MÃ ĐỘC TỐNG TIỀN
TẤN CÔNG CƠ SỞ DỮ LIỆU
CỦA MỘT DOANH NGHIỆP NHƯ THẾ NÀO?

Ransomware là một loại phần mềm độc hại, có thể lây nhiễm vào máy tính nếu bạn nhấp vào một liên kết có chứa vi-rút.

Khi liên kết này được mở ra, kẻ tấn công sẽ kiểm soát hệ thống máy tính của doanh nghiệp, từ đó truy cập và mã hóa các tập file quan trọng trong máy tính.
Thủ phạm sau đó sẽ yêu cầu một khoản tiền đổi lấy các tập file đã bị đánh cắp.

RANSOMWARE TẤN CÔNG MÁY TÍNH NHƯ THẾ NÀO?

1.
PHÂN PHỐI
Thủ phạm gửi email có đường link chứa vi-rút đến mục tiêu là các tổ chức và doanh nghiệp.

2.
LÂY NHIỄM
Khi người nhận mở đường link vi-rút sẽ được tải vào máy tính.

3.
KIỂM SOÁT
Thủ phạm sau đó sẽ truy cập được vào thiết bị và kiểm soát hệ thống đã bị hack.

4.
PHÁT HIỆN
Sau khi kiểm soát được hệ thống, ransomware sẽ tìm kiếm dữ liệu quan trọng nhằm mục đích mã hóa.

5.
ĐÁNH CẮP
Một khi được tìm thấy, những dữ liệu quan trọng sẽ bị đánh cắp khỏi hệ thống.

6.
MÃ HÓA
Các file bị đánh cắp được mã hóa, màn hình của nạn nhân sẽ bị khóa, đồng thời hiển thị thông báo máy bị nhiễm ransomware.

7.
YÊU CẦU
Kẻ tấn công sẽ yêu cầu một khoản tiền chuộc để nạn nhân đổi lấy mật mã và mở khóa hệ thống.

KẾT LUẬN

- Trả tiền chuộc không chắc chắn là bạn sẽ truy cập lại được vào dữ liệu của mình.
- Kể cả sau khi đã thanh toán khoản tiền được yêu cầu, một số nạn nhân thậm chí bị bắt trả nhiều tiền hơn để đổi lấy chìa khóa giải mã.
- Một số khác báo cáo rằng họ tiếp tục trở thành mục tiêu của tội phạm trên không gian ảo mặc dù đã trả tiền chuộc trước đó.
- Trả tiền chuộc sẽ khuyến khích mô hình kinh doanh bất hợp pháp của tội phạm không gian mạng.

MỘT SỐ MẸO GIÚP PHÒNG CHỐNG RANSOMWARE

- Tránh nhấp vào liên kết lạ, không rõ nguồn gốc
- Không chia sẻ thông tin cá nhân
- Không sử dụng USB không rõ nguồn gốc
- Không mở email và tập đính kèm lạ
- Thường xuyên nâng cấp, cập nhật hệ thống vận hành và chương trình
- Chỉ tải dữ liệu từ các nguồn đáng tin cậy
- Sử dụng VPN trên hệ thống wifi công cộng

References

- Ransomware attacks, a growing threat that needs to be countered. (n.d.) Www.unodc.org. https://www.unodc.org/southeastasiaandpacific/en/2021/10/cybercrime-ransomware-attacks/story.html
- Cybersecurity Infographic: 7 Stages of a Ransomware Attack. (2021, July 7). Securance Consulting. https://www.securanceconsulting.com/7-stages-of-a-ransomware-attack/
- ProofPoint. (2016, August 15). What Is Ransomware, How to Prevent Attacks, Remove, & More | Proofpoint. Proofpoint. https://www.proofpoint.com/us/threat-reference/ransomware

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

QUÁ TRÌNH
MÃ ĐỘC TỐNG TIỀN
TẤN CÔNG CƠ SỞ DỮ LIỆU
CỦA NGƯỜI DÙNG

Mã độc tống tiền (ransomware) là một loại phần mềm độc hại có thể tấn công dữ liệu của người dùng.

Khi lây nhiễm vào máy tính, ransomware sẽ mã hóa dữ liệu, yêu cầu người dùng trả một khoản tiền để đổi lấy dữ liệu bị đánh cắp.

Quá trình một cuộc tấn công ransomware xảy ra như sau:

1 GIẢ MẠO

Thủ phạm gửi email giả mạo đến người dùng.

2 LÂY NHIỄM

Nếu người dùng nhận được email giả mạo và nhấp vào đường link, phần mềm độc hại sẽ lây nhiễm vào máy tính và bắt đầu khai thác thông tin trên thiết bị của người dùng.

4 MÃ HÓA

Các tập file bị mã hóa, và màn hình sẽ hiển thị thông điệp máy bị nhiễm ransomware.

3 KIỂM SOÁT

Phần mềm độc hại giành quyền kiểm soát public key (mã hóa khóa công cộng), tài khoản và mật khẩu của người dùng.

5 TỐNG TIỀN

Người dùng được yêu cầu trả một khoản tiền để khôi phục dữ liệu đã bị đánh cắp.

6 GIẢI MÃ

Sau khi thanh toán được hoàn tất, thủ phạm sẽ có thể gửi private key (khóa riêng tư) dùng để giải mã các file bị đánh cắp trước đó hoặc không.

KẾT LUẬN

- Trả tiền chuộc không chắc chắn là bạn sẽ truy cập lại được vào dữ liệu của mình.
- Một số nạn nhân thậm chí bị bắt trả nhiều tiền hơn để đổi lấy chìa khóa giải mã, kể cả sau khi đã thanh toán khoản tiền được yêu cầu.
- Một số khác báo cáo rằng họ tiếp tục trở thành mục tiêu của tội phạm trên không gian ảo mặc dù đã trả tiền chuộc trước đó.
- Trả tiền chuộc sẽ khuyến khích mô hình kinh doanh bất hợp pháp của tội phạm không gian mạng.

MỘT SỐ MẸO GIÚP PHÒNG CHỐNG RANSOMWARE

- Tránh nhấp vào liên kết lạ, không rõ nguồn gốc
- Không chia sẻ thông tin cá nhân
- Không sử dụng USB không rõ nguồn gốc
- Không mở email và tập đính kèm lạ
- Thường xuyên nâng cấp, cập nhật hệ thống vận hành và chương trình máy tính
- Chỉ tải xuống từ các nguồn đáng tin cậy
- Sử dụng VPN trên hệ thống wifi công cộng

References

- Ransomware protection: How to keep your data safe in 2021. (2021, June 15). usa.kaspersky.com. https://usa.kaspersky.com/resource-center/threats/how-to-prevent-ransomware
- Akara.umapornsakula. (n.d.). Ransomware attacks, a growing threat that needs to be countered. United Nations Office on Drugs and Crime. https://www.unodc.org/southeastasiaandpacific/en/2021/10/cybercrime-ransomware-attacks/story.html
- The real cost of a ransomware attack, and how to mitigate ransom threats. (n.d.). Global Security Mag Online. https://www.globalsecuritymag.fr/The-Real-Cost-of-a-Ransomware,20201019,103952.html

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

Hành động quan trọng cần thực hiện đối với người dùng

Trở thành nạn nhân của mã độc tống tiền (ransomware) có thể khiến dữ liệu cá nhân, hoặc cả doanh nghiệp của bạn có nguy cơ "một đi không trở lại".

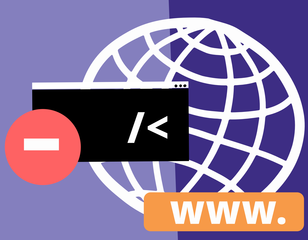
Bạn có thể thực hiện các bước dưới đây để ngăn ransomware đánh cắp dữ liệu quan trọng của mình.

ACTION 1

THƯỜNG XUYÊN SAO LƯU DỮ LIỆU

Luôn cập nhật bản sao lưu là cách hiệu quả nhất để khôi phục sau một cuộc tấn công ransomware.

ACTION 2



Ngăn chặn phần mềm độc hại lây nhiễm vào máy tính bằng cách không nhấp vào liên kết không rõ nguồn gốc

Có thể giảm thiểu nguy cơ nội dung độc hại lây nhiễm vào thiết bị của bạn bằng cách kết hợp lọc và chặn các trang web độc hại, luôn kiểm tra nội dung và sử dụng chữ ký để chặn các mã độc hại đã biết.

ACTION 3

NGĂN PHẦN MỀM ĐỘC HẠI CHẠY TRÊN THIẾT BỊ

Phương pháp tiếp cận 'phòng thủ theo chiều sâu' giả định rằng phần mềm độc hại sẽ nhắm vào thiết bị của bạn. Do đó, bạn cần trang bị kỹ năng để có thể ngăn phần mềm độc hại lây nhiễm vào máy tính của mình.

Từng thiết bị sẽ áp dụng các biện pháp khác nhau, nhưng nhìn chung, bạn sẽ cần sử dụng các tính năng bảo mật ở cùng cấp độ với thiết bị.

ACTION 4

CHUẨN BỊ ỨNG PHÓ VỚI SỰ CỐ

Một cuộc tấn công ransomware có thể phá hoại nhiều thứ, kể đến như làm ngưng trệ hệ thống vận hành và gây tổn hại đến uy tín thương hiệu.

Để ngăn chặn một cuộc tấn công ransomware, bạn nên thực hiện các bước dưới đây:

1. Đánh giá trước mức độ rủi ro ransomware có thể gây ra cho hoạt động vận hành
2. Phát triển kế hoạch đảm bảo kinh doanh liên tục
3. Lập kế hoạch chi tiêu
4. Chú trọng phòng chống ransomware

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

Các loại mã độc tống tiền (RANSOMWARE)

Tội phạm trên không gian ảo đang ngày càng trở nên nguy hiểm hơn với nhiều thủ thuật tấn công ransomware. Dưới đây là thông tin các loại ransomware phổ biến nhất.

1 Crypto ransomware

Crypto ransomware được thiết kế để mã hóa thông tin quan trọng của người dùng, nhưng không can thiệp vào các chức năng cơ bản của máy tính.

Thủ phạm đằng sau Crypto sẽ tạo thời gian đếm ngược để đòi tiền chuộc với tin nhắn như "Yêu cầu trả tiền chuộc trước thời hạn, nếu không các tập file của bạn sẽ bị xóa".

Locker ransomware 2

Locker ransomware can thiệp vào chức năng của máy tính, yêu cầu người dùng trả tiền chuộc để lấy lại quyền truy cập.

Locker ransomware không nhắm đến các tập file mà nó sẽ khóa cả máy tính, khiến người dùng hoàn toàn không truy cập được vào thiết bị của mình.

3 Scareware

Scareware hoạt động như một chương trình bảo mật, đánh lừa người dùng bằng cách giả vờ phát hiện ra vi-rút hoặc vấn đề khác trên máy tính, sau đó sẽ đưa ra hướng dẫn trả tiền để giải quyết vấn đề.

Một số loại scareware sẽ khóa máy tính, trong khi những loại khác chỉ hiện lên cảnh báo trên màn hình mà không thực sự ảnh hưởng đến tập file trong máy của bạn.

Doxware hay Leakware 4

Doxware đe dọa công khai lên mạng các thông tin nhạy cảm của người dùng hoặc doanh nghiệp.

Nạn nhân buộc phải trả tiền chuộc để ngăn dữ liệu cá nhân không rơi vào tay kẻ xấu hoặc bị công khai đến tất cả mọi người.

5 Ransomware như một dịch vụ (RaaS)

RaaS là một loại ransomware được lưu trữ trên các trang dark net dưới dạng thị trường mua bán, qua đó tội phạm có thể đặt mua ransomware định kì như một món hàng.

Một khi tội phạm lấy được tiền chuộc từ nạn nhân, một phần tiền sẽ được trích ra trả cho người tạo ra RaaS theo các điều khoản đã thỏa thuận trước đó.

