NGÂN HÀNG TÍN DỤNG ABC

CHÍNH SÁCH VỀ NHÓM ỨNG PHÓ SỰ CỐ MÁY TÍNH (CIRT)

QUYỀN TRUY CẬP ỦY QUYỀN

Tuyên Bố Chính Sách

Trong thời gian xảy ra sự cố bảo mật được công bố, Ban Giám đốc Ngân hàng Tín dụng ABC trao cho Nhóm Ứng phó Sự cố Máy tính (CIRT) quyền hạn tối cao để truy cập, kiểm soát và thực hiện mọi hành động cần thiết đối với tất cả các tài sản CNTT của tổ chức, bao gồm hệ thống, ứng dụng, dữ liệu và cơ sở vật chất. Quyền hạn này được trao để cho phép CIRT điều tra, ngăn chặn, khắc phục và phục hồi sau sự cố một cách hiệu quả, đồng thời duy trì tính toàn vẹn và chuỗi lưu trữ cho tất cả bằng chứng kỹ thuật số. Việc tuân thủ các chỉ thị do Trưởng nhóm CIRT đưa ra trong thời gian xảy ra sự cố là bắt buộc đối với tất cả nhân viên.

Mục Đích/Mục Tiêu

Chính sách này thiết lập và ủy quyền chính thức cho Nhóm Ứng phó Sự cố Máy tính (CIRT) để quản lý và phản hồi các sự cố bảo mật một cách phối hợp và hiệu quả. Các mục tiêu chính là:

- Giảm thiểu tác động hoạt động, tổn thất tài chính và thiệt hại danh tiếng từ các sự cố bảo mật.
- Bảo quản bằng chứng để hỗ trợ phân tích pháp y và duy trì chuỗi lưu trữ có giá trị pháp lý.
- Khôi phục hoạt động bình thường và tính bảo mật, toàn vẹn, khả dụng của các hệ thống quan trọng một cách nhanh nhất có thể.

- Đảm bảo tuân thủ các nghĩa vụ quy định, bao gồm Đạo luật Gramm-Leach-Bliley (GLBA).
- Xác định các thành viên của CIRT và quyền hạn cụ thể được trao cho họ trong cuộc khủng hoảng bảo mật.

Phạm Vi

Chính sách này áp dụng cho tất cả nhân viên, nhà thầu, nhà cung cấp và bất kỳ cá nhân nào truy cập hoặc quản lý tài sản thông tin của Ngân hàng Tín dụng ABC. Nó bao gồm tất cả bảy lĩnh vực của cơ sở hạ tầng CNTT, như được chi tiết trong bảng dưới đây. CIRT được cấp quyền truy cập và quyền hạn đầy đủ đối với tất cả các tài sản vật lý và kỹ thuật số trong các lĩnh vực này. Thẩm quyền này thay thế các giao thức truy cập tiêu chuẩn và bao gồm quyền cách ly hệ thống, thu hồi quyền truy cập và giám sát tất cả lưu lượng mạng và truyền thông khi cần thiết.

Lĩnh vực CNTT	Mô tả & Thẩm quyền của CIRT
Lĩnh vực Người dùng	**Bao gồm:** Tất cả người dùng (nhân viên, nhà thầu). **Thẩm quyền CIRT:** Điều tra hoạt động người dùng, thu hồi quyền truy cập, yêu cầu người dùng thực hiện hành động bảo mật.
Lĩnh vực Trạm làm việc	**Bao gồm:** Máy tính để bàn, máy tính xách tay, thiết bị di động. **Thẩm quyền CIRT:** Cách ly, thu giữ và phân tích pháp y.

Lĩnh vực Mạng cục bộ (LAN)	**Bao gồm:** Bộ chuyển mạch, bộ định tuyến, WiFi nội bộ. **Thẩm quyền CIRT:** Ngắt kết nối thiết bị, cách ly các phân đoạn mạng, thu thập nhật ký mạng.
Lĩnh vực Kết nối LAN-WAN	**Bao gồm:** Tường lửa, Hệ thống Phát hiện/Phòng ngừa Xâm nhập (IDS/IPS). **Thẩm quyền CIRT:** Sửa đổi quy tắc tường lửa, điều tra cảnh báo, thu thập nhật ký kết nối.
Lĩnh vực Mạng diện rộng (WAN)	**Bao gồm:** Kết nối Internet, VPN, dịch vụ ngân hàng trực tuyến. **Thẩm quyền CIRT:** Thu thập nhật ký từ ISP, điều tra các cuộc tấn công DDoS, phân tích lưu lượng WAN.
Lĩnh vực Truy cập Từ xa	**Bao gồm:** Hệ thống VPN. **Thẩm quyền CIRT:** Vô hiệu hóa quyền truy cập VPN của người dùng cụ thể hoặc toàn bộ, điều tra các lần đăng nhập từ xa.
Lĩnh vực Hệ thống/Ứng dụng	**Bao gồm:** Máy chủ, cơ sở dữ liệu, ứng dụng ngân hàng lõi, email. **Thẩm quyền CIRT:** Quyền truy cập quản trị đầy đủ, tắt ứng dụng, phân tích nhật ký, thu thập bằng chứng.

