Ảnh có chứa văn bản, Phông chữ, ảnh chụp màn hình, tài liệu

Mô tả được tạo tự động

Nếu 1 công ty C nhập sản phẩm tương tự với sản phẩm X từ công ty nước ngoài về tiêu thụ trong nước thì sẽ vi phạm Luật Sở hữu trí tuệ năm 2005

Vi phạm điều khoản

Công ty C sẽ bị xử lý theo điều

Ảnh có chứa văn bản, Phông chữ, ảnh chụp màn hình, màu trắng

Mô tả được tạo tự động

Ảnh có chứa văn bản, Phông chữ, ảnh chụp màn hình, tài liệu

Mô tả được tạo tự động



* Mục tiêu 1: xây dựng một thương hiệu có tiếng về đồ uống giải khát trong vòng 6 tháng, thuộc top 10 quán bán chạy nhất trong khu vực lận cận về nước giải khát.

|  |  |
| --- | --- |
| Chiến lược | Chiến thuật |
| Facebook | 1) Chạy các chiến dịch khuyến mãi nhắm đến khách hàng tiềm năng.  2) Trả lời để đăng bình luận một cách thường xuyên để làm cho khách hàng cảm thấy có giá trị.  3) Đăng tải video review về sản phẩm  4) Tạo các nội dung vui nhộn như câu đố và trò chơi và tăng cường sự tham gia của người xem. |
| Instagram | 1. Đăng tải các hình ảnh, video ngắn về sản phẩm, cửa hàng 2. Đằng thông tin về sản phẩm mới, khuyến mãi, giảm giá.. |
| Cửa hàng | 1. Thiết kế một logo và biển hiệu độc đáo nhằm để thu hút và tạo ấn tượng cho khách hàng 2. Tặng phiếu giảm giá khi mua số lượng lớn 3. Tạo chương trình tích điểm cho khách quen 4. Pha chế nhiều công thức khác nhau 5. Chương trình dùng thử sản phẩm mới |
| Tiktok | 1. Chạy quảng cáo trên nền tảng bằng các video thu hút 2. Xây dựng kênh Tiktok riêng cho cửa hàng 3. Cộng tác với các Tiktoker review food |

* Mục tiêu 2: Tăng doanh thu 30% trong năm 2023 so với năm 2022.

|  |  |
| --- | --- |
| Chiến lược | Chiến thuật |
| Nâng cao chất lượng sản phẩm và dịch vụ | Đào tạo nhân viên về kỹ năng phục vụ khách hàng, cải thiện quy trình sản xuất và phục vụ. |
| Phát triển chương trình khuyến mại | Tổ chức các chương trình khuyến mại hấp dẫn như giảm giá, tặng quà, ưu đãi cho khách hàng thân thiết, để thu hút khách hàng mới và giữ chân khách hàng cũ. |
| Mở rộng địa điểm kinh doanh | Mở thêm một số cửa hàng mới ở các vị trí thuận tiện và phù hợp để thu hút khách hàng mới. |
| Tăng công nghệ truyền thông | Quảng bá quán giải khát thông qua các kênh truyền thông xã hội, đặt quảng cáo trên các phương tiện thông tin đại chúng để tăng tính nhận thức của thương hiệu. |
| Theo dõi và đánh giá kết quả | Đánh giá kết quả thực hiện kế hoạch hành động, đưa ra điều chỉnh và cập nhật kế hoạch mới để đạt được mục tiêu doanh thu. |

1. Biến pháp ứng phó khắc phục

Ảnh có chứa văn bản, Phông chữ, ảnh chụp màn hình, hàng

Mô tả được tạo tự động

Mô tả: Một nhóm startup đã xây dựng app và website hỗ trợ học tập. Người dùng có thể thảo luận về kiến thức các môn học, bài tập ứng dụng, chat riêng, hoặc cùng chơi các game phát triể trí não như đánh cờ,…và mua tài liệu tham khảo. Văn phòng của công ty ở trong tòa nhà X tại Tp.HCM, hiện có 20 nhân viên. Tất cả các nhân viên đều được cấp thẻ nhân viên để vào tòa nhà, một chiếc iPhone và máy tính xách tay. Tất cả nhân viên đều nhận được email hướng dẫn các giải pháp an ninh mạng, nhưng không phải nhân viên nào cũng đọc hết nội dung trong email. Nhân viên chưa trải qua bất kỳ khóa đào tạo bắt buộc nào về an ninh mạng. Gần đây, công ty đã xảy ra một mối đe dọa an ninh mạng. Do đó, họ đang tìm cách cải thiện an ninh mạng và đang tìm kiếm chuyên gia an ninh mạng để giúp đỡ. Sự cố an ninh mạng gần đây của công ty: Một nhân viên đã để quên máy tính xách tay trên tàu khi đi công tác. Trên máy tính xách tay đã lưu các tài khoản để đăng nhập vào trang quản trị ứng dụng và website của công ty, cơ sở dữ liệu và một số tài liệu của công ty. Nhân viên đã báo mất cho công ty ngay khi phát hiện sự cố, và máy tính xách tay đã bị xóa dữ liệu từ xa. Công ty không thể chắc chắn có dữ liệu nào đã được truy cập trước khi dữ liệu máy tính bị xóa từ xa. Chú ý: Các quy định quan trọng của chính phủ về bảo vệ thông tin cá nhân Yêu cầu: Nhóm của bạn gồm các chuyên gia an ninh mạng và sẽ phải đề xuất các giải pháp cho các mối đe dọa an ninh mạng của họ. Tài sản chính của công ty là gì? Họ cần bảo vệ điều gì? (Tài sản là một hạng mục tài sản thuộc sở hữu của một người hoặc công ty. Đây có thể là tài sản vật chất hoặc thông tin họ nắm giữ). Các biện pháp bảo vệ, phát hiện, ứng phó, khắc phục đối với mỗi mối đe dọa.