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

10 Nguyên tắc giúp doanh nghiệp xây dựng hệ thống an ninh mạng để phòng chống mã độc tống tiền

Quản trị rủi ro

Đảm bảo đánh giá phù hợp nhất mức độ rủi ro có thể xảy ra đối với các hệ thống, công nghệ và thông tin trong doanh nghiệp.

Kiến tạo và cấu hình

Đảm bảo rằng an ninh mạng tốt được tích hợp vào các hệ thống và dịch vụ ngay từ ban đầu, và thường xuyên bảo trì, cập nhật hệ thống và dịch vụ này.

Quản lý tài sản

Nắm vững, hiểu rõ về dữ liệu và hệ thống mà doanh nghiệp cần quản lý.

Đăng nhập và giám sát

Thiết kế hệ thống để có thể phát hiện hoạt động đăng nhập và điều tra sự cố do ransomware gây ra.

Tham gia và tập huấn

Khuyến khích, hỗ trợ nhân viên xây dựng kỹ năng và kiến thức về an ninh mạng và ransomware.

Bảo mật thông tin

Bảo vệ những dữ liệu dễ bị tấn công và gặp rủi ro. Sao lưu dữ liệu và thực hiện kiểm tra thường xuyên.

Quản lý lỗ hổng bảo mật

Cập nhập hệ thống thường xuyên là cách bảo vệ hệ thống trong suốt vòng đời phát triển. Ngoài ra, quy trình quản lý lỗ hổng bảo mật cũng cần được nâng cao.

Quản lý sự cố

Lập kế hoạch ứng phó với sự cố trên không gian mạng và cuộc tấn công ransomware, trong đó đảm bảo sự tham gia của các bên liên quan.

Quản lý truy cập và nhận dạng

Kiểm soát người dùng nào có thể truy cập vào hệ thống dữ liệu của doanh nghiệp.

Bảo mật chuỗi cung ứng

Hợp tác với nhà cung cấp và đối tác bằng các điều khoản bảo mật trong quy trình ký hợp đồng.

Một điều cần làm là hỗ trợ các doanh nghiệp trong chuỗi cung ứng tham gia tập huấn phòng chống ransomware.

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

Triển khai kế hoạch tập huấn nhân viên về ransomware

dành cho doanh nghiệp nhỏ

Tội phạm ransomware không phân biệt doanh nghiệp lớn hay nhỏ. Tất cả doanh nghiệp đều có nguy cơ trở thành nạn nhân của chúng.

Do đó, tiến hành tập huấn cho nhân viên trong công ty là một trong những biện pháp phòng chống tốt nhất để bảo vệ doanh nghiệp của bạn.

Dưới đây là một số cách giúp triển khai buổi tập huấn cho nhân viên về ransomware.

CÂN NHẮC

Tập huấn nâng cao nhận thức về bảo mật

Tổ chức đào tạo nâng cao nhận thức về bảo mật cho nhân viên là một trong những biện pháp phòng chống tốt nhất để bảo vệ doanh nghiệp của bạn.

Nhân viên sẽ không chỉ được giới thiệu về các mối đe dọa trên không gian mạng mà còn hiểu được vai trò của mình trong việc bảo vệ hệ thống và dữ liệu của công ty.

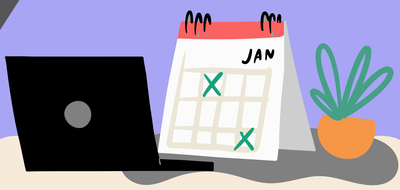
Đi sâu vào một số cuộc tấn công cụ thể trên mạng

Tập huấn cho nhân viên về các thủ thuật hoặc phương pháp mà tội phạm trên không gian ảo có thể sử dụng, bao gồm một số cách phổ biến khiến máy tính và thiết bị lây nhiễm phần mềm độc hại.

Chương trình tập huấn cho nhân viên phi kỹ thuật

Tập huấn toàn diện với nội dung dễ hiểu cho tất cả nhân viên về an ninh mạng là một cách khác vô cùng hiệu quả.

Điều quan trọng cần lưu ý là phòng chống ransomware và các cuộc tấn công mạng không chỉ là nhiệm vụ của các chuyên gia công nghệ thông tin.



Các buổi tập huấn thường xuyên

Nâng cao kiến thức cho nhân viên, khuyến khích nhân viên báo cáo về các hoạt động đáng ngờ, nhắc nhở về tầm quan trọng của việc tuân thủ an ninh mạng và áp dụng biện pháp phòng chống là một số cách tối ưu để bảo vệ doanh nghiệp nhỏ khỏi tội phạm trên không gian ảo.

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

Triển khai kế hoạch tập huấn nhân viên về mã độc tống tiền (ransomware)

dành cho doanh nghiệp lớn

Một công ty lớn thường gồm nhiều phòng ban và nhân viên. Việc tổ chức tập huấn thường xuyên cho tất cả nhân viên là một trong những biện pháp tốt nhất giúp một doanh nghiệp lớn phòng chống tội phạm trên không gian ảo.

Dưới đây là một số biện pháp giúp một doanh nghiệp lớn xây dựng kế hoạch tập huấn cho nhân viên về ransomware.

CÂN NHẮC

Chương trình tập huấn cập nhật thường xuyên

Chương trình tập huấn được cập nhật thường xuyên sẽ giúp trau dồi các thói quen tốt tại nơi làm việc.

Trung bình, một chương trình tập huấn có thể kéo dài trong 2 tháng.

Giáo dục về tội phạm trên không gian ảo

Tập huấn nâng cao nhận thức về bảo mật giúp nhân viên xác định các hành động có nguy cơ rủi ro và áp dụng tốt hơn các biện pháp bảo vệ an ninh mạng.

Phương pháp thực hành

Tổ chức diễn tập mô phỏng sẽ giúp theo dõi sự tiến bộ của nhân viên và xác định nhân viên nào cần tập huấn thêm.

Tập huấn về lĩnh vực bảo mật cụ thể

Do số lượng các cuộc tấn công ransomware và giả mạo đang tăng lên đáng kể, những buổi tập huấn về một số lĩnh vực bảo mật cụ thể là rất quan trọng.

Thay đổi nội dung tập huấn tùy theo phòng ban

Công ty nên điều chỉnh nội dung tập huấn về an ninh mạng để phù hợp với từng vai trò khác nhau của nhân viên.

Ví dụ như, các nhóm không thuộc bộ phận IT có thể tập trung vào biện pháp phòng chống, nâng cao nhận thức về an ninh mạng và báo cáo hành vi đáng ngờ, trong khi phòng IT có nhiệm vụ kịp thời giải quyết khi xảy ra sự cố.

Hướng dẫn cách báo cáo

Tất cả nhân viên nên được hướng dẫn về cách báo cáo các hoạt động của ransomware.

Hướng dẫn có thể bao gồm bộ phận nào sẽ nhận báo cáo, cách thức báo cáo và các thông tin liên quan khác.

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

Chính sách Mạng xã hội và Internet

Internet là nơi hoàn hảo để tội phạm thực hiện các cuộc tấn công ransomware.

Dưới đây là năm cách giúp bạn bảo mật thông tin trên mạng xã hội, Internet và các ứng dụng trực tuyến khác.

Bản sao lưu offline

Chính sách tốt nhất để bảo mật dữ liệu là sao lưu dữ liệu bên ngoài ở nhiều nơi khác nhau.

Điều này giúp giảm thiểu nguy cơ bị đánh cắp thông tin mã hóa và giúp người dùng khôi phục lại hệ thống trong trường hợp bị ransomware tấn công.

Bộ lọc thư rác

Bộ lọc thư rác có thể lấy thông tin về các mối đe dọa dựa trên điện toán đám mây. Do đó, bạn có thể ngăn chặn được 99% các mối đe dọa đến từ email nếu sử dụng bộ lọc thư rác một cách hiệu quả.

Email Security Gateway

Email Security Gateway là một biện pháp bảo mật sử dụng địa chỉ URL và tệp đính kèm công nghệ Sandbox để xác định rủi ro và phòng chống các cuộc tấn công. Điều này ngăn chặn ransomware xâm nhập vào hệ thống điểm cuối, đồng thời ngăn chặn nguy cơ người dùng vô tình cài đặt mã độc vào thiết bị của mình.

Kiểm tra bằng Sandbox

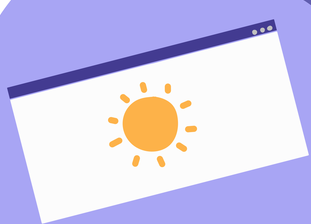
Sandbox là một kỹ thuật được sử dụng bởi các chuyên gia bảo mật để kiểm tra các tập file mới hay file không có nguồn gốc rõ ràng.

Sandbox tạo ra môi trường an toàn để kiểm tra các tập file đáng ngờ, cùng lúc cô lập nó với phần còn lại của hệ thống.

Bộ lọc Web

Công nghệ lọc Web có thể hạn chế người dùng truy cập các trang web nguy hiểm hay tải xuống các file độc hại cho máy tính.

Điều này giúp ngăn các loại vi-rút như ransomware được tải xuống qua mạng Internet.



UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

Thiết lập kế hoạch an ninh hệ thống

Kế hoạch an ninh hệ thống (SSP) là tài liệu phác thảo cách thức một doanh nghiệp thực hiện các yêu cầu về bảo mật.

Kế hoạch sẽ vạch ra vai trò và trách nhiệm của nhân viên an ninh, đồng thời cũng nêu chi tiết các tiêu chuẩn và hướng dẫn bảo mật mà tổ chức cần thực hiện.

Có bốn bước cơ bản để bạn tạo ra một bản SSP cho doanh nghiệp của mình.

1

Thu thập tất cả các thông tin bảo mật

Thu thập tất cả các tài liệu, chính sách và quy trình mô tả vị trí bảo mật hiện tại cho hệ thống của bạn nằm "trong phạm vi" của Chứng nhận Mô hình Bảo mật An ninh Mạng trưởng thành (CMMC) hoặc đánh giá tuân thủ của NIST 800-171.

2

Tham khảo ý kiến của các chuyên gia bảo mật

Lấy thông tin từ những người phụ trách bảo mật hệ thống, ví dụ như nhân viên quản lý hệ thống, nhân viên vận hành và chủ dữ liệu để đảm bảo thông tin trong tài liệu khớp với thực trạng của môi trường làm việc.

3

Bổ sung thông tin còn thiếu

Hãy bổ sung những thông tin còn thiếu trong bản kế hoạch dựa vào các cuộc phỏng vấn, bài nghiên cứu và các nguồn đáng tin cậy khác.

4

Tổ chức và hoàn thiện kế hoạch an ninh hệ thống

Theo khuyến nghị của Bộ Quốc phòng, hãy thiết kế các đầu mục của SSP theo một template nhất định để đảm bảo sự chính xác, đầy đủ và rõ ràng.

Lời khuyên

Nếu doanh nghiệp có bộ phận bảo mật an ninh nội bộ, nhân viên IT/ bảo mật có thể điền thông tin vào template SSP.

Một nhược điểm của phương pháp này là thiếu tính khách quan trong việc xác định các lỗ hổng mà sau này kiểm tra viên có thể phát hiện ra.

Một lựa chọn khác là thuê chuyên gia bên thứ ba để trợ giúp quá trình này. Điều này không chỉ giúp tiết kiệm thời gian và tiền bạc hơn so với việc tự làm, mà còn đảm bảo kết quả tuân thủ đầy đủ các yêu cầu và hữu ích cho người kiểm tra.

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

Lorem ipsum

Tầm quan trọng của việc sử dụng phần mềm cập nhật và có bản quyền

Có thể bạn thấy việc sử dụng phần mềm cập nhật và có bản quyền không đem lại điều gì khác biệt, nhưng đây là một quan điểm sai lầm vì việc sử dụng phần mềm cũ hoặc không có bản quyền sẽ khiến hacker dễ dàng truy cập vào thông tin cá nhân của bạn hơn, khiến bạn rơi vào nguy cơ bị trộm cắp danh tính, mất tiền, bị gian lận thẻ tín dụng, và còn nhiều rủi ro khác nữa.