Tiêu Chuẩn

Chính sách này phù hợp và tham chiếu các tiêu chuẩn tổ chức và kỹ thuật sau:

- **NIST SP 800-61 (Hướng dẫn Xử lý Sự cố Bảo mật Máy tính):** Cung cấp phương pháp luận nền tảng cho vòng đời ứng phó sự cố của chúng tôi.
- **Tiêu chuẩn Phần mềm Pháp y:** Sử dụng các công cụ tiêu chuẩn ngành (ví dụ: FTK, EnCase) để thu thập và phân tích bằng chứng nhằm đảm bảo tính toàn vẹn của dữ liệu.
- **Tiêu chuẩn Cấu hình:** Tất cả các hệ thống bảo mật (SIEM, IDS/IPS) phải được cấu hình để tạo cảnh báo cho CIRT dựa trên các Chỉ số Xâm nhập (IOCs).

Quy Trình

Việc triển khai chính sách này được quản lý bởi Kế hoạch Ứng phó Sự cố của Ngân hàng Tín dụng ABC, kết hợp phương pháp luận 6 bước sau:

1. **Chuẩn bị:** CIRT được duy trì với các thành viên từ Quản lý CNTT, An ninh mạng, Hệ thống CNTT, Pháp chế, Nhân sự và Truyền thông. Các bài tập diễn tập được tiến hành thường xuyên.
2. **Nhận diện:** Các hệ thống giám sát cảnh báo CIRT về các sự cố tiềm ẩn. Sự cố được phân loại dựa trên tác động tiềm năng.
3. **Ngăn chặn:** CIRT sẽ ngay lập tức cách ly các hệ thống bị ảnh hưởng để ngăn chặn thiệt hại thêm.
4. **Khắc phục:** Nguyên nhân gốc rễ được xác định và loại bỏ khỏi môi trường.
5. **Phục hồi:** Hệ thống được khôi phục từ các bản sao lưu sạch và đưa trở lại vận hành sau

khi xác thực.

6. **Bài học Kinh nghiệm:** Một phân tích sau sự cố được tiến hành và Kế hoạch Ứng phó Sự cố được cập nhật.

Chuỗi Lưu trữ: *Trong suốt quá trình điều tra, CIRT sẽ duy trì một chuỗi lưu trữ chặt chẽ cho tất cả các bằng chứng, ghi chép lại mọi việc xử lý và chuyển giao để bảo tồn tính toàn vẹn cho các thủ tục pháp lý.*

Hướng Dẫn

Các thách thức triển khai tiềm năng và giải pháp của chúng:

- **Thách thức:** Sự phản đối từ trưởng các bộ phận khi CIRT thực thi quyền hạn.
    - **Hướng dẫn:** Chính sách này, được chứng thực bởi quản lý cấp cao, sẽ được truyền đạt đến tất cả các phòng ban. Việc không tuân thủ là một vi phạm nghiêm trọng.
- **Thách thức:** Cân bằng giữa điều tra với nhu cầu khôi phục nhanh chóng các hoạt động dịch vụ khách hàng quan trọng.
    - **Hướng dẫn:** CIRT sẽ ưu tiên ngăn chặn và phục hồi cho các hệ thống hỗ trợ các chức năng kinh doanh quan trọng nhất.
- **Thách thức:** Ma sát từ việc loại bỏ sử dụng cá nhân tài sản CNTT.
    - **Hướng dẫn:** Chính sách Sử dụng Chấp nhận Được sẽ được thực thi nghiêm ngặt. Việc giám sát của CIRT trong một sự cố là tối quan trọng.

Lab Assessment Questions & Answers

1. 6 bước trong phương pháp luận ứng phó sự cố là gì?

