Lớp: NT207.P11.ATCL

Họ và tên Sinh viên: Hồ Hải Dương Mã Số SV: 21520202

BÁO CÁO PHÂN TÍCH RỦI RO VỀ "MAN-IN-THE-CLOUD ATTACKS (MITC)"

STT	Nội dung phân tích	Kết quả
1.	Mục đích của Báo cáo	• Mục đích của việc phân tích tấn công MITC là để hiểu rõ cơ chế và bản chất của mối đe dọa này, qua đó nhận diện các lỗ hổng trong quản lý token đám mây. Phân tích giúp xác định các điểm yếu trong bảo mật, đặc biệt là về quyền truy cập và xác thực, để phát triển các biện pháp phòng ngừa phù hợp như xác thực đa yếu tố và giám sát hoạt động bất thường.
2.	Bản chất của MITC	• MITC là một dạng tấn công khai thác lỗ hổng bảo mật trong cơ chế đồng bộ hóa của các dịch vụ đám mây. • Kẻ tấn công chiếm token đồng bộ hóa của nạn nhân thông qua kỹ thuật lừa đảo (phishing) hoặc khai thác lỗ hổng bảo mật. Với token này, kẻ tấn công có thể truy cập và đồng bộ hóa dữ liệu đám mây của nạn nhân trên thiết bị của mình mà không cần thông tin đăng nhập.
3.	Đặc trưng của rủi ro do MITC gây ra	MitCloud vi phạm các yêu cầu về an toàn thông tin như sau: • **Thuộc tính bảo mật:** Người dùng bị mất quyền kiểm soát và kẻ tấn công có thể truy cập vào dữ liệu nhạy cảm, gây mất tính bảo mật. • **Thuộc tính sẵn sàng:** Dữ liệu có thể bị chỉnh sửa, xóa bỏ hoặc ngăn chặn quyền truy cập, dẫn đến gián đoạn hoạt động của người dùng hoặc tổ chức. • **Tính toàn vẹn:** Dữ liệu có thể bị thay đổi một cách trái phép, làm ảnh hưởng đến độ tin cậy và tính chính xác của thông tin lưu trữ trên hệ thống đám mây.
4.	Mức độ rủi ro	☐ Thấp ☐ Trung bình ☒ Cao
5.	Nguồn rủi ro	• Chủ yếu đến từ các tội phạm công nghệ cao (Hacker/Attacker). • Ngoài ra, rủi ro này cũng có thể bắt nguồn từ các nhân viên nội bộ thiếu nhận thức về an toàn thông tin, vô tình tiết lộ thông tin đăng nhập hoặc truy cập vào các liên kết và tệp tin đáng ngờ.
6.	Hệ quả	• Dữ liệu bị thay đổi làm gián đoạn quy trình làm việc và gây ảnh hưởng đến hiệu suất. • Hacker có thể truy cập và đánh cắp thông tin quan trọng, dẫn đến tiêu cực về mặt danh tiếng, kinh doanh và pháp lý. • Hacker có thể đe dọa doanh nghiệp bằng cách công bố dữ liệu nếu không trả tiền chuộc. • Doanh nghiệp cần đầu tư nhiều nguồn lực (tài chính, nhân lực,…) để khắc phục và tăng cường bảo mật sau sự cố.
7.	Khả năng xảy ra	☐ Thấp ☐ Trung bình ☒ Cao
8.	Một số sự kiện khi bị tấn công bởi MITC	Một số sự kiện tấn công có tính chất liên quan đến MITC: **1) Tấn công vào Dropbox Cloud Storage (tháng 7/2012)** ***1.1) Nguyên nhân xảy ra:*** Kẻ tấn công thực hiện một cuộc tấn công lừa đảo (phishing) để đánh cắp thông tin đăng nhập của một nhân viên Dropbox.

