HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÀI TẬP CHƯƠNG 3

Quản lý an toàn thông tin

Giảng viên: Nguyễn Ngọc Điệp

Nhóm lớp: 01

Sinh viên: Hoàng Trung Kiên

Mã sinh viên: B20DCAT098

Hà Nội – 2024

1.Tìm thông tin trên các trang web của công ty nào có kế hoạch ứng phó sự cố, phục hồi sau thảm họa và đảm bảo kinh doanh liên tục. Đưa ra một số dẫn chứng (tên và link tài liệu tiếng Anh/tiếng Việt).

- Kế hoạch ứng phó sự cố của Microsoft: https://www.microsoft.com/en-us/security/business/security-101/what-is-incident-response#Incident-response-plan-and-steps

Các bước ứng phó sự cố

Có nhiều cách để tiếp cận ứng phó sự cố và nhiều tổ chức dựa vào tổ chức tiêu chuẩn bảo mật để hướng dẫn cách tiếp cận của họ. SysAdmin Audit Network Security (SANS) là một tổ chức tư nhân cung cấp khung phản hồi gồm sáu bước, được nêu bên dưới. Nhiều tổ chức cũng áp dụng khuôn khổ khắc phục sự cố của Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST).

Chuẩn bị - Trước khi xảy ra sự cố, điều quan trọng là phải giảm thiểu các lỗ hổng và xác định các chính sách và quy trình bảo mật. Trong giai đoạn chuẩn bị, các tổ chức tiến hành đánh giá rủi ro để xác định điểm yếu của họ và ưu tiên tài sản. Giai đoạn này bao gồm viết và cải tiến các quy trình bảo mật, xác định vai trò và trách nhiệm cũng như cập nhật hệ thống để giảm thiểu rủi ro. Hầu hết các tổ chức thường xuyên xem lại giai đoạn này và cải tiến các chính sách, thủ tục và hệ thống khi họ rút ra bài học hoặc thay đổi công nghệ.

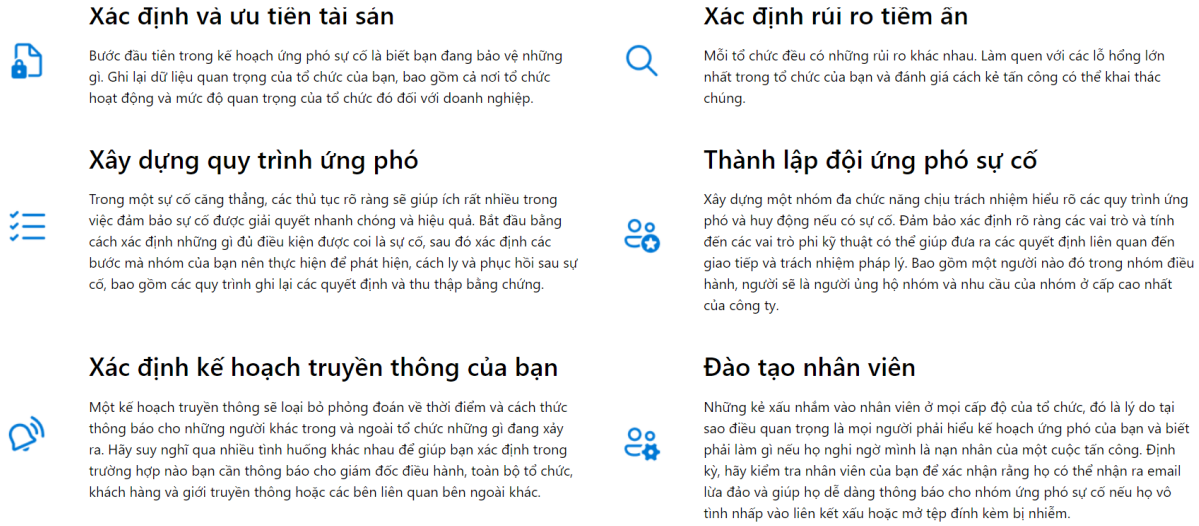
Nhận dạng mối đe dọa - Trong bất kỳ ngày nào, nhóm bảo mật có thể nhận được hàng nghìn cảnh báo cho biết hoạt động đáng ngờ. Một số trong số đó là dương tính giả hoặc có thể không đạt đến mức độ của một sự cố. Sau khi xác định được sự cố, nhóm sẽ tìm hiểu bản chất của vi phạm và ghi lại các phát hiện, bao gồm nguồn vi phạm, loại tấn công và mục tiêu của kẻ tấn công. Trong giai đoạn này, nhóm cũng cần thông báo cho các bên liên quan và trao đổi về các bước tiếp theo.

