## Phụ lục 3

# I. CÁC ĐIỂM YẾU TRONG KIẾN TRÚC MẠNG CÓ THỂ BỊ KHAI THÁC

**Điểm yếu** kiến trúc mạng ('network architecture') có thể làm lộ ra các lỗ hổng mà kẻ tấn công có thể khai thác để truy cập trái phép, phá vỡ dịch vụ hoặc đánh cắp dữ liệu nhạy cảm. Dưới đây là một số **Điểm yếu** về kiến trúc phổ biến và cách chúng có thể bị khai thác.

**1. Kiến trúc mạng không phân đoạn/ mạng phẳng**

• **Điểm yếu**: Trong mạng phẳng ('Flat Network'), tất cả các thiết bị đều nằm trong cùng một phân đoạn ('segment'), nghĩa là có rất ít hoặc không có phân đoạn giữa các tài sản quan trọng và các phần khác của mạng.

• Khai thác: Khi kẻ tấn công có quyền truy cập vào bất kỳ phần nào của mạng, chúng có thể di chuyển ngang sang các hệ thống khác với ít rào cản nhất, xâm phạm các tài nguyên nhạy cảm hoặc leo thang đặc quyền.

**2. Phân đoạn mạng yếu hoặc không phân đoạn**

• **Điểm yếu**: Phân đoạn không đầy đủ giữa các hệ thống hướng đến người dùng, hệ thống nội bộ và kho lưu trữ dữ liệu nhạy cảm.

• Khai thác: Kẻ tấn công có thể lợi dụng sự thiếu phân đoạn này để truy cập vào các phần nhạy cảm của mạng sau khi xâm phạm các điểm cuối kém an toàn hơn, chẳng hạn như thiết bị của người dùng hoặc máy chủ công khai. Điều này thường được sử dụng trong các cuộc tấn công ransomware và đánh cắp dữ liệu.

**3. Tường lửa và Kiểm soát truy cập được cấu hình kém**

• **Điểm yếu**: Tường lửa được cấu hình sai hoặc có các quy tắc quá dễ dãi cho phép quá nhiều lưu lượng truy cập vào hoặc ra hoặc không hạn chế quyền truy cập vào các hệ thống nhạy cảm.

• Khai thác: Các tác nhân đe dọa có thể khai thác các cổng mở, phạm vi IP không bị hạn chế hoặc quyền quá rộng để vượt qua tường lửa, quét mạng và tìm lỗ hổng để khai thác.

**4. Điểm truy cập từ xa không an toàn (VPN, RDP, SSH)**

• **Điểm yếu**: Xác thực yếu đối với các dịch vụ truy cập từ xa như VPN, Giao thức máy tính từ xa (RDP) hoặc Secure Shell (SSH).

• Khai thác: Kẻ tấn công có thể sử dụng thông tin xác thực bị đánh cắp hoặc các cuộc tấn công 'brute-force attacks' để có quyền truy cập thông qua các điểm truy cập từ xa này. Khi đã vào bên trong, chúng có thể leo thang đặc quyền và xâm phạm các hệ thống mạng khác.

**5. Giám sát mạng không đủ**

• **Điểm yếu**: Thiếu giám sát và ghi nhật ký ('logging') toàn diện đối với lưu lượng truy cập mạng, khiến các hoạt động độc hại ('malicious activities') không bị phát hiện.

• Khai thác: Các tác nhân đe dọa có thể di chuyển lén lút trong mạng mà không kích hoạt cảnh báo ('triggering alerts'), cho phép chúng thực hiện đánh cắp dữ liệu, cài đặt phần mềm độc hại hoặc thiết lập cửa hậu ('backdoors').

**6. Hệ thống cũ và phần mềm không được hỗ trợ**

• **Điểm yếu**: Các hệ thống cũ không còn được nhà cung cấp hỗ trợ thường chứa các lỗ hổng chưa được vá.

• Khai thác: Kẻ tấn công có thể khai thác các lỗ hổng đã biết trong phần mềm hoặc phần cứng lỗi thời không còn nhận được bản cập nhật bảo mật. Các hệ thống này là điểm vào phổ biến cho các cuộc tấn công như 'ransomware' hoặc tấn công từ chối dịch vụ (DoS).

**7. Mã hóa yếu hoặc thiếu mã hóa**

• **Điểm yếu**: Dữ liệu nhạy cảm, chẳng hạn như thông tin đăng nhập của người dùng hoặc thông tin độc quyền, được truyền hoặc lưu trữ mà không được mã hóa phù hợp.