		Sử dụng thông tin đăng nhập này, hacker đã truy cập vào dữ liệu nhạy cảm của người dùng. ***1.2) Khả năng xảy ra:*** Đây là một trong những vụ tấn công lớn đầu tiên nhắm vào dịch vụ lưu trữ đám mây, và khả năng xảy ra tấn công dạng này cao khi không có các biện pháp bảo mật bổ sung như xác thực hai yếu tố (2FA). ***1.3) Hệ quả:*** Hơn 68.6 triệu mật khẩu bị đánh cắp, gây ra một cú sốc lớn về bảo mật cho Dropbox và làm dấy lên lo ngại về sự an toàn của các dịch vụ lưu trữ đám mây, công ty phải nỗ lực nhiều năm để lấy lại niềm tin từ người dùng. Mặc dù Dropbox không công bố chính xác tổn thất, các chuyên gia ước tính rằng vụ tấn công này đã gây thiệt hại hàng triệu USD cho công ty, bao gồm chi phí khôi phục hệ thống, tăng cường bảo mật, và tổn thất về danh tiếng. **<u>2) Tấn công vào OneDrive của một công ty tài chính (2019)</u>** ***2.1) Nguyên nhân xảy ra:*** Một nhân viên của công ty tài chính bị đánh cắp token đồng bộ hóa thông qua một email lừa đảo giả mạo từ một đối tác. Kẻ tấn công đã lợi dụng token này để đăng nhập vào tài khoản OneDrive của nhân viên mà không cần mật khẩu. Token này cho phép hacker truy cập vào toàn bộ hơn 10.000 tệp tin của công ty, bao gồm báo cáo tài chính và hồ sơ khách hàng. ***2.2) Khả năng xảy ra:*** Một báo cáo từ công ty bảo mật McAfee năm 2019 cho thấy 30% các công ty tài chính đã từng đối mặt với các cuộc tấn công vào dịch vụ đám mây của họ, chủ yếu là qua việc chiếm đoạt token. ***2.3) Hệ quả:*** Công ty tài chính bị mất quyền kiểm soát tạm thời đối với tài khoản OneDrive, dẫn đến việc mất hàng nghìn tệp dữ liệu nhạy cảm. Công ty đã phải chi hơn 200.000 USD cho việc khôi phục dữ liệu và tăng cường các biện pháp bảo mật sau cuộc tấn công.
9.	Các kịch bản thực hiện trước và sau khi bị MITC tấn công để đáp ứng theo yêu cầu tại Nhóm A.16 Yêu cầu A.16.1 Điều A.16.1.5 [ISO 27001:2013]	**<u>1) Trước khi thiết bị bị tấn công bởi MITC:</u>** • Sử dụng xác thực đa yếu tố (MFA) cho tất cả các tài khoản đám mây để ngăn chặn truy cập trái phép. • Triển khai các biện pháp quản lý token chặt chẽ, bao gồm việc kiểm soát thời hạn của token và thu hồi ngay khi không cần thiết. • Đào tạo nhân viên về nhận biết các hình thức lừa đảo (phishing) và cách bảo vệ thông tin đăng nhập khỏi các trang giả mạo. • Áp dụng giám sát hoạt động bất thường trong hệ thống đám mây để phát hiện sớm các hành vi truy cập trái phép. **<u>2) Sau khi thiết bị bị tấn công bởi MITC:</u>** ***2.1 Tự khắc phục:*** • Bước 1: Thu hồi tất cả token đồng bộ hóa của tài khoản bị xâm nhập và yêu cầu thay đổi mật khẩu cho các tài khoản liên quan.