Trả lời: Phương pháp luận ứng phó sự cố 6 bước, được định nghĩa trong chính sách của Ngân hàng Tín dụng ABC, là:

1. Chuẩn bị
2. Nhận diện
3. Ngăn chặn
4. Khắc phục
5. Phục hồi
6. Bài học Kinh nghiệm

2. Nếu một tổ chức không có ý định truy tố thủ phạm hoặc kẻ tấn công, họ có cần một đội ứng phó sự cố để xử lý pháp y không?

Trả lời: Có, hoàn toàn cần. Pháp y không chỉ để truy tố. Nó rất quan trọng để:

- Xác định nguyên nhân gốc rễ của sự cố để ngăn ngừa tái diễn.
- Hiểu toàn bộ phạm vi thiệt hại (những gì được truy cập, đánh cắp hoặc thay đổi).
- Hoàn thành nghĩa vụ báo cáo quy định (ví dụ: GLBA cho một ngân hàng tín dụng).
- Cung cấp dữ liệu cho các yêu cầu bảo hiểm.

- Thông báo cho giai đoạn "Bài học Kinh nghiệm" để cải thiện tư thế bảo mật trong tương lai.

3. Tại sao nên đưa bộ phận nhân sự vào Nhóm Quản lý Ứng phó Sự cố?

Trả lời: Nhân sự là thiết yếu vì nhiều sự cố liên quan đến nhân viên (mối đe dọa từ nội bộ, rò rỉ dữ liệu vô tình, vi phạm chính sách). Nhân sự quản lý khía cạnh con người nhạy cảm của phản hồi, bao gồm:

- Tiến hành điều tra nội bộ với nhân viên.
- Thực thi các hành động kỷ luật phù hợp với luật lao động.
- Quản lý truyền thông và hỗ trợ cho nhân viên bị ảnh hưởng.
- Thu hồi quyền truy cập vật lý và hệ thống trong quy trình chấm dứt hợp đồng.

4. Tại sao nên đưa bộ phận pháp chế hoặc cố vấn pháp lý vào Nhóm Quản lý Ứng phó Sự cố?

Trả lời: Cố vấn pháp lý là rất quan trọng để:

- Tư vấn về nghĩa vụ pháp lý và quy định để báo cáo vi phạm (ví dụ: cho khách hàng và cơ quan quản lý theo GLBA).
- Quản lý tương tác với cơ quan thực thi pháp luật.
- Bảo vệ đặc quyền luật sư-khách hàng khi áp dụng.
- Đảm bảo việc thu thập bằng chứng (Chuỗi Lưu trữ) được xử lý một cách có giá trị pháp lý.

- Đánh giá và giảm thiểu rủi tố tụng tiềm năng.

5. Kế hoạch và nhóm ứng phó sự cố giúp giảm thiểu rủi ro cho tổ chức như thế nào?

Trả lời: Nó giảm thiểu rủi ro bằng cách cung cấp một phản hồi có cấu trúc, phối hợp và kịp thời để:

- **Giảm thiểu Tác động Hoạt động & Tài chính:** Bằng cách ngăn chặn sự cố nhanh chóng, nó làm giảm thời gian ngừng hoạt động và chi phí phục hồi.
- **Bảo vệ Danh tiếng:** Một phản hồi chuyên nghiệp quản lý nhận thức công chúng và duy trì niềm tin của khách hàng.
- **Đảm bảo Tuân thủ:** Nó giúp đáp ứng các yêu cầu pháp lý và quy định để báo cáo sự cố.
- **Cải thiện Tư thế Tương lai:** Giai đoạn "Bài học Kinh nghiệm" trực tiếp phản hồi để tăng cường khả năng phòng thủ, biến một quy trình phản ứng thành một chu kỳ cải tiến chủ động.

6. Nếu bạn đang phản ứng với một cuộc tấn công phần mềm độc hại như virus và nó đang lây lan, bạn đang cố gắng giảm thiểu sự lây lan của nó trong bước nào của quy trình ứng phó sự cố?

Trả lời: Đây là bước **Ngăn chặn**. Mục tiêu ngay lập tức là cách ly các hệ thống bị ảnh hưởng để ngăn chặn thiệt hại thêm và ngăn chặn sự lây lan.

7. Nếu bạn không thể ngăn chặn sự lây lan, bạn nên làm gì để bảo vệ các tài sản cơ sở hạ tầng CNTT quan trọng không bị ảnh hưởng của mình?

