**1. Tấn công mạng (Cyber Attacks)**

**Giải thích:** Các tấn công mạng như tấn công DDoS (Distributed Denial of Service) có thể làm tê liệt hoạt động của website, khiến khách hàng không thể truy cập vào dịch vụ để tìm hiểu thông tin hoặc thực hiện giao dịch. Hơn nữa, các hình thức tấn công như phishing có thể đánh cắp thông tin cá nhân của khách hàng khi họ tương tác với website.

**2. Rò rỉ dữ liệu (Data Breaches)**

**Giải thích:** Website chứa thông tin nhạy cảm của khách hàng như thông tin cá nhân, tài chính và các hợp đồng bảo hiểm. Nếu hệ thống bảo mật không được duy trì chặt chẽ, có thể xảy ra các vụ rò rỉ dữ liệu, làm lộ thông tin khách hàng cho các đối tượng không mong muốn. Điều này không chỉ ảnh hưởng đến khách hàng mà còn làm giảm uy tín của công ty.

**3. Lỗi bảo mật trong ứng dụng (Application Security Vulnerabilities)**

**Giải thích:** Các lỗi bảo mật trong mã nguồn của website có thể cho phép kẻ tấn công khai thác và truy cập trái phép vào hệ thống. Ví dụ, nếu không có các biện pháp bảo vệ thích hợp (như xác thực người dùng và mã hóa dữ liệu), kẻ tấn công có thể chiếm quyền điều khiển tài khoản của khách hàng, truy cập vào các thông tin bảo hiểm hoặc thậm chí thực hiện các giao dịch trái phép.

**Biện pháp giảm thiểu rủi ro:**

* **Triển khai tường lửa và hệ thống phát hiện xâm nhập** để bảo vệ website khỏi các tấn công mạng.
* **Mã hóa thông tin nhạy cảm** và áp dụng xác thực đa yếu tố để bảo vệ tài khoản người dùng.
* **Thường xuyên kiểm tra và cập nhật phần mềm** để vá các lỗ hổng bảo mật và cải thiện hệ thống bảo mật tổng thể.

■ Công ty VCCloud là một trong nhiều công ty viễn thông, cung cấp các dịch vụ CDN cho các cá nhân và doanh nghiệp tại Việt Nam. Dịch vụ CDN là mạng lưới gồm nhiều máy chủ lưu trữ đặt tại nhiều vị trí địa lý khác nhau, cùng làm việc chung để phân phối nội dung, truyền tải hình ảnh, CSS, Javascript, Video clip, Real-time media streaming, File download đến người dùng cuối. Cơ chế hoạt động của CDN giúp cho khách hàng truy cập nhanh vào dữ liệu máy chủ web gần họ nhất thay vì phải truy cập vào dữ liệu máy chủ web tại trung tâm dữ liệu.

- Hãy nhận dạng và giải thích được ít nhất 3 mối đe dọa ảnh hưởng đến an toàn đến dịch vụ CDN mà VCCloud đang cung cấp

**1. Tấn công DDoS (Distributed Denial of Service)**

**Giải thích:** Tấn công DDoS là khi nhiều máy chủ hoặc thiết bị cùng nhau gửi một lượng lớn yêu cầu đến hệ thống mục tiêu để làm tê liệt dịch vụ. Đối với dịch vụ CDN, một cuộc tấn công DDoS có thể làm giảm khả năng phục vụ của mạng lưới, dẫn đến tình trạng mất kết nối hoặc giảm tốc độ tải trang cho người dùng. Điều này không chỉ ảnh hưởng đến trải nghiệm của khách hàng mà còn có thể gây thiệt hại về doanh thu cho công ty.

**2. Gián đoạn dịch vụ (Service Interruption)**

**Giải thích:** Các sự cố vật lý hoặc kỹ thuật như hỏng hóc phần cứng, mất điện, hoặc thảm họa tự nhiên có thể làm gián đoạn hoạt động của các máy chủ CDN. Nếu một số máy chủ trong mạng lưới không hoạt động, khả năng phân phối nội dung đến người dùng sẽ bị ảnh hưởng, dẫn đến việc người dùng không thể truy cập vào các tài nguyên mà họ cần, gây ra sự không hài lòng và mất uy tín.

**3. Rò rỉ dữ liệu (Data Leakage)**

**Giải thích:** Dịch vụ CDN thường xử lý và lưu trữ nội dung nhạy cảm của khách hàng. Nếu không được bảo vệ đúng cách, có thể xảy ra các vụ rò rỉ dữ liệu, cho phép kẻ tấn công truy cập vào thông tin riêng tư hoặc nội dung của khách hàng. Điều này không chỉ làm tổn hại đến sự riêng tư của người dùng mà còn có thể dẫn đến các vụ kiện tụng và phạt tiền từ các cơ quan quản lý.

**Biện pháp giảm thiểu rủi ro:**

* **Triển khai các giải pháp chống DDoS** để giảm thiểu tác động của các cuộc tấn công DDoS và duy trì tính khả dụng của dịch vụ.
* **Đảm bảo dự phòng và sao lưu dữ liệu thường xuyên** để khôi phục nhanh chóng trong trường hợp xảy ra sự cố gián đoạn.
* **Sử dụng mã hóa và bảo mật thông tin** để bảo vệ dữ liệu nhạy cảm khỏi các lỗ hổng bảo mật, đồng thời thực hiện kiểm tra bảo mật định kỳ để phát hiện và khắc phục các lỗ hổng có thể.