SỔ TAY ỨNG CỨU SỰ CỐ

SỰ CỐ MÃ ĐỘC (MALWARE) VÀ SỰ CỐ GIẢ MẠO (PHISHING)

MỤC LỤC

1. Giới thiệu 3
2. Quy trình xử lý sự cố 4
2.1. Tóm tắt quy trình 4
2.2. Giai đoạn 1: Chuẩn bị 5
2.3. Giai đoạn 2: Nhận diện 6
2.4. Giai đoạn 3: Phân tích 9
2.5. Giai đoạn 4: Xử lý 13
2.6. Giai đoạn 5: Khôi phục 16
2.7. Giai đoạn 6: Hậu sự cố 19

1. Giới thiệu

Chương trình Diễn tập An toàn thông tin thực chiến được tổ chức nhằm nâng cao khả năng nhận diện, phân tích, điều tra, xử lý và khôi phục hệ thống trước các sự cố an ninh mạng thực tế. Chương trình giúp các đội thi tiếp cận với mô hình diễn tập mô phỏng theo các cuộc tấn công thực tế, đồng thời rèn luyện kỹ năng ứng phó trong các tình huống khẩn cấp.

Thông qua cuộc thi, các đội thi sẽ được:

Tiếp cận và làm việc trên hệ thống thực tế, bao gồm cả mạng doanh nghiệp, máy chủ web, cơ sở dữ liệu, hệ thống giám sát log.

Rèn luyện kỹ năng nhận diện, điều tra và xử lý sự cố dựa trên các bài tập được thiết kế theo cấp độ từ dễ đến khó.

Sử dụng các công cụ chuyên nghiệp như Splunk, ModSecurity (WAF), ITSM Ivanti để giám sát và khắc phục sự cố.

Nâng cao tư duy phản biện, khả năng làm việc nhóm và xử lý sự cố theo quy trình tiêu chuẩn..

Cải thiện quy trình giám sát và phản ứng sự cố, giúp nâng cao năng lực bảo mật tổng thể của tổ chức.

Nâng cao ý thức bảo mật và xây dựng chính sách an toàn thông tin phù hợp với môi trường doanh nghiệp.

2. Quy trình xử lý sự cố

2.1. Tóm tắt quy trình

Hình 1: Mô tả các bước của Ứng cứu sự cố

2.2.Giai đoạn 1: Chuẩn bị

Tạo và duy trì các danh sách về: các domain thuộc sở hữu của tổ chức; những người có thể đăng ký domain của tổ chức.

Tạo các mẫu email:

- Thông báo cho tất cả nhân viên về chiến dịch tấn công mã độc đối với tổ chức;
- Liên hệ với Cơ quan điều phối quốc gia nhằm báo cáo và gỡ bỏ domain độc hại
- Thông báo cho bên thứ 3 có hành động chống lại mã độc (Microsoft, FedEx, Apple, v.v.).

Thực hiện và đảm bảo:

- Áp dụng các giải pháp chống phần mềm chống mã độc/chống spam/chống giả mạo.
- Người dùng biết cách báo cáo giả mạo (cách thức nhận biết, nơi báo cáo).

- Phát hiện các tệp tài liệu (documents: docx, xlsx, pptx,...) tạo ra các tiến trình: PowerShell, CMD, WMI, MSHTA,…

- Phát hiện các tệp đính kèm có khả năng là mã độc: Exe, psl, sh, batch/cmd, lnk, dll,…

Theo dõi thông tin tình báo (threat intelligence):

- Các mối đe dọa đối với tổ chức, ngành.

- Các kiểu tấn công phổ biến.

- Rủi ro và lỗ hổng mới phát hiện.

Bảo đảm quyền truy cập vào các Sổ tay sự cố mất an toàn thông tin vào bất kỳ lúc nào:

- Sự cố giả mạo (Phishing).

- Sự cố mã độc (Malware).