Ngăn chặn mối đe dọa - Ngăn chặn mối đe dọa càng nhanh càng tốt là ưu tiên tiếp theo. Những kẻ xấu được phép truy cập càng lâu thì thiệt hại mà chúng có thể gây ra càng lớn. Nhóm bảo mật làm việc để nhanh chóng cô lập các ứng dụng hoặc hệ thống đang bị tấn công khỏi phần còn lại của mạng. Điều này giúp ngăn chặn những kẻ tấn công truy cập vào các phần khác của doanh nghiệp.

Loại bỏ mối đe dọa - Sau khi quá trình ngăn chặn hoàn tất, nhóm sẽ loại bỏ kẻ tấn công và mọi phần mềm độc hại khỏi các hệ thống và tài nguyên bị ảnh hưởng. Điều này có thể liên quan đến việc đưa hệ thống vào chế độ ngoại tuyến. Nhóm cũng tiếp tục thông báo cho các bên liên quan về tiến độ.

Phục hồi và phục hồi - Việc khôi phục sau sự cố có thể mất vài giờ. Sau khi mối đe dọa biến mất, nhóm sẽ khôi phục hệ thống, khôi phục dữ liệu từ bản sao lưu và giám sát các khu vực bị ảnh hưởng để đảm bảo kẻ tấn công không quay trở lại.

Phản hồi và sàng lọc - Khi sự cố được giải quyết, nhóm sẽ xem xét những gì đã xảy ra và xác định những cải tiến có thể được thực hiện đối với quy trình. Học hỏi từ giai đoạn này giúp nhóm tăng cường khả năng phòng thủ của tổ chức.



- Kế hoạch khắc phục thảm họa sau sự cố của Microsoft: https://learn.microsoft.com/en-us/dynamicsax-2012/appuser-itpro/plan-for-disaster-recovery

- Kế hoạch đảm bảo kinh doanh liên tục của Microsoft: https://learn.microsoft.com/en-us/dynamicsax-2012/appuser-itpro/plan-for-disaster-recovery

https://learn.microsoft.com/en-us/compliance/assurance/assurance-resiliency-and-continuity

Microsoft làm cách nào để đảm bảo tính liên tục của hoạt động kinh doanh nếu xảy ra thảm họa hoặc mối đe dọa khác đối với tính khả dụng của dịch vụ?

Nhóm Quản lý khủng hoảng và phục hồi doanh nghiệp (ERCM) của Microsoft giám sát các hoạt động quản lý kinh doanh liên tục và khắc phục thảm họa trên các dịch vụ và dịch vụ đám mây của Microsoft. Đại diện từ các đơn vị kinh doanh của Microsoft phối hợp với nhóm ERCM để phát triển các kế hoạch kinh doanh liên tục và xác thực việc tuân thủ các yêu cầu về tính liên tục trong kinh doanh.

Vòng đời Quản lý kinh doanh liên tục (BCM) là cốt lõi của phương pháp BCM của chúng tôi. Quy trình ba giai đoạn này được thiết kế để có khả năng thích ứng để có thể triển khai bởi nhiều mô hình kinh doanh khác nhau trên khắp Microsoft. Nó bắt đầu bằng giai đoạn Đánh giá để xác định các quy trình và mục tiêu quan trọng cần được đưa vào chương trình kinh doanh liên tục. Giai đoạn Đánh giá cũng yêu cầu Phân tích tác động kinh doanh (BIA). Giai

đoạn Lập kế hoạch tập trung vào việc phát triển và triển khai các chiến lược phục hồi và phục hồi, đồng thời ghi lại chúng trong các kế hoạch kinh doanh liên tục chính thức. Cuối cùng, Xác thực Năng lực kiểm tra các kế hoạch kinh doanh liên tục và việc triển khai chúng để xác minh tính hiệu quả và xác định các cải tiến tiềm năng.

