ĐA SỐ LỖ HỔNG ZERO-DAY CHỈ ĐƯỢC PHÁT HIỆN SAU... 1 NĂM

Tuổi t

Tuổi thọ trung bình của một lỗ hổng zero-day là 348 ngày trước khi nó được phát hiện ra hoặc vá lại. Nhiều lỗ hổng thậm chí còn sống "thọ" hơn thế, Giám đốc điều hành hãng bảo mật Immunity cho biết.

Lỗ hổng Zero-day là một thuật ngữ để chỉ những lỗ hổng chưa được công bố hoặc chưa được khắc phục. Lợi dụng những lỗ hổng này, hacker và bọn tội phạm mạng có thể xâm nhập được vào hệ thống máy tính của các doanh nghiệp, tập đoàn để đánh cắp hay thay đổi dữ liệu.

Hệ quả là có cả một thị trường chợ đen giao dịch, mua bán lỗ hổng Zero-day hết sức đông vui, nhộn nhịp trên mạng Internet.

"Bọn tội phạm mạng sẵn sàng trả khoản tiền rất lớn để mua lại các lỗ hổng zero-day", bà Justine Aitel phát biểu trước các cử tọa của Hội thảo bảo mật SyScan'07 đang diễn ra tại Singapore.

Không ai được an toàn tuyệt đối!

Nguồn: Techshout

Immunity chuyên đứng ra mua lại các lỗ hổng zero-day, để rồi cất kỹ và theo dõi xem phải mất bao lâu thì những lỗ hổng đó mới được các hãng tìm ra hay vá lại.

Tuổi thọ trung bình của một lỗ hổng zero-day là 348 ngày, dù cũng có những lỗ hổng chỉ tồn tại vẻn vẹn 99 ngày thì đã bị lôi ra ánh sáng. Trong khi ấy, lập kỷ lục về độ "Cao niên" là một lỗ hổng tồn tại suốt 1080 ngày, tương đương gần 3 năm mà chưa bị phát hiện.

"Lỗ hổng zero-day "chết" khi chúng được công bố rộng rãi và được bịt lại", bà Austin giải thích.

Để bảo vệ các dữ liệu quan trọng của doanh nghiệp, nhóm bảo mật cần phải thường xuyên đào sới, kiểm tra và dò quét các lỗ hổng zero-day bên trong hệ thống. "Đây là một nhiệm vụ hết sức quan trọng nhưng lại bị gần như tất cả các hãng phớt lờ, bỏ qua".

Nếu lực lượng IT nội bộ không đủ năng lực, doanh nghiệp đừng nên ngần ngại cầu viện các hãng bảo mật chuyên nghiệp. "Hãy nhớ rằng bất cứ cái gì cũng có lỗ hổng. Không bao giờ là tuyệt đối an toàn", bà Austin tuyên bố.

Trọng Cầm