AN TOÀN VÀ TIỆN LỢI, LỰA CHỌN BÊN NÀO?

Nhiều chuyên gia bảo mật quốc tế nhận yếu tố tiện lợi trong một chừng mực nhất định đã làm giảm mức độ an toàn của các phần mềm bảo mật. Tại Hội nghị "Nhóm người dùng Unix Australia" (AUUG) ở Melbourne hôm qua, các hãng phát triển bảo mật phần mềm giải thí

Nhiều chuyên gia bảo mật quốc tế nhận yếu tố tiện lợi trong một chừng mực nhất định đã làm giảm mức độ an toàn của các phần mềm bảo mật. Tại Hội nghị "Nhóm người dùng Unix Australia" (AUUG) ở Melbourne hôm qua, các hãng phát triển bảo mật phần mềm giải thích vì sao công nghiệp IT vẫn còn bị phó mặc theo nhiều vấn đề. Các tiêu chuẩn bảo mật được viết ra từ 10 năm trước làm sao bắt kịp được tốc độ phát triển của các hacker với những malware và thủ đoạn phá hoại ngày càng tinh ranh.

Nguồn: crcitalia

"Nhiều 'món' bảo mật do chuyên viên mật mã thiết kế thiếu tính tiện lợi. Mọi người không thể sử dụng chúng một cách phù hợp", Gutmann - giảng viên bộ môn khoa học máy tính tại đại học Auckland nói. Ông còn nhấn mạnh rằng tính tiện lợi quan trọng như "đưa ra một nhóm mật mã rồi bảo mọi người giải mã chúng". Các giao thức hiện nay cũng chưa được thiết kế mang tính tiện lợi. Thậm chí nếu một giao diện đồ hoạ người dùng (GUI) thân thiện được xây dựng hoàn chỉnh, chưa chắc các hãng phát triển nguyên gốc đã chấp nhận nó. "Họ thích 100% phần mềm hoàn chỉnh không tiện lợi hơn là 99% không dùng được + 1% nhỏ nhoi hoàn thiện tiện lợi". Bởi tính đồng bộ được đặt lên hàng đầu. Nhà phát triển Ryan McBride của OpenBSD, người làm việc với bộ lọc gói và mã IPSec phản ứng gay gắt trước các hệ thống dò tìm xâm phạm. Ông cho rằng mấy hệ thống này là vô dụng, chẳng có cách nào xác định được liệu một virus có đang tấn công mạng hay không. McBride dí dỏm: "Tôi sử dụng IDS để làm việc với công ty Fortune 50 và một hôm nó báo 'Một hộp khác đang có virus, hãy tới mà tắt nó đi'!". Đúng là "thật khó để tự động tắt tất cả mọi thứ an toàn". IDS không giải quyết được vấn đề, nhưng cái bên trong nó thì có. Giảng viên công nghệ thông tin Lawrie Brown của Đại học NSW School giải thích rằng vấn đề chủ yếu ở các phần mềm hiện đại không an toàn là phần thân mã nguồn khổng lồ có thể để lại nhiều lỗ hổng nếu mọi người tiếp tục sử dụng. Đến nay ở nhiều khu vực trên thế giới máy tính vẫn còn khá mới mẻ và mọi người chưa có thói quen quan trọng là bảo mật thông tin. Một sinh viên bảo mật mạng ở Đức, phụ tá trong vấn đề này cũng nêu ra nhận xét rằng người dùng cuối không được rèn luyện các kỹ năng đối phó với nguy cơ bảo mật. "Sẽ phải mất khoảng 20 đến 30 năm để dạy cho mọi người hiểu phải xử lý các vấn đề bảo mật máy tính ra sao. Bạn chẳng muốn giao chìa khoá ngôi nhà mình cho một người lạ. Vậy thì tại sao lại làm thế với mật khẩu của mình?"

T.Thu