Liệt kê danh sách các tài nguyên và cơ quan chủ quản:

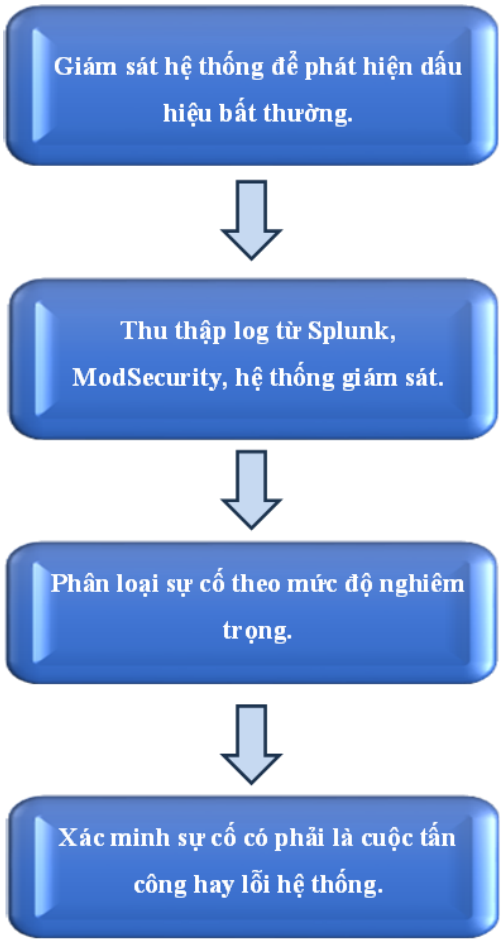
- Tài nguyên của khách hàng: cơ quan chủ quản, thông tin liên lạc, các hành động được ủy quyền.

- Tài nguyên của tổ chức: người vận hành, thông tin liên lạc, các hành động được ủy quyền.

Các loại tài nguyên cần liệt kê: Endpoints, máy chủ, thiết bị mạng, thiết bị bảo mật/an toàn, phạm vi mạng (công khai; nội bộ; VPN: nhân viên, đối tác, khách hàng).

2.3. Giai đoạn 2: Nhận diện

Giai đoạn nhận diện bắt đầu với việc xác định phạm vi ban đầu của một cảnh báo bảo mật:



Hình 2: Quy trình nhận diện

Xác định mối đe doạ

- Cảnh báo: Cảnh báo được tạo ra bởi các hệ thống khác nhau của nhóm Security/SOC. Các nguồn cảnh báo chủ yếu đến từ: Ticket, SIEM Anti-virus / EDR, báo cáo, DNS, Web Proxy, lỗi từ máy chủ mail.

- Thông báo: Thông báo đến từ các nguồn bên ngoài, thường qua email, tin nhắn hoặc điện thoại. Các nguồn thông báo chủ yếu đến từ: người dùng (nội bộ), người nhận email (bên ngoài), các bên đối tác, ISP, nhà cung cấp dịch vụ mail, máy tính chậm hoặc bị lỗi.

Thu thập thông tin

Các thông tin cần thu thập về mục tiêu:

- Domain: danh tiếng, công ty đăng ký, người sở hữu, IP, Công nghệ của trang web

(WordPress, Joomla, trang tùy chỉnh)

- IP: danh tiếng, người sở hữu, vị trí địa lý, các domain khác trên IP đó.

- Các file đính kèm: hash, danh tiếng, nhà phát hành,…

Xác minh sự cố

Kết hợp với một chuyên gia SOC: kiểm tra kỹ dữ liệu trước đó, loại trừ báo động giả.

Xác định loại tấn công

Xác định loại mã độc:

- Ransomware.

- Exfiltration.

- Worm/lateral Movement.

- Credential Theft.

- Banking.

- Trojan/RAT.

- Adware/PUP.

Sự cố đã có sổ tay

Thời gian là vấn đề quan trọng khi bị nhiễm mã độc, nếu đã xác định được loại sự cố:

- Gửi thông tin tới đội ứng cứu sự cố nội bộ.

- Chuyển tiếp tới sổ tay của loại sự cố đó.

Phân loại sự cố

- Xác định mức độ nghiêm trọng: Mã độc phá huỷ dữ liệu / dịch vụ / hệ điều hành, lây lan sang các máy khác trong mạng nội bộ,…

- Xác định phạm vi: Số máy được phát hiện: có tập tin / registry keys, có kết nối

đến URL, IP, cổng, hoặc bất cứ IOCs nào khác.

2.4.Giai đoạn 3: Phân tích

Phần 1: Xác định phạm vi

Giai đoạn này xác định phạm vi, mức độ nghiêm trọng của sự cố:

Hình 3: Quy trình phân tích - 1

- Xác định mã băm (hash): VirusTotal, Hybrid Analysis.