Dưới đây là những lợi ích của việc sử dụng phần mềm cập nhật và có bản quyền.

Bảo mật tốt hơn

Hacker có thể sử dụng các lỗ hổng trong phần mềm đã lỗi thời để khai thác, gây hại cho hệ thống máy tính và đánh cắp dữ liệu cá nhân.

Phần mềm cũ có thể kết nối hacker đến hệ thống máy tính của bạn.

Bảo vệ tốt hơn

Các báo cáo chỉ ra rằng người dùng và doanh nghiệp sử dụng phần mềm máy tính không có giấy phép thường gặp phải nhiều phần mềm độc hại hơn so với những người sử dụng phần mềm hợp pháp.

Điều này là do tội phạm trên không gian ảo có thể cài đặt trước hoặc nhúng phần mềm độc hại vào phần mềm và sử dụng nó để truy cập trái phép vào thông tin của người dùng.

Hỗ trợ 24/7

Phần mềm bản quyền thường đi kèm với hỗ trợ kỹ thuật thường trực 24/7.

Bất cứ khi nào có vấn đề, bạn có thể yên tâm vì mình sẽ nhận được sự hỗ trợ nhanh chóng.

Bảo vệ người xung quanh

Nếu thiết bị của bạn bị nhiễm vi rút do lỗ hổng ở trong phần mềm đã bị cũ, vi-rút có thể dễ dàng lây sang thiết bị khác của bạn bè, gia đình và đối tác kinh doanh của bạn.

Cải thiện hiệu quả công việc

Phần mềm cũ thường tiêu tốn nhiều công suất máy tính hơn mức cần thiết. Nếu phần mềm đang mất nhiều thời gian hoặc không chạy mượt như trước đây, thì có thể đã đến lúc cập nhật phiên bản mới nhất rồi.

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

Cài đặt mật khẩu mạnh

Đặt mật khẩu mạnh là một biện pháp chủ động giúp bảo vệ bạn khỏi các cuộc tấn công mã độc tống tiền (ransomware).

Dưới đây là một số mẹo hữu ích:

ĐỘ DÀI CỦA MẬT KHẨU

Một mật khẩu với tối thiểu tám ký tự, kết hợp giữa các ký tự đặc biệt và ký tự số sẽ gây khó khăn cho việc hack mật khẩu.

Ví dụ: Donald-Mouse49!

LỊCH SỬ CÀI ĐẶT MẬT KHẨU

Không nên sử dụng cùng một mật khẩu cho mọi trang web vì tin tặc có thể đánh cắp tất cả các tài khoản trực tuyến của bạn nếu chúng xâm nhập được vào một trong số các tài khoản đó.

THÔNG TIN CÁ NHÂN

Tránh sử dụng ngày sinh, họ tên hay số điện thoại vì mật khẩu của bạn sẽ rất dễ đoán.

BẬT THÔNG BÁO Ở EMAIL

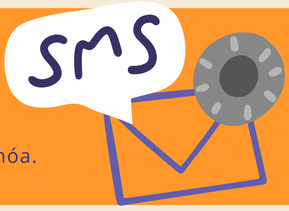
Sử dụng chế độ "Thông báo qua email" mỗi khi đăng nhập để phát hiện bất kỳ hoạt động đăng nhập bất thường nào.

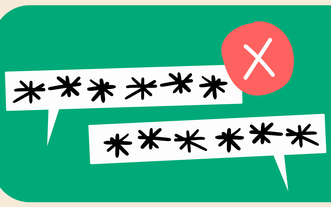
THỜI GIAN SỬ DỤNG MẬT KHẨU

Bạn nên thay đổi mật khẩu sau mỗi 30, 60 hoặc 90 ngày.

QUẢN LÝ

Sử dụng ứng dụng được mã hóa để quản lý mật khẩu của bạn. Điều này ngăn không cho tin tặc dễ dàng truy cập thông tin đã được mã hóa.



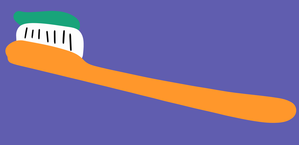


XÁC THỰC HAI YẾU TỐ

Xác thực 2 yếu tố (2FA) là phương pháp hiệu quả để tạo thêm "bức tường bảo mật" cho tài khoản của bạn.

CHIA SẺ ĐĂNG NHẬP

Trong cùng một doanh nghiệp, bạn không nên chia sẻ mật khẩu hoặc sử dụng chung tài khoản với những nhân viên khác.



"Hãy coi mật khẩu của bạn như chiếc bàn chải đánh răng. Đừng để bất kỳ ai sử dụng nó và hãy thay mới sáu tháng một lần".

-Clifford Stoll-

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

Ba cách để xác định các mối đe dọa ransomware

Người dùng và doanh nghiệp có thể sử dụng một số biện pháp để phát hiện mã độc. Có ba phương pháp sau:

1. Dựa trên chữ ký

Phương pháp này sử dụng kỹ thuật phân tích tĩnh trong một thời gian ngắn để phát hiện mã độc.

Các nền tảng bảo mật có thể kiểm tra dữ liệu chiết xuất từ các tập file thực thi được để biết đó có phải là ransomware hay không.

2. Dựa trên hành vi

Phát hiện dựa trên hành vi bằng cách sử dụng một công cụ để so sánh hành vi gần đây với hành vi trong quá khứ.

Ví dụ như trong cùng một ngày, khi nhân viên truy cập vào máy tính tại văn phòng, có một truy cập bất thường vào máy tính từ một tỉnh thành khác.

3. Dựa trên cảnh báo lừa đảo

Phương pháp này bao gồm dò tìm, phân tích và phòng thủ để chống lại các vụ khai thác lỗ hổng Zero-day và các cuộc tấn công có chủ đích, thường xảy ra trong thời gian thực. Quá trình này cung cấp thông tin chi tiết về các hoạt động độc hại trong hệ thống mạng nội bộ.

Những điều cần đưa vào báo cáo

Khi báo cáo về một vụ tấn công ransomware, mỗi quốc gia thường có những yêu cầu khác nhau.

Để có thể cung cấp thông tin hữu ích cho bộ phận thực thi pháp luật hoặc pháp y liên quan, hãy chuẩn bị sẵn sàng các thông tin dưới đây trong báo cáo của bạn.

1. Phần mở rộng của các tập file được mã hóa
2. Ngày và giờ của cuộc tấn công ransomware
3. Ảnh hoặc bản copy yêu cầu đòi tiền chuộc
4. Tên đầy đủ của ransomware, thường có trong ghi chú đòi tiền chuộc hoặc tậpfile được mã hóa
5. IP 1xx.xxx.xxx.xxx — Bất kỳ địa chỉ IP nào kết nối với hệ thống mạng mà bạn chưa từng thấy
6. Thông tin tổ chức của bạn: lĩnh vực, loại hình kinh doanh, quy mô và người liên hệ thích hợp.
7. Phương thức tấn công, có thể là từ một đường link email hoặc tệp đính kèm, trình duyệt Internet hoặc các phương tiện lây nhiễm khác.
8. Địa chỉ email, URL của tội phạm hoặc bất kỳ phương tiện liên lạc nào khác
9. Các bản sao thư điện tử với thủ phạm (nếu có)
10. Địa chỉ ví bitcoin của tội phạm trên không gian ảo, thường được xác định trên trang đòi tiền chuộc.
11. Số tiền được yêu cầu thanh toán và số tiền chuộc đã trả
12. Những tổn thất liên quan đến cuộc tấn công ransomware, bao gồm nhưng không giới hạn ở số tiền chuộc.

References

1.eJohnson, K. (2021, September 7). 3 ransomware detection techniques to catch an attack. SearchSecurity. Retrieved November 22, 2021, from https://www.techtarget.com/searchsecurity/feature/3-ransomware-detection-techniques-to-catch-an-attack.

2.Report Ransomware Crime. (n.d.). Retrieved November 22, 2021, from https://www.provendatarecovery.com/report-ransomware-crime/

3.Ransomware detection. Unitrends. (2021, July 1). Retrieved November 22, 2021, from https://www.unitrends.com/solutions/ransomware-detection.

UNODC United Nations Office on Drugs and Crime

CYBERCRIME

From the People of Japan

RansomAware

Lợi ích của việc thuê chuyên gia về an ninh mạng bên ngoài

Bảo hiểm có thể giúp phục hồi dữ liệu, nhưng không thể ngăn chặn các cuộc tấn công trên không gian mạng. Biện pháp phòng chống tốt nhất là sử dụng dịch vụ an ninh mạng quản lý bởi các chuyên gia uy tín.

Tiết kiệm ngân sách

Duy trì một đội ngũ nhân viên an ninh mạng nội bộ có thể gây tốn kém. Thuê đội ứng phó bên ngoài sẽ giúp doanh nghiệp tiết kiệm chi phí thuê nhân viên và chi phí thành lập hẳn một bộ phận IT mới trong công ty.

Dịch vụ thường trực 24/7

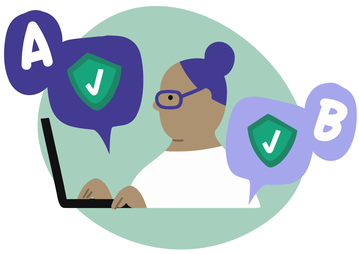
Các cuộc tấn công mã độc tống tiền (ransomware) có thể xảy ra bất kì lúc nào. Được các chuyên gia theo dõi cả ngày lẫn đêm là sự lựa chọn an toàn cho hệ thống máy tính của doanh nghiệp.

Đội ngũ nhân viên nhiều kỹ năng và kinh nghiệm hơn

Khi các cuộc tấn công ransomware trở nên thay đổi, các chuyên gia có thể loại bỏ mối đe dọa bằng các chiến thuật, kỹ thuật và quy trình hiện đại nhất.

Nhà cung cấp dịch vụ bảo mật có chuyên môn và kỹ năng cao

Thuê các chuyên gia an ninh mạng bên ngoài có kỹ năng chuyên môn sẽ đáp ứng nhu cầu của doanh nghiệp trong việc giải quyết các vấn đề kỹ thuật.



Linh hoạt hơn

Một điều quan trọng là cần chủ động nâng cấp các hoạt động vận hành bảo mật để ứng phó với bối cảnh kinh doanh và các mối đe dọa thay đổi nhanh chóng.

Công nghệ phát hiện ransomware hiệu quả hơn

Với các công cụ hiện đại nhất, hệ thống an ninh mạng có thể hỗ trợ doanh nghiệp ngăn chặn các mối đe dọa và dễ dàng quản lý công nghệ.

References
Loyer, S. (2021). 6 Reasons/Benefits of Outsourcing Cyber Security Services. TGVT. https://tgvt.net/reasons-why-outsourcing-cyber-security-services/
Team, T. R. (2020). Five reasons to consider outsourcing your organisation's cyber security. Redscan. https://www.redscan.com/news/five-reasons-to-consider-outsourcing-your-organisations-cyber-security/
Cybriant. (n.d.). 9 unique reasons to outsource cyber security monitoring. https://cybriant.com/outsource-cyber-security-monitoring/

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

Tại sao an ninh mạng không phức tạp đến vậy?

Mã độc tống tiền là gì?

Mã độc tống tiền (ransomware) là một loại phần mềm độc hại, có thể lây nhiễm vào máy tính và mã hóa tập file của người dùng. Thủ phạm sau đó sẽ yêu cầu một khoản tiền chuộc để người dùng khôi phục dữ liệu.

Thiết bị của bạn bị nhiễm ransomware qua hình thức nào?

Một trong những thủ đoạn phổ biến nhất là email giả mạo, hay email rác chứa tệp đính kèm đánh lừa người dùng đó là tệp đáng tin cậy.