Chiến lược kinh doanh liên tục của dịch vụ trực tuyến của Microsoft sử dụng dự phòng phần cứng, mạng và trung tâm dữ liệu. Sao chép dữ liệu giữa các trung tâm dữ liệu mang lại tính sẵn sàng và độ tin cậy cao trong một sự cố thảm khốc. Nó cũng tăng khả năng phục hồi trước các sự cố thông thường như lỗi phần cứng bị cô lập hoặc hỏng dữ liệu.

Microsoft kiểm tra tính liên tục trong kinh doanh và các kế hoạch khắc phục thảm họa như thế nào?

Chính sách Quản lý khủng hoảng và khả năng phục hồi doanh nghiệp (ERCM) của Microsoft quy định rằng tất cả các kế hoạch khắc phục thảm họa và duy trì hoạt động kinh doanh của Microsoft phải được kiểm tra, cập nhật và xem xét hàng năm. Các dịch vụ trực tuyến của Microsoft kiểm tra kế hoạch kinh doanh liên tục của họ ít nhất mỗi năm một lần theo chính sách ERCM. Báo cáo Sau hành động được tạo và xem xét để xác thực, kiểm tra kết quả và thông báo cập nhật kế hoạch nhằm ứng phó với bất kỳ vấn đề nào được phát hiện trong quá trình thử nghiệm.

Để xác thực các chiến lược phục hồi và phục hồi trước nhiều sự cố tiềm ẩn, Chương trình ERCM xác định nhiều loại kịch bản thử nghiệm ảnh hưởng đến con người, địa điểm và công nghệ. Mức độ xác thực cần thiết cho mỗi dịch vụ dựa trên mức độ quan trọng của dịch vụ, với các dịch vụ quan trọng hơn sẽ nhận được xác thực nghiêm ngặt hơn. Mỗi nhóm dịch vụ trực tuyến của Microsoft kiểm tra kế hoạch kinh doanh liên tục của họ theo hướng dẫn của ERCM để đo lường tính hiệu quả của kế hoạch và mức độ sẵn sàng thực hiện kế hoạch của nhóm dịch vụ.

Theo hướng dẫn của ERCM, việc đánh giá hàng năm về kế hoạch kinh doanh liên tục và xác nhận năng lực phải diễn ra trong vòng 12 tháng kể từ lần đánh giá cuối cùng. Xác thực năng lực phải bao gồm việc xem xét tài liệu hỗ trợ, chẳng hạn như BIA, để đảm bảo tài liệu vẫn chính xác. Microsoft cung cấp kết quả xác thực khả năng cho các dịch vụ trực tuyến chọn lọc của Microsoft cho khách hàng của chúng tôi thông qua các báo cáo hàng quý.

2. Truy cập http://csrc.nist.gov. Trong phần “Publications”, hãy chọn NIST Special Publications, sau đó tìm SP 800-34, Hướng dẫn Contingency Planning Guide for Federal Information Systems (Lập kế hoạch Dự phòng cho Hệ thống Công nghệ Thông tin). Tải xuống và xem lại tài liệu này. Tóm tắt những điểm chính của tài liệu. (Có thể tìm kiếm trên mạng tóm tắt về tài liệu này)