		• Bước 2: Xác định và cô lập các tài khoản bị ảnh hưởng để ngăn chặn sự lan rộng của cuộc tấn công vào các hệ thống khác. • Bước 3: Kiểm tra và khôi phục lại dữ liệu từ các bản sao lưu trước khi xảy ra sự cố để đảm bảo tính toàn vẹn của dữ liệu. • Bước 4: Phân tích nguyên nhân và giám sát hoạt động hệ thống sau sự cố, đồng thời triển khai các biện pháp bảo mật bổ sung để giảm thiểu nguy cơ xảy ra các cuộc tấn công tương tự trong tương lai. ***2.2 Nếu không thể tự khắc phục:*** • Sử dụng dịch vụ từ các chuyên gia bảo mật bên ngoài để phân tích và khôi phục hệ thống. • Báo cáo sự cố cho cơ quan quản lý an toàn thông tin và tuân thủ các quy định pháp lý về bảo vệ dữ liệu.
10.	Các kiểm soát phòng chống MITC để đáp ứng theo Nhóm A.12 Yêu cầu A.12.6 Điều A.12.6.1 [ISO 27001:2013] trong trường hợp mối đe dọa này là lỗ hổng bảo mật	**<u>1) Tên kiểm soát:</u>** Các biện pháp kiểm soát rủi ro do tấn công MITC bao gồm nhưng không giới hạn các biện pháp sau đây: • Triển khai xác thực đa yếu tố (MFA) cho tất cả các tài khoản đám mây để ngăn chặn truy cập trái phép khi token đồng bộ hóa bị đánh cắp. • Quản lý vòng đời của token, thu hồi token khi không còn cần thiết, đặt thời hạn sử dụng ngắn và yêu cầu làm mới định kỳ để giảm nguy cơ bị chiếm quyền sử dụng. • Cài đặt hệ thống cảnh báo để phát hiện các hành vi đăng nhập bất thường từ các thiết bị hoặc vị trí không xác định, nhằm phát hiện sớm sự xâm nhập trái phép. • Tăng cường đào tạo cho nhân viên về nhận diện các hình thức tấn công lừa đảo (phishing) và các phương pháp bảo vệ thông tin đăng nhập khỏi các trang giả mạo. • Thực hiện sao lưu định kỳ dữ liệu quan trọng và đảm bảo bản sao lưu được bảo vệ chặt chẽ để có thể phục hồi dữ liệu khi cần thiết. • Cài đặt các phần mềm bảo mật để giám sát và lọc lưu lượng mạng, ngăn chặn các hoạt động bất thường liên quan đến việc đồng bộ hóa và truy cập dữ liệu trên đám mây. • Đảm bảo chỉ những nhân viên cần thiết mới có quyền truy cập và đồng bộ hóa dữ liệu đám mây, hạn chế quyền truy cập đối với các tài khoản không cần thiết để giảm thiểu rủi ro. • Thực hiện kiểm tra bảo mật định kỳ, cập nhật cấu hình và vá các lỗ hổng bảo mật để ngăn chặn nguy cơ bị xâm nhập. **<u>2) Hiệu lực của kiểm soát:</u>** Các biện pháp kiểm soát này không đảm bảo ngăn chặn hoàn toàn rủi ro từ tấn công MITC vì chưa có kết quả khảo sát cụ thể từ các tổ chức an toàn thông tin trên thế giới nhưng sẽ giúp giảm thiểu đáng kể nguy cơ truy cập trái phép vào dữ liệu đám mây. Chẳng hạn như: ▪ Xác thực đa yếu tố (MFA) tăng cường an ninh cho tài khoản đám mây, nhưng không hoàn toàn loại bỏ nguy cơ nếu kẻ tấn công vượt qua hoặc phá vỡ lớp bảo vệ này.

