**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 |
| 4. Phạm Lê Kiều | Nhi | 20003075 | 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.
* Lộ thông tin 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.
* **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.

**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.
* **Thay đổi mật khẩu và cấp quyền truy cập:** Đảm bảo rằng tất cả các mật khẩu và thông tin đăng nhập trong hệ thống được thay đổi. Kiểm tra và cập nhật lại các cấp quyền truy cập để đảm bảo rằng chỉ những người cần thiết mới có quyền truy cập vào các tài nguyên quan trọng.
* **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.
* **Triển khai ngay quy trình khẩn cấp**: Kích thích ngay lập tức các quy trình khẩn cấp để giảm thiểu thiệt hại và ngăn chặn thông tin quan trọng rơi vào tay người không đáng tin cậy.

**Biện pháp bảo vệ:**

* **Mã hóa dữ liệu trong CSDL:** Mã hóa các thông tin nhạy cảm trong CSDL như mật khẩu, thông tin tài khoản ngân hàng, thông tin cá nhân của khách hàng và nhân viên. Các thuật toán mã hóa mạnh mẽ như AES (Advanced Encryption Standard) có thể được sử dụng để mã hóa dữ liệu.
* **Cập nhật hệ điều hành và phần mềm ứng dụng:** Đảm bảo rằng hệ điều hành (như Windows, macOS, Linux) và tất cả các ứng dụng trên máy tính đều được cập nhật đầy đủ. Các bản vá và cập nhật thường chứa các sửa lỗi bảo mật để khắc phục các lỗ hổng đã biết.
* **Xác thực và ủy quyền:** Thực hiện các biện pháp xác thực mạnh mẽ để đảm bảo rằng chỉ những người được ủy quyền mới có thể truy cập vào CSDL. Sử dụng các cơ chế ủy quyền để quản lý quyền truy cập của người dùng và giảm thiểu nguy cơ bị xâm nhập từ bên trong.
* **Ngừng toàn bộ quyền truy cập không cần thiết**: Tạm ngừng toàn bộ quyền truy cập hệ thống của những người không cần thiết để ngăn chặn sự lan truyền của thông tin
* **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.
* **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.
* **Cập nhật chính sách và quy trình an ninh mạng:** Kiểm tra và cập nhật lại chính sách và quy trình an ninh mạng của tổ chức để đảm bảo rằng chúng phản ánh các mối đe dọa và thách thức mới, cũng như các biện pháp bảo mật tiên tiến.
* **Đảm bảo bảo mật cho các kết nối từ xa:** Đối với các kết nối từ xa, sử dụng các kỹ thuật như VPN (Virtual Private Network) để bảo vệ dữ liệu trong quá trình truyền tải và cung cấp các cơ chế xác thực và mã hóa mạnh mẽ.

**Phát hiện**

* **Giám sát log hệ thống:** Theo dõi và phân tích các log hệ thống để xác định các hoạt động đáng ngờ hoặc không thường xuyên, như các đăng nhập không thành công, thay đổi quyền truy cập, hoặc truy cập từ địa điểm không phù hợp.
* **Xác định tài khoản đáng nghi ngờ**: Vô hiệu hóa những tài khoản đó, tìm hiểu nguyên nhân kẻ tấn công đó có những tài khoản này.
* **Sử dụng Hệ thống phát hiện xâm nhập (IDS) và Hệ thống phòng thủ xâm nhập (IPS):** Triển khai các giải pháp IDS và IPS để phát hiện và ngăn chặn các hành vi bất thường, bao gồm các cuộc tấn công mạng và việc sử dụng phần mềm độc hại.
* **Kiểm tra hệ thống mạng và dữ liệu:** Thực hiện kiểm tra hệ thống mạng và dữ liệu để xác định xem có bất kỳ hoạt động nào không thường xuyên hoặc đáng ngờ. Điều này có thể bao gồm kiểm tra log hệ thống, giám sát hoạt động mạng, và phân tích các yếu tố động trong hệ thống.
* **Phân tích dữ liệu lưu lượng mạng:** Sử dụng các công cụ và kỹ thuật phân tích dữ liệu lưu lượng mạng để phát hiện các mẫu hoạt động không bình thường, bao gồm lưu lượng mạng lớn đột ngột, giao tiếp với địa chỉ IP đáng ngờ, hoặc các giao thức không phù hợp.
* **Phân tích Email đòi tiền chuộc:** Phân tích kỹ lưỡng email đòi tiền chuộc để xác định nguồn gốc, cú pháp, và bất kỳ đặc điểm nào đặc biệt. Kiểm tra đường dẫn và đính kèm trong email để đảm bảo rằng không có mã độc hại được triển khai.
* **Phân tích mẫu chi tiết cá nhân:** Phân tích mẫu chi tiết cá nhân được đính kèm để xác định liệu nó có chứa phần mềm độc hại hay không. So sánh thông tin trong mẫu với dữ liệu gốc để xác định mức độ chính xác.