UBND TỈNH HÀ TĨNH
TIỂU BAN ATANM

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 1580/TBATANM

Hà Tĩnh, ngày 30 tháng 5 năm 2024

V/v tăng cường bảo mật thông tin đăng nhập tài khoản trực tuyến

Kính gửi: Thủ trưởng các cơ quan, đơn vị, địa phương trên địa bàn tỉnh.

Qua theo dõi, giám sát hoạt động tấn công mạng, cơ quan chuyên trách đảm bảo an toàn, an ninh mạng phát hiện mối đe dọa mới có tính chất nguy hiểm, nguy cơ gây ảnh hưởng đến an toàn, an ninh mạng của nhiều cơ quan, tổ chức tại Việt Nam: **rò rỉ thông tin đăng nhập các loại tài khoản trên không gian mạng**. Theo thống kê của Trung tâm An ninh mạng quốc gia 63/63 tỉnh, thành phố đều có thông tin đăng nhập thuộc hệ thống tên miền *"*.gov.vn"* đã bị đánh cắp, riêng Hà Tĩnh có hơn **1000** thông tin bị lộ, lọt trên không gian mạng. Đặc biệt một số cơ quan cấp Trung ương, khối Chính phủ cũng bị lộ, lọt các tài khoản giáo dục, tài chính, ngân hàng và các tài khoản email cá nhân.

Một số nguyên nhân dẫn đến lộ, lọt thông tin đăng nhập tài khoản trực tuyến:

- Do cá nhân người dùng: (1) Người dùng tự cung cấp tài khoản/mật khẩu cho trang web giả mạo hoặc trang web bị kiểm soát bởi tin tặc hoặc sử dụng mạng công cộng không an toàn. (2) Người dùng tải xuống tập tin độc hại có chứa mã độc, stealer hoặc keylogger (thường là các phần mềm bẻ khóa) và các loại mã độc âm thầm thu thập tài khoản trên máy nạn nhân gửi về cho tin tặc.

- Do chủ quản hệ thống : (1) Chủ quản để lộ lọt thông tin tài khoản mặc định hoặc công khai hướng dẫn các cách đăng nhập thay thế, tắt mã captcha,... (2) Hệ thống lưu trữ username/password dưới dạng bản rõ (không mã hóa) bị tấn công xâm nhập.

Nguy cơ và hậu quả của việc lộ, lọt thông tin đăng nhập tài khoản trực tuyến:

- Cá nhân: (1) Mất quyền truy cập vào tài khoản: Hacker có thể thay đổi mật khẩu của người dùng và khiến họ không thể truy cập vào các tài khoản cá nhân. (2) Mất tiền: Hacker sử dụng thông tin đăng nhập để truy cập vào tài khoản ngân hàng, thẻ tín dụng hoặc các tài khoản tài chính khác và đánh cắp tiền. (3) Bị giả mạo danh tính: Hacker lợi dụng tài khoản của người dùng để gửi đi các tin nhắn/email giả mạo vào mục đích vi phạm pháp luật. (4) Bị tống tiền: Hacker có thể sử dụng thông tin đăng nhập bị rò rỉ để truy cập, thu thập thông tin nhạy cảm của nạn nhân và sử dụng tống tiền.

- Tổ chức: (1) Hệ thống có nguy cơ bị tấn công mạng: Hacker sử dụng thông tin đăng nhập bị đánh cắp để tấn công khai thác các lỗ hổng post-auth hoặc duy trì sự xâm nhập trên hệ thống. (2) Rò rỉ dữ liệu của tổ chức, đặc biệt là dữ liệu nhạy cảm như các loại tài khoản Thư điện tử; Quản lý văn bản; Quản lý công việc; Quản lý cán bộ, công chức, viên chức,...có thể dẫn đến lộ, mất tài liệu

nội bộ, tài liệu bí mật nhà nước. (3) Lưu trữ, phát tán phần mềm độc hại: Hacker lợi dụng tài khoản bị rò rỉ để tải mã độc lên hệ thống, sau đó lợi dụng danh tính của tài khoản để phát tán mã độc, tấn công mục tiêu khác trên hệ thống.

Từ tình hình trên, để tăng cường bảo mật các tài khoản trực tuyến, Tiểu ban An toàn, An toàn mạng tỉnh Hà Tĩnh đề nghị Thủ trưởng các cơ quan, đơn vị, địa phương trên địa bàn tỉnh chỉ đạo triển khai thực hiện các nội dung sau:

1. Tiếp tục tổ chức triển khai hiệu quả các nội dung tại Công văn số 1202/TBATANM-CQTT ngày 27/4/2024 của Công an tỉnh - Cơ quan Thường trực Tiểu ban về việc tăng cường bảo mật tài khoản trực tuyến.

2. Rà soát, kiểm tra mức độ an toàn của các tài khoản trực tuyến của cán bộ, công nhân viên chức *(có hướng dẫn kèm theo)*, báo cáo Tiểu ban An toàn, An ninh mạng (*qua Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao - Công an tỉnh trước ngày **30/6/2024***) để tập hợp.

Đầu mối liên hệ: Đồng chí Thiếu tá Đặng Đôn Thắng, Đội trưởng Phòng An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao - Công an tỉnh, điện thoại: 0985.377.197.