Bài làm

Tài sản chính của công ty là thông tin khách hàng, cơ sở dữ liệu, tài liệu công ty, trang web và ứng dụng của công ty. Họ cần bảo vệ các thông tin này để đảm bảo sự riêng tư và bảo mật của khách hàng, đảm bảo tính toàn vẹn và sẵn sàng của dữ liệu, tránh mất mát thông tin, và đảm bảo hoạt động ổn định của trang web và ứng dụng.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Tài sản vật chất** | **Các mối đe dọa an ninh mạng tiềm ẩn** | **Bảo vệ** | **Phát hiện** | **Ứng phó** | **Khắc phục** |
| 1) IPhone của công ty cho tất cả nhân viên | - Mất mát, rò rỉ thông tin, dữ liệu của nhân viên, công ty khi kẻ xấu truy cập bằng điện thoại | - Bảo vệ thiết bị bằng mật khẩu mạnh và ủy quyền sử dụng.  - Bảo mật dữ liệu icloud, đặt mật khẩu icloud  - Thường xuyên sao lưu dữ liệu icloud  - Tạo chính sách quản lý thiết bị di động cho phép theo dõi và quản lý. | - Sử dụng các phần mềm quản lý thiết bị di động  - Nhật ký truy cập icloud từ iphone  - Các tài liệu bị truy cập từ iphone  - Sử dụng các ứng dụng bảo mật.  - Kiểm tra các ứng dụng được cài đặt trên iPhone.  - Kiểm tra các cập nhật bảo mật.  - Thường xuyên dám sát thao tác, hoạt động của nhân viên.  - Thường xuyên kiểm tra nhật ký để phát hiện khi bị tấn công. Giám sát để xem tài khoản nào có thao tác bất thường. | - Tăng cường đào tạo nhân viên về an ninh mạng.  - Đào tạo nhân viên về bảo mật dữ liệu.  - Xác thực, nguyên nhân tấn công  - Vô hiệu hóa cuộc tấn công  - Báo cáo vs cơ quan chức năng  - Cài đặt các giải pháp bảo mật.  - Giám sát hoạt động mạng.  - Thực hiện kế hoạch phòng chống khẩn cấp.  - Hợp tác với chuyên gia an ninh mạng. | - Sử dụng các thiết bị khác để đăng xuất tài khoản và xóa tài khoản khỏi iphone  - Thu hồi quyền người dùng trên máy nếu nhận thấy bất thường |
| 2) Máy tính, laptop | - Mất dữ liệu quan trọng, truy cập trái phép.  - Nguy cơ mất website  - Kết nối không an toàn. | - Sử dụng mật khẩu mạnh.  - Mã hóa dữ liệu: để ngăn chặn truy cập trái phép.  - Bảo mật dữ liệu có trong máy, đặt tường lửa, mật khẩu cho dữ liệu nhạy cảm trong máy  -Tạo bản full bakup cho dữ liệu và thông tin quan trọng trong máy  - Cài đặt phần mềm bảo mật.  - Thiết lập các cơ chế xác thực (vân tay…).  - Sử dụng phần mềm quản lý thiết bị. | - Kiểm tra và đánh giá các hệ thống bảo mật hiện tại.  - Sử dụng các công cụ giám sát mạng và máy tính.  - Phát hiện truy cập lạ, truy xuất dữ liệu bất thường kích hoạt cảnh báo cho người dùng máy | - Xác định và vô hiệu hóa nguồn gây hại ngay lập tức  - Áp dụng chính sách an ninh mạng.  - Đào tạo nhân viên về bảo mật an toàn thông tin  - Điều chỉnh các quyền truy cập, phần quyền người dùng.  - Sao lưu dữ liệu thường xuyên. | - Tổ chức các khóa đào tạo bắt buộc về an ninh mạng.  - Thực hiện thay đổi mật khẩu định kỳ.  - Cập nhật hệ thống bảo mật để đảm bảo rằng chỉ có những người được ủy quyền mới có thể truy cập. |
| 3) Thẻ nhân viên | - Bị kẻ xấy lấy cắp, mất thông tin của nhân viên | - Mã hóa các dữ liệu quan trọng của nhân viên  - Tạo bản full bakup cho dữ liệu và thông tin quan trọng của nhân viên  - Vô hiệu hóa thẻ cũ và cấp thẻ mới cho nhân viên | - Phát hiện thông tin của nhân viên bị truy cập và truy xuất từ các nguồn lạ một cách bất thường | - Đào tạo nhân viên về bảo mật  - Kích hoạt hệ thống bảo mật bảo vệ thông tin  - Mã hóa các dữ liệu quan trọng ngay lập tức  - Ngăn chặn các truy cập, truy xuất dữ liệu lạ, bất thường từ nguồn lạ | - Restore các dữ liệu đã backup  - Thông báo với nhân viên về các hoạt động phản hồi và phục hồi dữ liệu |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Tài sản thông tin** | **Các mối đe dọa an ninh mạng tiềm ẩn** | **Bảo vệ** | **Phát hiện** | **Ứng phó** | **Khắc phục** |
| 1) Thông tin cá nhân của khách hàng | - Tấn công hacker  - Rò rỉ dữ liệu  - Mất mát thông tin dữ liệu của công ty khi truy cập vào gmail của điện thoại | - Mã hóa dữ liệu  - Kiểm soát truy cập và đảm bảo an toàn cho cơ sở dữ liệu.  - Sử dụng các phần mềm chống virus, tường lửa và các giải pháp mã hóa để đảm bảo an toàn cho dữ liệu. | - Sử dụng các công cụ giám sát mạng .các dấu hiệu của một cuộc tấn công mạng.  - Sử dụng các phần mềm phát hiện xâm nhập hoặc các cuộc tấn công từ bên ngoài. | - Quy trình hành động cụ thể để xử lý vấn đề.  - Thiết lập các giải pháp khẩn cấp để đảm bảo rằng các thông tin quan trọng và tài sản của công ty được bảo vệ.  - Thông báo cho khách hàng về các vấn đề rủi ro bảo mật dữ liệu  - Báo cho cơ quan chức năng | - Khắc phục những tổn thất và thiệt hại gây ra bởi cuộc tấn công mạng.  - Đưa ra các biện pháp cải thiện để ngăn chặn các cuộc tấn công tương tự xảy ra trong tương lai.  - Điều tra và đánh giá các cuộc tấn công để hiểu rõ hơn về cách thức và cố gắng ngăn chặn các cuộc tấn công tương tự trong tương lai. |
| 2) Cơ sở dữ liệu (Tài liệu ,hệ thống lưu trữ của công ty, dữ liệu nhân viên, đối tác, hợp đồng, sản phầm, kế hoạch… ) | - Tấn công mạng từ bên ngoài  - Mất mật khẩu hoặc lỗi phần mềm.  -Sử dụng phần mềm giả mạo.  - Đánh cắp thông tin bằng cách lừa đảo  - Lỗi phần mềm | - Mã hóa dữ liệu.  - Giám sát người dùng.  - Cập nhật phần mềm định kỳ.  - Cài đặt và cập nhật các phần mềm bảo mật đầy đủ trên tất cả các máy tính  - Áp dụng các biện pháp bảo mật mạng hiệu quả như tường lửa, phát hiện xâm nhập, chống DDoS...  - Đào tạo nhân viên về các cuộc tấn công phishing để giảm thiểu nguy cơ bị đánh cắp dữ liệu.  - Xây dựng chính sách bảo mật CSD.  - Giám sát hoạt động của CSDL. | - Sử dụng phần mềm chống virus và phần mềm bảo mật mạng.  - Giám sát và kiểm soát truy cập vào hệ thống.  - Kiểm tra định kỳ các thiết bị kết nối với hệ thống mạng.  - Theo dõi hoạt động của các hệ thống lưu trữ tài liệu.  - Xây dựng các hệ thống cảnh báo | - Tăng cường việc giám sát và phân tích để nhanh chóng phát hiện các cuộc tấn công và khắc phục .  - Đào tạo nhân viên về các biện pháp khẩn cấp  - Đào tạo nhân viên về an ninh mạng.  - Đổi mật khẩu.  -Kiểm tra và cập nhật phần mềm.  -Phân quyền truy cập.  -Đánh giá và nâng cao cơ chế bảo mật. | - Khôi phục các tài liệu bị mất bằng cách sử dụng các bản sao lưu dự phòng.  - Kiểm tra và đánh giá lại các biện pháp bảo mật hiện tại để xem xét các cải tiến có thể được thực hiện. |

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, tài liệu

Mô tả được tạo tự động

Câu a: các phương thức tấn công hacker có thể sử dụng đế lấy cắp thông tin người dùng là

Phishing: Hacker có thể gửi email giả mạo để đánh lừa nhân viên cung cấp thông tin đăng nhập vào trang web giả mạo. Thông tin này được sử dụng để truy cập vào tài khoản của nhân viên trên trang web chính thức.

Keylogging: Hacker có thể sử dụng phần mềm độc hại để theo dõi hoạt động của nhân viên trên máy tính và lưu trữ thông tin đăng nhập được nhập vào.

Brute-force attack: Hacker có thể sử dụng phương pháp này để thử tất cả các kết hợp có thể của tên đăng nhập và mật khẩu cho tài khoản của nhân viên, nhằm tìm ra thông tin đăng nhập chính xác.

Social engineering: Hacker có thể sử dụng kỹ thuật xâm nhập xã hội để đánh lừa nhân viên tiết lộ thông tin đăng nhập hoặc truy cập vào máy tính của họ để lấy cắp thông tin.

Sử dụng mã độc: Hacker có thể sử dụng các mã độc để truy cập vào tài khoản của nhân viên hoặc truy cập vào các thông tin được lưu trữ trên máy tính của họ.

Câu b:

Phishing là một phương thức tấn công mạng mà hacker sử dụng email giả mạo để lừa đảo người dùng cung cấp thông tin đăng nhập vào trang web giả mạo. Trang web giả mạo này thường được thiết kế giống hệt với trang web chính thức của một tổ chức nào đó, nhưng thực tế nó là một trang web giả mạo mà hacker tạo ra để lấy cắp thông tin đăng nhập của người dùng.

Phươn thức tấn công phishing thường bắt đầu bằng việc hacker gửi một email giả mạo cho người dùng với một đường dẫn đến trang web giả mạo. Đường dẫn này thường được thiết kế để đưa người dùng đến trang web giả mạo mà không hề nhận ra.

Khi người dùng truy cập vào trang web giả mạo, nó sẽ yêu cầu người dùng nhập thông tin đăng nhập, bao gồm tên đăng nhập và mật khẩu. Khi người dùng nhập thông tin đăng nhập, hacker sẽ có được thông tin này và sử dụng nó để truy cập vào tài khoản của người dùng trên trang web chính thức.

Để tránh bị tấn công phishing, người dùng nên luôn luôn kiểm tra địa chỉ URL trước khi nhập thông tin đăng nhập. Nếu đường dẫn không giống hệt với địa chỉ URL của trang web chính thức, người dùng nên không nhập thông tin đăng nhập và liên hệ với tổ chức đó để xác nhận địa chỉ URL. Ngoài ra, người dùng cũng nên cập nhật và sử dụng các phần mềm chống virus và bảo mật để giảm thiểu nguy cơ bị tấn công phishing.