- Xác định liên kết: VirusTotal, Hybrid Analysis, URLScan.

- Các ID khác, domain, IPs: VirusTotal, Hybrid Analysis, Talos Intelligence.

- Tìm kiếm trên các nguồn thông tin tình báo: VirusTotal, Hybrid Analysis, Talos Intelligence.

- Thực hiện pháp y ổ cứng (Disk Forensics) trên thiết bị của người nhận.

Trích xuất IOCs

Sử dụng Sandbox Private để trích xuất các IOCs từ mẫu mã độc. Cần thu thập các thông tin sau:

- Kết nối mạng
- Registry đã sửa đổi
- Tập tin: tạo, sửa, xoá,…
- Powershell script: thu thập từ Script Block
- Services mới: được tạo, chạy
- Scheduled tasks mới

Gửi mẫu mã độc đến đối tác

Nếu mã độc không bị phát hiện/chặn bởi các sản phẩm bảo mật

- Gửi mẫu cho đối tác
- Gửi URL, IP, Domain

Dò quét diện rộng

- Cập nhật AV/EDR: Engine, tập luật, chính sách,…
- Cập nhật tập luật FW, IDS, vv.
- Tìm kiếm IOC trên SIEM.
- Tìm kiếm IOC trong nhật ký firewall, proxy, DNS,…
- Dò quét trên endpoints với EDR.

Cập nhật phạm vi sự cố

Tìm kiếm các dấu hiệu leo thang đặc quyền: từ firewall, endpoints, lưu lượng mạng,…

Cập nhật danh sách:

- Endpoints bị ảnh hưởng.
- Các khu vực bị ảnh hưởng.
- Đơn vị bị ảnh hưởng.

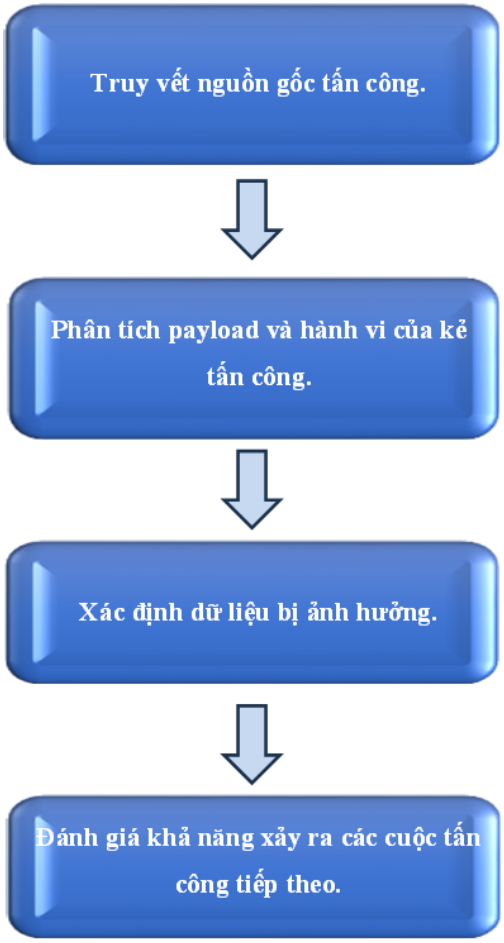
Xác định các thiết bị bị ảnh hưởng

Nếu đội điều tra tìm thấy dấu vết của tấn công hoặc IOC mới => quay trở lại bước **Xác định phạm vi**.

- Khi đã hoàn thành bước này, ta cần xác định tất cả các: host.
- Và điều tra tất cả: URL, domain, IP, cổng (Port), các tập tin, hash.
- Đã thu thập được ở các bước trên.

Phần 2: Phân tích nguồn gốc sự cố

Giai đoạn này xác định nguồn gốc, các yếu tố rủi do của sự cố:



Hình 4: Quy trình phân tích – 2

Yêu cầu hỗ trờ từ bên ngoài

Tùy thuộc vào mức độ xâm nhập và lan truyền của mã độc, chủ quản hệ thống có thể cần một số tư vấn về:

- Hỗ trợ kỹ thuật, chỉ dẫn, phản ứng: đội Taskforce hoặc chuyên gia an ninh mạng.
- Tư vấn pháp lý (Phạm vi dữ liệu, khách hàng bị ảnh hưởng,…)