Các hình thức khác bao gồm tải xuống tập file từ trang web giả mạo hoặc từ các ứng dụng mạng xã hội, sau đó bạn nhấp vào liên kết 'bị nhiễm vi-rút'.

Cách phòng chống ransomware

Có rất nhiều cách giúp ngăn chặn ransomware. Bạn có thể thực hiện một số cách như bên dưới:

- Không nhấp vào liên kết lạ, không rõ nguồn gốc
- Tránh chia sẻ thông tin cá nhân
- Không mở tệp đính kèm lạ trong email
- Không sử dụng USB không rõ nguồn gốc
- Thường xuyên nâng cấp, cập nhật hệ thống vận hành và chương trình máy tính
- Chỉ tải xuống từ các nguồn đáng tin cậy

Cần làm gì nếu bạn trở thành nạn nhân của ransomware?

Báo cho cơ quan liên quan có thẩm quyền về cuộc tấn công ransomware.

Xem xét trước hậu quả của cuộc tấn công ransomware. Cần lưu ý rằng trả tiền chuộc không có nghĩa bạn sẽ lấy lại được dữ liệu của mình!

Bạn nên tìm lời khuyên hoặc sự hỗ trợ từ các chuyên gia có kinh nghiệm.

Xin lưu ý rằng trên đây chỉ là một số biện pháp giúp bạn bảo vệ dữ liệu cá nhân khỏi ransomware và các mối đe dọa an ninh mạng.

Đối với những vấn đề phức tạp hơn, bạn nên tìm lời khuyên trực tiếp từ các chuyên gia Công nghệ thông tin.

UNODC United Nations Office on Drugs and Crime | CYBERCRIME | From the People of Japan | RansomAware

Người dùng không quen với công nghệ cần làm gì để bảo vệ dữ liệu của mình?

Dù bạn là người mới sử dụng Internet,
bạn vẫn có thể sử dụng mạng một cách
an toàn và bảo vệ thông tin cá nhân của mình.

NÊN

Thường xuyên nâng cấp,
cập nhật hệ thống vận hành
và chương trình máy tính

Luôn bật chế độ riêng tư

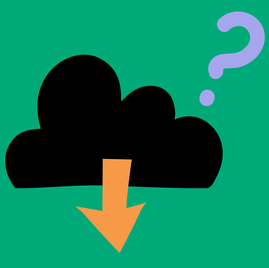
Đảm bảo rằng kết nối mạng
Internet được bảo mật

Chọn mật khẩu mạnh

KHÔNG NÊN

Tránh chia sẻ thông tin
cá nhân trên mạng

Tránh nhấp vào đường link trong
tin nhắn rác hoặc trên trang web
không rõ nguồn gốc



Chỉ tải xuống từ các nguồn
đáng tin cậy

Không mở email và
tệp đính kèm lạ

Bạn đã sẵn sàng?

Với kiến thức về các biện pháp an toàn khi sử dụng mạng, bạn có thể
ngăn chặn nhiều vấn đề trong tương lai. Hãy nhớ điều quan trọng là
bất kỳ ai cũng có thể trở thành mục tiêu nếu bạn chủ quan và mất cảnh giác.

REFERENCES

HTTPS://WWW.MCAFEE.COM/BLOGS/INTERNET-SECURITY/8-TIPS-FOR-STAYING-SAFE-FROM-RANSOMWARE-ATTACKS/
HTTPS://WWW.ESECURITYPLANET.COM/THREATS/RANSOMWARE-PROTECTION/ HTTPS://USA.KASPERSKY.COM/RESOURCE-CENTER/THREATS/HOW-TO-PREVENT-RANSOMWARE

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

Cần làm gì khi doanh nghiệp của bạn bị đe dọa bởi ransomware?

Một quy trình đơn giản để giải quyết sự cố ransomware

Phát hiện

Ransomware được phát hiện ra nhờ nhân viên hoặc công nghệ.

Công nghệ phát hiện hiệu quả sẽ báo hiệu ngay khi thấy điều gì đó không ổn.

Tất cả nhân viên cần phải biết cách báo cáo khi sự cố xảy ra.

Phân tích

Cần phân tích đầy đủ chi tiết để vạch ra các bước hành động tiếp theo.

Xác nhận sự cố đã xảy ra.

Xác định phạm vi ảnh hưởng của ransomware.

Báo cáo

Nếu sự cố nghiêm trọng, hãy báo cáo và chuyển tiếp cho Đội Phản ứng Sự cố Bảo vệ Máy tính (CSIRT), nhóm ứng phó thảm họa hoặc cộng đồng doanh nghiệp.

Ngăn chặn

Với sự ủy quyền thích hợp, hãy ngắt kết nối máy tính khỏi hệ thống của doanh nghiệp.

Đây là một quyết định kinh doanh, không phải là quyết định mang tính kỹ thuật.

Việc ngắt kết nối phải có sự chấp thuận của bộ phận có thẩm quyền trong doanh nghiệp.

Khôi phục

Sửa chữa

- Khôi phục dữ liệu từ các bản sao lưu
- Cài đặt lại phần mềm

Tường trình

Giải thích chi tiết về mối đe dọa và thiệt hại có thể xảy ra, cũng như các hành động bồi thường cho nạn nhân, nếu có.

Hình phạt

- Xác định nhân viên chịu trách nhiệm về việc tải xuống phần mềm ransomware. Hãy lưu ý rằng phần mềm độc hại có thể vô tình được tải xuống mà người dùng không nhận ra.
- Đưa ra quyết định có cần truy cứu trách nhiệm hình sự hay không.
- Thu thập và quản lý bằng chứng.

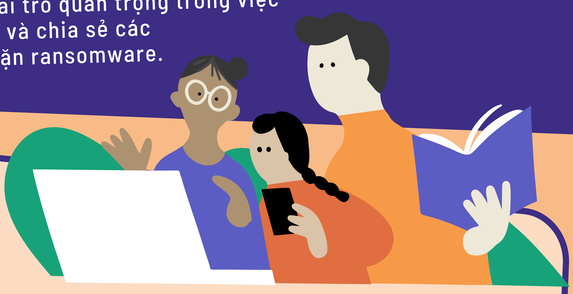
Đánh giá sau sự cố

- Đánh giá lại sự cố và lập kế hoạch theo dõi tiếp theo.
- Đặt câu hỏi: doanh nghiệp có thể làm gì khác trong những lần tới để ngăn chặn ransomware?

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

Nhóm chia sẻ thông tin giúp ngăn chặn ransomware như thế nào?

Nhóm chia sẻ thông tin đóng vai trò quan trọng trong việc nâng cao nhận thức cộng đồng và chia sẻ các biện pháp hiệu quả để ngăn chặn ransomware.



1 Nâng cao nhận thức

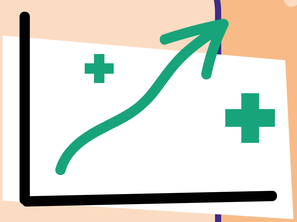
Nhận thức của cộng đồng về ransomware được nâng cao thông qua việc chia sẻ kiến thức.

2 Cung cấp thông tin cần thiết

Các chuyên gia và thành viên tâm huyết ở trong nhóm có thể chia sẻ thông tin và kinh nghiệm tìm kiếm những giải pháp phù hợp với nhu cầu cụ thể của từng cá nhân trong nhóm.

3 Đóng góp vào sự cải thiện của từng thành viên

Chia sẻ thông tin trong nhóm với nhau giúp mọi người thực hiện các biện pháp bảo mật tốt hơn. Các lời khuyên cũng được cá nhân hóa, phù hợp với hoàn cảnh từng thành viên trong nhóm.

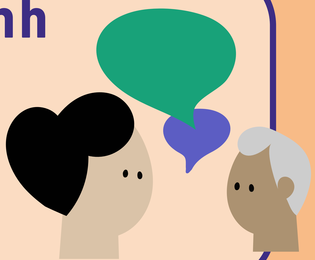


4 Cập nhật thông tin

Bằng cách chia sẻ các sự cố tấn công ransomware gần đây nhất, các nhóm chia sẻ thông tin có thể thông báo cho thành viên để thực hiện các biện pháp ngăn chặn hiệu quả.

5 Tăng cường an ninh của tổ chức

Bằng cách chia sẻ kiến thức thực tiễn và giải pháp an ninh mạng hiệu quả nhất, an ninh tổng thể của tổ chức sẽ được đẩy mạnh.



UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

BẤT KỲ AI CŨNG CÓ THỂ LÀ NẠN NHÂN CỦA RANSOMWARE

Cùng với sự phát triển của công nghệ và tiến bộ kỹ thuật số là sự gia tăng của các cuộc tấn công mã độc tống tiền (ransomware). Tội phạm mạng này nhắm đến người dùng ở mọi ngành nghề - bất kỳ ai cũng có thể trở thành nạn nhân của ransomware.

NGÀNH Y TẾ

Đối với các cơ sở y tế, một cuộc tấn công ransomware có thể là mối nguy hiểm lớn, dẫn đến sự cố đe dọa mạng sống của nhiều bệnh nhân và khách hàng. Lý do là vì các cơ sở y tế và bệnh viện lưu trữ nguồn thông tin quan trọng của rất nhiều bệnh nhân và nhân viên.

NGÀNH GIÁO DỤC

Do ngân sách hạn chế, phòng Công nghệ thông tin (CNTT) ở hầu hết các cơ sở giáo dục có quy mô nhỏ hơn so với phòng CNTT của một doanh nghiệp. Điều này khiến trường học dễ bị tấn công bởi ransomware, vì phòng ban nhỏ nhưng lại phải quản lý một số lượng lớn tập file được chia sẻ trực tuyến.

DOANH NGHIỆP VỪA VÀ NHỎ (SMEs)

Các doanh nghiệp vừa và nhỏ thường phân bổ ít nguồn lực hơn cho việc bảo vệ an ninh mạng do ngân sách hạn chế và quan niệm sai lầm rằng doanh nghiệp nhỏ sẽ không trở thành mục tiêu của tội phạm trên không gian ảo.

NGÀNH LUẬT

Các cơ quan pháp luật được coi là "con mồi béo bở" của ransomware vì lưu trữ vô số dữ liệu mật, bao gồm cả thông tin liên quan đến an ninh quốc gia và tình hình quốc tế.

NGÀNH TÀI CHÍNH

Bản chất của lĩnh vực tài chính là công việc liên quan đến xử lý thông tin cá nhân của khách hàng, ví dụ như số thẻ tín dụng, số an sinh xã hội, thông tin liên hệ, v.v. khiến ngành này trở thành mục tiêu hoàn hảo cho tội phạm trên không gian ảo.

Và còn nhiều ngành nghề khác nữa!

References

1. Martin, J. A. (2017, July 14). Who is a target for ransomware attacks? CSO Online. Retrieved November 22, 2021, from https://www.csoonline.com/article/3208111/who-is-a-target-for-ransomware-attacks.html.
2. Who is a target for ransomware attacks? Cyber Security Solutions, Compliance, and Consulting Services - IT Security. (2019, October 21). Retrieved November 22, 2021, from https://www.infoguardsecurity.com/who-is-a-target-for-ransomware-attacks/.
3. Irei, A. (2021, September 29). Top 10 ransomware targets in 2021 and Beyond. SearchSecurity. Retrieved November 22, 2021, from https://www.techtarget.com/searchsecurity/feature/Top-10-ransomware-targets-in-2021-and-beyond.

UNODC United Nations Office on Drugs and Crime | CYBERCRIME | From the People of Japan | RansomAware

DANH SÁCH KIỂM TRA AN TOÀN CÁ NHÂN

ĐỂ BẢO VỆ BẠN KHỎI MÃ ĐỘC TỐNG TIỀN VÀ CÁC CUỘC TẤN CÔNG TRÊN MẠNG

Mã độc tống tiền (ransomware) là một loại phần mềm độc hại xâm nhập làm khóa máy cho đến khi người dùng trả một khoản tiền để lấy lại dữ liệu. Dịch bệnh COVID-19 đã và đang khiến nhiều người lựa chọn làm việc từ xa, kết quả là số lượng cuộc tấn công ransomware đã tăng 148% (AFCEA, 2021).

