**Bài tập nhóm chương 3**

**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 |

Nhóm của bạn gồm các chuyên gia an ninh mạng cần xây dựng chính sách an ninh mạng cho công ty sản xuất ống hút cỏ Greenjoy. Hãy điền vào nội dung các cột trong bảng sau.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Tài sản** | **Các mối đe dọa an ninh mạng tiềm ẩn** | **Bảo vệ** | **Phát hiện** | **Ứng phó** | **Khắc phục** |
| 1) Dữ liệu của khách hàng | - Rò rỉ thông tin do tấn công Malware  - Bị chỉnh sửa, xóa thông tin | - Áp dụng mã hóa cho dữ liệu khách hàng, đặc biệt là thông tin nhạy cảm như thông tin cá nhân, thông tin tài khoản ngân hàng và thông tin thẻ tín dụng. | - Thiết lập giám sát hệ thống và log  - Triển khai hệ thống cảnh báo để cảnh báo về các hoạt động không bình thường hoặc đáng ngờ liên quan đến dữ liệu khách hàng | - Cô lập máy tính hoặc thiết bị bị nhiễm malware khỏi mạng nội bộ bằng cách ngắt kết nối mạng hoặc tắt thiết bị. Điều này giúp ngăn chặn sự lây lan của malware sang các hệ thống khác.  - Cảnh giác với các web có domain kết thúc bằng tập hợp các chữ cái riêng lẻ, và có đuôi không giống như bình thường (.com, .vn hay .org,... ). | - Thiết lập các quy tắc tường lửa để ngăn chặn hoặc giảm thiểu rủi ro từ các loại malware phổ biến.  - Thường xuyên cập nhật hệ điều hành, ứng dụng hay plugin. |
| 2) Thông tin của nhân viên | - Lừa đảo, mất quyền truy cập | - Kiểm soát truy cập dựa trên vai trò.  - Kiểm tra định kỳ | - Theo dõi hoạt động người dùng | - Thu hồi quyền truy cập | - Đào tạo nhân viên về nhận thức về an ninh |
| 3) Quy trình sản xuất | -Tấn công vào hệ thống tự động hóa  -Rủi ro về dữ liệu sản xuất  -Rủi ro từ nhân viên và bên thứ ba  - Sự nguy hiểm từ thiết bị kết nối | -Giám sát hệ thống  - Mã hóa dữ liệu  - Kiểm tra truy cập và cập nhập hệ thống  - Đào tạo nhân viên | -Sử dụng các hệ thống giám sát tự động để theo dõi các thông tin quan trọng trong quy trình sản xuất  -Phân tích dữ liệu để phát hiện sớm các xu hướng hay biểu hiện không bình thường trong quy trình sản xuất.  -Đảm bảo nhân viên nhận biết và báo cáo các vấn đề và sự cố.  -Thực hiện hệ thống cảnh báo để tự động thông báo | - Xác minh và kiểm tra tính bảo mật của thiết bị kết nối  Theo dõi và kiểm tra hoạt động của nhân viên và bên thứ ba | -Khôi phục từ bản sao lưu  - Mã hóa dữ liệu sản xuất để đảm bảo tính bảo mật và ngăn chặn truy cập trái phép. |
| 3) Máy tính điều khiển dây chuyền sản xuất | Hacker xâm nhập vào hệ thống, mã hóa dữ liệu bằng tấn công ransomware | - Mã hóa dữ liệu để bảo vệ dữ liệu khỏi bị đánh cắp.  - Sử dụng tường lửa (firewall) để lọc các truy cập trái phép vào hệ thống.  - Sao lưu dữ liệu thường xuyên vào ổ cứng ngoài hoặc lưu trữ đám mây.  - Sử dụng hệ thống ngăn chặn xâm nhập (IPS) của các cuộc tấn công mạng. | - Ngắt kết nối máy tính khỏi mạng ngăn chặn hacker lan truyền tấn công sang các thiết bị khác.  - Sử dụng các công cụ trí tuệ nhân tạo AI có thể giúp phát hiện các mẫu tấn công ransomware mới và ngăn chặn chúng trước khi chúng xảy ra | - Ngắt kết nối máy tính khỏi mạng, khôi phục dữ liệu từ bản sao lưu. | - Nâng cấp phần mềm bảo mật, tăng cường đào tạo nhân viên về an ninh mạng. |
| 5) Ứng dụng di động của công ty | - Bị tấn công bởi malware, mã độc  - Bị lợi dụng để truy cập trái phép vào dữ liệu cá nhân của người dùng | - Mã hóa dữ liệu  - Xác thực hai yếu tố  - Cập nhật mã nguồn | - Sử dụng công cụ theo dõi hoạt động ứng dụng di động để phát hiện các hoạt động không bình thường | - Ngắt kết nối của ứng dụng di động với mạng để ngăn chặn việc truy cập trái phép vào hệ thống hoặc dữ liệu quan trọng.  - Thông báo cho các bên liên quan như quản lý, bộ phận an ninh mạng và người dùng về sự cố, cũng như triển khai kế hoạch hồi đáp sự cố để giảm thiểu thiệt hại. | - Cập nhật ứng dụng.  - Kiểm tra lại mã nguồn.  - Đào tạo nhân viên về an ninh. |