Phân tích nguồn gốc sự cố

Xác định nguồn gốc lây nhiễm mã độc trong hệ thống:

- Lừa đảo
- Tải xuống các phần mềm/chương trình độc hại
- Lỗ hổng bảo mật: RCE, XSS, LFI,…
- Các dịch vụ từ xa được bảo vệ chưa tốt: mật khẩu yếu, mã hoá yếu,…
- Sử dụng USB để lây lan mã độc

Xác định các giai đoạn MITRE ATT&CK

Mitre ATT&CK Framework bao gồm nhiều chiến thuật khác nhau. Đội ứng cứu sự cố cần biết cuộc tấn công đã được phát hiện và ngăn chặn ở giai đoạn nào của Kill Chain với các thông tin sau:

Giai đoạn phát hiện Giai đoạn
ngăn chặn
Các hành động trên mục tiêu:

- Files bị mã hóa
- Bị đánh cắp dữ liệu
- Mất quyền kiểm soát tài khoản

Dữ liệu có bị lộ lọt

Nếu đội ứng cứu sự cố xác nhận hoặc nghi ngờ rằng dữ liệu đã bị lộ lọt, hãy chuyển tiếp đến **Sổ tay sự cố nghe trộm, gián điệp, lấy cắp thông tin, dữ liệu.**

Xác định các yếu tố

- Thông thường: trộm cắp thông tin, lây nhiễm mã độc, tống tiền / mã hoá dữ liệu
- Tổ chức: mất uy tín, thiệt hại tài chính, mất hợp đồng, không được gia hạn hợp đồng, phạt / giảm giá.

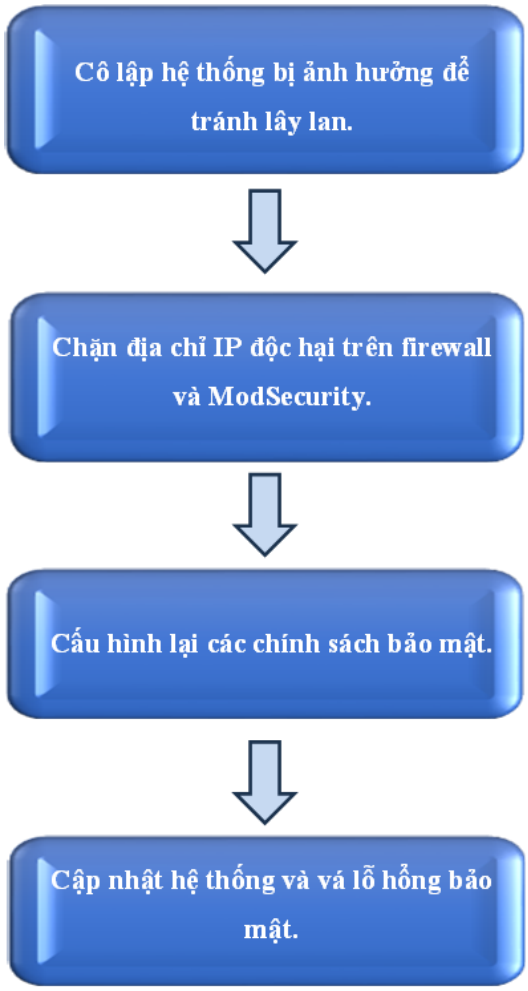
Liên lạc

Cập nhật thông tin đến:

- Đội ứng cứu sự cố nội bộ
- Đội quản trị hệ thống
- Những khách hàng bị ảnh hưởng bởi sự cố
- Những khách hàng cần lưu ý về sự cố

2.5. Giai đoạn 4: Xử lý

Giai đoạn này liên quan đến việc điều tra chi tiết sự cố, đảm bảo tất cả các thông tin đã được phát hiện. Bên cạnh đó, chuyên viên điều tra sự cố sẽ ghi nhận phạm vi cuối cùng của sự cố ở giai đoạn này:



Hình 5: Quy trình xử lý

Host có EDR

Xác định EDR đã được cài đặt trên host, nếu chưa có:

- Cài đặt EDR trên host
- Ngắt kết nối / tắt nguồn nếu không thể cài EDR: tắt switch, đưa vào VLAN cách ly, dừng NAT,…

Cách ly

- Cập nhật tập luật Firewall, Proxy, vv.
- Blackhole DNS.