Dưới đây là một số điều cần làm để bảo vệ bạn khỏi mối đe dọa an ninh mạng trong thời gian giãn cách xã hội.

BẢO MẬT DỮ LIỆU RIÊNG TƯ

Bạn cần thận trọng khi chia sẻ thông tin cá nhân của mình trên mạng xã hội, ví dụ như họ tên, số CMND/CCCD, thông tin về tài khoản ngân hàng, v.v.

CẢNH GIÁC CAO ĐỘ

Tạo nhiều lớp hàng rào bảo mật là một cách để bảo vệ máy tính của bạn. Bạn có thể sử dụng mã bảo mật hai yếu tố, tạo mật khẩu mạnh, cài đặt tường lửa và tải chương trình chống vi-rút.

THƯỜNG XUYÊN SAO LƯU DỮ LIỆU

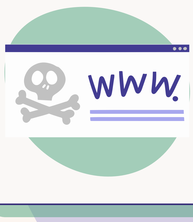
Sao lưu dữ liệu dự phòng là tạo bản sao trên ổ cứng ngoài hoặc trên bộ nhớ đám mây. Hãy thường xuyên cập nhật bản sao lưu mới nhất để đảm bảo bạn luôn có sẵn thông tin cần thiết nhé.

CẬP NHẬT PHẦN MỀM

Việc cập nhật phần mềm mới nhất cho hệ thống và chương trình vận hành của bạn là rất quan trọng. Các phiên bản cập nhật sẽ bảo vệ thiết bị của bạn trước nguy cơ xảy ra một cuộc tấn công an ninh mạng mới.

TẠO MẬT KHẨU MẠNH

Một mật khẩu mạnh cần có 8 kí tự, có đầy đủ chữ số, chữ in hoa và ký tự đặc biệt. Mật khẩu không nên sử dụng thông tin cá nhân của bạn như ngày sinh nhật hoặc địa chỉ email. Bạn cũng nên tạo mật khẩu khác nhau cho từng tài khoản nhé.



TRÁNH TRUY CẬP VÀO CÁC TRANG WEB ĐÁNG NGỜ

Mở một email, tập file hoặc trang web đáng ngờ là một trong những cách phổ biến nhất để "mời gọi" một cuộc tấn công ransomware. Tránh nhấp vào những liên kết bạn không biết rõ để không trở thành nạn nhân của tội phạm trên không gian ảo nhé.

References

- Security National Bank of South Dakota. (n.d.). Internet Safety Tips For Everyone Who Spends Time Online. Blue Compass, Des Moines, Iowa, www.Bluecompass.Com. https://www.snbsd.com/about/online-safety-guide
- Datto's 2019 State of the MSP Report. (2021, October 25). Datto. https://www.datto.com/resources/dattos-2019-state-of-the-msp-report
- Kaspersky. (2021, July 12). Ransomware protection: how to keep your data safe in 2021. Usa.Kaspersky.Com. https://usa.kaspersky.com/resource-center/threats/how-to-prevent-ransomware

UNODC United Nations Office on Drugs and Crime

CYBERCRIME

From the People of Japan

RansomAware

CHECKLIST
CÁC QUY ĐỊNH AN TOÀN CHO DOANH NGHIỆP

Lây nhiễm phần mềm độc hại có thể gây tổn hại đến doanh nghiệp, và quá trình khôi phục dữ liệu quan trọng cũng không phải dễ dàng. Việc này thường yêu cầu dịch vụ từ các chuyên gia khôi phục dữ liệu.

Do đó, người dùng và quản trị viên nên thực hiện các biện pháp phòng chống dưới đây để bảo vệ hệ thống máy tính khỏi lây nhiễm mã độc tống tiền (ransomware).

1 XÁC ĐỊNH TÀI SẢN

Xác định tài sản của doanh nghiệp, chẳng hạn như những thiết bị, dữ liệu và ứng dụng quan trọng có thể trở thành mục tiêu của kẻ tấn công ransomware.

2 SAO LƯU & PHỤC HỒI

Thường xuyên thực hiện và kiểm tra bản sao lưu để giảm thiểu thiệt hại do tổn thất hệ thống hoặc dữ liệu, đồng thời giúp cải thiện tốc độ khôi phục dữ liệu trong tương lai.

Bản sao lưu kết nối toàn hệ thống cũng có thể bị ảnh hưởng bởi ransomware. Do đó, các bản sao lưu quan trọng nên được tách riêng khỏi hệ thống để được bảo vệ một cách tốt nhất.

3 HỆ THỐNG VẬN HÀNH VÀ PHẦN MỀM

Luôn cập nhật phiên bản mới nhất cho hệ điều hành và phần mềm trong máy tính. Các ứng dụng và hệ điều hành dễ bị tấn công sẽ làm tăng nguy cơ lây nhiễm phần mềm độc hại.

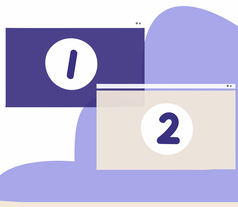
4 PHẦN MỀM CHỐNG VI-RÚT

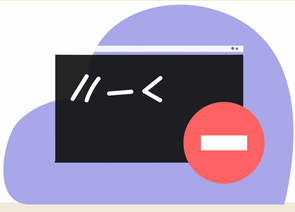
Duy trì phần mềm chống vi-rút mới nhất và kiểm tra tất cả phần mềm được tải xuống từ mạng Internet trước khi chạy và sử dụng trên máy tính.

5 HẠN CHẾ HOẠT ĐỘNG CỦA NGƯỜI DÙNG

Hạn chế khả năng cài đặt và chạy phần mềm không mong muốn của người dùng trên máy tính.

Áp dụng nguyên tắc "Đặc quyền tối thiểu" cho tất cả các hệ thống và dịch vụ để ngăn chặn hoặc hạn chế ảnh hưởng của phần mềm độc hại.





6 TẮT MACRO

Trong tệp đính kèm ở email, tránh bật macro - một mật mã đặc biệt thay thế cho thông tin cụ thể. Việc mở tệp đính kèm và bật macro cùng lúc sẽ khiến mã nhúng tạo ra phần mềm độc hại trên máy tính.

7 LIÊN KẾT KHÔNG ĐƯỢC YÊU CẦU

Tránh nhấp vào những liên kết website không được yêu cầu ở trong email. Tham khảo thêm thông tin về các nguồn giả mạo trên mạng mà có thể vô tình gây tổn hại cho doanh nghiệp.

Xin lưu ý rằng trên đây chỉ là một số biện pháp giúp doanh nghiệp của bạn bảo vệ dữ liệu quan trọng của mình khỏi ransomware và các mối đe dọa an ninh mạng.

Đối với những vấn đề phức tạp hơn, bạn nên tìm lời khuyên trực tiếp từ các chuyên gia Công nghệ thông tin.

References

- National Institute of Standards and Technology (NIST). (2020b, October 1). Securing Data Integrity Against Ransomware Attacks: Using the NIST Cybersecurity Framework and NIST Cybersecurity Practice Guides. NIST. https://miro.com/app/board/o9J_lOAZb0=/?moveToWidget=3074457388175839345&cot=14
- National Institute of Standards and Technology (NIST). (n.d.). Ransomware Protection and Response. NIST Computer Security Resource Center | CSRC. Retrieved October 20, 2021, from https://csrc.nist.gov/projects/ransomware-protection-and-response
- Australian Government. (n.d.). What to do if you're held to ransom: Step 6: Notify and report. ACSC. https://www.cyber.gov.au/ransomware/step-6-notify-and-report
- What Do I Do To Protect Against Ransomware? https://security.berkeley.edu/faq/ransomware/what-do-i-do-protect-against-ransomware

UNODC United Nations Office on Drugs and Crime | CYBERCRIME | From the People of Japan | RansomAware

CHECKLIST

NHỮNG QUY ĐỊNH AN TOÀN GIỮA CÁC DOANH NGHIỆP

Khi doanh nghiệp làm việc với nhiều nền văn hóa khác nhau, thì cũng là lúc vấn đề đảm bảo an ninh trên không gian mạng trở nên thách thức hơn.

Do vậy, quy định an toàn giữa các doanh nghiệp cần được thực hiện để đảm bảo không xảy ra các cuộc tấn công an ninh mạng trong quá trình trao đổi liên doanh nghiệp.

Bạn nên thực hiện các biện pháp phòng chống dưới đây để ngăn mã độc tống tiền (ransomware) tấn công trong quá trình hợp tác giữa các doanh nghiệp.

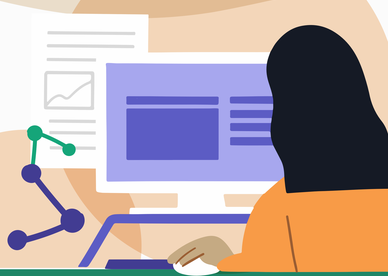
THIẾT LẬP QUY ĐỊNH DOANH NGHIỆP CHUNG

Đối với các doanh nghiệp thường xuyên chia sẻ hoặc trao đổi thông tin, thiết lập một số quy định chung là điều cần thiết.

Quy định này bao gồm, nhưng không giới hạn, các giao thức an toàn chung cho người dùng và doanh nghiệp, chính sách chung về sử dụng mạng Internet và email, cũng như thống nhất về hệ thống báo cáo và bảo mật.

GIÁM SÁT HỆ THỐNG

Dù hoạt động dưới hình thức nào, doanh nghiệp cũng cần chọn hệ thống bảo mật nhất định để theo dõi các hoạt động đáng ngờ và có nguy cơ dẫn đến một cuộc tấn công ransomware.

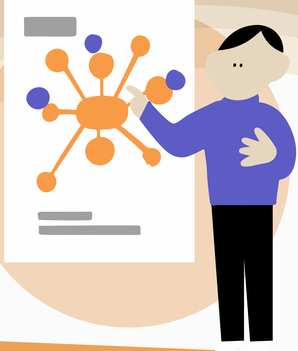


SỬ DỤNG TRI THỨC AN NINH MẠNG

Tất cả các doanh nghiệp trao đổi thông tin với nhau cần cập nhật thông tin mới nhất về những mối đe dọa an ninh mạng cho nhân viên của mình và dự đoán rủi ro có thể ảnh hưởng đến doanh nghiệp hoặc các đối tác trong cùng ngành hoặc khu vực.

TRÁNH CHIA SẺ THÔNG TIN RIÊNG TƯ

Để ngăn chặn rò rỉ dữ liệu, doanh nghiệp nên chọn lọc trong việc cung cấp thông tin cá nhân hoặc chia sẻ tài khoản, dù cho đã có thỏa thuận của hai bên.



TỔ CHỨC ĐÀO TẠO VÀ NÂNG CAO NHẬN THỨC VỀ AN NINH MẠNG

Các doanh nghiệp có thể cùng nhau tổ chức những buổi tập huấn đào tạo cho nhân viên để đảm bảo mọi người có cùng mức độ nhận thức, hiểu biết về mối đe dọa an ninh mạng và các phương pháp phòng chống.

Xin lưu ý rằng trên đây chỉ là một số biện pháp giúp doanh nghiệp của bạn bảo vệ dữ liệu quan trọng của mình khỏi ransomware và các mối đe dọa an ninh mạng.

Đối với những vấn đề phức tạp hơn, bạn nên tìm lời khuyên trực tiếp từ các chuyên gia Công nghệ thông tin.

