**Bài tập nhóm tình huống**

**Danh sách thành viên nhóm 5**

|  |  |  |  |
| --- | --- | --- | --- |
| **Họ đệm** | **Tên** | **MSSV** | **Chức vụ** |
| 1. Nguyễn Thành | Phát | 21010471 | Nhóm trưởng |
| 2. Châu Công | Thoại | 21009641 | Thư ký |
| 3. Dương Huy | Hoàng | 19631051 | Thành viên |

**Tình huống**

Ban Giám đốc của một tổ chức dịch vụ tài chính quốc tế đang xem xét kế hoạch sáp nhập bí mật.

CIO nhận được một email đòi tiền chuộc từ một nguồn không xác định nói rằng họ biết về kế hoạch sáp nhập và có thông tin cá nhân của 150.000 khách hàng. Một mẫu chi tiết cá nhân của 500 khách hàng đã được đưa vào email đòi tiền chuộc làm "bằng chứng".

Tổ chức phải trả khoản tiền chuộc đáng kể bằng Bitcoin. Nếu không, kế hoạch sáp nhập sẽ bị công bố và thông tin khách hàng sẽ bị bán công khai trên mạng.

**1. Xác định tài sản bị tấn công**:

* Thông tin cá nhân của 150.000 khách hàng bị đe dọa. Đây có thể bao gồm thông tin như tên, địa chỉ, số điện thoại, email, và thông tin tài chính nhạy cảm.
* Kế hoạch sáp nhập bí mật của tổ chức.

**2. Bị tấn công theo cách nào:**

* **Social Engineering:** Kẻ tấn công có thể sử dụng kỹ thuật xâm nhập xã hội để lừa đảo nhân viên của tổ chức, như giả vờ là nhân viên IT hoặc đối tác tin cậy, để thu thập thông tin đăng nhập hoặc truy cập vào hệ thống.
* **SQL Injection:** Kẻ tấn công có thể cố gắng thâm nhập vào cơ sở dữ liệu của tổ chức thông qua lỗ hổng SQL Injection để truy cập, sửa đổi hoặc xóa dữ liệu nhạy cảm.
* **Malware:** Truy cập các trang web độc hại, file nhạc nhiễm Malware, cài đặt thanh công cụ/phần mềm từ nhà cung cấp lạ, mở tệp đính kèm [email](https://www.thegioididong.com/game-app/gmail-cua-google-gui-email-nhanh-chong-220098) độc hại (malspam) hoặc các dữ liệu tải xuống không được quét bởi phần mềm bảo mật để theo dõi hoạt động của nhân viên hoặc đánh cắp thông tin.

**3. Cách ứng phó:**

* **Thông báo khẩn cấp bảo mật**: triển khai các biện pháp bảo mật hiệu quả như mã hóa dữ liệu, kiểm soát truy cập, và giám sát hệ thống.
* **Lập kế hoạch ứng phó:** Phát triển kế hoạch cụ thể để xử lý tình huống, gồm cả việc xác định vai trò và trách nhiệm của từng thành viên trong tổ chức.
* **Thông báo cho khách hàng:** Nếu thông tin khách hàng đã bị tấn công, cần thông báo cho khách hàng về tình trạng an ninh thông tin và cung cấp hướng dẫn về cách bảo vệ thông tin cá nhân của họ.
* **Không trả tiền chuộc:** Không nên trả tiền chuộc theo yêu cầu của hacker vì không đảm bảo rằng dữ liệu sẽ được trả về hoặc không bị lợi dụng.
* **Phát triển và triển khai chiến lược truyền thông:** Xây dựng một chiến lược truyền thông mạnh mẽ để quản lý thông tin và tương tác với cộng đồng, giúp giảm thiểu ảnh hưởng tiêu cực đến hình ảnh của tổ chức.
* **Liên hệ với cơ quan chức năng:** Tổ chức cần thông báo vụ việc cho cơ quan an ninh mạng hoặc cơ quan thích hợp để được hỗ trợ và hướng dẫn về các biện pháp cụ thể để xử lý tình huống.
* **Thực hiện giám sát và kiểm soát:** Theo dõi và giám sát mọi hoạt động trên hệ thống để phát hiện và ngăn chặn các hoạt động đáng ngờ hoặc tiềm ẩn của kẻ tấn công.
* **Xác định tài khoản đáng nghi ngờ, vô hiệu hóa những tài khoản đó, tìm hiểu nguyên nhân kẻ tấn công đó có tk này**

**4. Biện pháp khắc phục**

* **Khôi phục dữ liệu từ bản sao lưu:** Tổ chức cần sử dụng các bản sao lưu dữ liệu đã được tạo trước đó để khôi phục dữ liệu khách hàng và các thông tin quan trọng khác.
* **Thiết lập các biện pháp phòng ngừa**: Tổ chức cần thiết lập các biện pháp phòng ngừa như tường lửa, phát hiện xâm nhập, và mã hóa dữ liệu để ngăn chặn sự xâm nhập và truy cập trái phép vào hệ thống thông tin của mình. Điều này giúp bảo vệ dữ liệu khách hàng và ngăn chặn các cuộc tấn công tương lai.
* **Thông báo cho khách hàng:** Thông báo ngay lập tức đến khách hàng về tình trạng sự cố, cung cấp thông tin chi tiết và hướng dẫn về các biện pháp bảo vệ mình.
* **Hợp tác với chuyên gia an ninh mạng**: Liên hệ ngay với các chuyên gia an ninh mạng để họ có thể đưa ra đánh giá chi tiết về tình hình, giúp định rõ nguyên nhân và đề xuất biện pháp khắc phục.
* **Đào tạo nhân viên về an ninh mạng:** Tổ chức cần cung cấp đào tạo cho nhân viên về các kỹ thuật phòng chống cuộc tấn công, như nhận dạng email độc hại, cách xử lý thông tin nhạy cảm, và cách thực hiện các biện pháp bảo mật cơ bản. Điều này giúp nâng cao nhận thức và kỹ năng của nhân viên trong việc bảo vệ hệ thống thông tin của tổ chức.
* **Chuẩn bị cho việc kiện toàn và tuân thủ pháp lý**: Hợp tác chặt chẽ với bộ phận pháp lý để đảm bảo rằng mọi hoạt động được thực hiện tuân thủ các quy định và chuẩn mực pháp lý.

**Biện pháp bảo vệ:**

**Pháp hiện**