- Gửi báo cáo cho bên thứ ba: cơ quan điều phối quốc gia, Google Safe Browsing, nhà cung cấp bộ lọc web,…

Xác định các hành động đã thực hiện

Hành động phía người dùng:

- Mở tài liệu
- Chạy tập tin thực thi
- Chạy script

Hành động phía máy tính:

- Kết nối đến trang web bên ngoài
- Ghi tập tin vào ổ đĩa
- Tạo / chạy các tác vụ mới

Hành động phía EDR:

- Chặn việc thực thi
- Cách ly tệp tin

Quyền quản trị

Để có thể loại bỏ mã độc, đội ứng cứu sự cố cần kiểm tra mã độc được thực thi bằng quyền gì. Nếu mã độc đã chiếm quyền quản trị của hệ thống:

- Xoá dữ liệu của máy vật lý
- Xoá máy ảo

Nếu không:

- Xoá tất cả IOC: tập tin, registry keys, services, scheduled tasks,…

Tập luật mới đã được phát hành

Kiểm tra đối tác đã cung cấp công cụ, tập luật hoặc chính sách mới để giải quyết vấn đề liên

quan đến mã độc chưa?

Nếu có:

- Cập nhật giải pháp bảo mật
- Cập nhật tập luật
- Kích hoạt chính sách
- Quét toàn hệ thống, bao gồm cả khách hàng (nếu cần)

Giám sát chặt chẽ

Giám sát các: kết nối Internet với IOC, các tệp mới khớp với mã hash được xác định, các tiến trình, hành vi phù hợp với dấu hiệu đã biết.

Cách ly các Endpoints

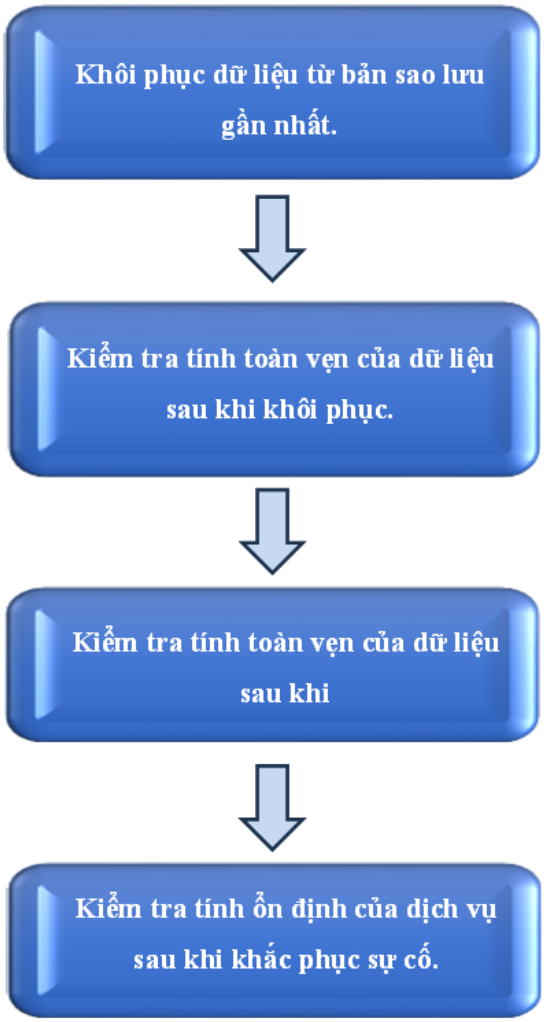
Nếu tất cả các endpoint bị ảnh hưởng đã được cách ly, ta có thể đi đến giai đoạn tiếp theo.

Phát hiện IOC mới

Nếu phát hiện được IOC mới, hãy quay lại Giai đoạn **Phân tích.**

2.6. Giai đoạn 5: Khôi phục

Giai đoạn này bao gồm các bước ngăn chặn và khắc phục, giảm thiểu ảnh hưởng của sự cố



Hình 6: Quy trình khôi phục

Dựng hệ thống

Cài đặt hệ điều hành được hỗ trợ, các giải pháp an ninh mạng, cập nhật ứng dụng, phục hồi dữ liệu từ bản sao lưu.

Rà quét lỗ hổng

Thực hiện:

- Rà quét từ bên ngoài
- Nếu có thể: thực hiện rà quét với tài khoản truy cập, rà quét trên từng thiết bị.