• Khai thác: Kẻ tấn công có thể chặn dữ liệu trong quá trình truyền bằng các cuộc tấn công trung gian (MitM) hoặc truy cập vào cơ sở dữ liệu không được mã hóa, có được quyền truy cập vào thông tin bí mật.

**8. Thiếu kiến trúc Zero Trust**

• **Điểm yếu**: Nhiều mạng truyền thống hoạt động theo giả định rằng người dùng hoặc thiết bị bên trong chu vi mạng được tin cậy, dẫn đến kiểm soát nội bộ yếu.

• Khai thác: Khi đã vào bên trong, kẻ tấn công có thể khai thác sự tin cậy này để di chuyển ngang qua mạng mà không cần kiểm tra xác thực thêm, thường dẫn đến xâm phạm rộng rãi.

**9. API và dịch vụ vi mô ('Microservices') dễ bị tấn công**

• **Điểm yếu**: Trong môi trường đám mây hoặc ứng dụng hiện đại, API hoặc dịch vụ vi mô được bảo mật kém là những lỗ hổng phổ biến.

• Khai thác: Kẻ tấn công có thể khai thác lỗ hổng trong 'API endpoints' để bỏ qua xác thực, lây nhiễm mã độc hoặc thực hiện các hoạt động trái phép.

**10. Quá phụ thuộc vào bảo mật vòng ngoài ('Perimeter Security')**

• **Điểm yếu**: Phụ thuộc quá nhiều vào các biện pháp phòng thủ vòng ngoài như tường lửa (Firewall) và Hệ thống phát hiện xâm nhập (IDS) mà ít hoặc không tập trung vào kiểm soát nội bộ hoặc bảo vệ điểm cuối.

• Khai thác: Nếu kẻ tấn công xâm phạm vòng ngoài, chúng có thể hoạt động tự do bên trong mạng mà không gặp phải các lớp bảo mật bổ sung.

**11. Cấu hình mặc định ('Default Configurations')**

• **Điểm yếu**: Nhiều thiết bị, hệ thống và ứng dụng có cấu hình mặc định không được củng cố hoặc tối ưu hóa cho bảo mật.

• Khai thác: Kẻ tấn công có thể khai thác thông tin xác thực mặc định, dịch vụ mở hoặc các tính năng không cần thiết được bật, tạo cho chúng chỗ đứng trong mạng.

**12. Quản lý bản vá yếu**

• **Điểm yếu**: Chậm trễ vá các lỗ hổng trong phần mềm và phần cứng có thể khiến hệ thống bị khai thác.

• Khai thác: Kẻ tấn công thường sử dụng các công cụ tự động để quét các hệ thống có lỗ hổng đã biết, chưa được vá, cho phép chúng khai thác các lỗ hổng đã được công khai.

**13. Điểm lỗi duy nhất ('Single Points of Failure (SPoFs)')**

• **Điểm yếu**: Kiến trúc mạng có điểm lỗi duy nhất (SPoF) không có dự phòng, nghĩa là sự xâm phạm hoặc lỗi của một thành phần có thể làm sập các dịch vụ quan trọng. *((*)A single point of failure (SPoF) is a potential risk posed by a flaw in the design, implementation or configuration of a circuit or system. SPoF refers to one fault or malfunction that can cause an entire system to stop operating or if it fails, will stop the entire system from working.*)

• Khai thác: Kẻ tấn công có thể nhắm mục tiêu vào các SPoF này (ví dụ: máy chủ DNS trung tâm hoặc máy chủ xác thực) để phát động các cuộc tấn công DoS, làm sập toàn bộ mạng hoặc các dịch vụ quan trọng.

**14. Thiếu bảo vệ DDoS**

• **Điểm yếu**: Một số mạng không được chuẩn bị để xử lý các cuộc tấn công từ chối dịch vụ phân tán (DDoS), có thể làm quá tải máy chủ bằng lưu lượng truy cập ('traffic').

• Khai thác: Kẻ tấn công có thể sử dụng các cuộc tấn công DDoS để làm sập dịch vụ, gây thiệt hại về tài chính hoặc hoạt động như một sự chuyển hướng trong khi thực hiện các cuộc tấn công khác như đánh cắp dữ liệu.