Thêm

 Tấn công từ chối dịch vụ (DDoS): Kẻ tấn công có thể tấn công vào website bằng cách gửi một lượng lớn yêu cầu đến server, khiến server không thể xử lý đủ số lượng yêu cầu và website sẽ bị tê liệt.

 Tấn công mạng lưới botnet: Kẻ tấn công có thể sử dụng mạng lưới botnet để tấn công vào website và tiến hành các hoạt động độc hại như lấy cắp thông tin người dùng, mã độc, phá hủy dữ liệu,...

 Tấn công phishing: Kẻ tấn công có thể giả mạo thông tin của tài khoản quản trị viên để lừa đảo người dùng truy cập vào website và đánh cắp thông tin.

 Tấn công từ điển: Kẻ tấn công có thể sử dụng danh sách từ điển để thử tất cả các mật khẩu có thể của tài khoản quản trị viên.

 Tấn công gián điệp: Kẻ tấn công có thể lấy cắp thông tin tài khoản quản trị viên bằng cách gián điệp hoặc cài đặt phần mềm gián điệp trên máy tính của người dùng.

Tấn công mạng lưới botnet là một phương thức tấn công mạng phổ biến, trong đó kẻ tấn công sử dụng các máy tính đã bị lây nhiễm mã độc (virus, malware) để tạo thành một mạng lưới các máy tính bị chiếm đoạt quyền điều khiển từ xa. Các máy tính bị chiếm đoạt này được gọi là "bot" và được điều khiển bởi một server điều khiển từ xa, còn được gọi là "command and control" (C&C).

Khi kẻ tấn công sử dụng mạng lưới botnet, họ có thể tiến hành các cuộc tấn công phức tạp và có tính toán trên một quy mô lớn, bao gồm tấn công từ chối dịch vụ (DDoS), phá hoại hệ thống, lấy cắp thông tin, thực hiện spam email, và thậm chí cài đặt phần mềm độc hại lên các máy tính khác trong mạng.

Mạng lưới botnet thường được tạo ra bằng cách lây nhiễm máy tính của người dùng thông qua các email lừa đảo, các trang web độc hại, hoặc các lỗ hổng bảo mật trên hệ thống máy tính. Sau khi bị lây nhiễm, các máy tính này sẽ trở thành một phần của mạng lưới botnet và trở thành công cụ tấn công cho kẻ tấn công.

Để ngăn chặn tấn công mạng lưới botnet, người dùng nên duy trì các hệ thống an ninh mạng mạnh mẽ và cập nhật các bản vá bảo mật mới nhất cho các phần mềm và hệ điều hành của họ. Họ cũng nên tránh mở các email lạ hoặc các tập tin đính kèm không rõ nguồn gốc, và sử dụng các giải pháp phần mềm chống virus và phần mềm chống độc hại để bảo vệ hệ thống của mình.

Câu c: Mạng lưới botnet là một trong những mối đe dọa lớn nhất đối với an ninh mạng, và để bảo vệ mình khỏi cuộc tấn công này, các biện pháp bảo vệ cần được thực hiện. Dưới đây là một số biện pháp bảo vệ đối với tấn công mạng lưới botnet:

o Sử dụng phần mềm bảo mật đáng tin cậy: Sử dụng phần mềm bảo mật đáng tin cậy để phát hiện và ngăn chặn các cuộc tấn công của botnet. Phần mềm bảo mật đáng tin cậy cần được cập nhật thường xuyên để đảm bảo tính hiệu quả của nó.

o Phát hiện và ngăn chặn các tấn công từ phía người dùng: Để tránh các thiết bị bị nhiễm botnet, các tổ chức cần đào tạo nhân viên và người dùng cách phát hiện và ngăn chặn các tấn công từ phía người dùng. Điều này có thể bao gồm việc giảm thiểu việc sử dụng các trang web bất hợp pháp, giảm thiểu việc nhấp chuột vào các liên kết không rõ nguồn gốc và sử dụng các trình duyệt web được cập nhật.

o Cấu hình tường lửa: Cấu hình tường lửa để ngăn chặn các lưu lượng mạng đến và đi từ các máy tính có khả năng bị nhiễm botnet. Tường lửa cũng có thể được sử dụng để phát hiện các lưu lượng mạng bất thường và báo cáo về chúng.

o Giám sát mạng: Giám sát mạng là một phương pháp hiệu quả để phát hiện và ngăn chặn các hoạt động của botnet. Tổ chức có thể sử dụng các công cụ giám sát mạng để phát hiện các kết nối đến các máy chủ không rõ nguồn gốc hoặc các lưu lượng mạng bất thường.

o Thực hiện các bản vá hệ thống: Các bản vá hệ thống cần được thực hiện đầy đủ để đảm bảo tính bảo mật của hệ thống. Điều này bao gồm việc cập nhật các bản vá và các phiên bản phần mềm mới nhất.

Câu c:

Thông báo cho người dùng: Tổ chức cần phải thông báo cho tất cả các người dùng bị ảnh hưởng về sự cố bảo mật và yêu cầu họ thay đổi mật khẩu trên trang web chính thức của tổ chức. Các người dùng cũng nên được cung cấp thông tin về cách phát hiện các hoạt động bất thường trên tài khoản của họ và các biện pháp để bảo vệ thông tin cá nhân của mình.

Thay đổi mật khẩu và cập nhật các hệ thống bảo mật: Tất cả các nhân viên của tổ chức cần phải thay đổi mật khẩu đăng nhập vào hệ thống và cập nhật các hệ thống bảo mật để đảm bảo an toàn thông tin cá nhân của họ. Tổ chức cũng nên đặt chính sách bảo mật mạnh mẽ hơn và cung cấp các khóa đăng nhập kép (2FA) để tăng cường bảo mật.

Khảo sát và khắc phục lỗ hổng bảo mật: Tổ chức cần phải tiến hành khảo sát và phát hiện các lỗ hổng bảo mật trong hệ thống của mình để ngăn chặn các cuộc tấn công tương tự. Sau đó, các lỗ hổng này cần được khắc phục và các hệ thống bảo mật cần được cập nhật để ngăn chặn các cuộc tấn công trong tương lai.

Học hỏi từ kinh nghiệm: Tổ chức cần phải học hỏi từ kinh nghiệm và cải thiện chính sách bảo mật để giảm thiểu rủi ro bị tấn công mạng trong tương lai. Điều này có thể bao gồm việc đào tạo nhân viên về cách phát hiện các hoạt động bất thường và phát triển các kế hoạch khắc phục sự cố nhanh chóng.

Câu d:

Đảm bảo an toàn tài khoản nhân viên: Tổ chức cần hướng dẫn nhân viên sử dụng mật khẩu đủ mạnh, khuyến khích sử dụng hệ thống xác thực hai yếu tố và yêu cầu thay đổi mật khẩu định kỳ. Hơn nữa, tổ chức nên cài đặt phần mềm quản lý mật khẩu để giúp quản lý tài khoản nhân viên một cách hiệu quả.

Nâng cao khả năng phát hiện xâm nhập: Tổ chức cần đầu tư vào giám sát hệ thống, phát hiện và ngăn chặn các cuộc tấn công. Các giải pháp này bao gồm việc cài đặt các giải pháp bảo mật mạng, phân tích hành vi người dùng và xây dựng các biện pháp ngăn chặn dựa trên các mẫu tấn công phổ biến.

Đảm bảo an toàn thông tin khách hàng: Tổ chức cần cải thiện các chính sách bảo mật và quản lý thông tin khách hàng bằng cách mã hóa thông tin trước khi lưu trữ và sử dụng các giải pháp để phát hiện các cuộc tấn công đánh cắp thông tin.

Tăng cường nâng cao nhận thức về an ninh mạng của nhân viên: Tổ chức nên đào tạo nhân viên về an ninh mạng, giúp họ nhận biết các mối đe dọa bảo mật phổ biến, các biện pháp phòng ngừa và hướng dẫn họ báo cáo các hoạt động nghi ngờ liên quan đến bảo mật.

Xây dựng kế hoạch ứng phó sự cố: Tổ chức cần xây dựng kế hoạch ứng phó sự cố và tổ chức các cuộc kiểm tra thường xuyên để đảm bảo tính khả thi và hiệu quả của kế hoạch ứng phó. Kế hoạch nên gồm các phương thức xử lý các sự cố bảo mật, phục hồi dữ liệu và khôi phục hoạt động kinh doanh.

Câu e:

Đặt giám sát trên website: Tổ chức nên cài đặt các phần mềm giám sát để theo dõi các hoạt động trên website, phát hiện các dấu hiệu của cuộc tấn công mạng và cảnh báo sớm cho quản trị viên.

