Process Safety Beacon
Thông điệp an toàn cho nhân sự sản xuất
www.aiche.org/ccps/process-safety-beacon

An AIChE Technology Alliance
CCPS Center for Chemical Process Safety
aiche.org/ccps

This issue sponsored by
ioMosaic®
Minimizing risk. Maximizing potential.®
www.iomosaic.com

An ninh mạng và vận hành hóa chất

Tháng 7 2021

Hình 1. Nhà máy xử lý nước Oldmar, bang Florida

Vào ngày 5 tháng 2 năm 2021, một nhân viên nhà máy xử lý nước ở Quận Oldsmar bang Florida, nhận thấy rằng con trỏ di chuyển kỳ lạ trên màn hình máy tính điều khiển. Ban đầu, anh ấy thấy không có gì đáng lo ngại bởi nhà máy có sử dụng phần mềm truy cập từ xa để cho phép nhân viên chia sẻ màn hình và khắc phục sự cố IT. Người giám sát cũng thường kết nối với máy tính của mình để giám sát hệ thống của nhà máy. Vài giờ sau, người vận hành nhận thấy con trỏ di chuyển và nhấp qua các nút điều khiển của nhà máy xử lý nước. Trong vòng vài giây, kẻ xâm nhập đã cố gắng thay đổi ngưỡng vận hành của natri hydroxit trên hệ thống từ 100 phần triệu (ppm) thành 11.100 ppm. Người vận hành phát hiện ra sự xâm nhập bất thường và nhanh chóng đưa natri hydroxit về mức bình thường. May mắn thay, chất lượng nước không bị ảnh hưởng.

Gần đây, một dạng mã độc đã tấn công vào hệ thống đường ống dẫn xăng do công ty Colonial Pipeline điều hành khiến tê liệt toàn bộ hệ thống cấp nhiên liệu tới bờ biển phía Đông Hoa kỳ trong vài ngày.

Hệ thống của công ty bạn có thể được kết nối với mạng Internet và cần được bảo vệ khỏi các cuộc tấn công không gian mạng. Có nhiều biện pháp được các công ty sử dụng để ngăn chặn các mối đe dọa mạng như: tường lửa, phần mềm chống vi rút và các chính sách bảo vệ chống lại phần mềm độc hại và các vi rút máy tính gây ra. Nhiều người đang làm việc từ xa; điều này đã làm tăng cơ hội cho các cuộc tấn công mạng.

Bạn có biết?

- Tội phạm mạng sử dụng phần mềm độc hại tinh vi để tận dụng nhiều lỗ hổng và hoàn thành mục tiêu của chúng.
- Các cuộc tấn công bằng mã độc ngày càng gia tăng do các tội phạm có tổ chức sử dụng nó như một công cụ kiếm tiền.
- Theo một nghiên cứu gần đây, cứ 39 giây lại có một cuộc tấn công mạng xảy ra. (Nguồn tham khảo. https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds)
- Bằng phương thức là gửi email, trên danh nghĩa các công ty danh tiếng, để khiến các cá nhân tiết lộ thông tin cá nhân. Cách tấn công này là phương pháp xâm nhập chính của các phần mềm độc hại.
- Các cuộc tấn công không gian mạng có thể xâm nhập vào hệ thống của công ty thông qua email, tệp đính kèm và từ các thiết bị lưu trữ di động, chẳng hạn như ổ USB hoặc các thiết bị lưu trữ di động khác.
- Chín mươi lăm phần trăm vi phạm an ninh mạng là do lỗi của con người. (Tham khảo nguồn. https://www.cybintsolutions.com/employee-education-reduces-risk/)

Bạn có thể làm gì?

- Luôn xác minh các yêu cầu cập nhật phần mềm với bộ phận IT trước khi làm theo và cài đặt các bản cập nhật đã được phê duyệt một cách kịp thời.
- Đảm bảo tường lửa và phần mềm khác của bạn được cập nhật và bật.
- Đảm bảo sao lưu hệ thống và dữ liệu của bạn thường xuyên.
- Sử dụng mật khẩu mạnh để đăng nhập. Không chia sẻ mật khẩu hoặc tài khoản và nên thay đổi mật khẩu thường xuyên.
- Không lưu mật khẩu trên các trình duyệt.
- Đừng nhấp vào các liên kết hoặc tệp đính kèm trong email được gửi từ người mà bạn không biết.
- Không bao giờ cài đặt phần mềm mà chưa được phê duyệt trên bất kỳ máy tính nào của công ty; đảm bảo các khóa truy cập và các thiết bị bảo mật vật lý khác được bảo mật đúng cách.
- Nếu bạn sử dụng quyền truy cập từ xa, hãy làm theo yêu cầu của công ty. Hãy đặc biệt cảnh giác nếu sử dụng các trang web internet công cộng.
- Nếu có điều gì đó trên máy tính của bạn có vẻ kỳ lạ hoặc khác biệt, hãy yêu cầu trợ giúp! Đó có thể là một tin tặc đang cố gắng truy cập vào máy tính của bạn.

Các cuộc tấn công mạng là có thật. Bạn là một phần quan trọng trong việc ngăn chặn.