References

- Bisson, D. (2020, October 5). 30 Ransomware Prevention Tips. The State of Security. https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/22-ransomware-prevention-tips/
- Check Point software technologies LTD. (n.d.). Why Anti-Ransomware? : Sophisticated, Evasive, Disruptive. Check Point. https://www.checkpoint.com/harmony/anti-ransomware/
- Kaspersky. (2021). Ransomware protection: how to keep your data safe in 2021. https://usa.kaspersky.com/resource-center/threats/how-to-prevent-ransomware

UNODC United Nations Office on Drugs and Crime | CYBERCRIME | From the People of Japan | RansomAware

VAI TRÒ CỦA CHÍNH PHỦ TRONG VIỆC PHÁT TRIỂN MÔ HÌNH AN NINH MẠNG

TẠO NỀN TẢNG VỮNG CHẮC

Chính phủ đóng vai trò quan trọng trong việc thiết lập, duy trì một mô hình an ninh mạng toàn diện và hợp pháp dựa trên các chính sách an ninh mạng quốc gia.

Hệ thống này cần được xây dựng dựa trên các nguyên tắc chính như dưới đây.

Dựa trên rủi ro và ưu tiên

Các mối đe dọa trên không gian ảo đang liên tục thay đổi. Việc thiết lập hệ thống phân cấp ưu tiên đối với các tài sản hoặc lĩnh vực quan trọng là bước đầu hiệu quả.

Công nghệ trung tính

Phương pháp tiếp cận công nghệ trung tính đảm bảo việc tiếp cận được các giải pháp hiệu quả nhất trên thị trường.

Chính sách yêu cầu sử dụng một số công nghệ nhất định có thể làm hạn chế sự phát triển của một số phương pháp hiệu quả khác.

Thực tiễn

Bất kỳ chiến lược nào cũng chỉ hiệu quả khi được thực hiện trên phạm vi rộng.

Chính phủ giám sát các doanh nghiệp tư nhân quá mức có thể gây phản tác dụng, dẫn đến việc tập trung quá nhiều vào việc tuân thủ chính sách.

Linh hoạt

Không có phương pháp nào có thể áp dụng để quản lý tất cả rủi ro trên không gian mạng. Mỗi doanh nghiệp phải đối mặt với những thách thức riêng và đòi hỏi sự linh hoạt để giải quyết các nhu cầu của mình.

Tôn trọng quyền riêng tư và quyền tự do cá nhân

Các yêu cầu bảo mật cần được cân bằng với nhu cầu bảo vệ quyền riêng tư và quyền tự do cá nhân.

Đảm bảo rằng các yêu cầu này không xâm phạm đến các quyền cơ bản của người dùng.

THÀNH LẬP CÁC TỔ CHỨC BẢO MẬT

Chính phủ nên thành lập các tổ chức hoạt động để ngăn chặn tội phạm mạng, ví dụ như các nhóm ứng cứu bảo mật máy tính.

2 1 3

TẠO SỰ TIN TƯỞNG VÀ HỢP TÁC LÀM VIỆC

Không một quốc gia hoặc chính phủ nào có thể giải quyết rủi ro về an ninh mạng một mình.

Hợp tác với các tổ chức phi chính phủ và các đối tác quốc tế là một cách tối ưu để đảm bảo an ninh mạng hiệu quả.

Hợp tác với khối doanh nghiệp tư nhân

Hầu hết các cơ sở hạ tầng thuộc sở hữu của khối tư nhân, nên việc hợp tác giữa khối nhà nước và tư nhân là điều cần thiết.

Hợp tác góp phần nâng cao quản lý rủi ro, củng cố lòng tin và tránh các trở ngại pháp lý.

Toàn cầu hóa thay vì cô lập

Các chính sách và chiến lược an ninh mạng hiệu quả sẽ cần duy trì các mối quan hệ hợp tác toàn cầu.

Mô hình cần duy trì các tiêu chuẩn quốc tế, tự nguyện và theo định hướng thị trường để tối đa hóa việc chia sẻ và bảo vệ thông tin trên toàn cầu.

TUYÊN TRUYỀN GIÁO DỤC NHẬN THỨC VỀ RỦI RO AN NINH MẠNG

Con người, quy trình và công nghệ là những yếu tố cần thiết trong việc đảm bảo an ninh mạng. Các chính phủ cần nâng cao nhận thức, tổ chức giáo dục và đào tạo về các ưu tiên, chính sách cũng như chương trình an ninh mạng như một phần quan trọng của các chiến lược an ninh mạng.

Citation

- National Institute of Standards and Technology. (2021, May 13). NIST Releases Tips and Tactics for Dealing With Ransomware. NIST. https://www.nist.gov/news-events/news/2021/05/nist-releases-tips-and-tactics-dealing-ransomware
- United States Secret Service. (n.d.). Preparing for a Cyber Incident. Secretservice.Gov. https://www.secretservice.gov/investigation/Preparing-for-a-Cyber-Incident
- Asia-pacific Cybersecurity Dashboard: Summary: Bsa: The Software Alliance BSA Alliance – https://cybersecurity.bsa.org/2015/apac/

UNODC United Nations Office on Drugs and Crime

CYBERCRIME

From the People of Japan

RansomAware

ĐIỂM LẠI CÁC CUỘC TẤN CÔNG RANSOMWARE NGHIÊM TRỌNG

Ở KHU VỰC CHÂU Á – THÁI BÌNH DƯƠNG

Một báo cáo[1] tiết lộ khu vực châu Á – Thái Bình Dương có tỉ lệ trung bình gặp phải các cuộc tấn công ransomware cao gấp 1,7 lần so với phần còn lại của thế giới.

Dưới đây là những sự cố nghiêm trọng nhất trong năm 2020 và năm 2021.

[1] Microsoft

2020

ẤN ĐỘ

74% doanh nghiệp ở Ấn Độ là nạn nhân của các cuộc tấn công ransomware, với 1/3 trong số đó đã trả hacker con số tiền chuộc từ 1 triệu đến 2,5 triệu đô la Mỹ (khoảng 23 tỷ đến 57 tỷ Việt Nam đồng).

05/09/2020

THÁI LAN

Một bệnh viện ở Thái Lan[2] đã không thể truy cập dữ liệu của mình do bị ransomware tấn công, tuy nhiên không có yêu cầu thanh toán nào được gửi tới bệnh viện này.

Tuy nhiên, một số doanh nghiệp khác đã bị buộc phải trả đến 1 triệu baht tiền chuộc (khoảng 32.000 đô la Mỹ) để khôi phục dữ liệu.

[2] Bệnh viện Saraburi

THÁNG 4-12/2020

NHẬT BẢN

Vào năm ngoái, Nhật Bản đã phải đối mặt với nhiều cuộc tấn công ransomware mà Cơ quan Cảnh sát Quốc gia mô tả là "rất nghiêm trọng".

Các tập đoàn ở Nhật Bản báo cáo đã có tới 93 vụ lây nhiễm ransomware trong năm 2020, tăng 80% so với năm trước đó.

31/10/2020

INDONESIA

Thông tin của 2,9 triệu thành viên thuộc một công ty khởi nghiệp công nghệ tài chính[3] đã bị đánh cắp và rao bán trên một diễn đàn hacker.

Thông tin này bao gồm họ tên đầy đủ, địa chỉ email, số điện thoại, tài khoản ngân hàng cũng như mã số thuế và số CMND của các thành viên.

[3] Công ty khởi nghiệp công nghệ tài chính Cermati

THÁNG 9/2020

MALAYSIA

Một công ty dịch vụ lưu trữ dữ liệu ở Malaysia đã trở thành mục tiêu tấn công của ransomware.

Thủ phạm đã yêu cầu công ty này trả 900.000 đô la Mỹ (hơn 20 tỷ Việt Nam đồng) bằng tiền mã hóa.

THÁNG 5/2020

HỒNG KÔNG

Công ty con của một công ty bảo hiểm quốc tế ở Hồng Kông đã bị tấn công bởi ransomware, trong đó hacker yêu cầu một khoản tiền chuộc là 20 triệu đô la Mỹ (tương đương 455 tỷ Việt Nam đồng).

THÁNG 5/2020

PHILIPPINES

Công ty con của một tập đoàn bảo hiểm quốc tế hoạt động tại Philippines đã bị tội phạm mạng yêu cầu trả 20 triệu đô la Mỹ (tương đương 455 tỷ Việt Nam đồng) tiền chuộc.

References

- Ransomware attacks, a growing threat that needs to be countered. (n.d.). Www.unodc.org. https://www.unodc.org/southeastasiaandpacific/en/2021/10/cybercrime-ransomware-attacks/story.html
- Timeline of Cyber Incidents Involving Financial Institutions. (2016). Carnegie Endowment for International Peace. https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline
- Asia Pacific cyber incidents in 2020 hold big implications for this year's cyber insurance market | Munich Re Topics Online. (n.d.). Munichre.com. https://www.munichre.com/topics-online/en/digitalisation cyber/asia-pacific-cyber-incidents-in-2020.html ;
- Thai hospitals and companies hit by ransomware attacks. (2020, September 10). Reuters. https://www.reuters.com/article/us-thailand-hospital-ransomware/thai-hospitals-and-companies-hit-by-ransomware-attacks-idUSKBN2611WV ;
- Huge rise in ransomware cyberattacks on Japan firms an extreme threat: police. (2021, March 4). Mainichi Daily News. https://mainichi.jp/english/articles/20210304/p2a/00m/0na/020000c

UNODC United Nations Office on Drugs and Crime

CYBERCRIME

From the People of Japan

RansomAware

TRƯỜNG HỢP VỀ CÁC DOANH NGHIỆP NHÀ NƯỚC VÀ TƯ NHÂN

THÁI LAN
THÁNG 9/2020

BỆNH VIỆN, DOANH NGHIỆP NHÀ NƯỚC

TRƯỜNG HỢP 1

CÁC BỆNH VIỆN Ở THÁI LAN KHÔNG THỂ TRUY CẬP VÀO DỮ LIỆU DO BỊ HACKER TẤN CÔNG

Tóm tắt:

Các bệnh viện ở Thái Lan đã bị tấn công và đòi tiền chuộc bởi một mã độc ransomware.

Vào ngày 05/09, cuộc tấn công đã khiến một bệnh viện[3] không thể truy cập vào dữ liệu của mình, dẫn đến nhiều thiệt hại gây nguy hiểm đến tính mạng của bệnh nhân, đồng thời làm ngưng trệ các hoạt động hàng ngày do bệnh viện chỉ có thể duy trì vận hành một cách thủ công.

[3] Bệnh viện Saraburi

ĐÀI LOAN
THÁNG 3/2021

TẬP ĐOÀN SẢN XUẤT MÁY TÍNH, DOANH NGHIỆP TƯ NHÂN

TRƯỜNG HỢP 2

ACER BỊ TỐNG TIỀN ĐẾN 100 TRIỆU ĐÔ LA MỸ SAU KHI HACKER TẤN CÔNG VÀO HỆ THỐNG

Tóm tắt:

Nhóm ransomware REvil đã đánh cắp một lượng lớn thông tin nhạy cảm từ hệ thống của Acer. Các thông tin này được bán đấu giá trên Dark Web đến khi Acer đồng ý thanh toán khoản tiền chuộc được yêu cầu.

ÚC
THÁNG 6/2021

TẬP ĐOÀN CHẾ BIẾN THỰC PHẨM, DOANH NGHIỆP TƯ NHÂN

TRƯỜNG HỢP 3

JBS, TẬP ĐOÀN CHẾ BIẾN THỊT LỚN NHẤT THẾ GIỚI TẠM DỪNG HOẠT ĐỘNG

Tóm tắt:

Tập đoàn chế biến thịt hàng đầu thế giới[4] đã phải dừng hoạt động tại nhiều cơ sở trên khắp các châu lục cho đến khi chấp nhận thanh toán cho hacker khoản tiền 11 triệu đô (khoảng 7,8 triệu bảng Anh).

[4] JBS

Các đối tác liên quan bình luận rằng:

Công ty[4] cho rằng việc thanh toán là cần thiết để bảo vệ khách hàng, và thực tế là JBS đã trả tiền bởi sự phức tạp của cuộc tấn công, mặc dù "phần lớn" các cơ sở nhà máy vẫn hoạt động bình thường.