Cài đặt các giải pháp bảo mật website: Tổ chức nên cài đặt các giải pháp bảo mật website, bao gồm phần mềm chống vi-rút, tường lửa, mã hóa dữ liệu và xác thực người dùng.

Xác định các điểm yếu trên website: Tổ chức nên thực hiện kiểm tra định kỳ để xác định các điểm yếu trên website và đưa ra các biện pháp bảo mật phù hợp nhằm khắc phục các lỗ hổng này.

Đào tạo nhân viên về an ninh mạng: Tổ chức cần đào tạo nhân viên về an ninh mạng để có khả năng phát hiện các dấu hiệu bất thường trên website và báo cáo sớm cho quản trị viên.

Thực hiện kiểm tra bảo mật định kỳ: Tổ chức cần thực hiện kiểm tra bảo mật định kỳ để đảm bảo rằng website không có các lỗ hổng bảo mật và đưa ra các biện pháp khắc phục khi cần thiết.

Cập nhật hệ thống và phần mềm thường xuyên: Tổ chức cần cập nhật hệ thống và phần mềm thường xuyên để bảo đảm tính bảo mật và khắc phục các lỗ hổng bảo mật mới xuất hiện.

Cài đặt giải pháp phát hiện xâm nhập: Tổ chức nên cài đặt giải pháp phát hiện xâm nhập để phát hiện các hoạt động bất thường trên website và cảnh báo sớm cho quản trị viên.

Câu f: giải thích

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, tài liệu

Mô tả được tạo tự động

Mục tiêu 1: doanh số bán hàng đạt 50 triệu đồng trong vòng 2 tháng

|  |  |
| --- | --- |
| **Chiến lược** | **Chiến thuật** |
| Nghiên cứu thị trường | Công ty cần phải tìm hiểu về thị trường và đối tượng khách hàng mà họ muốn tiếp cận. Công ty nên tìm hiểu về sở thích và nhu cầu của khách hàng, mức độ cạnh tranh trong ngành và chiến lược tiếp thị của các đối thủ cạnh tranh. |
| Tối ưu hóa trang web | Công ty nên tối ưu hóa trang web của mình để thu hút khách hàng. Điều này bao gồm việc thiết kế trang web hiện đại và thu hút mắt, cải thiện trải nghiệm người dùng, tăng khả năng tìm thấy trang web trên các công cụ tìm kiếm và tăng tính năng của trang web. |
| Quảng cáo trực tuyến | Công ty nên sử dụng các nền tảng quảng cáo trực tuyến như Google Ads, Facebook Ads, Instagram Ads,.. để quảng bá sản phẩm và dịch vụ của mình tới khách hàng tiềm năng. |
| Tạo chương trình khuyến mãi | Công ty có thể tạo ra các chương trình khuyến mãi hấp dẫn để thu hút khách hàng và tăng doanh số bán hàng trực tuyến. |
| Gửi email marketing | Công ty nên sử dụng email marketing để giới thiệu sản phẩm mới, chương trình khuyến mãi và các thông tin hữu ích liên quan đến sản phẩm của mình tới khách hàng đã đăng ký nhận thông tin từ công ty. |
| Sử dụng công nghệ để tăng tính năng và tốc độ | Công ty nên sử dụng công nghệ để nâng cao tính năng và tốc độ xử lý đơn hàng, tăng độ chính xác trong quá trình đóng gói và giao hàng. |
| Theo dõi và đánh giá kết quả | Công ty nên theo dõi và đánh giá kết quả của chiến lược tiếp thị của mình để điều chỉnh và cải thiện chiến lược nếu cần thiết. |

Mục tiêu 2: Tăng lượng khách hàng mới tìm đến công ty và sản phẩm của công ty từ 100 người/tháng lên 500 người/tháng trong vòng 6 tháng

|  |  |
| --- | --- |
| Chiến lược | Chiến thuật |
| Facebook | 1) Chạy các chiến dịch khuyến mãi nhắm đến khách hàng tiềm năng.  2) Trả lời để đăng bình luận một cách thường xuyên để làm cho khách hàng cảm thấy có giá trị.  3) Đăng tải video review về sản phẩm  4) Tạo các nội dung vui nhộn như câu đố và trò chơi và tăng cường sự tham gia của người xem. |
| Instagram | 1. Đăng tải các hình ảnh, video ngắn về sản phẩm, cửa hàng 2. Đằng thông tin về sản phẩm mới, khuyến mãi, giảm giá.. |
| Cửa hàng | 1. Thiết kế một logo và biển hiệu độc đáo nhằm để thu hút và tạo ấn tượng cho khách hàng 2. Tặng phiếu giảm giá khi mua số lượng lớn 3. Tạo chương trình tích điểm cho khách quen 4. Pha chế nhiều công thức khác nhau 5. Chương trình dùng thử sản phẩm mới |
| Tiktok | 1. Chạy quảng cáo trên nền tảng bằng các video thu hút 2. Xây dựng kênh Tiktok riêng cho cửa hàng 3. Cộng tác với các Tiktoker review food |
|  |  |

|  |  |
| --- | --- |
| Nghiên cứu thị trường | Tìm hiểu về thị trường, đối tượng khách hàng tiềm năng và đối thủ cạnh tranh. Công ty cần tìm hiểu rõ về các đặc điểm của khách hàng tiềm năng như độ tuổi, giới tính, thu nhập, sở thích, v.v. |
| Xây dựng chiến lược quảng cáo trên mạng | Tạo nhiều hình thức quảng cáo trên các mạng xã hội như Facebook, Instagram, Zalo, v.v. để giới thiệu sản phẩm và thương hiệu đến đối tượng khách hàng tiềm năng. Công ty nên đầu tư vào các quảng cáo trên mạng để thu hút lượng khách hàng mới tới với sản phẩm và thương hiệu của mình. |
| Tham gia các sự kiện trên mạng | Tận dụng các sự kiện online để quảng bá sản phẩm của công ty. Tham gia các trò chơi trên mạng để tăng độ tương tác với khách hàng, tạo sự quan tâm và thu hút khách hàng mới đến với công ty. |
| Phát triển chương trình giới thiệu khách hàng | Tạo ra chương trình giới thiệu khách hàng để khuyến khích khách hàng hiện tại giới thiệu sản phẩm của công ty đến những người khác. Các chương trình giới thiệu khách hàng sẽ giúp công ty thu hút khách hàng mới và tăng doanh số bán hàng. |
| Cập nhật website và SEO | Công ty cần cập nhật website thường xuyên, đảm bảo website đáp ứng nhu cầu tìm kiếm của khách hàng. Đồng thời, công ty cần tối ưu hóa website để tăng khả năng hiển thị trên các công cụ tìm kiếm như Google, Bing, Yahoo, v.v. Việc tối ưu hóa SEO sẽ giúp tăng lượng truy cập trang web của công ty, từ đó thu hút lượng khách hàng mới. |
| Tạo nội dung chất lượng trên blog và mạng xã hội | Tạo nội dung có giá trị để khách hàng thấy được giá trị của sản phẩm và thương hiệu của công ty. Nội dung này có thể bao gồm các bài viết, hướng dẫn sử dụng sản phẩm, video |

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, số

Mô tả được tạo tự động

Câu a: ransomware

Nguyên nhân:

Thiếu các biện pháp bảo mật đủ mạnh: Nếu JBS không đầu tư đủ tiền vào bảo mật mạng và hệ thống của mình, thì chúng có thể dễ bị tấn công bởi các hacker có kỹ năng.

Sử dụng phần mềm lỗi thời: Nếu JBS không đưa các phần mềm và hệ thống của mình lên phiên bản mới nhất, thì chúng có thể dễ bị khai thác bởi các hacker sử dụng các lỗ hổng bảo mật đã được khắc phục trong các phiên bản mới hơn.

Không đào tạo đội ngũ nhân viên về an ninh mạng: Nếu nhân viên của JBS không được đào tạo về các biện pháp bảo mật mạng và cách phát hiện và ngăn chặn các cuộc tấn công, thì họ có thể không nhận ra được các hoạt động bất thường và dễ bị lừa đảo bởi các hacker.

Phụ thuộc quá nhiều vào các nhà cung cấp bảo mật mạng: Nếu JBS không có khả năng tự bảo vệ hệ thống của mình và phụ thuộc quá nhiều vào các nhà cung cấp bảo mật mạng bên ngoài, thì họ có thể gặp nguy cơ bị tấn công thông qua các lỗ hổng trong hệ thống của nhà cung cấp bảo mật mạng đó.