Trả lời: Nếu việc ngăn chặn ở cấp độ máy chủ thất bại, bạn phải tăng cường ngăn chặn lên cấp độ mạng. Điều này có thể bao gồm:

- Ngắt kết nối toàn bộ các phân đoạn mạng hoặc VLAN bị ảnh hưởng.
- Chặn lưu lượng tại tường lửa (Lĩnh vực Kết nối LAN-WAN) đến và từ các mạng con bị nhiễm.
- Như một biện pháp cuối cùng, tạm thời đưa các hệ thống quan trọng, không bị ảnh hưởng ngoại tuyến để tạo ra "khoảng cách không khí" và bảo vệ chúng cho đến khi mối đe dọa được khắc phục.

8. Khi một sự cố bảo mật đã được công bố, một kỹ thuật viên máy tính có được toàn quyền truy cập và có thẩm quyền để thu giữ và tịch thu máy tính xách tay của một phó chủ tịch không? Tại sao hoặc tại sao không?

Trả lời: Không, một kỹ thuật viên máy tính không tự động có thẩm quyền này. Theo chính sách, chỉ các thành viên được ủy quyền của CIRT mới được cấp "quyền hạn tối cao" này. Một kỹ thuật viên máy tính chỉ có thể thực hiện hành động này nếu họ là thành viên được chỉ định chính thức của CIRT cho sự cố đó và đang hành động theo sự chỉ đạo của Trưởng nhóm CIRT. Điều này đảm bảo các hành động được phối hợp, ghi chép chính xác cho Chuỗi Lưu trữ và có thể bào chữa về mặt pháp lý.

9. Bước nào trong phương pháp luận ứng phó sự cố bạn nên ghi chép lại các bước và quy trình để nhân rộng giải pháp?

Trả lời: Việc ghi chép này chủ yếu xảy ra trong bước **Phục hồi**, nơi các quy trình khôi phục hệ thống được xác định và làm theo. Tuy nhiên, nó cũng được hoàn thiện và chính thức hóa trong bước **Bài học Kinh nghiệm**, nơi toàn bộ phản hồi được ghi chép cho cơ sở kiến thức.

10. Tại sao việc xem xét sau sự cố (post mortem) là bước quan trọng nhất trong phương pháp luận ứng phó sự cố?

Trả lời: Việc xem xét **Bài học Kinh nghiệm** (post-mortem) là bước quan trọng nhất vì nó là cơ chế chính của tổ chức để **cải tiến liên tục**. Nó biến một sự cố phản ứng thành học tập chủ động bằng cách xác định những gì đã sai, những gì đã đúng và làm thế nào để cải thiện con người, quy trình và công nghệ để ngăn ngừa tái diễn hoặc phản hồi hiệu quả hơn trong tương lai. Nếu không có bước này, một tổ chức chắc chắn sẽ lặp lại những sai lầm của mình.

11. Tại sao cần có một định nghĩa chính sách cho Nhóm Ứng phó Sự cố Bảo mật Máy tính?

Trả lời: Một định nghĩa chính sách chính thức là cần thiết để:

- **Trao Thẩm quyền Hợp pháp:** Nó cung cấp cho CIRT sự hậu thuẫn pháp lý và tổ chức để thực hiện các hành động cực đoan (như tắt hệ thống hoặc tịch thu tài sản) mà không sợ bị trả đũa.
- **Thiết lập Quy định Bắt buộc:** Nó làm cho việc tuân thủ các chỉ thị của CIRT trở thành bắt buộc đối với tất cả nhân viên.
- **Xác định Phạm vi và Cấu trúc:** Nó chính thức thiết lập thành phần, vai trò và trách nhiệm của nhóm.
- **Đảm bảo Tính nhất quán:** Nó cung cấp một khuôn khổ tiêu chuẩn hóa để phản hồi tất cả các sự cố.

12. Mục đích của việc có các chính sách được ghi chép rõ ràng liên quan đến chức năng CSIRT và phân biệt sự kiện với sự cố là gì?

Trả lời: Các chính sách được ghi chép rõ ràng cung cấp **đường cơ sở và tiêu chí** cần thiết để thực hiện sự phân biệt này. Chúng xác định:

- Điều gì cấu thành một "sự cố" so với một "sự kiện" đơn giản (ví dụ: một lần đăng nhập thất bại là một sự kiện; 1.000 lần thử thất bại trong 5 phút là một sự cố).
- Các ngưỡng mức độ nghiêm trọng và tác động để công bố một sự cố và kích hoạt CSIRT.
- Các quy trình chính xác để làm theo một khi sự cố được công bố. Sự rõ ràng này ngăn ngừa mệt mỏi cảnh báo, đảm bảo nguồn lực được phân bổ phù hợp và đảm bảo một phản hồi nhanh chóng, có cân nhắc đối với các mối đe dọa thực sự.