Link tài liệu: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf
Tài liệu này được thiết kế để hướng dẫn người đọc một cách hợp lý về quá trình xây dựng kế hoạch dự phòng. Quá trình này bao gồm thiết kế chương trình lập kế hoạch dự phòng, đánh giá nhu cầu của tổ chức so với các lựa chọn chiến lược dự phòng dựa trên mức độ tác động của hệ thống, kiểm soát bảo mật và cân nhắc kỹ thuật, đồng thời ghi lại chiến lược dự phòng thành kế hoạch dự phòng, thử nghiệm kế hoạch và duy trì nó. Kế hoạch dự phòng được tạo ra sẽ đóng vai trò như một "sổ tay hướng dẫn sử dụng" để thực hiện chiến lược trong trường hợp có sự gián đoạn. Nếu có thể, các ví dụ hoặc tình huống giả định sẽ được đưa vào để giúp bạn hiểu rõ hơn. Các chương còn lại của tài liệu này đề cập đến các lĩnh vực lập kế hoạch dự phòng sau:
Chương 2, Bối cảnh, cung cấp thông tin cơ bản về lập kế hoạch dự phòng, bao gồm mục đích của các kế hoạch liên quan đến quản lý tình huống khẩn cấp và an ninh khác nhau, mối quan hệ của chúng với ISCP và cách thức thực hiện các kế hoạch này. được tích hợp vào chiến lược phục hồi tổng thể của tổ chức bằng cách triển khai sáu bước của Khung quản lý rủi ro (RMF).5 Ngoài ra, cách thức mà các mức tác động của FIPS 199 và các biện pháp kiểm soát lập kế hoạch dự phòng NIST SP 800-53 phải được xem xét trong quá trình lập kế hoạch dự phòng quá trình cũng được giải thích.
Chương 3, Quy trình lập kế hoạch dự phòng hệ thống thông tin, nêu chi tiết các nguyên tắc lập kế hoạch cơ bản cần thiết để phát triển khả năng dự phòng hiệu quả. Các nguyên tắc được nêu trong phần này có thể áp dụng cho tất cả các hệ thống thông tin. Phần này trình bày các hướng dẫn lập kế hoạch dự phòng cho tất cả các yếu tố của chu trình lập kế hoạch, bao gồm phân tích tác động kinh doanh, lựa chọn địa điểm thay thế và chiến lược phục hồi. Phần này cũng thảo luận về việc phát triển các nhóm lập kế hoạch dự phòng cũng như vai trò và trách nhiệm thường được giao cho nhân sự trong quá trình kích hoạt kế hoạch.
Chương 4, Phát triển Kế hoạch Dự phòng Hệ thống Thông tin, chia nhỏ các hoạt động cần thiết để ghi lại chiến lược dự phòng và phát triển ISCP. Việc duy trì, kiểm tra, đào tạo và thực hiện kế hoạch dự phòng cũng được thảo luận trong phần này.
Chương 5, Cân nhắc lập kế hoạch dự phòng kỹ thuật, mô tả các mối lo ngại về lập kế hoạch dự phòng cụ thể cho ba loại nền tảng phổ biến được liệt kê trong Phần 1.3, Phạm vi. Phần này giúp người lập kế hoạch dự phòng xác định, lựa chọn và thực hiện các biện pháp dự phòng kỹ thuật phù hợp cho hệ thống nhất định của họ.
Tài liệu này bao gồm chín phụ lục. Phụ lục A cung cấp ba mẫu ISCP mẫu, dựa trên mức độ tác động của FIPS 199. Phụ lục B trình bày mẫu BIA mẫu. Phụ lục C chứa danh sách các câu hỏi thường gặp về lập kế hoạch dự phòng hệ thống thông tin. Các vấn đề liên quan đến việc