Hành động của các hacker: Các hacker có thể sử dụng các kỹ thuật tinh vi để xâm nhập vào hệ thống mạng của JBS và tấn công thông qua các lỗ hổng bảo mật để mã hóa dữ liệu và đòi tiền chuộc.

Câu b:

Ransomware là một loại phần mềm độc hại được thiết kế để khóa một số tài nguyên quan trọng trên hệ thống, như các tệp tin, cơ sở dữ liệu hoặc toàn bộ máy tính của người dùng. Sau đó, tên lửa phát mã độc sẽ yêu cầu một khoản tiền chuộc để giải khóa tài nguyên.

Cách thức tấn công thường bắt đầu bằng việc gửi một email giả mạo với đính kèm file độc hại đến các nhân viên của JBS. Khi một nhân viên mở tệp tin đính kèm, nó sẽ tự động cài đặt mã độc Ransomware lên máy tính của họ. Mã độc sẽ sau đó bắt đầu khóa lại các tài nguyên quan trọng trên hệ thống của JBS và yêu cầu một khoản tiền chuộc để giải khóa.

Trong trường hợp của JBS, các hacker đã sử dụng phần mềm độc hại để tấn công vào các máy chủ của công ty, khóa các tài nguyên và yêu cầu một khoản tiền chuộc lớn để giải khóa. Tình huống này đã gây ra những hậu quả nghiêm trọng cho công ty và ngành công nghiệp chế biến thịt bởi vì tất cả nhà máy chế biến thịt bò của JBS đều bị đóng cửa trong khi công ty đang tìm cách khắc phục tình trạng tấn công mạng.

Câu c:

Nâng cao ý thức an ninh thông tin cho nhân viên: Đào tạo nhân viên về các nguy cơ an ninh mạng, cách phát hiện và ngăn chặn các cuộc tấn công mạng, và cách bảo vệ thông tin quan trọng.

Cập nhật và bảo mật hệ thống: Đảm bảo các phần mềm, ứng dụng và thiết bị được cập nhật bản vá mới nhất và áp dụng các chính sách bảo mật mạnh để ngăn chặn các lỗ hổng bảo mật.

Sử dụng các giải pháp bảo vệ đa lớp: Bao gồm cả giải pháp phần mềm và phần cứng để ngăn chặn các cuộc tấn công từ các mối đe dọa khác nhau.

Tạo ra các bản sao dữ liệu và thực hiện sao lưu định kỳ: Đảm bảo rằng các bản sao dữ liệu được lưu trữ tại nhiều địa điểm khác nhau để tránh mất dữ liệu trong trường hợp xảy ra sự cố.

Giám sát mạng và hệ thống: Theo dõi các hoạt động trên mạng và hệ thống để phát hiện và ngăn chặn các hoạt động bất thường hoặc các cuộc tấn công mạng.

Tạo ra các kế hoạch khẩn cấp và phòng chống tấn công mạng: Đảm bảo rằng tổ chức có một kế hoạch phản ứng khẩn cấp và có thể xử lý các sự cố mạng nhanh chóng để giảm thiểu thiệt hại.

Tăng cường hợp tác và chia sẻ thông tin: Các tổ chức và doanh nghiệp nên hợp tác với nhau để chia sẻ thông tin về các mối đe dọa an ninh mạng, các phương pháp tấn công mới và cách phòng chống chúng.

Theo dõi các hoạt động mạng: Các doanh nghiệp cần có các giải pháp giám sát mạng để theo dõi các hoạt động mạng và phát hiện các hành vi bất thường. Các giải pháp này có thể bao gồm các công cụ phát hiện xâm nhập (IDS) hoặc phát hiện xâm nhập và phản ứng (IDPS).

Phân tích dữ liệu và đối tượng: Các doanh nghiệp cần phân tích các dữ liệu và đối tượng được truy cập trên hệ thống của họ để phát hiện các hoạt động bất thường. Việc giám sát các lưu lượng mạng, các tệp và thư mục được truy cập, và các truy cập vào các ứng dụng quan trọng cũng là cách hiệu quả để phát hiện các hoạt động độc hại.

Sử dụng giải pháp bảo mật tiên tiến: Các doanh nghiệp cần sử dụng các giải pháp bảo mật tiên tiến như phần mềm diệt virus, tường lửa và phần mềm chống thâm nhập để phát hiện và ngăn chặn các tấn công

Đào tạo nhân viên về an ninh mạng: Các doanh nghiệp nên đào tạo nhân viên của mình về an ninh mạng và giúp họ nhận biết các dấu hiệu của các cuộc tấn công mạng. Điều này có thể giúp nâng cao khả năng phát hiện và phản ứng của các doanh nghiệp khi có các cuộc tấn công xảy ra.

Kiểm tra bảo mật định kỳ: Các doanh nghiệp nên kiểm tra bảo mật định kỳ để phát hiện và khắc phục các lỗ hổng bảo mật trong hệ thống của họ trước khi các kẻ tấn công khai thác chúng.

Ngắt kết nối mạng: Khi phát hiện các hoạt động bất thường trên mạng, các doanh nghiệp cần phải ngắt kết nối mạng để ngăn chặn các kẻ tấn công tiếp tục truy cập vào hệ thống của họ.

Thực hiện các bước khẩn cấp: Các doanh nghiệp cần phải thực hiện các bước khẩn cấp để ngăn chặn sự lây lan của các hoạt động độc hại trên hệ thống của họ. Điều này có thể bao gồm việc thay đổi mật khẩu, phân tích dữ liệu, cập nhật phần mềm bảo mật và thiết lập các giải pháp khôi phục dữ liệu.

Hợp tác với chính quyền và nhà cung cấp dịch vụ bảo mật: Các doanh nghiệp nên hợp tác với chính quyền và nhà cung cấp dịch vụ bảo mật để giúp phát hiện và giải quyết các vấn đề liên quan đến các cuộc tấn công mạng.

Thông báo với khách hàng và đối tác: Các doanh nghiệp cần thông báo với khách hàng và đối tác của họ về các cuộc tấn công mạng và các hoạt động khẩn cấp để bảo vệ thông tin của họ

Đánh giá lại các giải pháp bảo mật hiện có: Các doanh nghiệp cần đánh giá lại các giải pháp bảo mật hiện có của họ để phát hiện các lỗ hổng bảo mật và cải thiện chúng. Việc đánh giá lại này cũng giúp các doanh nghiệp cập nhật và sử dụng các giải pháp mới nhất để đảm bảo an toàn cho hệ thống của họ.

Điều tra và xác định nguyên nhân gốc rễ của cuộc tấn công: Điều tra sự cố bảo mật để tìm ra nguyên nhân và khắc phục chúng.

Khôi phục hệ thống: Sau khi phát hiện và loại bỏ các phần mềm độc hại, cần khôi phục lại hệ thống để đảm bảo hoạt động bình thường của các máy chủ và các dịch vụ liên quan.

Tăng cường bảo mật mạng: Nâng cao bảo mật mạng bằng cách sử dụng các phần mềm bảo mật, tường lửa và các biện pháp bảo mật mạng khác để ngăn chặn các cuộc tấn công tiếp theo.

Đào tạo nhân viên: Đào tạo nhân viên về các mối đe dọa mạng và các biện pháp bảo vệ cần thiết để họ có thể phát hiện và tránh các cuộc tấn công mạng.

Nâng cao quản lý bảo mật: Nâng cao quản lý bảo mật để đảm bảo sự an toàn và bảo mật của hệ thống thông tin của công ty.

Thực hiện kiểm tra thường xuyên: Thực hiện kiểm tra định kỳ trên hệ thống để phát hiện các lỗ hổng bảo mật và đảm bảo rằng hệ thống đang hoạt động đúng cách.

Xây dựng kế hoạch khẩn cấp: Xây dựng kế hoạch khẩn cấp để ứng phó với các cuộc tấn công mạng và đảm bảo rằng công việc của công ty không bị gián đoạn quá nhiều khi xảy ra sự cố.

Câu d: Tôi đề xuất các biện pháp bảo vệ, phát hiện, ứng phó và khắc phục để đối phó với các cuộc tấn công mạng như vụ tấn công mạng đối với JBS SA, vì đó là các biện pháp cơ bản và hiệu quả trong việc giảm thiểu rủi ro của các cuộc tấn công mạng.