		▪ Giám sát đăng nhập và cảnh báo bất thường, nhưng hiệu quả phụ thuộc vào độ chính xác của hệ thống giám sát và khả năng phản ứng kịp thời của đội ngũ bảo mật. ▪ Đào tạo và nâng cao nhân viên về an toàn thông tin, nhưng khó có thể ngăn ngừa hoàn toàn khi các phương thức tấn công ngày càng tinh vi. ▪ Sao lưu dữ liệu định kỳ, nhưng có thể không khôi phục hoàn toàn dữ liệu mới nhất do độ trễ giữa các lần sao lưu. ▪ Kiểm tra và rà soát bảo mật định kỳ giúp duy trì an ninh hệ thống, nhưng hiệu quả phụ thuộc vào tần suất và độ sâu của các cuộc kiểm tra, cũng như khả năng khắc phục nhanh chóng các lỗ hổng được phát hiện.
11.	Mức độ phức tạp của việc phòng chống MITC	• **Thấp:** Doanh nghiệp triển khai các biện pháp bảo mật cơ bản như xác thực đa yếu tố (MFA) và đào tạo nhân viên về cách nhận biết tấn công phishing. Những biện pháp này có thể ngăn chặn các tấn công phổ biến, nhưng khi đối mặt với những kỹ thuật tấn công phức tạp, khả năng phòng ngừa vẫn hạn chế. • **Trung bình:** Doanh nghiệp sử dụng các giải pháp bảo mật tiên tiến hơn, chẳng hạn như hệ thống giám sát và cảnh báo đăng nhập bất thường, quản lý token đồng bộ hóa và sao lưu dữ liệu định kỳ. Mức độ này giúp tăng cường khả năng phát hiện và ứng phó nhanh với các cuộc tấn công MITC, nhưng vẫn yêu cầu sự phối hợp chặt chẽ và có khả năng phát hiện kịp thời các hoạt động bất thường. • **Cao:** Doanh nghiệp phải đối mặt với sự phức tạp lớn nếu không có biện pháp phòng ngừa từ trước và phải tự khắc phục sau khi bị tấn công MITC. Trong trường hợp này, việc thu hồi quyền truy cập và khôi phục dữ liệu đòi hỏi quy trình phức tạp và nguồn lực đáng kể. Kể cả khi đã thực hiện các biện pháp khắc phục, vẫn có nguy cơ kẻ tấn công tiếp tục có quyền truy cập vào dữ liệu đám mây thông qua token bị đánh cắp.
12.	Kết nối với các tổ chức theo yêu cầu tại Nhóm A.6 Yêu cầu A.6.1 Điều A.6.1.3 và A.6.1.4 [ISO 27001:2013] để tìm kiếm sự hỗ trợ	**1) Sử dụng các dịch vụ an toàn thông tin của bên thứ ba để bảo vệ dữ liệu đám mây và quản lý quyền truy cập:** • AWS Cloud Security: Dịch vụ bảo mật của Amazon giúp quản lý quyền truy cập và giám sát các hoạt động bất thường trên hệ thống đám mây. • Microsoft Azure Security: Giải pháp bảo mật từ Microsoft cung cấp các công cụ phát hiện và ngăn chặn hành vi bất thường, bảo vệ quyền truy cập của tài khoản người dùng. • Google Workspace Security: Cung cấp xác thực đa yếu tố (MFA), quản lý token, và cảnh báo hoạt động bất thường nhằm tăng cường bảo vệ dịch vụ đám mây của Google. **2) Thông báo cho các tổ chức và bên liên quan khi xảy ra sự cố an toàn thông tin:** • Thông báo cho các cơ quan chính phủ hoặc các tổ chức an toàn thông tin quốc gia để nhận được sự hỗ trợ và hướng dẫn khắc phục. • Liên hệ với các đối tác công nghệ và nhà cung cấp dịch vụ để đánh giá tác động của sự cố và phối hợp xử lý nhằm hạn chế rủi ro lan rộng.

