

Nhiều chiến dịch tấn công mã hóa dữ liệu quy mô lớn nhằm vào hệ thống các máy chủ dữ liệu của các cơ quan, doanh nghiệp

17:00 29/11/2022

Công ty Công nghệ an ninh mạng quốc gia Việt Nam (NCS) vừa phát hành báo cáo đánh giá về tình hình an ninh mạng năm 2022 và dự báo năm 2023.



Ảnh minh họa. (Ảnh: internet)

Theo nghiên cứu của NCS, lừa đảo sử dụng công nghệ cao bùng phát, thông tin người dùng bị rao bán tràn lan, tấn công có chủ đích quy mô lớn vào các cơ sở trọng yếu, mã độc mã hóa dữ liệu tiếp tục hoành hành là những tiêu điểm trong bức tranh an toàn, an ninh mạng Việt Nam năm 2022.

Trong năm qua, mã độc mã hóa dữ liệu tống tiền (Ransomware) nhằm vào người dùng cá nhân đã giảm mạnh. Tuy vậy, đã có nhiều chiến dịch tấn công mã hóa dữ liệu quy mô lớn nhằm vào hệ thống các máy chủ dữ liệu, đặc biệt máy chủ kế toán của các cơ quan, doanh nghiệp.

Theo phân tích của NCS, có 02 điểm yếu lớn khiến các máy chủ dữ liệu tại Việt Nam bị khai thác, tấn công: do sử dụng mật khẩu yếu cho dịch vụ truy cập từ xa và dùng mật khẩu mặc định cho tài khoản quản trị cơ sở dữ liệu. Cao điểm vào

tháng 04/2022, hàng loạt máy chủ kế toán tại Việt Nam đã bị mã hóa toàn bộ dữ liệu, ảnh hưởng nghiêm trọng đến hoạt động của các cơ quan, tổ chức bị tấn công.

Để phòng chống hình thức tấn công này, các quản trị cần thiết lập mật khẩu mạnh cho tài khoản quản trị từ xa. Nếu truy cập từ xa cần sử dụng kênh truyền riêng có mã hoá (VPN). Đóng các cổng dịch vụ không cần thiết, đổi mật khẩu mặc định của các tài khoản quản trị cơ sở dữ liệu. Các cơ quan, doanh nghiệp cần xây dựng hệ thống sao lưu dữ liệu thường xuyên và trang bị phần mềm diệt virus để bảo vệ thường trực.

Các chuyên gia NCS khuyến nghị, các đơn vị cần định kỳ chủ động rà soát lại toàn bộ hệ thống tối thiểu 1 lần trong năm, khắc phục các lỗ hổng hoặc phát hiện các nguy cơ an ninh mạng; dành từ 10% kinh phí đầu tư CNTT đầu tư cho an ninh mạng.

Bên cạnh đầu tư giải pháp công nghệ, cần trang bị hệ thống giám sát và xây dựng các quy trình phản ứng lại nếu xảy ra sự cố. Đặc biệt, cần chú trọng đào tạo nhận thức an ninh mạng cho người sử dụng cũng như nâng cao kỹ năng giám sát cho đội ngũ quản trị vận hành.

Dự báo về an toàn thông tin mạng năm 2023, các chuyên gia NCS cho rằng, các cuộc tấn công APT sẽ diễn ra nhiều hơn, đặc biệt là tấn công đánh cắp dữ liệu từ các kho dữ liệu được hình thành trong quá trình chuyển đổi số.

Hà Trần (t/h)