Các biện pháp bảo vệ sẽ giúp ngăn chặn các cuộc tấn công từ các hacker hoặc phần mềm độc hại từ việc xâm nhập vào hệ thống. Các biện pháp phát hiện sẽ giúp cho hệ thống có thể phát hiện và báo cáo các cuộc tấn công kịp thời để có thể đưa ra các biện pháp phòng ngừa. Các biện pháp ứng phó sẽ giúp cho tổ chức có thể xử lý các cuộc tấn công khi chúng xảy ra để giảm thiểu thiệt hại gây ra. Cuối cùng, các biện pháp khắc phục sẽ giúp cho tổ chức có thể khôi phục hệ thống sau khi bị tấn công và giảm thiểu thời gian gián đoạn hoạt động.

Tổng thể, các biện pháp này sẽ giúp cho tổ chức có thể đối phó với các cuộc tấn công mạng hiệu quả hơn, giảm thiểu thiệt hại gây ra và tăng cường sự bảo vệ cho hệ thống của tổ chức.

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, tài liệu

Mô tả được tạo tự động

Tăng doanh số bán hàng lên 20% trong năm nay bằng cách tập trung vào khách hàng tiềm năng.

|  |  |
| --- | --- |
| Nghiên cứu thị trường | Tìm hiểu về thị trường tiềm năng, nhu cầu và đặc tính của khách hàng trong lĩnh vực thời trang công sở nữ. Đưa ra các phân tích về đối thủ cạnh tranh, khách hàng tiềm năng và xu hướng thị trường. |
| Tạo nội dung | Tạo ra nội dung trên trang web của cửa hàng để giới thiệu về sản phẩm và quảng bá thương hiệu. Sử dụng các hình ảnh và mô tả sản phẩm rõ ràng, hấp dẫn để thu hút khách hàng. Viết các bài blog về xu hướng thời trang công sở nữ, chia sẻ các mẹo và cập nhật về sản phẩm mới. |
| Tối ưu hóa SEO | Tối ưu hóa trang web của cửa hàng để tăng khả năng hiển thị trên các công cụ tìm kiếm như Google. Điều này giúp tăng khả năng khách hàng tìm thấy cửa hàng khi tìm kiếm các sản phẩm thời trang công sở nữ trên internet. |
| Quảng cáo trực tuyến | Sử dụng các kênh quảng cáo trực tuyến để tiếp cận khách hàng tiềm năng, bao gồm quảng cáo trên Facebook, Instagram và Google Ads. Để đảm bảo hiệu quả cao, cần chọn các đối tượng khách hàng phù hợp và tối ưu chi phí quảng cáo. |
| Tạo khuyến mãi hấp dẫn | Tạo các chương trình khuyến mãi hấp dẫn để thu hút khách hàng mới và khách hàng quay lại mua sản phẩm. Các khuyến mãi có thể bao gồm giảm giá, tặng quà, miễn phí vận chuyển,... |
| Tạo các chương trình thưởng khách hàng | Tạo các chương trình thưởng khách hàng thân thiết để giữ chân khách hàng hiện có. Các chương trình này có thể bao gồm điểm thưởng, giảm giá cho các đơn hàng tiếp theo, ưu đãi đặc biệt và cập nhật mới nhất về sản phẩm. |
| Sử dụng email marketing | gửi email quảng cáo, email thông tin hoặc email giải quyết thắc mắc trực tiếp đến khách hàng hoặc đối tác tiềm năng của họ. Email marketing có thể được sử dụng để giới thiệu sản phẩm mới, khuyến mãi, thông báo sự kiện hoặc cung cấp nội dung giá trị như tin tức, bài viết, blog, v.v. |

Tăng nhận diện thương hiệu bằng cách tăng số lượng người theo dõi trang Instagram của cửa hàng lên ít nhất 5.000 trong vòng 3 tháng và tăng số lượt tìm kiếm trên Google bằng cách tối thiểu 2 lần trong vòng 6 tháng.

|  |  |
| --- | --- |
| Nâng cao chất lượng sản phẩm | Cửa hàng cần đảm bảo sản phẩm độc đáo và chất lượng tốt để thu hút khách hàng. Đồng thời, cửa hàng cần chú ý đến giá cả để sản phẩm vẫn giữ được tính cạnh tranh. |
| Nâng cao trải nghiệm mua sắm trên website | Cửa hàng cần cải thiện giao diện, tốc độ tải trang và tính năng của website để khách hàng có trải nghiệm mua sắm tốt hơn. Đồng thời, cửa hàng cần đảm bảo tính bảo mật cho khách hàng khi thanh toán trực tuyến. |
| Tăng sự hiện diện trên mạng xã hội | Cửa hàng nên sử dụng mạng xã hội để quảng bá sản phẩm và tương tác với khách hàng. Cửa hàng có thể sử dụng các kênh như Facebook, Instagram, Pinterest để đăng tải hình ảnh sản phẩm, chương trình khuyến mãi và thu hút khách hàng. |
| Thực hiện chương trình khuyến mãi | Cửa hàng có thể tổ chức các chương trình khuyến mãi để thu hút khách hàng. Các chương trình khuyến mãi có thể bao gồm giảm giá, tặng quà, free ship và các ưu đãi khác. |
| Tăng tương tác với khách hàng | Cửa hàng cần thường xuyên tương tác với khách hàng để đáp ứng nhu cầu và giải đáp thắc mắc của khách hàng. Cửa hàng có thể sử dụng các kênh như email, tin nhắn và điện thoại để liên lạc với khách hàng. |

Tăng lượng khách hàng trung thành bằng cách giảm tỷ lệ đổi trả hàng xuống dưới 5% trong vòng 1 năm và tăng số lượng khách hàng mua lại bằng cách tối thiểu 30% trong vòng 6 tháng.

|  |  |
| --- | --- |
| Khuyến mãi giảm giá cho các sản phẩm phổ biến | Tạo ra một chương trình khuyến mãi giảm giá cho một số sản phẩm phổ biến trong cửa hàng như áo sơ mi, quần tây,...Giảm giá khoảng 10-20% cho các sản phẩm này có thể giúp cửa hàng tăng doanh số bán hàng và thu hút được nhiều khách hàng mới. |
| Khuyến mãi tặng phẩm | Tạo ra chương trình khuyến mãi tặng quà cho khách hàng khi mua hàng với số tiền nhất định. Ví dụ như khách hàng mua sản phẩm với giá trị từ 1.500.000 VNĐ trở lên sẽ được tặng một chiếc khẩu trang vải, hoặc một chiếc kẹp tóc. |
| Quảng cáo trên các kênh truyền thông xã hội | Sử dụng quảng cáo trên Facebook, Instagram để tiếp cận đến khách hàng tiềm năng. Cửa hàng có thể sử dụng các hình ảnh, video quảng cáo để giới thiệu sản phẩm, các chương trình khuyến mãi, giảm giá, tặng quà,... |
| Email Marketing | Gửi email đến các khách hàng hiện có và khách hàng tiềm năng để giới thiệu các sản phẩm mới nhất, chương trình khuyến mãi, giảm giá. Tuy nhiên, cửa hàng cần chú ý không gửi quá nhiều email để không làm phiền khách hàng. |
| Tăng tính tương tác với khách hàng | Tạo ra một kênh giao tiếp để khách hàng có thể tư vấn, hỏi đáp về các sản phẩm của cửa hàng. Cửa hàng có thể sử dụng các ứng dụng như Facebook Messenger, Zalo để tương tác với khách hàng một cách nhanh chóng và thuận tiện. |
| Tham gia sự kiện | Tham gia các sự kiện về thời trang, triển lãm, hay hội chợ để giới thiệu sản phẩm của cửa hàng đến với nhiều khách hàng mới. Cửa hàng có thể bày bán các sản phẩm của mình tại các gian hàng, tham gia trình diễn thời trang,... |

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, tài liệu

Mô tả được tạo tự động

Câu a: hành vi của X vi phạm quy định liên quan đến thư điện tử, tin nhắn cung cấp thông tin về sản phẩm, dịch vụ được quy định trong Nghị định 15/2020/NĐ-CP

Câu b: hành vi sẽ bị xử lý theo khoản 2 Điều 94

Lý do vì cty X thu thập thông tin email khách hàng là để tạo tài khoản nhưng sau đó lại sử dụng email của khách hàng để gới thiệu về chương trình khuyến mại sắp tới, điều này là chưa được sự cho phép của khách hàng và vi phạm theo nghị định 15/2020/NĐ-CP về việc gửi thư điện tử quảng cáo đến người nhận nhưng chưa được sự đồng ý của người nhận. Theo điểm a khoản 2 điều 94 thì công ty X bị phạt tiền từ 5-10tr đối với hành vi này

Ảnh có chứa văn bản, Phông chữ, ảnh chụp màn hình, số

Mô tả được tạo tự động

1. Phần mềm độc hại được sử dụng trong cuộc tấn công mạng trên là loại ransomware (phần mềm chuộc tiền).

Các nguyên nhân có thể dẫn đến tình huống trên bao gồm:

Sự lơ là trong việc bảo vệ an ninh mạng của công ty Colonial Pipeline, bao gồm việc không cập nhật phần mềm đầy đủ và không thực hiện các biện pháp bảo mật hiệu quả để ngăn chặn các cuộc tấn công mạng.

