tế, sẽ là không thấm vào đâu khi so với thời gian và tiền bạc mà các công phải bỏ ra khi phải chiến đấu với malware, virus, worm, Trojan, spam và các hình thức tấn công khác. Cho dù, trên thực tế, việc kiểm soát 100% những gì nhân viên cài đặt hoặc tải xuống từ Internet gần như không thể, nhưng các công ty cũng có thể kiểm soát được các rủi ro về an ninh máy tính nếu xây dựng được một kế hoạch kiểm soát trên cơ sở cân nhắc những yếu tố sau đây: - Thiết lập và giáo dục nhân viên về chính sách cài đặt phần mềm của công ty, chẳng hạn như họ phải biết được rằng phần mềm mà họ có ý định cài đặt cần phải có sự phê chuẩn của admin hay không. - Khuyến cáo nhân viên những loại phần mềm nào tránh cài đặt, làm cho họ hiểu rằng bất kỳ một phần mềm nào cũng tiềm ẩn, dù ít hay nhiều, trực tiếp hay gián tiếp, các nguy cơ đối với an ninh mạng. - Đưa ra một cơ chế cho phép admin biết được các nhân viên đang chạy những chương trình gì trên máy tính của họ. Nếu công ty không thể kiểm soát việc cài đặt thì phải biết được nhân viên đang chạy những chương trình nào. - Xây dựng một quy trình để đảm bảo các ứng dụng mới được cài đặt một cách an toàn, chẳng hạn như công ty muốn loại bỏ một số ứng dụng của phần mềm như chia sẻ file (file-sharing) hay peer-to-peer. - Đảm bảo kích hoạt tính năng tự động cập nhật (auto-update), nếu có, của các phần mềm. Tuy nhiên, cũng không nên hoàn toàn tin tưởng vào tính năng này bởi một số phiên bản mới của các phần mềm không có khả năng loại bỏ những mã cũ, dễ bị

tấn công như các phiên bản mới của Adobe Acrobat hay Java của Sun Microsystems. - Gỡ bỏ tất cả các chương trình có độ rủi ro bảo mật cao, song song với việc phạt những nhân viên tái phạm trong việc cài đặt phần mềm. - Thiết lập một phương thức giám sát các lớp nội dung (content layer) để ngăn các giao thức không được cấp phép xâm nhập vào hệ thống máy tính khi tiến hành cài đặt các chương trình ứng dụng. - Nâng cao ý thức của admin đối với các chương trình mới và yêu cầu họ báo cáo ngay cho Trưởng phòng CNTT về các nguy cơ mới được phát hiện để phân tích và có biện pháp kịp thời. Có một điều chắc chắn là các nhân viên văn phòng sẽ tiếp tục cài đặt, download ngày càng nhiều phần mềm và như thế nguy cơ đe dọa đối với an ninh mạng sẽ rất khó lường. Điều mà chúng ta có thể làm được là kiểm soát những gì đã được cài đặt và đang chạy trên các máy tính được quản lý. Bá Lâm