AN NINH MẠNG 2006: SẼ CÓ BIẾN HÓA VỀ TỘI PHẠM TRÊN MẠNG

IBM đã công bố nội dung Báo cáo chỉ số an ninh kinh doanh toàn cầu 2005 và đưa ra dự đoán về các mối đe dọa tiềm ẩn về an ninh mạng sẽ có thể xảy ra năm 2006. IBM dự báo rằng sẽ có một sự chuyển dịch căn bản, hay còn gọi là một sự biến hóa về tội phạm t

IBM đã công bố nội dung Báo cáo chỉ số an ninh kinh doanh toàn cầu 2005 và đưa ra dự đoán về các mối đe dọa tiềm ẩn về an ninh mạng sẽ có thể xảy ra năm 2006. IBM dự báo rằng sẽ có một sự chuyển dịch căn bản, hay còn gọi là một sự biến hóa về tội phạm trên mạng, chuyển từ các cơn bùng phát toàn cầu sang các cuộc tấn công diện nhỏ, lẻ, lén lút hơn, và nhằm vào các tổ chức cụ thể với mục đích kiếm lời. Báo cáo này do Nhóm nghiên cứu thông tin an ninh toàn cầu của IBM đưa ra. Theo báo cáo, phần lớn mối đe dọa công nghệ thông tin toàn cầu trong năm 2005 mới chỉ dừng ở mức độ trung bình. Mặc dù con virus Zotob đã thu hút được sự chú ý của toàn thế giới, gây ảnh hưởng tới các cơ quan thông tin đại chúng có tên tuổi, nhưng năm vừa qua, thế giới cũng ít phải chứng kiến các bùng phát toàn cầu về phần mềm phá hoại malware hơn những năm trước đó. Tuy nhiên, điều này chưa nói lên được toàn bộ câu chuyện. Các thư rác mang tính chất tội phạm, các phần mềm phá hoại và các cuộc tấn công công nghệ thông tin đã trở nên rõ ràng hơn trong năm qua. Tại Mỹ và trên khắp thế giới, nhiều tên tội phạm nguy hiểm đã bị bắt. Đây là những tội phạm có tổ chức với động cơ kiếm tiền. Trong khi các phần mềm và hệ thống mạng trên thế giới đang ngày càng trở nên an toàn hơn sau hàng loạt những cải tiến, người ta dự đoán rằng các tội phạm chủ yếu sẽ tập trung vào các điểm tiếp cận dễ bị tổn thương nhất, ví dụ như nhân sự của công ty và tổ chức đó, để thực hiện một cuộc tấn công. Theo ông Cal Slemp, Phó Chủ tịch Bộ phận dịch vụ an ninh và thông tin cá nhân của IBM: " sự suy giảm về số lượng các cuộc tấn công hàng loạt năm 2005 đã đi ngược lại với dự đoán của phần đông xã hội và là gây ra một mối đe dọa lớn tới các thông tin cá nhân. IBM tin rằng môi trường đã thay đổi, việc bảo vệ an ninh trên các hệ thống mạng ngày càng được tăng cường và các hình phạt ngày càng trở nên nghiêm khắc hơn. Chúng tôi nhận thấy rằng ngày càng có nhiều các tổ chức hoạt động quy củ, có cam kết rõ ràng và chặt chẽ tham gia vào lĩnh vực này. Điều này có nghĩa là các tấn công sẽ chuyển sang các mục tiêu cụ thể hơn và nguy cơ phá hoại sẽ cao hơn. Các tổ chức trên thế giới, cho dù thuộc khu vực công hay tư nhân, đều sẽ phải nhanh chóng hợp tác với nhau để cùng giải quyết các thách thức ngày càng lớn này." Báo cáo chỉ số an ninh kinh doanh toàn cầu của IBM cũng cho biết các mối đe dọa tiềm ẩn trong năm 2006, gồm có: - Tấn công từ bên trong – Khi phần mềm ngày càng trở nên an toàn hơn, người sử dụng máy tính sẽ là một mục tiêu cụ thể để tấn công trong các công ty và các tổ chức. Tội phạm sẽ tập trung các nỗ lực của chúng vào việc thuyết phục người sử dụng thực hiện việc tấn công thay vì mất thời gian phát hiện các lỗi trong các phần mềm được viết rất dài dòng để phá hoại. Việc sử dụng nguồn lực toàn cầu, việc cắt giảm nhân công, các vụ sáp nhập và mua lại đều có thể ẩn chứa những thách thức cho các công ty và tổ chức khi họ tìm cáchngười sử dụng trước những nguy cơ này. - Các thị trường mới nổi – Tội phạm mạng sẽ tận dụng những điểm yếu trong liên kết quốc tế về phòng chống tội phạm mạng để tiến hành các cuộc tấn công vượt biên giới, vì vậy, mối đe dọa bắt nguồn từ và nhằm vào các nước đang phát triển và các thị trường mới nổi sẽ ngày càng tăng cao. Khi đó, việc truy tìm dấu vết của các vụ tấn công sẽ trở nên khó khăn hơn nhiều, đặc biệt là khi xu hướng cho thấy các vụ tấn công thường bắt nguồn từ các khu vực như Đông Âu và Châu Á, nơi mà các mức hình phạt không nghiêm khắc và việc thực thi luật pháp còn nhiều hạn chế. - Blogging –Việc gia tăng sử dụng các công cụ làm việc như blogging cũng làm tăng khả năng rò rỉ các tài liệu kinh doanh bí mật. - Instant Messaging (Tin