Sự chuyên nghiệp và tinh vi của các nhóm tội phạm công nghệ, khiến cho họ có thể phát hiện và khai thác các lỗ hổng trong hệ thống mạng của Colonial Pipeline để tiến hành cuộc tấn công.

Sự phụ thuộc quá mức vào các công nghệ kỹ thuật số và việc kết nối chúng với một hệ thống trung tâm duy nhất, khiến cho một cuộc tấn công thành công có thể ảnh hưởng đến toàn bộ hệ thống vận hành của Colonial Pipeline.

Thiếu kiểm soát bảo mật: Đường ống của Colonial Pipeline sử dụng nhiều công nghệ kỹ thuật số tối tân để giám sát và quản lý dòng chảy của nhiên liệu, và tất cả các thiết bị này được kết nối với một hệ thống trung tâm. Nếu hệ thống này không được bảo mật tốt, nó sẽ trở thành mục tiêu dễ bị tấn công cho các tin tặc.

Sử dụng phần mềm lỗi thời: Nếu Colonial Pipeline sử dụng phần mềm cũ hoặc không được cập nhật thường xuyên, những lỗ hổng bảo mật có thể được tìm thấy và khai thác bởi các tin tặc.

Sự chủ quan trong bảo mật: Nếu Colonial Pipeline không có chính sách bảo mật tốt và đào tạo nhân viên về các mối đe dọa mạng, nhân viên có thể trở thành điểm yếu và làm cho hệ thống dễ bị tấn công hơn.

Tấn công từ các nhóm tội phạm công nghệ chuyên nghiệp: Các nhóm tội phạm công nghệ ngày càng trở nên tinh vi và chuyên nghiệp hơn, sử dụng các công nghệ tiên tiến và các chiến lược tấn công mới để thâm nhập vào hệ thống của các công ty và tổ chức.

1. Một trong những phương thức tấn công thông dụng mà có thể dẫn đến tình huống trên là "phishing". Phishing là một kỹ thuật lừa đảo trực tuyến, trong đó tin tặc sử dụng các phương tiện giả mạo để lừa người dùng cung cấp thông tin nhạy cảm như tên đăng nhập, mật khẩu hoặc thông tin thẻ tín dụng. Thông thường, một cuộc tấn công phishing bắt đầu bằng việc gửi một email, tin nhắn hoặc trang web giả mạo, được thiết kế để giả mạo một doanh nghiệp hay tổ chức nào đó mà nạn nhân đang tin tưởng, và yêu cầu nạn nhân cung cấp thông tin cá nhân hoặc bấm vào một liên kết để đăng nhập vào tài khoản của họ.

Trong trường hợp tấn công Colonial Pipeline, tin tặc có thể đã sử dụng phương thức này để đánh cắp thông tin đăng nhập của một hoặc nhiều tài khoản nhân viên của Colonial Pipeline. Sau đó, họ có thể sử dụng thông tin này để truy cập vào hệ thống của Colonial Pipeline và triển khai phần mềm độc hại để mã hóa dữ liệu và yêu cầu chuộc tiền.

Bảo vệ

Tăng cường an ninh mạng: Các tổ chức cần tăng cường khả năng phát hiện, phòng chống, và giảm thiểu rủi ro tấn công mạng. Các biện pháp bảo vệ an ninh mạng bao gồm: cập nhật phần mềm, cài đặt các giải pháp bảo mật như tường lửa, chống virus, phát hiện xâm nhập, giám sát mạng, bảo mật dữ liệu, đào tạo nhân viên về an ninh mạng.

Sao lưu dữ liệu thường xuyên: Các tổ chức cần định kỳ sao lưu dữ liệu quan trọng, đảm bảo dữ liệu có thể khôi phục được trong trường hợp bị mã hóa hoặc bị xóa.

Điều tra và phản ứng kịp thời: Các tổ chức cần có kế hoạch ứng phó khi bị tấn công mạng. Kế hoạch này cần bao gồm việc giám sát, phát hiện, xử lý các mối đe dọa an ninh mạng. Điều tra sự cố mạng và xác định nguyên nhân cũng là một yếu tố quan trọng để phòng ngừa các cuộc tấn công tương tự trong tương lai.

Kiểm soát truy cập: Tăng cường kiểm soát truy cập vào các tài khoản và hệ thống quan trọng, sử dụng các phương pháp chứng thực mạnh, quản lý mật khẩu chặt chẽ, đảm bảo rằng chỉ có người dùng có quyền truy cập mới được phép truy cập vào các thông tin quan trọng.

Đầu tư vào công nghệ bảo mật: Đầu tư vào công nghệ bảo mật như mã hóa dữ liệu, quản lý khóa, hệ thống xác thực, và các công nghệ mới như trí tuệ nhân tạo, học sâu, học máy để phát hiện các mối đe dọa mạng.

Nâng cao ý thức về an ninh mạng: Đào tạo nhân viên về các mối đe dọa an ninh mạng và cách phòng chống, nâng cao ý thức về an toàn thông tin, đảm bảo người

Dưới đây là một số biện pháp phát hiện có thể được đề xuất để phòng ngừa tình huống tấn công mạng tương tự như vụ việc Colonial Pipeline:

Thực hiện kiểm tra bảo mật định kỳ: Các doanh nghiệp và tổ chức cần thường xuyên kiểm tra các hệ thống của mình để phát hiện các lỗ hổng bảo mật, phát hiện sớm các mối đe dọa mới và giảm thiểu nguy cơ bị tấn công.

Áp dụng các giải pháp bảo mật nâng cao: Các giải pháp bảo mật như tường lửa, phần mềm diệt virus, phát hiện xâm nhập (IDS/IPS), mã hóa dữ liệu, xác thực hai yếu tố và quản lý nhận dạng và truy cập có thể được áp dụng để giảm thiểu nguy cơ bị tấn công mạng.

Thực hiện giám sát hệ thống: Các tổ chức cần theo dõi liên tục các hệ thống của mình để phát hiện các hoạt động bất thường, có thể là dấu hiệu của các cuộc tấn công mạng.

Tập huấn nhân viên: Các nhân viên của các tổ chức cần được đào tạo để phát hiện và phòng ngừa các cuộc tấn công mạng.

Sử dụng phần mềm phát hiện độc hại: Các phần mềm phát hiện độc hại có thể giúp phát hiện các phần mềm độc hại và các cuộc tấn công mạng.

Thiết lập các quy trình và chính sách bảo mật: Các tổ chức cần phát triển các chính sách và quy trình bảo mật để đảm bảo rằng các hoạt động của họ tuân thủ các tiêu chuẩn bảo mật và giảm thiểu nguy cơ bị tấn công mạng.

Để ứng phó với tình huống tấn công mạng và khắc phục hệ quả của vụ việc, có thể đề xuất một số biện pháp ứng phó như sau:

Khôi phục dữ liệu: Nếu dữ liệu đã bị mã hóa, cần phải có kế hoạch khôi phục dữ liệu sớm nhất có thể. Các bản sao lưu dữ liệu nên được tạo thường xuyên để giảm thiểu tác động của việc mất dữ liệu trong trường hợp này.

Đưa ra thông báo: Thông báo về vụ tấn công mạng cần được đưa ra ngay lập tức để nhân viên và khách hàng của công ty được cảnh báo và thực hiện các biện pháp phòng ngừa như thay đổi mật khẩu, kiểm tra thông tin cá nhân, v.v.

Phân tích sự cố: Các chuyên gia bảo mật mạng nên được triệu tập để phân tích sự cố và đưa ra kế hoạch khắc phục.

Đưa ra kế hoạch khắc phục: Kế hoạch khắc phục cần được xây dựng dựa trên các phân tích của các chuyên gia bảo mật mạng. Các biện pháp khắc phục có thể bao gồm việc loại bỏ phần mềm độc hại, cập nhật phần mềm và khôi phục dữ liệu.

Nâng cao an ninh mạng: Các biện pháp an ninh mạng cần được nâng cao để đảm bảo an toàn cho hệ thống mạng. Các biện pháp này có thể bao gồm việc thay đổi mật khẩu thường xuyên, giám sát mạng liên tục, cập nhật phần mềm, v.v.