Vá lỗ hổng

Bất kỳ lỗ hổng nào ở mức Nghiêm trọng hoặc Cao đều phải được vá trước khi hệ thống được đưa vào hoạt động, bao gồm:

- Hệ điều hành
- Ứng dụng
- Các thiết bị mạng

Lỗ hổng mức trung bình và thấp nên được vá ngay nếu có thể, tuy nhiên không cần thiết để có thể đưa dịch vụ trở lại hoạt động.

Cập nhật hệ thống phòng thủ

Xác định rule nào cần phải được xóa và cần phải tiếp tục sử dụng trong danh sách sau: Firewall Rules, EDR (Ban hashes, Ban domains, cách ly), Proxy Block, DNS Sinkhole,…

Khôi phục dịch vụ

Tuỳ thuộc vào các biện pháp cách ly được sử dụng, cần thực hiện các hành động sau:

- Gỡ cách ly trên EDR
- Di chuyển máy chủ về VLAN vận hành.
- Bật switch, mở NAT,…

Nếu tất cả các endpoint bị ảnh hưởng đã được cách ly, ta có thể đi đến giai đoạn tiếp theo**Xác định các biện pháp đối phó**

- Xác định xem các yêu cầu hợp lệ có bị chặn không: Spam Filters, Proxy, Firewall, EDR.
- Nếu có, hãy quay lại **Cập nhật hệ thống phòng thủ.**
- Nếu không thì đi đến giai đoạn tiếp theo.

Mã độc đã được biết đến

Nếu mã đọc chưa được phát hiện, cần gửi mẫu mã độc cho các đối tác và bên thứ ba như:

VirusTotal, Hybird Analysis, Any.run, Threat Grig, Google Safe Browsing, OpenIOC,…

2.7. Giai đoạn 6: Hậu sự cố

Giai đoạn này bao gồm các đánh giá cuối cùng về sự cố, cập nhật rule và hồ sơ:

Hình 7: Quy trình hậu sự cố

Đánh giá sự cố

- Những gì đã hoạt động.
- Những gì không hoạt động.

Cập nhật quy trình làm việc

- Cập nhật các tài liệu sau: chính sách, quy trình, sổ tay, hướng dẫn vận hành hệ

thống.

- Cập nhật các rule trong: SIEM, Malware Gateway, EDR, các giải pháp bảo mật khác.

Đánh giá hệ thống phòng thủ

- Lên lịch đánh giá tập luật mỗi 6 tháng
- Xác định xem các luật sau còn hoạt động: Firewall, Proxy, AV / EDR, IPS,…

Cập nhật/nâng cấp hệ thống phòng thủ

Xác nhận hệ thống phòng thủ có thể phát hiện các mã độc tương tự trong tương lai. Sau khi gửi mẫu đến đối tác, cần đảm bảo:

- Cập nhật tập luật, công cụ
- EDR có thể phát hiện hành vi của mã độc
- Dịch vụ mail: Chống spam, chống lừa đảo

Gia cố hệ thống

Nếu nguyên nhân của sự cố do chưa gia cố hệ thống hoặc chưa cập nhật bản vá:

- Cập nhật quy trình gia cố hệ thống
- Áp dụng các bản vá, cập nhật ứng dụng
- Nâng cấp / thay thế ứng dụng, thiết bị không phù hợp

Đào tạo nhận thức của người dùng

Đảm bảo rằng người dùng được nâng cao nhận thức về: cách nhận biết giả mạo, cách báo cáo giả mạo, nguy hiểm của các liên kết lạ, nguy hiểm của việc mở tập tin đính kèm.

Đánh giá thiệt hại gây ra bởi sự cố

Đánh giá các thiệt hại gây ra bởi sự cố dẫn đến:

- Chi phí bảo hiểm khi thông tin bi mật bị lộ.

- Chi phí khi kết nối không gian mạng không được bảo vệ hiệu quả khỏi phần mềm độc hại, tấn công, từ chối dịch vụ đi kèm hoặc sử dụng hay truy cập trái phép.
- Chi phí điều tra để xác định vị trí dễ bị hại, phân tích tác động, đảm bảo ngăn chặn và tính toán mức độ thiệt hại.
- Chi phí liên quan đến việc giải quyết các mối đe dọa tống tiền trong việc tiết lộ thông tin hoặc mã độc hại nếu các khoản tống tiền không được thanh toán.