nhắn trực tiếp) – Botnets, tập hợp các robot phần mềm cho phép kiểm soát hệ thống mà không cần người sở hữu phải biết thao tác đó, sẽ tiếp tục là một trong những hiểm họa lớn nhất đối với Internet. Các botnet mới có các tế bào nhỏ hơn, dễ dàng ngụy trang hơn, có thể sẽ chuyển sang hệ tin nhắn tức thời trên mạng và các hệ thống mạng bình đẳng ngang hàng để ra lệnh và kiểm soát các hệ thống bị nhiễm virus. - Các thiết bị di động – Các phần mềm phá hoại gây ảnh hưởng tới điện thoại di động, PDA và các thiết bị không dây khác đã tăng lên một cách đáng kể trong năm vừa qua, nhưng chưa biến thành các cuộc tấn công diện rộng vì chúng chưa thể tự mình lan rộng ra. Vì vậy, xu hướng này sẽ tiếp tục được theo dõi trong năm 2006. Hiện tượng truyền virus qua email đã giảm trong năm 2005. Chỉ có 1 trong 36.15 email, tức là 2.8 % số email gửi ra, có chứa virus hoặc Trojan. So với năm 2004, con số này đã giảm đáng kể. Trong năm 2004, tỉ lệ này là 6.1%, tức là 1 trong 16.39 email. Phishing (thư điện tử với mục đích lấy trộm thông tin) – Phishing tiếp tục là mối đe dọa lớn trong năm 2005. Trong năm này, tính trung bình, cứ 304 email lại có một email phising, trong khi đó, năm 2004, cứ 943 email mới có một email phishing. Malware Ingenuity (Phần mềm phá hoại tinh vi) – Năm 2005 chứng kiến sự gia tăng các mối đe dọa phức tạp và kết hợp các tính năng tự động vào trong các phần mềm phá hoại có sẵn. Ví dụ như Mytob được dựa trên con sâu Mydoom và có bổ sung thêm tính năng tự động và một số cải tiến khác, nhằm tạo ra các phần mềm phá hoại nguy hiểm hơn. Chính vì vậy, sau một thời gian ngắn, các biến thể của Mytob đã xuất hiện. Báo cáo chỉ số an ninh kinh doanh toàn cầu của IBM là báo cáo hàng tháng nhằm đánh giá và phân tích các mối đe dọa an ninh mạng tiềm tàng dựa trên các dữ liệu và thông tin mà IBM thu thập được từ 3000 chuyên gia an ninh thông tin trên toàn thế giới và hàng ngàn các thiết bị kiểm soát cũng như các đối tác kinh doanh an ninh chiến lược. Lê Quang