Câu 1:

Câu a: Hàng giả được đề cập đến trong nghị định 98/2020/ND-CP

Công ty vi phạm: Điều 3 khoản 7: chứng minh túi giả (thế nào là hàng giả)

Câu b: Nếu công ty B bị khởi kiện sẽ phải bị xử phạt 30-50tr đồng theo điểm E khoản 1 điều 11 theo nghị định 98/2020/ND-CP

giải thích: vì số tiến chiếc túi này làm giả có giá 59tr, nằm trong mức xử phạt của điểm E (Ghi rõ cái điểm e quy định ra)

Câu 2

Câu a: các phương thức tấn công hacker có thể sử dụng đế lấy cắp tài khoản nhân viên là

Phishing: Hacker có thể gửi email giả mạo để đánh lừa nhân viên của Ebay, yêu cầu 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.

Phương 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.

Câu c: ứng phó

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.

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

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.

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.

Câu d: bảo vệ

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.

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.

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

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

Tăng cường bảo mật cho hệ thống mạng bằng cách sử dụng các giải pháp bảo mật như tường lửa, phần mềm chống virus, mã hóa dữ liệu

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.

Câu e: phát hiện

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: tại sao đề xuất bảo vệ như trên

Đề xuất là phải đưa ra vấn đề -> vấn đề về các cuộc tấn công

Vì doanh nghiệp sẽ phải đối mặt với những nguy cơ tiềm ẩn về vấn đề an ninh, bảo mật nên cần có các biện pháp bảo vệ phù hợp, kịp thời và chính xác. Điều này sẽ đảm bảo an toàn về tính bảo mật vì dù cho sự cố lớn hay nhỏ cũng đều có những tác hại làm ảnh hưởng đến công ty. Các biện pháp đã đề xuất như …(nếu ra) là những biện pháp phù hợp nhằm giúp góp phần tăng cường….(câu dưới)

Các biện pháp bảo vệ được đề xuất nhằm tăng cường bảo mật cho hệ thống mạng và giảm thiểu rủi ro có thể xảy ra tình huống tương tự trong tương lai.

Các biện pháp nhằm sớm phát hiện khi website bị tấn công giúp giám sát hoạt động của trang web và phát hiện các hoạt động bất thường sớm nhất có thể để có biện pháp xử lý kịp thời.

Câu 3

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

|  |  |
| --- | --- |
| 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 |