		• Cung cấp thông tin minh bạch về tình hình an toàn thông tin của doanh nghiệp để duy trì sự tin tưởng và hỗ trợ từ các cổ đông và khách hàng quan trọng.
13.	Các yếu tố liên quan đến thời gian	**<u>1) Thời gian xảy ra sự kiện/sự cố:</u>** Tấn công MITC có thể xảy ra bất cứ lúc nào khi: • Người dùng vô tình tiết lộ token đồng bộ hóa qua các cuộc tấn công phishing. • Token đồng bộ hóa không được thu hồi khi nhân viên rời khỏi tổ chức. • Doanh nghiệp không giám sát các đăng nhập bất thường trên hệ thống đám mây. • Quản lý token đồng bộ hóa không đặt giới hạn thời gian sử dụng. **<u>2) Yếu tố liên quan đến thời gian và sự biến động:</u>** • Càng kéo dài thời gian phát hiện tấn công, kẻ xâm nhập càng có thêm cơ hội truy cập và sửa đổi dữ liệu. Do đó, khả năng giám sát và phản hồi nhanh chóng là yếu tố then chốt. • Doanh nghiệp cần nhanh chóng thu hồi token bị chiếm và khôi phục hệ thống, đảm bảo tính toàn vẹn dữ liệu trước khi hoạt động trở lại. • Dữ liệu phải được sao lưu thường xuyên để đảm bảo khả năng khôi phục nhanh nhất. Thời gian khôi phục càng ngắn, mức độ ảnh hưởng đến hoạt động kinh doanh và lòng tin của khách hàng càng giảm. • Kiểm tra bảo mật định kỳ là cần thiết để phát hiện sớm các lỗ hổng hoặc các hoạt động bất thường có thể dẫn đến tấn công MITC.
14.	Quan điểm, định kiến và cảm nhận về rủi ro do MITC gây ra	Theo quan điểm chung, không ai mong muốn dữ liệu nhạy cảm của mình bị xâm phạm, vì vậy các quan điểm thống nhất về rủi ro từ MITC là: • Bằng cách chiếm quyền truy cập thông qua token đồng bộ hóa, MITC có thể dẫn đến rủi ro nghiêm trọng về mất mát và xâm phạm dữ liệu. • Các biện pháp bảo mật mạnh mẽ, như xác thực đa yếu tố và giám sát đăng nhập, là cần thiết để ngăn chặn tấn công MITC và bảo vệ quyền truy cập dữ liệu. • Cần nâng cao nhận thức cho nhân viên và người dùng về các mối đe dọa, đặc biệt là tấn công phishing, để giảm thiểu nguy cơ bị chiếm token.
15.	Các hạn chế kỹ thuật phòng chống MITC để đáp ứng theo Nhóm A.12 Yêu cầu A.12.1 Điều A.12.6.1 [ISO 27001:2013]	• Các biện pháp kiểm soát phòng chống MITC thường gặp hạn chế ở chỗ chỉ được cập nhật và vá lỗi sau khi phát hiện ra cuộc tấn công hoặc khi đã xảy ra rủi ro xâm phạm. Việc phụ thuộc vào token đồng bộ hóa, nếu không được quản lý chặt chẽ, có thể tạo ra lỗ hổng bảo mật khó phát hiện kịp thời. Bên cạnh đó, việc sử dụng xác thực đa yếu tố (MFA) và giám sát hoạt động bất thường vẫn chưa đảm bảo an toàn tuyệt đối, vì những kỹ thuật tấn công mới có thể vượt qua các lớp bảo vệ này.
16.	Tác động kinh tế của MITC	• **<u>Chi phí khôi phục hệ thống:</u>** Tùy vào mức độ tấn công, chi phí khôi phục có thể dao động từ 10,000 - 50,000 USD, bao gồm chi phí cho đội ngũ IT nội bộ và các chuyên gia bảo mật bên ngoài để khắc phục và kiểm tra hệ thống. • **<u>Mất doanh thu:</u>** Các gián đoạn hoạt động có thể khiến doanh nghiệp mất từ 50,000 - 100,000 USD mỗi ngày, đặc biệt đối với các doanh nghiệp có quy mô lớn và phụ thuộc vào hệ thống đám mây để vận hành kinh doanh.

<table>
<tr><td></td><td></td><td>

- **<u>Chi phí tăng cường bảo mật:</u>** Sau sự cố, chi phí nâng cấp bảo mật có thể rơi vào khoảng 20,000 - 100,000 USD, bao gồm triển khai xác thực đa yếu tố (MFA), giám sát hoạt động bất thường, và các giải pháp bảo mật khác.
- **<u>Thiệt hại uy tín và lòng tin khách hàng:</u>** Mất uy tín và niềm tin khách hàng có thể ảnh hưởng đến doanh thu dài hạn, với ước tính tổn thất lên đến 100,000 - 500,000 USD hoặc hơn, tùy thuộc vào quy mô và mức độ tin cậy của thương hiệu trên thị trường.
- **<u>Chi phí pháp lý và tuân thủ:</u>** Doanh nghiệp có thể đối mặt với các khoản phạt pháp lý do vi phạm các quy định bảo mật, thường dao động từ 10,000 - 200,000 USD (tùy thuộc vào quy định địa phương và quốc tế mà doanh nghiệp phải tuân thủ).
- **<u>Chi phí cơ hội:</u>** Việc tập trung vào khắc phục và bảo mật thay vì phát triển kinh doanh có thể dẫn đến mất cơ hội, ước tính từ 50,000 - 150,000 USD, vì doanh nghiệp có thể chậm trễ trong việc nắm bắt các cơ hội thị trường hoặc phát triển sản phẩm.
- **<u>Chi phí bảo hiểm an ninh mạng:</u>** Chi phí bảo hiểm an ninh mạng có thể tăng thêm từ 5,000 - 20,000 USD mỗi năm sau sự cố, tùy thuộc vào mức độ rủi ro và mức độ bảo hiểm doanh nghiệp lựa chọn.