Tăng cường giám sát và phòng ngừa: Các biện pháp giám sát và phòng ngừa cần được tăng cường để ngăn chặn các cuộc tấn công mạng trong tương lai. Các biện pháp này có thể bao gồm việc giám sát các hệ thống mạng, xác thực người dùng và tăng cường kiểm soát truy cập.

Để khắc phục tình huống trên, có thể áp dụng các biện pháp sau:

Phục hồi hệ thống: Các chuyên gia bảo mật mạng nên được triệu tập để kiểm tra và phục hồi hệ thống. Họ cần xác định quy trình khôi phục dữ liệu, đảm bảo các thiết bị bị tấn công đã được bảo vệ và tiến hành khôi phục từ dữ liệu sao lưu.

Đưa ra các giải pháp đối phó với tấn công: Nếu đã xác định được các nguyên nhân và hình thức tấn công, có thể đưa ra các giải pháp đối phó như cập nhật phần mềm, đổi mật khẩu, thiết lập các cơ chế kiểm tra và bảo vệ hệ thống

Nâng cao năng lực phòng ngừa: Hệ thống bảo mật mạng cần được nâng cao, bao gồm cả việc cập nhật phần mềm, đảm bảo các thông tin cá nhân được bảo vệ và áp dụng các biện pháp bảo vệ khác để phòng chống tấn công trong tương lai.

Tăng cường giám sát: Việc giám sát và theo dõi các hoạt động trên hệ thống mạng cần được tăng cường. Các chuyên gia bảo mật mạng cần phải xác định các hành vi đáng ngờ và cập nhật thông tin liên tục để phòng ngừa các tấn công tiềm năng.

Tăng cường đào tạo nhân viên: Nhân viên của Colonial Pipeline cần được đào tạo về các biện pháp bảo mật mạng, đặc biệt là về việc phát hiện và ngăn chặn các tấn công mạng. Ngoài ra, cần phải xây dựng chính sách an ninh mạng và áp dụng nghiêm các quy định liên quan để ngăn chặn các lỗ hổng bảo mật.

Ảnh có chứa văn bản, ảnh chụp màn hình, Phông chữ, tài liệu

Mô tả được tạo tự động

Tăng số lượng người dùng đăng ký tài khoản miễn phí lên 500 người trong vòng 3 tháng đầu tiên bằng cách chạy chiến dịch quảng cáo trực tuyến mạnh mẽ.

|  |  |
| --- | --- |
| Tạo và tối ưu hóa trang landing page | Tạo một trang landing page chuyên nghiệp, thuyết phục và dễ sử dụng để giới thiệu ứng dụng và giá trị của nó đến khách hàng mục tiêu. Tối ưu hóa trang landing page để đảm bảo tốc độ tải nhanh và thân thiện với thiết bị di động. |
| Chạy chiến dịch quảng cáo trực tuyến | Sử dụng các kênh quảng cáo trực tuyến như Google Ads, Facebook Ads, LinkedIn Ads để tiếp cận đối tượng khách hàng mục tiêu và giới thiệu về ứng dụng. Tạo các quảng cáo có hình ảnh và nội dung hấp dẫn, chính xác và cụ thể để thu hút sự chú ý và tăng tỉ lệ nhấp vào trang landing page. |
| Sử dụng email marketing | Sử dụng email marketing để giới thiệu ứng dụng và các tính năng mới đến khách hàng mục tiêu. Tạo các email thân thiện, chuyên nghiệp và dễ đọc, bao gồm hình ảnh và liên kết trực tiếp đến trang landing page. |
| Sử dụng nội dung và SEO | Tạo nội dung giáo dục và hấp dẫn để thu hút người dùng đến trang web của bạn thông qua kết quả tìm kiếm tự nhiên. Tối ưu hóa trang web của bạn cho SEO bằng cách sử dụng các từ khóa phù hợp và tối ưu hóa đường dẫn trang. |
| Sử dụng marketing trên mạng xã hội | Sử dụng các mạng xã hội như Facebook, LinkedIn, Twitter để chia sẻ nội dung giới thiệu về ứng dụng và các tính năng mới của nó. Tạo các bài đăng có hình ảnh và nội dung hấp dẫn, bao gồm liên kết đến trang landing page của bạn. |
| Sử dụng các trang web giáo dục để quảng bá | Liên hệ với các trang web giáo dục uy tín để quảng bá về ứng dụng của bạn. Cung cấp thông tin chi tiết về ứng dụng, tính năng mới và lợi |

Tăng doanh thu lên 20% so với quý trước bằng cách tăng số lượng khách hàng VIP đăng ký trong vòng 6 tháng đầu tiên.

|  |  |
| --- | --- |
| Xây dựng nội dung chất lượng | Nội dung là yếu tố quan trọng nhất để thu hút và giữ chân người dùng. Chúng ta cần tạo ra những chương trình học chất lượng cao, phù hợp với nhu cầu và yêu cầu của học viên. Đồng thời, nên đưa các giáo viên có uy tín, có kinh nghiệm, tâm huyết vào nền tảng ứng dụng để giảng dạy. |
| Tìm kiếm đối tác | Đối tác chính của chúng ta là các trung tâm đào tạo và giáo viên. Chúng ta cần tìm kiếm và đàm phán với các trung tâm, giáo viên để họ đăng ký tài khoản VIP và sử dụng nền tảng ứng dụng của chúng ta. Đồng thời, chúng ta cũng có thể cung cấp chương trình học miễn phí hoặc giảm giá để thu hút và giữ chân các trung tâm, giáo viên. |
| Tiếp thị trực tuyến | Tiếp thị trực tuyến là một phương tiện hiệu quả để giới thiệu ứng dụng của chúng ta đến với khách hàng mục tiêu. Chúng ta có thể sử dụng các kênh tiếp thị trực tuyến như quảng cáo Google, quảng cáo trên mạng xã hội như Facebook, Instagram, LinkedIn... để tăng khả năng nhìn thấy và tìm thấy ứng dụng của chúng ta. Ngoài ra, chúng ta cũng có thể sử dụng email marketing, chương trình khuyến mãi và các chiến dịch khác để giới thiệu sản phẩm của mình. |
| Marketing liên kết | Marketing liên kết là một hình thức tiếp thị khác giúp chúng ta thu hút người dùng mới và tăng doanh số. Chúng ta có thể tìm kiếm các đối tác liên kết có liên quan đến lĩnh vực giáo dục để đăng ký và chia sẻ các chương trình học của chúng ta đến với học viên của họ. Các đối tác này sẽ nhận được tiền hoa hồng dựa |

Tăng số lượng lớp học trên ứng dụng lên 20 lớp bằng cách đăng ký các giáo viên và trung tâm đào tạo mới trong vòng 12 tháng đầu tiên.

|  |  |
| --- | --- |
| Xác định khách hàng mục tiêu | Tìm kiếm các trung tâm đào tạo và giáo viên mới trong ngành giáo dục trực tuyến  Tìm kiếm học viên tiềm năng và đối tượng khách hàng của các trung tâm đào tạo mới |
| Xây dựng chiến lược truyền thông và tiếp thị | Tăng cường quảng bá thông tin về ứng dụng trên các kênh truyền thông xã hội và trang web của doanh nghiệp, với nội dung hấp dẫn và có tính tương tác cao để thu hút khách hàng mới.  Tạo ra các chiến dịch quảng cáo trên Google Ads hoặc các nền tảng quảng cáo trực tuyến khác để tăng lưu lượng truy cập và giới thiệu về ứng dụng tới khách hàng tiềm năng.  Xây dựng chương trình khuyến mãi để thu hút khách hàng mới sử dụng ứng dụng hoặc các dịch vụ VIP của ứng dụng. |
| Tạo sự hấp dẫn và chuyên nghiệp trên ứng dụng | Cập nhật liên tục các nội dung giảng dạy, bài giảng mới, tạo nên sự đa dạng và hấp dẫn cho học viên khi truy cập ứng dụng.  Xây dựng chương trình đào tạo và hỗ trợ giáo viên, trung tâm đào tạo mới sử dụng ứng dụng, cung cấp các công cụ và tài nguyên hỗ trợ cho việc giảng dạy và quản lý các lớp học trên ứng dụng. |
| Đo lường và theo dõi hiệu quả kế hoạch tiếp thị | Đo lường lưu lượng truy cập và tần suất đăng ký tài khoản trên ứng dụng để đánh giá hiệu quả của chiến lược quảng bá và tiếp thị.  Theo dõi và đánh giá số lượng giáo viên và trung tâm đào tạo mới đăng ký và sử dụng ứng dụng.  Thực hiện điều chỉnh và cải thiện kế hoạch tiếp thị theo kết quả đánh giá được. |