2006: NĂM BÙNG NỔ LỖI BẢO MẬT

5.450 lỗ hổng được phát hiện trong vòng 9 tháng - con số này quá đủ để năm 2006 trở thành năm kỷ lục về số lượng lỗi bảo mật. Ngày 9-10 vừa qua, ISS (Internet Security Systems) đã cho công bố bản thống kê về lỗi bảo mật trong 9 tháng đầu năm nay. Với 5.450 lỗ hổng được ghi n
5.450 lỗ hổng được phát hiện trong vòng 9 tháng - con số này quá đủ để năm 2006 trở thành năm kỷ lục về số lượng lỗi bảo mật. Ngày 9-10 vừa qua, ISS (Internet Security Systems) đã cho công bố bản thống kê về lỗi bảo mật trong 9 tháng đầu năm nay. Với 5.450 lỗ hổng được ghi nhận, các chuyên gia của ISS dự kiến đến hết năm nay sẽ có tổng cộng 7.500 lỗi bảo mật, tăng 41% so với năm 2005 (5.195 lỗ hổng). Nhiều công ty bảo mật cũng đã phải lên tiếng cảnh báo về tình trạng số lượng lỗi bảo mật gia tăng chóng mặt, trong đó có cả iDefense, eEye Digital Security và Symantec. Hãng phát triển Norton Antivirus vừa công bố báo cáo Internet Security Threat (báo cáo về các mối đe dọa bảo mật internet) 6 tháng đầu năm 2006. Theo đó, đã có 2.249 lỗ hổng được phát hiện, tăng 18% so với cùng kỳ năm 2005.

Nguồn: computer-security-news

Microsoft đã tung ra 55 bản vá lỗi chỉ trong 9 tháng đầu năm nay trong khi cả năm ngoái, hãng phần mềm số 1 thế giới chỉ phát hành 45 bản vá. ZERT - một nhóm các chuyên gia bảo mật tình nguyện cũng đã phải vào cuộc với việc tung ra 2 bản vá lỗi cho người sử dụng Windows trước khi Microsoft kịp "ra tay". Gunter Ollmann - giám đốc nhóm nghiên cứu và phát triển X-Force của ISS đã gọi đây là một "huge jump" (bước nhảy vọt) về số lượng lỗ hổng bảo mật. Nguyên nhân dẫn đến tình trạng này, theo các chuyên gia, chủ yếu là do số lượng phần mềm đang tăng nhanh, mã nguồn cũng phức tạp hơn trước nhiều. Kết quả là số lỗi cũng tăng theo. Một lý do khác nữa là… trình độ của các lập trình viên và các "thợ săn lỗi". Những chuyên gia này ngày một giỏi hơn nên họ phát hiện ra lỗi nhanh và nhiều hơn. Các công cụ dò lỗi tự động (được gọi là "fuzzer" - từ tiếng lóng chỉ cảnh sát) tiên tiến hơn cũng góp phần quan trọng vào việc "đánh hơi" lỗ hổng báo mật. Dù vậy, tỉ lệ lỗi nguy hiểm (xếp hạng "critical") đang có xu hướng giảm. 28% số lỗ hổng của năm 2005 được đánh giá nguy hiểm, trong khi con số này trong 9 tháng đầu năm nay là 17%. Các chuyên gia bảo mật cho rằng tỉ lệ trên sẽ không thay đổi trước khi bước sang năm 2007. Dĩ nhiên, điều này không có nghĩa là người dùng máy tính đã có thể yên tâm. Những con số thống kê "cao ngất ngưởng" về lỗi bảo mật và số lượng các đợt tấn công của hacker đủ để làm bất kỳ một người sử dụng "can trường" nào cũng phải ít nhiều lo lắng. Thậm chí kết quả cuộc điều tra Get Safe Online của chính phủ Anh đã cho thấy nhiều người dân xứ sương mù sợ tội phạm ảo tới mức không kết nối internet nữa. "Giới mũ đen" đã có những thay đổi chiến thuật quan trọng, nhất là tập trung khai thác lỗi của các ứng dụng chạy trên máy tính của người sử dụng. Lỗi zero-day (giúp hacker chiếm quyền điều khiển máy "nạn nhân" từ xa) đã trở thành át chủ bài của tin tặc trong vài

tháng gần đây. Đó là chưa kể tới việc các chuyên gia chỉ khẳng định tỉ lệ lỗi "chí mạng" (critical) giảm chứ chưa ai dám đảm bảo rằng mức độ nguy hiểm của các lỗi đó không tăng. Các hacker cũng không phải chỉ tận dụng lỗi "cao cấp". Lỗ hổng "tầm trung" cũng là vũ khí ưa thích của các tay đạo tặc trong thế giới số. Các đợt tấn công vào máy tính cá nhân chủ yếu dựa vào những website có chèn mã độc, thường được ngụy trang bằng nội dung hài hước (hoặc khiêu dâm). "Đại dịch virus Việt" và "tháng 9 kinh hoàng" vừa qua chính là một ví dụ điển hình cho phương pháp tấn công này. Đối với mục tiêu là các công ty, hacker lại đóng giả khách hàng và tấn công bằng các file tài liệu có đính kèm mã độc. Các mã này sẽ khai thường nhắm vào lỗ hổng trên các ứng dụng như MS Word (soạn thảo văn bản) hay Internet Explorer (trình duyệt) và cao hơn là lỗ hổng của hệ điều hành. Tình hình hiện tại đã đáng lo ngại nhưng tương lai còn có phần… mù mịt hơn. Microsoft vẫn rất tự tin về khả năng bảo mật của Windows Vista nhưng sự kiện đại hội mũ đen (Black Hat) hồi tháng 8 vừa qua khiến cho giới bảo mật hết sức nghi ngờ về độ an toàn của hệ điều hành mới. Khi đó Microsoft có buổi giới thiệu tính năng bảo mật của Vista nhưng ngay ở phòng bên cạnh, người ta giới thiệu cách… hack nó. ISS cũng kết thúc thống kê của mình với nhận định của ông Ollmann, cho rằng nửa đầu năm 2007 sẽ chứng kiến thêm một "bước nhảy vọt" nữa của lỗi bảo mật, nhất là các lỗi "chí mạng" và đương nhiên Vista là nguồn gốc của những lỗ thủng ấy. HOÀNG MINH