Tiểu ban An toàn, An ninh mạng tỉnh Hà Tĩnh đề nghị các cơ quan, đơn vị, địa phương tổ chức thực hiện nghiêm túc./.

Nơi nhận:
- Thường trực Tỉnh ủy (để báo cáo);
- Thường trực HĐND tỉnh (để báo cáo);
- Đ/c Chủ tịch UBND tỉnh - Trưởng Tiểu ban An toàn, An ninh mạng (để báo cáo);
- Các Ban Đảng, UBKT, VP - Tỉnh ủy;
- Các Đảng ủy trực thuộc Tỉnh ủy;
- Văn phòng UBND tỉnh;
- Văn phòng Đoàn ĐBQH - HĐND tỉnh;
- Các sở, ban, ngành, đoàn thể cấp tỉnh;
- Các Huyện ủy, Thành ủy, Thị ủy;
- UBND các huyện, thành phố, thị xã;
- Các công ty, doanh nghiệp Nhà nước trên địa bàn;
- Lưu: VT, ANM.

KT. TRƯỞNG TIỂU BAN
PHÓ TRƯỞNG TIỂU BAN
THƯỜNG TRỰC

CỘNG HOÀ X.H.C.N VIỆT NAM
CÔNG AN TỈNH HÀ TĨNH

GIÁM ĐỐC CÔNG AN TỈNH
Đại tá Nguyễn Hồng Phong

HƯỚNG DẪN CÁCH TỰ KIỂM TRA VÀ CÁC BIỆN PHÁP BẢO VỆ THÔNG TIN ĐĂNG NHẬP CỦA TÀI KHOẢN TRỰC TUYẾN

(Ban hành kèm theo Công văn số: 2417/TBATANM ngày 30 tháng 5 năm 2024)

* Cách tự kiểm tra: các cá nhân, cơ quan, đơn vị có thể kiểm tra thông tin đăng nhập (liên quan đến email, tên miền, tên tổ chức,...) bị rò rỉ tại các ứng dụng sau: (1) https://haveibeenpwned.com; (2) https://socradar.io/labs/dark-web-report; (3) https://intelx.io;

* Các bước xử lý khi phát hiện thông tin đăng nhập bị rò rỉ:

1. Detect: Trường hợp tìm kiếm thấy tài khoản của mình đã bị rò rỉ.

2. Respond: Những bước cơ bản:

- Đặt lại mật khẩu hoặc khóa tài khoản.

- Kiểm tra các hoạt động đăng nhập bất thường trong nhật ký giám sát để thu thập chứng cứ tìm kiếm kẻ tấn công.

- Kiểm tra mức độ truy cập: Kiểm tra quyền truy cập của tài khoản bị lộ lọt vào những hệ thống nào, từ đó tiếp tục kiểm tra và khắc phục các hệ thống có nguy cơ bị xâm nhập.

- Thông báo cho người dùng: Thay đổi mật khẩu, tài khoản sau đó thông báo trực tiếp cho người dùng.

3. Recover: Nghiên cứu các thông tin đăng nhập bị lộ lọt để xác định nguy cơ gây lộ, mất dữ liệu:

- Mật khẩu bị lộ có còn đăng nhập được hay không?

- Mật khẩu đó được sử dụng trong khoảng thời gian nào?

- Mật khẩu có phải mặc định hay không?

- Đề nghị người dùng phối hợp kiểm tra các máy tính đã được sử dụng để đăng nhập những tài khoản được xác định nguồn gây lộ lọt và bóc gỡ mã độc (*nếu có*), nhắc nhở người dùng về các nguyên nhân có thể dẫn đến rò rỉ thông tin đăng nhập.

4. Identify: Đánh giá lại rủi ro của bạn dựa trên thông tin lộ lọt:

- Có khoảng trống nào trong quy trình kiểm soát tài khoản không?

- Quản trị viên có biết mỗi tài khoản bị lộ lọt có quyền truy cập vào hệ thống nào không?

- Các tài khoản bị lộ lọt có được áp dụng nguyên tắc đặc quyền tối thiểu không? Nếu không, cần tìm nguyên nhân, do nội bộ phân quyền sai hay do kẻ

tấn công đã leo quyền thành công. Sau đó tiến hành giới hạn các quyền không cần thiết của tài khoản đó.

5. Các biện pháp bảo vệ:

5.1. Ngắn hạn:

- Thêm bước xác thực đa nhân tố;

- Đặt hạn sử dụng cho mật khẩu, yêu cầu người dùng phải thay đổi mật khẩu thường xuyên;

- Không sử dụng chung một mật khẩu cho nhiều hệ thống, sử dụng trình quản lý mật khẩu tập trung để tạo và lưu trữ mật khẩu phức tạp một cách an toàn;

- Người dùng thường xuyên tự kiểm tra tình trạng lộ lọt tài khoản.

5.2. Dài hạn:

- Giám sát và kiểm tra thường xuyên tình hình lộ lọt: Sử dụng công cụ để quét các thông tin lộ lọt.

- Thực hiện các kiểm tra bảo mật thường xuyên để phát hiện và khắc phục các lỗ hổng trong hệ thống.

- Đào tạo và nâng cao nhận thức cho cán bộ, nhân viên.

- Đội ngũ chuyên trách cần chuẩn bị trước các kế hoạch ứng cứu sự cố để thực hiện nhanh chóng và đúng, đủ quy trình.