## II. CÁC ĐIỂM YẾU TRONG GIAO THỨC MẠNG CÓ THỂ BỊ KHAI THÁC

Giao thức mạng ('Network protocols') là nền tảng cho giao tiếp trong mạng máy tính, nhưng nhiều giao thức có **Điểm yếu** hoặc không được thiết kế với mục đích bảo mật. Những **Điểm yếu** này có thể bị kẻ tấn công khai thác để chặn, sửa đổi hoặc chiếm đoạt lưu lượng mạng hoặc thậm chí xâm phạm toàn bộ hệ thống. Dưới đây là một số **Điểm yếu** phổ biến của giao thức mạng và cách chúng có thể bị khai thác:

**1. Giao thức không được mã hóa (ví dụ: HTTP, FTP, Telnet)**

• **Điểm yếu**: Nhiều giao thức cũ truyền dữ liệu dưới dạng văn bản thuần túy mà không được mã hóa, bao gồm HTTP, FTP, Telnet và các giao thức khác.

• Khai thác: Kẻ tấn công có thể sử dụng các công cụ đánh hơi gói tin để chặn thông tin nhạy cảm, chẳng hạn như tên người dùng, mật khẩu và dữ liệu phiên, trong quá trình truyền. Điều này thường được thực hiện trong các cuộc tấn công Man-in-the-Middle (MitM) khi kẻ tấn công chặn thông tin liên lạc giữa hai bên.

**2. Giả mạo DNS và Đầu độc bộ đệm (Giao thức DNS)**

• **Điểm yếu**: Giao thức Hệ thống tên miền (DNS) có thể bị thao túng thông qua việc giả mạo hoặc đầu độc ('can be manipulated through spoofing or poisoning'), khiến hệ thống liên kết tên miền với một địa chỉ IP độc hại.

• Khai thác: Kẻ tấn công có thể chuyển hướng người dùng đến các trang web độc hại, thường là cho mục đích lừa đảo ('phishing') hoặc phát tán phần mềm độc hại. Đầu độc bộ đệm ('Cache poisoning') có thể cho phép kẻ tấn công lan truyền hiệu ứng này đến nhiều người dùng bằng cách thay đổi bộ đệm DNS của máy chủ.

**3. Tấn công 'ARP Spoofing' (ARP protocol)**

• **Điểm yếu**: Giao thức phân giải địa chỉ (ARP) được sử dụng để ánh xạ địa chỉ IP thành địa chỉ MAC trong mạng cục bộ, nhưng giao thức này thiếu cơ chế xác thực và xác minh.

• Khai thác: Trong một cuộc tấn công 'ARP spoofing', kẻ tấn công sẽ gửi tin nhắn ARP giả để liên kết địa chỉ MAC của chúng với địa chỉ IP của thiết bị khác, thường là cổng mặc định hoặc máy chủ DNS. Điều này cho phép kẻ tấn công chặn, sửa đổi hoặc chặn lưu lượng truy cập. Đây thường là cơ sở cho các cuộc tấn công Man-in-the-Middle (MitM) trên các mạng cục bộ.

**4. Điểm yếu trong ngăn xếp giao thức TCP/IP**

• **Điểm yếu**: Bộ giao thức TCP/IP ('Transmission Control Protocol/Internet Protocol') là nền tảng cho giao tiếp Internet nhưng có lỗ hổng cố hữu trong một số triển khai nhất định.

• Khai thác:

o IP Spoofing: Kẻ tấn công có thể làm giả địa chỉ IP nguồn trong các gói tin để xuất hiện như thể chúng đến từ một nguồn đáng tin cậy.

o TCP SYN Flooding: Kẻ tấn công có thể khai thác bắt tay ba chiều trong TCP bằng cách gửi một loạt yêu cầu SYN mà không hoàn tất bắt tay, dẫn đến cạn kiệt tài nguyên và gây ra Từ chối dịch vụ (DoS).

o Session Hijacking: Kẻ tấn công có thể chiếm quyền điều khiển phiên đang hoạt động bằng cách dự đoán số thứ tự TCP và đưa các gói tin độc hại vào một giao tiếp đang diễn ra.

**5. Khai thác SMB (Giao thức chặn tin nhắn máy chủ)**

• **Điểm yếu**: SMB là giao thức chia sẻ tệp, máy in và cổng nối tiếp, nhưng các phiên bản cũ hơn (như SMBv1) có các lỗi bảo mật nghiêm trọng, chẳng hạn như thiếu mã hóa và dễ bị tấn công tràn bộ đệm.

• Khai thác: Kẻ tấn công có thể khai thác các lỗ hổng như EternalBlue để phát tán phần mềm tống tiền và phần mềm độc hại khác. Các lỗ hổng SMB chưa được vá có thể cho phép thực thi mã từ xa.