[4] JBS

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

TRƯỜNG HỢP VỀ DOANH NGHIỆP NHỎ VÀ NGƯỜI DÙNG CÁ NHÂN

SINGAPORE THÁNG 8/2020

- NGÀNH NHÀ HÀNG, ẨM THỰC

Tóm tắt:
Một doanh nghiệp kinh doanh nhà hàng và đồ uống đã phát hiện máy chủ của mình bị nhiễm ransomware NetWalker, khiến hệ thống công ty bị dẫn đến một Dark Web để đòi tiền chuộc.

Tất cả dữ liệu đã bị mất vì các bản sao lưu được lưu trữ trên máy chủ đã bị tấn công, dẫn đến việc doanh nghiệp này phải xây dựng hệ thống IT lại từ đầu.

Kết luận:
Câu chuyện này cho thấy các doanh nghiệp nhỏ thường thiếu kinh nghiệm hoặc hệ thống bảo mật để có thể ngăn chặn và giảm thiểu thiệt hại của các cuộc tấn công ransomware.

THÁI LAN, THÁNG 7/2019

- NGƯỜI DÙNG

Phân loại:
Người dùng cá nhân

Tóm tắt:
Một người dùng Facebook ở Thái Lan báo cáo rằng máy tính của mình bị nhiễm ransomware. Một lá thư từ tin tặc tiết lộ rằng một nửa số dữ liệu của công ty đã bị mã hóa và yêu cầu 6.500 đô la Bitcoin tiền chuộc để nạn nhân khôi phục các tập file bị đánh cắp.

Kết luận:
Trường hợp này cho thấy ai cũng có thể trở thành nạn nhân của các vụ tấn công trên không gian mạng. Bất kỳ người dùng cá nhân hay doanh nghiệp nào sử dụng máy tính để quản lý dữ liệu đều có thể gặp rủi ro.

VIỆT NAM, THÁNG 4/2018

- CÔNG TY IT

Phân loại:
Doanh nghiệp nhỏ

Tóm tắt:
Bộ phận IT của một công ty tại Thành phố Hồ Chí Minh đã thông báo cho nhân viên IT[5]của mình về sự lây lan của vi rút ransomware có tên GandCrab được cảnh báo bởi Nhóm Ứng cứu Khẩn cấp Máy tính Việt Nam.

Rất may mắn là công ty không gặp thiệt hại nào vì đã được thông báo trước về loại ransomware này.

[5]Kim Ngọc

Kết luận:
Trường hợp này5 cho thấy việc sở hữu các cơ chế ngăn chặn hiệu quả sẽ làm giảm nguy cơ cũng như thiệt hại của các cuộc tấn công ransomware.

[5]Kim Ngọc

References

- How ransomware is a big problem for small business – and what to do about it. (n.d.). Insureon. https://www.insureon.com/blog/how-ransomware-is-a-big-problem-for-small-business
- T. (2019, July 13). โจรไซเบอร์ส่ง "ไวรัสเรียกค่าไถ่" ป่วนออฟฟิศ ยิบเหยื่อจ่ายเงินแลกปลดล็อก. www.thairath.co.th. https://www.thairath.co.th/news/society/1614458
- Van Anh Vietnam Investment Review. (2018, April 7). Ransomware GandCrab attacks Vietnam. Vietnam Investment Review - VIR. https://vir.com.vn/ransomware-gandcrab-attacks-vietnam-58065.html
- Yu, E. (2021, July 8). Singapore sees spikes in ransomware, botnet attacks. ZDNet. https://www.zdnet.com/article/singapore-sees-spikes-in-ransomware-botnet-attacks/

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

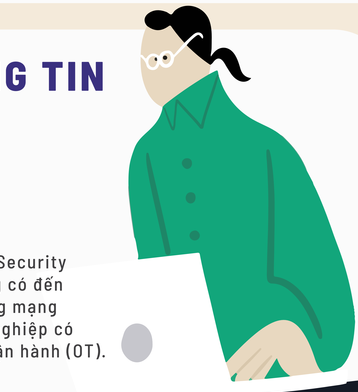
MỘT SỐ NGÀNH DỄ TRỞ THÀNH MỤC TIÊU CỦA MÃ ĐỘC TỐNG TIỀN (RANSOMWARE)

NGÀNH Y TẾ

Sự xuất hiện của đại dịch COVID-19 đã biến các cơ sở y tế trở thành mục tiêu hấp dẫn của tội phạm trên không gian ảo.

Ngành Y tế bao gồm các bệnh viện và trung tâm xét nghiệm điều trị và cứu sống bệnh nhân COVID-19.

NGÀNH CÔNG NGHỆ THÔNG TIN



Dịch bệnh cũng ảnh hưởng đến ngành Công nghệ thông tin do nhiều công ty đã chuyển sang hình thức làm việc từ xa.

Hình thức mới này giúp kẻ tấn công dễ dàng khai thác các lỗ hổng công nghệ thông tin và tìm được mục tiêu ransomware.

Trong năm 2020, IBM Security X-Force cho thấy rằng có đến 41% các cuộc tấn công mạng nhắm vào các doanh nghiệp có hệ thống công nghệ vận hành (OT).

NGÀNH BÁN LẺ

Nhu cầu mua sắm trực tuyến tăng cao đã làm gia tăng những thách thức bảo mật hiện có mà lĩnh vực bán lẻ phải đối mặt.

Bản chất của doanh nghiệp bán lẻ là nắm giữ nhiều thông tin nhạy cảm của khách hàng, bao gồm họ tên, địa chỉ và thông tin tài chính.

NGÀNH GIÁO DỤC

Nhiều trường học trên khắp thế giới buộc phải chuyển sang hình thức dạy học trực tuyến trong bối cảnh của dịch bệnh COVID-19.
Do áp lực phải đảm bảo việc dạy học diễn ra thường xuyên liên tục, ngành Giáo dục dễ rơi vào tình huống "nhắm mắt" trả tiền chuộc trong trường hợp bị tấn công bởi tội phạm trên không gian ảo.

Ngành Giáo dục thường có ngân sách eo hẹp cho vấn đề liên quan đến công nghệ và an ninh mạng.
Cùng với đó, nhân viên IT phải đảm bảo an ninh cho một hệ thống lỗi thời bằng nguồn tài nguyên và công cụ khá hạn chế, chẳng hạn qua việc phải tải các phần mềm đã cũ.

CÁC CƠ QUAN CHÍNH PHỦ

Các cơ quan chính phủ và cơ sở hạ tầng dễ bị tấn công bởi ransomware vì bản chất công việc nhạy cảm về thời gian và mang tính chiến lược đối với khu vực.

Các cơ quan này phải đối phó nhanh với mọi trường hợp khẩn cấp. Trong quá trình khôi phục dữ liệu, họ cũng sẽ sẵn sàng trả tiền chuộc hơn và hoàn thành việc thanh toán nhanh hơn.

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

XU HƯỚNG AN NINH MẠNG KHU VỰC CHÂU Á – THÁI BÌNH DƯƠNG

Giải pháp an ninh mạng giúp người dùng và doanh nghiệp duy trì việc bảo mật dữ liệu bằng cách phát hiện, giám sát, báo cáo và xử lý các mối đe dọa trên mạng.

Dưới đây là tổng quan về xu hướng an ninh mạng trong giai đoạn 2000-2021.

CÁC GIẢI PHÁP AN NINH MẠNG ĐƯỢC ÁP DỤNG

Các giải pháp an ninh mạng sẽ được áp dụng nhiều hơn trong bối cảnh Internet phủ sóng mạnh mẽ ở các nước đã và đang phát triển.

SỰ GIA TĂNG CÁC VẤN ĐỀ VỀ AN NINH MẠNG

Nhiều quốc gia châu Á đang gặp phải nhiều vấn đề liên quan đến an ninh mạng hơn.

Theo một báo cáo của công ty an ninh quốc tế,[1] Ấn Độ là quốc gia chiếm 37% các vụ vi phạm trên thế giới xét về yếu tố hồ sơ bị xâm phạm hoặc bị đánh cắp.

[1]Gemalto

THỊ TRƯỜNG AN NINH MẠNG KHU VỰC CHÂU Á – THÁI BÌNH DƯƠNG ĐƯỢC KỲ VỌNG TĂNG TRƯỞNG MẠNH

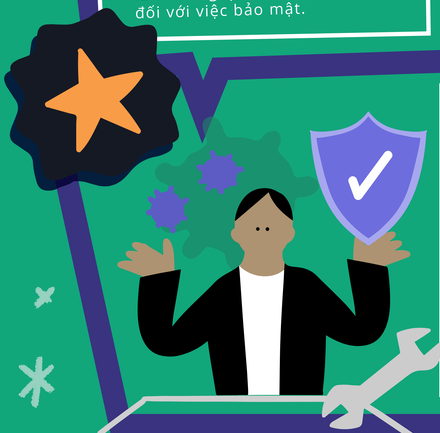
Số lượng vụ tấn công mạng do mã độc tống tiền (ransomware) gây ra đã gia tăng trong thời điểm dịch, khi các doanh nghiệp chuyển sang hình thức làm việc từ xa.

Một nghiên cứu[2] tiết lộ rằng có khoảng 19 triệu vụ tấn công ransomware và tấn công giả mạo liên quan đến COVID-19 đã được phát hiện ở châu Á, chỉ tính riêng trong năm 2020.

[2]Microsoft

MÁY CHỦ ĐÁM MÂY ĐƯỢC SỬ DỤNG NHIỀU HƠN

Việc gia tăng sử dụng máy chủ đám mây trở thành điểm nóng cho các cuộc tấn công mạng khi mọi người dần chuyển sang làm việc trong môi trường lạ và kém an toàn.
Do đó, giải pháp an ninh mạng dựa trên điện toán đám mây là vô cùng quan trọng đối với việc bảo mật.



RANSOMWARE TRỞ NÊN PHÁT TRIỂN HƠN

Đi kèm với sự thay đổi của công nghệ là sự phát triển nhanh chóng của các mối đe dọa. Do đó, giải pháp an ninh mạng sẽ trở nên quan trọng hơn trong việc giúp doanh nghiệp phát hiện và chống lại các cuộc tấn công mạng.

Citation

- Lynett, M. (2015, November 25). A history of information security from past to present. Document Management | MES. https://blog.meslted.ca/a-history-of-information-security-from-past-to-present?hs_amp=true
- Asia-pacific Cybersecurity Market: 2021 - 26: Industry Share, Size, Growth - Mordor Intelligence https://www.mordorintelligence.com/industry-reports/asia-pacific-cyber-security-market
- The history of cyber security — Everything you ever wanted to know. (2021, June 10). SentinelOne. https://www.sentinelone.com/blog/history-of-cyber-security/
- A history of information security. (2019, June 27). IFSEC Global | Security and Fire News and Resources. https://www.ifsecglobal.com/cyber-security/a-history-of-information-security/

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

Các doanh nghiệp ở khu vực châu Á - Thái Bình Dương đã thật sự sẵn sàng đối đầu với các cuộc tấn công ransomware?

Các chuyên gia cho biết

KẾT QUẢ CHỈ SỐ BẢO VỆ DỮ LIỆU TOÀN CẦU (GDPI) TỪ DELL TECHNOLOGIES 2021

Doanh nghiệp phải đối mặt với nhiều thách thức trong việc bảo vệ dữ liệu thông qua công nghệ mới được phát triển như ứng dụng gốc đám mây, vùng chứa Kubernetes và trí tuệ nhân tạo (AI).

Ở khu vực châu Á - Thái Bình Dương, 82% những người đưa ra quyết định về Công nghệ thông tin lo ngại rằng các giải pháp bảo vệ dữ liệu hiện tại sẽ không giải quyết được tất cả khó khăn của doanh nghiệp trong tương lai.