13. Bốn bước nào trong quy trình xử lý sự cố yêu cầu tuân thủ Tiêu chuẩn Daubert về thu thập bằng chứng và chuỗi lưu ký (Chain of Custody)?

Trả lời:

Tiêu chuẩn **Daubert** được áp dụng cho mọi giai đoạn mà bằng chứng số được **xác định, thu thập, phân tích hoặc sử dụng trong điều tra**. Do đó, có **bốn bước** trong quy trình xử lý sự cố cần đảm bảo tuân thủ chuỗi lưu ký (Chain of Custody):

1. **Nhận dạng (Identification):** Bằng chứng ban đầu được phát hiện phải được ghi nhận đầy đủ, xác định rõ nguồn gốc và tính xác thực.
2. **Cô lập (Containment):** Khi cô lập hoặc cách ly hệ thống bị ảnh hưởng, mọi thao tác phải được ghi lại để bảo đảm tính toàn vẹn của bằng chứng.

3. **Loại bỏ (Eradication):** Trong quá trình loại bỏ mã độc hoặc yếu tố xâm nhập, việc sao lưu, chụp ảnh hệ thống và lưu giữ dữ liệu phải đảm bảo bằng chứng không bị thay đổi.

4. **Khôi phục (Recovery):** Khi khôi phục hệ thống từ bản sao sạch và kiểm chứng tính an toàn, chuỗi lưu ký được duy trì để đảm bảo bằng chứng phục vụ cho điều tra hoặc pháp lý vẫn nguyên vẹn.

Việc tuân thủ Tiêu chuẩn Daubert giúp bảo đảm rằng mọi bằng chứng số đều đáng tin cậy, có liên quan và có thể tái kiểm chứng, đáp ứng yêu cầu pháp lý nếu phải trình ra tòa.

14. Tại sao việc tương quan sự kiện giữa Syslog và nhật ký kiểm toán (Audit Trail) lại là công cụ quan trọng đối với CSIRT trong xử lý sự cố?

Trả lời: Việc tương quan sự kiện giữa Syslog và Audit Trail là nền tảng quan trọng giúp đội CSIRT (Computer Security Incident Response Team) hiểu và tái hiện toàn bộ chuỗi sự kiện trong một cuộc tấn công. Cụ thể:

- Các bản ghi từ nhiều hệ thống khác nhau (tường lửa, máy chủ, IDS/IPS, ứng dụng, v.v.) được tập trung về hệ thống giám sát (như SIEM).

- Việc tương quan sự kiện giúp xác định mẫu tấn công, hành vi bất thường và mối liên hệ giữa các sự kiện trong toàn bộ hạ tầng CNTT.

- Nhật ký sự kiện cung cấp **dấu vết pháp chứng (forensic traceability)**, duy trì **chuỗi lưu ký** để đảm bảo bằng chứng có giá trị pháp lý.

- Đây là nguồn dữ liệu quan trọng trong các giai đoạn Nhận dạng, Cô lập và Rút kinh nghiệm (Lessons Learned), giúp xác định nguyên nhân và phạm vi sự cố.

15. Tại sao cảnh báo từ hệ thống Giám sát Toàn vẹn Tệp (File Integrity Monitoring - FIM) là công cụ quan trọng đối với CSIRT trong giai đoạn nhận dạng sự cố?

Trả lời: Hệ thống **Giám sát Toàn vẹn Tệp (FIM)** đóng vai trò quan trọng trong **phát hiện sớm** các thay đổi trái phép trong môi trường CNTT. Cụ thể:

- FIM **theo dõi liên tục** mọi thay đổi trên tệp hệ thống, tệp cấu hình và ứng dụng quan trọng để phát hiện hành vi xâm nhập, cài mã độc hoặc leo thang đặc quyền.
- Khi có thay đổi so với **trạng thái chuẩn (baseline)**, FIM sẽ **phát cảnh báo ngay lập tức** cho CSIRT.
- Nhờ đó, đội phản ứng có thể **nhận dạng nhanh hệ thống bị xâm phạm**, đánh giá phạm vi sự cố và kịp thời cô lập trước khi lan rộng.
- Ngoài ra, FIM giúp **xác minh tính toàn vẹn của bằng chứng số**, đảm bảo dữ liệu phục vụ điều tra không bị thay đổi.

Nói cách khác, FIM là **hệ thống cảnh báo sớm (early warning system)** giúp CSIRT phát hiện và xác nhận sự cố ngay từ giai đoạn đầu, nâng cao khả năng phản ứng nhanh và hiệu quả.