**6. Lỗ hổng SSL/TLS**

• **Điểm yếu**: Giao thức SSL (Secure Sockets Layer) và TLS (Transport Layer Security) được sử dụng để mã hóa thông tin liên lạc, nhưng các phiên bản cũ hơn (SSL 3.0 và TLS 1.0) có lỗ hổng đã biết.

• Khai thác:

o Tấn công hạ cấp: Kẻ tấn công có thể buộc kết nối sử dụng phiên bản SSL/TLS cũ hơn, yếu hơn, chẳng hạn như thông qua cuộc tấn công POODLE, khai thác SSL 3.0.

o Bộ mã hóa yếu: Bộ mã hóa lỗi thời với mã hóa yếu có thể bị bẻ khóa, cho phép kẻ tấn công giải mã dữ liệu nhạy cảm trong quá trình truyền.

o Lỗ hổng Heartbleed: Một lỗ hổng trong một số phiên bản OpenSSL cho phép kẻ tấn công đọc bộ nhớ từ máy chủ, làm lộ khóa mã hóa và dữ liệu nhạy cảm.

**7. Khai thác ICMP (Ping of Death, Smurf Attack)**

• **Điểm yếu**: Giao thức tin nhắn điều khiển Internet (ICMP) được sử dụng cho mục đích chẩn đoán như khắc phục sự cố mạng (ví dụ: thông qua "ping"), nhưng nó có thể bị khai thác để gây ra các cuộc tấn công DoS.

• Khai thác:

o Ping of Death: Kẻ tấn công gửi các gói ICMP quá khổ, gây tràn bộ đệm trên hệ thống mục tiêu, có thể dẫn đến sự cố hoặc khởi động lại.

o Smurf Attack: Kẻ tấn công gửi các yêu cầu phản hồi ICMP đến địa chỉ phát sóng của mạng, với IP nguồn được giả mạo thành IP của mục tiêu. Kết quả là một loạt các phản hồi ICMP tràn ngập mục tiêu, gây ra DoS.

**8. BGP Hijacking (Giao thức Border Gateway bị chiếm đoạt)**

• **Điểm yếu**: Giao thức Border Gateway (BGP) được sử dụng để trao đổi thông tin định tuyến giữa các mạng khác nhau trên internet, nhưng nó thiếu các tính năng bảo mật mạnh mẽ, chẳng hạn như xác thực hoặc kiểm tra tính toàn vẹn ('authentication or integrity checking').

• Khai thác: Kẻ tấn công có thể đưa thông tin định tuyến sai ('false routing updates') vào bảng định tuyến toàn cầu, khiến lưu lượng bị định tuyến sai. Điều này có thể được sử dụng để chặn lưu lượng hoặc để phát động các cuộc tấn công từ chối dịch vụ (DoS) bằng cách áp đảo một số phân đoạn mạng nhất định. Việc chiếm quyền điều khiển BGP đặc biệt nguy hiểm vì nó có thể ảnh hưởng đến phần lớn lưu lượng truy cập Internet.

**9. Lỗ hổng RIP (Giao thức thông tin định tuyến)**

• **Điểm yếu**: RIP, một giao thức cũ hơn được sử dụng để trao đổi thông tin định tuyến, thiếu các tính năng bảo mật như mã hóa hoặc xác thực.

• Khai thác: Kẻ tấn công có thể đưa các bản cập nhật định tuyến sai vào mạng, chuyển hướng lưu lượng hoặc gây gián đoạn. Điều này được gọi là tấn công định tuyến ('routing attack') và có thể được sử dụng để phân tích lưu lượng, chặn lưu lượng hoặc DoS.

**10. Tấn công khuếch đại NTP (Giao thức thời gian mạng)**

• **Điểm yếu**: NTP được sử dụng để đồng bộ hóa đồng hồ trên các thiết bị, nhưng nó có một lỗ hổng là các yêu cầu nhỏ có thể tạo ra các phản hồi lớn không cân xứng, khiến nó dễ bị tấn công khuếch đại.

• Khai thác: Kẻ tấn công có thể gửi các yêu cầu NTP giả mạo đến các máy chủ dễ bị tấn công, các máy chủ này sẽ phản hồi bằng các phản hồi lớn hướng đến một IP mục tiêu. Điều này tạo ra một cuộc tấn công từ chối dịch vụ phân tán (DDoS), khiến mục tiêu bị quá tải lưu lượng truy cập.

**11. Tiêm LDAP (Giao thức truy cập thư mục nhẹ)**

• **Điểm yếu**: LDAP được sử dụng để truy cập và quản lý các dịch vụ thư mục, nhưng nó có thể dễ bị tấn công tiêm ('injection attacks') nếu các đầu vào không được xóa dữ liệu ('sanitized') đúng cách.

