[Cơ Bản] 2 . Quản lý Bảo mật Dữ liệu.

# Báo cáo: Phương pháp bảo vệ dữ liệu khi sử dụng công cụ nén và giải nén

1. Tại sao bảo mật dữ liệu quan trọng trong môi trường làm việc?

Trong môi trường công sở, dữ liệu thường bao gồm:

• Thông tin khách hàng

• Tài liệu nội bộ, hợp đồng

• Dữ liệu tài chính, chiến lược kinh doanh

• Thông tin cá nhân của nhân viên

Nếu những dữ liệu này bị rò rỉ, hậu quả có thể rất nghiêm trọng:

• Mất uy tín doanh nghiệp

• Thiệt hại tài chính

• Vi phạm pháp luật về bảo vệ dữ liệu (ví dụ: GDPR, Nghị định 13/2023/NĐ-CP tại Việt Nam)

• Nguy cơ bị tấn công mạng hoặc lừa đảo

Do đó, việc bảo vệ dữ liệu trong quá trình nén và giải nén là một phần thiết yếu của an ninh thông tin.

2. Các phương pháp bảo vệ dữ liệu khi nén và giải nén

a. Mã hóa tập tin nén

• Sử dụng các công cụ như WinRAR, 7-Zip để mã hóa nội dung tập tin bằng thuật toán AES-256.

• Mã hóa giúp ngăn chặn truy cập trái phép ngay cả khi tập tin bị đánh cắp.

b. Đặt mật khẩu bảo vệ

• Thiết lập mật khẩu khi tạo tập tin nén.

• Chỉ người có mật khẩu mới có thể giải nén và truy cập nội dung.

c. Chia nhỏ tập tin và đặt mật khẩu riêng

• Với dữ liệu lớn, có thể chia thành nhiều phần (.part1.rar, .part2.rar...) và đặt mật khẩu cho từng phần.

• Giảm rủi ro khi một phần bị lộ.

d. Sử dụng chữ ký số hoặc kiểm tra mã SHA/MD5

• Đảm bảo tập tin không bị thay đổi trong quá trình truyền tải.

• Phát hiện sớm các hành vi giả mạo hoặc chỉnh sửa.

e. Lưu trữ và truyền tải qua kênh bảo mật

• Sử dụng email mã hóa, VPN hoặc nền tảng lưu trữ có bảo mật cao (OneDrive, Google Drive có xác thực hai bước).

3. Cách bảo vệ thông tin nhạy cảm khi dùng WinRAR.

WinRAR là phần mềm nén phổ biến, hỗ trợ nhiều tính năng bảo mật:



# Thực hành Sử dụng WinRAR để nén các tập tin và thư mục, thiết lập mật khẩu để bảo vệ tệp nén và thử giải nén với mật khẩu đúng/sai.