BÁO CÁO TỪ SOPHOS - TỔ CHỨC BẢO MẬT CÔNG NGHỆ THÔNG TIN HÀNG ĐẦU

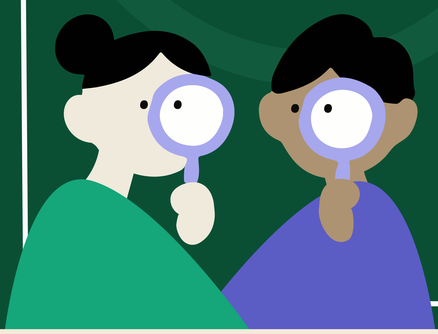
Dịch bệnh COVID-19 đã làm tăng các cuộc tấn công ransomware vào doanh nghiệp bán lẻ khi họ chuyển sang hình thức bán hàng trực tuyến để quảng cáo sản phẩm và dịch vụ của mình.

Một cuộc khảo sát bán lẻ[1] cho biết doanh nghiệp bán lẻ dễ bị ảnh hưởng bởi một xu hướng mới đang phát triển: tấn công tống tiền.

Tội phạm ransomware sẽ không mã hóa tập file mà đe dọa phát tán trên mạng thông tin chúng đánh cắp được trong trường hợp nếu nạn nhân không trả tiền chuộc.

[1] Khảo sát về "Trạng thái của Ransomware trong lĩnh vực Bán lẻ" của Sophos

GIÁM ĐỐC AN NINH KỸ THUẬT APJ TẠI VECTRA AI



Sự tiến hóa của ransomware là mối quan tâm hàng đầu ở khu vực châu Á - Thái Bình Dương. Vào năm 2021, các nhóm tội phạm trên không gian ảo đã thay đổi chiến thuật để hoạt động không chỉ dựa trên phần mềm độc hại tự động.

Sử dụng máy chủ đám mây sẽ cho phép kẻ tấn công truy cập để đòi tiền chuộc với tốc độ còn nhanh hơn so với thời gian 8-30 ngày như thông thường. Trên thực tế, những cuộc tấn công như vậy có thể chỉ cần một ngày để hoàn tất.

NHỮNG ĐIỀU CẦN LƯU Ý

Các doanh nghiệp thuộc khu vực châu Á – Thái Bình Dương cần thường xuyên tổ chức tập huấn về an ninh mạng cho nhân viên của mình.

Các thành viên điều hành cần nhận thức được những thiệt hại có thể xảy ra bởi các cuộc tấn công ransomware.

Diễn tập về sự cố ransomware là một biện pháp hiệu quả để từng cá nhân hiểu rõ vai trò của mình trong việc bảo vệ doanh nghiệp.

References

1. Accidental hero' halts ransomware attack and warns: This is not over. (2017, May 15). the Guardian. https://www.theguardian.com/technology/2017/may/13/accidental-hero-finds-kill-switch-to-stop-spread-of-ransomware-cyber-attack
2. Ransomware To Ransomops: Why Apac Enterprises Are Increasingly Vulnerable Cyber read-2021 Chris Fisher-November 18 - https://www.cpomagazine.com/cyber-security/ransomware-to-ransomops-why-apac-enterprises-are-increasingly-vulnerable/
3. Feiner, L. (n.d.). Amazon, Google and other tech companies join government effort to fight ransomware. CNBC. https://www.cnbc.com/2021/08/05/amazon-google-join-government-effort-to-fight-ransomware.html
4. Raj. (2021, September 16). Are Asian businesses really prepared to deal with ransomware attacks? Techwire Asia. https://techwireasia.com/2021/09/are-asian-businesses-really-prepared-to-deal-with-ransomware-attacks/

UNODC United Nations Office on Drugs and Crime
CYBERCRIME
From the People of Japan
RansomAware

CỘT MỐC QUAN TRỌNG LIÊN LIÊN QUAN ĐẾN MÃ ĐỘC TỐNG TIỀN (RANSOMWARE)

VÀ AN NINH MẠNG CỦA CƠ QUAN PHÒNG CHỐNG MA TÚY VÀ TỘI PHẠM CỦA LIÊN HỢP QUỐC (UNODC)

GIỚI THIỆU

UNODC đã và đang tích cực tham gia các hoạt động thúc đẩy nhận thức về ransomware và an ninh mạng ở khu vực châu Á - Thái Bình Dương.

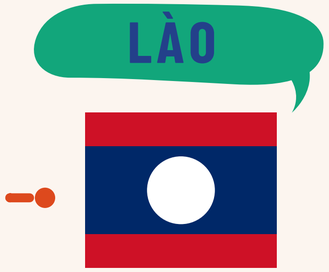
Tội phạm mạng đang tiếp tục phát triển trong khu vực, từ một mối đe dọa mới nổi nhanh chóng trở thành một mạng lưới tội phạm.

VIỆT NAM

- **Đông Hà, tỉnh Quảng Trị (Việt Nam), ngày 05/06/2015**

  Tổ chức tập huấn công nghệ cao cho các sĩ quan tiền tuyến Việt Nam.

  50 sĩ quan tiền tuyến đại diện cho Văn phòng Liên lạc Biên giới (BLO) và cơ quan hải quan, các chiến sĩ bộ đội biên phòng, cảnh sát phòng chống ma túy cùng các đơn vị kinh tế và môi trường khác đã xuất sắc hoàn thành khóa tập huấn chuyên sâu kéo dài 5 ngày.



LÀO

- **Viêng Chăn (Lào), ngày 20/08/2018**

  Lào và UNODC tổ chức hội nghị bàn tròn lần đầu tiên về tội phạm trên không gian ảo.

- **Viêng Chăn (Lào), ngày 23/08/2019**

  UNODC mở Phòng thí nghiệm chuyên về Pháp lý đầu tiên tại Lào, phục vụ cho công tác phân tích bằng chứng kỹ thuật số.

THÁI LAN

- **Băng Cốc (Thái Lan), ngày 31/07/2017**

  Thái Lan đẩy mạnh khả năng theo dõi và điều tra về tiền mã hóa.

- **Băng Cốc (Thái Lan), ngày 26/03/2018**

  UNODC và Thái Lan cùng nhau hợp tác đẩy lùi Tội phạm mạng ở khu vực Đông Nam Á.

- **Băng Cốc (Thái Lan), ngày 25/02/2021**

  UNODC đưa ra bản báo cáo "Mối đe dọa của tội phạm mạng Darknet đối với Đông Nam Á", bản phân tích đầu tiên thuộc thể loại này về các mối đe dọa darknet trong khu vực.

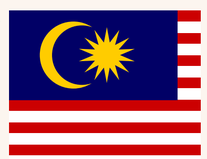
- **Băng Cốc (Thái Lan), ngày 05/07/2021**

  UNODC hợp tác với khối doanh nghiệp tư nhân để đào tạo các chuyên gia về an ninh mạng.

- **Băng Cốc (Thái Lan), ngày 18/10/2021**

  Được xác định là mối đe dọa ngày càng tăng, các cuộc tấn công ransomware cần phải bị đẩy lùi.

MALAYSIA



- **Langkawi (Malaysia), ngày 26/02/2019**

  UNODC thúc đẩy ASEAN tham gia hoạt động trong khu vực về hợp tác tình báo nhằm phát hiện mối đe dọa an ninh mạng để đẩy lùi tội phạm mạng và khủng bố.

UNODC United Nations Office on Drugs and Crime

CYBERCRIME

From the People of Japan

RansomAware

NĂM NGÀNH DỄ BỊ ẢNH HƯỞNG NHẤT BỞI RANSOMWARE Ở KHU VỰC CHÂU Á – THÁI BÌNH DƯƠNG

Trong thời điểm đại dịch COVID-19, tội phạm trên không gian ảo đã tăng 600% ở khu vực châu Á - Thái Bình Dương.

Trong số các cuộc tấn công trên không gian mạng, ransomware là phần mềm độc hại nhất đe dọa nhiều lĩnh vực khác nhau.

XẾP HẠNG	1.	2.	3.	4.	5.
PHÂN LOẠI NGÀNH	NGÀNH GIÁO DỤC	NGÀNH PHÂN PHỐI VÀ VẬN CHUYỂN	CÁC CƠ SỞ TÀI CHÍNH	DỊCH VỤ KINH DOANH VÀ CHĂM SÓC KHÁCH HÀNG	NGÀNH BÁN LẺ
CHI PHÍ PHỤC HỒI SAU MỘT CUỘC TẤN CÔNG RANSOMWARE (ĐƠN VỊ: triệu đô la Mỹ)	2,73 triệu đô la Mỹ (hơn 62 tỷ Việt Nam đồng)	2,44 triệu đô la Mỹ (hơn 55 tỷ Việt Nam đồng)	2,1 triệu đô la Mỹ (gần 48 tỷ Việt Nam đồng)	2 triệu đô la Mỹ (hơn 45 tỷ Việt Nam đồng)	1,97 triệu đô la Mỹ (gần 45 tỷ Việt Nam đồng)

VÍ DỤ VỀ SỰ CỐ NGHIÊM TRỌNG TRONG KHU VỰC

Hàn Quốc - Vào tháng 5/2017, ransomware từ Triều Tiên đã tấn công các trường đại học ở Hàn Quốc.

Một cơ quan an ninh mạng của Hàn Quốc[3] báo cáo rằng quốc gia này đã phải đối mặt với 130.000 vụ tấn công ransomware vào năm ngoái, làm tiêu tốn khoảng 300 tỷ Won (tương đương 268 triệu đô la Mỹ).

[2] WannaCry

[3] RanCERT

Ấn Độ - Vào tháng 6/2017, cảng container[4] lớn nhất của Ấn Độ đã bị nhiễm ransomware. [5]

Sự cố này khiến hệ thống máy tính bị khóa và làm chậm trễ tất cả các chuyến chuyên chở hàng hóa.

[4] Cảng Jawaharlal Nehru (JNPT)

[5] Petya ransomware

Khu vực châu Á – Thái Bình Dương – Vào tháng 11/2021, các chi nhánh của một tập đoàn bảo hiểm[6] có trụ sở tại Thái Lan, Malaysia, Hồng Kông và Philippines đã bị tấn công bởi một nhóm ransomware có tên là "Avaddon".

Kết quả là 3 Terabyte dữ liệu nhạy cảm của tập đoàn này đã bị đánh cắp.

[6] AXA Asian

Singapore – Vào tháng 8/2021, nền tảng dịch vụ thương mại hàng đầu châu Á đã bị một nhóm ransomware tên là BlackMatter tấn công.

Chúng đánh cắp thông tin về các dịch vụ quan trọng cũng như các thỏa thuận riêng giữa một công ty nền tảng thương mại hàng hóa Ấn Độ và nhiều ngân hàng[7] của Ấn Độ, cùng các thông tin cá nhân trong 500.000 bộ hồ sơ.

[7] Pine Labs

Thái Lan – Vào tháng 7/2020, Maze ransomware đã tấn công một công ty nước giải khát [8] và đưa ra yêu cầu tiền chuộc trên Dark Web.

Do hacker vẫn chưa công bố về dữ liệu bị đánh cắp, công ty vẫn chưa đưa ra quyết định sẽ chấp nhận hay từ chối trả tiền chuộc.

[8] Thai Beverage Public Company

References

1. The State of Ransomware in Education 2021. (n.d.). https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-in-education-2021-wp.pdf
2. Insurer AXA hit by ransomware after dropping support for ransom payments. (n.d.). BleepingComputer. Retrieved November 22, 2021, from https://www.bleepingcomputer.com/news/security/insurer-axa-hit-by-ransomware-after-dropping-support-for-ransom-payments/
3. Ransomware attacks, a growing threat that needs to be countered. (n.d.). https://www.unodc.org/southeastasiaandpacific/en/2021/10/cybercrime-ransomware-attacks/story.html

UNODC United Nations Office on Drugs and Crime

CYBERCRIME

From the People of Japan

RansomAware