lập kế hoạch cân nhắc nhân sự được thảo luận trong Phụ lục D. Phụ lục E cung cấp bản tóm tắt về các biện pháp kiểm soát và cải tiến kiểm soát lập kế hoạch dự phòng của NIST SP 800-53. Phụ lục F giải thích việc tích hợp kế hoạch dự phòng vào SDLC của tổ chức. Phụ lục G và H lần lượt chứa bảng chú giải các thuật ngữ và từ viết tắt.
Phụ lục I cung cấp các nguồn tài liệu và tài liệu tham khảo được đề xuất.
3. Sử dụng công cụ tìm kiếm trên Web, hãy truy cập một trong những trang web phục hồi sau thảm họa / tính liên tục của doanh nghiệp, chẳng hạn
như www.disasterrecoveryworld.com/, www.drj.com/, www.drie.org/, www.drii.org, hoặc csrc.nist.gov. Tìm kiếm các cụm từ "hot site", "warm site" và "cold site". Các mô tả được cung cấp có khớp với những mô tả của chương này không? Tại sao hoặc tại sao không?
Hot Site: "Cơ sở được trang bị đầy đủ các yêu cầu kỹ thuật bao gồm CNTT, viễn thông và cơ sở hạ tầng và có thể được sử dụng để khôi phục hoạt động nhanh chóng."
Warm site: "Một trang web xử lý thay thế được trang bị một số phần cứng và giao diện liên lạc, điều hòa điện và môi trường chỉ có khả năng cung cấp bản sao lưu sau khi thực hiện cung cấp, phần mềm hoặc tùy chỉnh bổ sung."
Cold site: "Một cơ sở được trang bị môi trường chỉ cung cấp không gian vật lý cho các hoạt động khôi phục trong khi tổ chức sử dụng không gian đó cung cấp thiết bị văn phòng, hệ thống phần cứng và phần mềm của riêng mình cũng như mọi nguồn lực cần thiết khác để thiết lập và tiếp tục hoạt động."

Trong chương 10 "Lập kế hoạch cho các tình huống dự phòng" của sách giáo khoa "Quản lý an ninh thông tin"1, Whitman định nghĩa các thuật ngữ này là:
Hot site: "Một cơ sở điện toán được cấu hình đầy đủ bao gồm tất cả các dịch vụ, liên kết truyền thông và hoạt động thực tế của nhà máy." (Whitman, 2017, tr.629)
Warm: "Một cơ sở cung cấp nhiều dịch vụ và tùy chọn giống như một trang web nóng, nhưng thường không có ứng dụng phần mềm được cài đặt và định cấu hình" (Whitman, 2017, trang 636)
Cold Site: "Một cơ sở chỉ cung cấp các dịch vụ thô sơ, không có phần cứng máy tính hoặc thiết bị ngoại vi." (Whitman, 2017, tr.626)
Khi so sánh cả hai bộ định nghĩa, có thể thấy rằng, định nghĩa www.drj.com của các trang web nêu rõ mức độ chi tiết hơn về nội dung kỹ thuật của môi trường, cũng như cung cấp lý do thiết lập chúng. Các định nghĩa trong sách giáo khoa chỉ đưa ra một tuyên bố chung chung về nội dung và không đề cập đến khả năng hoặc mục đích của chúng.

Hãy xem xét “hot site” được định nghĩa bởi www.drj.com trong đó đề cập đến “CNTT, viễn thông và cơ sở hạ tầng” cũng như “được sử dụng để giúp các hoạt động trở lại nhanh chóng”, trong khi sách giáo khoa chỉ đề cập đến “các liên kết truyền thông” và không đề cập rõ ràng đến chúng. mục đích.

“Warm site” và “cold stie” có cấu trúc tương tự nhau theo định nghĩa tương ứng.

“Warm site” được tuyên bố là có “phần cứng, giao diện liên lạc, điều hòa điện và môi trường” nhằm mục đích “dự phòng sau khi cung cấp bổ sung” bởi www.drj.com, trong khi sách giáo khoa chỉ đề cập đến nó như một phiên bản rút gọn của “hot site”.

www.drj.com định nghĩa “cold site” bằng cách sử dụng các từ “không gian vật lý” và tiếp tục đề cập rằng “tổ chức sử dụng không gian này cung cấp thiết bị văn phòng, hệ thống phần cứng và phần mềm của riêng mình” và sau đó tuyên bố rằng mục đích của nó là “tiếp tục hoạt động”. Sách giáo khoa chỉ đề cập nội dung là “các dịch vụ thô sơ, không có phần cứng máy tính hoặc thiết bị ngoại vi”.