</td></tr>
<tr><td>17.</td><td>So sánh ngắn gọn giữa MITC với rủi ro khác liên quan đến đám mây</td><td>

Tên rủi ro	Phương thức	Tính chất	Hậu quả	Biện pháp phòng chống
Man in the Cloud	Chiếm đoạt token đồng bộ hóa	Khó phát hiện, truy cập liên tục	Truy cập dữ liệu trái phép, mất toàn vẹn dữ liệu	Xác thực đa yếu tố, giám sát đăng nhập
Cloud Jacking	Chiếm quyền tài khoản đám mây	Công khai, kiểm soát toàn bộ tài khoản	Mất dữ liệu, sử dụng tài nguyên trái phép	Xác thực đa yếu tố, hạn chế quyền truy cập
Data Leakage	Cấu hình sai	Không có tấn công trực tiếp	Rò rỉ thông tin nhạy cảm, mất dữ liệu	Kiểm soát cấu hình bảo mật
Internal in the Cloud	Nhân viên lạm dụng quyền	Tính hợp pháp cao, khó phát hiện	Mất dữ liệu nhạy cảm, gián đoạn hoạt động	Quản lý quyền truy cập, giám sát hành vi nội bộ

</td></tr>
<tr><td>18.</td><td>Nâng cao nhận thức và đào tạo nhân viên để đáp ứng theo Nhóm A.7 Yêu cầu A.7.2 Điều A.7.2.2 [ISO 27001:2013]</td><td>

Các nội dung chính trong đào tạo bao gồm:

- Đào tạo cách phát hiện email, liên kết và tệp đính kèm đáng ngờ, giúp nhân viên tránh truy cập vào các trang web hoặc tải tệp có thể chứa mã độc.
- Hướng dẫn nhân viên về tầm quan trọng của token và cách bảo mật chúng, bao gồm việc không chia sẻ token hoặc đăng nhập vào các thiết bị không tin cậy.

</td></tr>
</table>

		• Khuyến khích nhân viên áp dụng MFA để bảo vệ tài khoản, giảm nguy cơ truy cập trái phép kể cả khi token bị đánh cắp. • Thiết lập quy trình để nhân viên nhanh chóng báo cáo khi phát hiện hoạt động đáng ngờ hoặc nghi ngờ bị tấn công. Điều này giúp đội ngũ an ninh mạng phản ứng kịp thời, hạn chế thiệt hại.
19.	Kiểm tra và đánh giá bảo mật để đáp ứng theo Nhóm A.18 Yêu cầu A.18.2 Điều A.18.2.3 [ISO 27001:2013]	Các hoạt động kiểm tra bao gồm: • Đảm bảo các cấu hình truy cập và đồng bộ hóa dữ liệu trên đám mây được thiết lập đúng cách, giảm thiểu nguy cơ truy cập trái phép qua các token đồng bộ hóa. • Kiểm tra định kỳ các biện pháp như xác thực đa yếu tố (MFA), quản lý token, và giám sát hoạt động đăng nhập bất thường, đảm bảo rằng chúng hoạt động hiệu quả và được áp dụng đầy đủ. • Thực hiện các cuộc kiểm tra để phát hiện các lỗ hổng mới hoặc điểm yếu trong hệ thống, từ đó kịp thời triển khai các bản vá và biện pháp bảo vệ bổ sung. • Đảm bảo rằng các biện pháp bảo mật của doanh nghiệp phù hợp với các quy định pháp lý và yêu cầu của ISO 27001:2013, giảm thiểu rủi ro pháp lý và bảo vệ dữ liệu người dùng.

Ngày 31 tháng 10 năm 2024

	Họ và tên người soạn báo cáo
	Hồ Hải Dương