Câu 1:

* **Tấn công DDoS:** Tội phạm mạng có thể thực hiện tấn công DDoS, làm cho website không thể truy cập được bằng cách gửi lượng lớn thông yêu cầu giả mạo cùng lúc đến máy chủ
  + Tác động:
    - Website ngừng hoạt động, gây gián đoạn dịch vụ trực tuyến như tra cứu hợp đồng, tư vấn và mua bảo hiểm
    - Ảnh hưởng đến trải nghiệm khách hàng, làm mất uy tín của công ty
  + Giải pháp:
    - Sử dụng hệ thống chống DDoS
    - Triển khai mạng phân phối nội dung (CDN) để giảm tải cho máy chủ
* **Phishing và tấn công trung gian:** Hacker có thể gửi email giả mạo từ công ty bảo hiểm hoặc chặn giao tiếp giữa khách hàng và website để đánh cắp thông tin đăng nhập, thông tin hợp đồng hoặc dữ liệu cá nhân
  + Tác động:
    - Khách hàng bị lừa tiết lộ thông tin nhạy cảm, ảnh hưởng đến quyền riêng tư
    - Hacker có thể chiếm quyền truy cập tài khoản khách hàng và thực hiện giao dịch trái phép
  + Giải pháp:
    - Sử dụng chứng SSL/TLS để mã hóa toàn bộ dữ liệu trao đổi
    - Áp dụng xác thực hai yếu tố (2FA) cho tài khoản người dùng
* **Rò rỉ và đánh cắp dữ liệu khách hàng:** Hacker có thể khai thác lỗ hổng bảo mật của website hoặc hệ thống quản lý để xâm nhập vào cơ sở dữ liệu, đánh cắp thông tin cá nhân, hợp đồng bảo hiểm, và thông tin thanh toán của khách hàng
  + Tác động:
    - Gây thiệt hại tài chính cho khách hàng nếu thông tin thanh toán bị lộ
    - Mất lòng tin từ khách hàng và ảnh hưởng nghiêm trọng đến danh tiếng công ty
    - Công ty có thể phải đối mặt với các vấn đề pháp lý do vi phạm quy định bảo vệ dữ liệu
  + Giải pháp:
    - **Mã hóa dữ liệu** lưu trữ và truyền tải
    - Thường xuyên kiểm tra, vá lỗi các lỗ hổng bảo mật của hệ thống
    - Phân quyền và giám sát chặt chẽ truy cập vào hệ thống dữ liệu quan trọng

Câu 2:

* **Tấn công DDoS**: Hacker gửi một lượng lớn yêu cầu giả mạo từ nhiều nguồn khác nhau, làm quá tải các máy chủ trong mạng lưới CDN.
  + Tác động:
    - **Mất khả năng phục vụ**: CDN sẽ không thể phân phối nội dung đến người dùng cuối, gây gián đoạn dịch vụ.
    - **Ảnh hưởng uy tín**: Các khách hàng sử dụng dịch vụ CDN của VCCloud sẽ không hài lòng và có thể rời bỏ dịch vụ.
  + Giải pháp:
    - Sử dụng các công cụ **phát hiện và chặn DDoS**.
    - Phân tải yêu cầu giữa các máy chủ bằng **cơ chế cân bằng tải**.
* **Poisoning Cache**: Hacker gửi dữ liệu độc hại hoặc sửa đổi nội dung được lưu trong bộ đệm của máy chủ CDN, khiến người dùng cuối nhận được dữ liệu sai hoặc bị nhiễm mã độc.
  + Tác động:
    - **Phân phối nội dung sai lệch**: Người dùng cuối có thể nhận được nội dung cũ hoặc đã bị chỉnh sửa, ảnh hưởng đến trải nghiệm người dùng.
    - **Nguy cơ phát tán mã độc**: Hacker có thể chèn mã độc vào các tệp tin được phân phối.
  + Giải pháp:
    - **Kiểm tra tính toàn vẹn dữ liệu** bằng cách dùng các **hàm băm** và **chữ ký số**.
    - **Quản lý thời gian sống (TTL)** của các đối tượng được lưu trong bộ đệm một cách hợp lý.
* **Tấn công Man-in-the-Middle**: Trong quá trình truyền tải dữ liệu giữa người dùng và các máy chủ CDN, hacker có thể chặn luồng dữ liệu, đánh cắp hoặc sửa đổi nội dung.
  + Tác động:
    - **Rò rỉ thông tin**: Thông tin nhạy cảm của người dùng và khách hàng của VCCloud có thể bị đánh cắp.
    - **Làm suy giảm hiệu năng**: Hacker có thể làm chậm quá trình truyền tải nội dung, gây ảnh hưởng đến trải nghiệm người dùng.
  + Giải pháp:
    - Sử dụng **HTTPS/SSL** để mã hóa dữ liệu trong quá trình truyền tải.
    - Áp dụng **chứng thực máy chủ** để đảm bảo tính xác thực của máy chủ CDN.Phân quyền và giám sát chặt chẽ truy cập vào hệ thống dữ liệu quan trọng