4. Sử dụng định dạng được cung cấp trong văn bản, thiết kế một kế hoạch ứng phó sự cố cho máy tính tại nhà của bạn. Bao gồm các hành động cần thực hiện nếu mỗi sự kiện sau đây xảy ra:

● Cuộc tấn công của vi-rút

● Cháy

Nêu những tình huống nào khác mà bạn nghĩ là quan trọng để lập kế hoạch?

1. Mục đích và phạm vi:

   Mục đích: Kế hoạch này mô tả các bước cần thực hiện để giảm thiểu thiệt hại và khôi phục hoạt động bình thường của máy tính tại nhà trong trường hợp xảy ra sự cố

   Phạm vi: Phạm vi của kế hoạch ứng phó trên bao gồm các sự cố có thể xảy ra với máy tính tại nhà,

2. Phát hiện và phân tích:

   - *Phương pháp phát hiện:*

   Cuộc tấn công virus:

   Phần mềm diệt virus: Sử dụng phần mềm diệt virus uy tín và cập nhật thường xuyên để quét và phát hiện virus.

   Theo dõi hoạt động của máy tính: Theo dõi các hoạt động bất thường của máy tính, chẳng hạn như CPU sử dụng cao, hoạt động mạng bất thường, v.v.

   Hệ thống phòng chống xâm nhập (IDS): Sử dụng hệ thống IDS để phát hiện các hoạt động mạng độc hại.

Phân tích nhật ký: Phân tích nhật ký hệ thống để phát hiện các hoạt động đáng ngờ.

Cháy:

Cảm biến khói: Lắp đặt cảm biến khói để phát hiện hỏa hoạn sớm.

- *Phân tích ban đầu:*

Bước 1: Xác định bản chất của sự cố:

Cuộc tấn công virus:

Loại virus (ransomware, malware,...)

Cách thức lây nhiễm (email, website, phần mềm độc hại,...)

Các tập tin bị ảnh hưởng

Dấu hiệu và triệu chứng (máy tính chạy chậm, màn hình xanh,...)

Cháy:

Nguyên nhân hỏa hoạn (chập điện, chập cháy,...)

Mức độ thiệt hại (bị hư hỏng một phần, toàn bộ,...)

Có ai bị thương hay không

Các yếu tố nguy cơ (vật liệu dễ cháy,...)

Bước 2: Đánh giá tác động của sự cố:

Mức độ ảnh hưởng đến hoạt động của máy tính

Mức độ ảnh hưởng đến dữ liệu

Mức độ ảnh hưởng đến tài chính

Mức độ ảnh hưởng đến danh tiếng

Bước 3: Xác định nguồn tiềm ẩn của sự cố:

Cuộc tấn công virus:

Nguồn gốc của virus (kẻ tấn công, website độc hại,...)

Lỗ hổng bảo mật bị khai thác

Cháy:

Lỗi hệ thống điện

Thiếu các biện pháp phòng chống hỏa hoạn

Yếu tố con người (bất cẩn,...)

- Kiểm soát và loại bỏ:

+ Cuộc tấn công virus:

Ngắt kết nối máy tính khỏi mạng internet.

Khởi động máy tính vào chế độ an toàn.

Chạy phần mềm diệt vi-rút để quét và loại bỏ vi-rút.

Khôi phục dữ liệu từ bản sao lưu nếu cần thiết.

Cập nhật phần mềm diệt vi-rút và hệ điều hành.

+ Cháy:

Tắt máy tính và rút phích cắm điện.

Di chuyển máy tính đến nơi an toàn, tránh xa đám cháy.

Liên hệ với dịch vụ cứu hỏa nếu cần thiết.

- Phục hồi và hoạt động:

+ Virus:

Khôi phục dữ liệu từ bản sao lưu nếu cần thiết.

Cập nhật phần mềm diệt vi-rút và hệ điều hành.

+ Cháy:

Sau khi đám cháy được dập tắt, đánh giá thiệt hại và khôi phục dữ liệu từ bản sao lưu nếu cần thiết.