• Khai thác: Kẻ tấn công có thể chèn các truy vấn LDAP độc hại vào các đầu vào, cho phép chúng thao túng dữ liệu thư mục, bỏ qua xác thực hoặc leo thang đặc quyền.

**12. Khai thác SNMP**

• **Điểm yếu**: SNMP được sử dụng để quản lý các thiết bị trên mạng, nhưng các phiên bản cũ hơn (như SNMPv1 và SNMPv2) không có mã hóa và gửi dữ liệu dưới dạng văn bản thuần túy.

• Khai thác: Kẻ tấn công có thể chặn lưu lượng SNMP và lấy thông tin nhạy cảm về các thiết bị mạng, chẳng hạn như cài đặt cấu hình. Chúng cũng có thể gửi các lệnh SNMP độc hại để cấu hình lại thiết bị hoặc phá vỡ các dịch vụ.

**13. DHCP Spoofing (Giao thức DHCP giả mạo)**

• **Điểm yếu**: DHCP được sử dụng để tự động gán địa chỉ IP cho các thiết bị trên mạng, nhưng nó không có xác thực tích hợp.

• Khai thác: Kẻ tấn công có thể hoạt động như một máy chủ DHCP giả mạo, gán địa chỉ IP giả hoặc cổng mặc định ('default gateways') cho các thiết bị trên mạng. Điều này cho phép kẻ tấn công chuyển hướng lưu lượng để tấn công 'man-in-the-middle' hoặc gây gián đoạn mạng.

**14. Điểm yếu của Giao thức VoIP và SIP**

• **Điểm yếu**: Thoại qua IP (VoIP) và Giao thức khởi tạo phiên (Session Initiation Protocol (SIP)) được sử dụng cho điện thoại qua Internet nhưng thường thiếu các biện pháp bảo mật mạnh mẽ.

• Khai thác: Kẻ tấn công có thể khai thác SIP để thực hiện các cuộc gọi chiếm đoạt, nghe lén hoặc tấn công từ chối dịch vụ, dẫn đến các cuộc gọi bị chặn, gian lận hoặc mất dịch vụ.

## III. CÁC ĐIỂM YẾU TRONG MÁY CHỦ (servers) CÓ THỂ BỊ KHAI THÁC

Hệ thống máy chủ, giống như bất kỳ môi trường điện toán phức tạp nào, có một số **điểm yếu** tiềm ẩn có thể bị các tác nhân đe dọa khai thác để truy cập trái phép, phá vỡ dịch vụ hoặc đánh cắp thông tin nhạy cảm. Sau đây là một số **điểm yếu** phổ biến nhất của hệ thống máy chủ:

**1. Lỗ hổng chưa vá**

• Mô tả: Phần mềm và hệ điều hành thường xuyên nhận được các bản cập nhật bảo mật để khắc phục lỗ hổng. Nếu máy chủ không được cập nhật các bản vá mới nhất, máy chủ vẫn có thể bị khai thác.

• Khai thác: Kẻ tấn công có thể sử dụng các công cụ tự động để quét các hệ thống chưa vá và khai thác các lỗ hổng đã biết để giành quyền kiểm soát máy chủ.

**2. Cơ chế xác thực yếu**

• Mô tả: Mật khẩu yếu hoặc mặc định, chính sách mật khẩu không đầy đủ và thiếu xác thực đa yếu tố (MFA) có thể khiến kẻ tấn công dễ dàng truy cập.

• Khai thác: Các cuộc tấn công 'Brute-force attacks' hoặc 'dictionary attacks' có thể đoán được mật khẩu yếu, trong khi thông tin đăng nhập bị đánh cắp từ vi phạm dữ liệu có thể được sử dụng lại để xâm phạm hệ thống.

**3. Máy chủ cấu hình sai**

• Mô tả: Cấu hình máy chủ không đúng có thể mở ra cánh cửa cho kẻ tấn công. Bao gồm các quyền hạn quá mức cho phép, giao diện quản trị bị lộ hoặc tường lửa được cấu hình không đúng cách.

• Khai thác: Kẻ tấn công có thể thăm dò máy chủ để tìm các dịch vụ hoặc giao diện bị lộ không được phép truy cập công khai.

**4. Cổng mở và dịch vụ không cần thiết**

• Mô tả: Máy chủ thường có các cổng mở ('ports open') để lắng nghe lưu lượng truy cập, nhưng không phải tất cả các cổng đều cần được truy cập từ Internet. Ngoài ra, các dịch vụ không cần thiết phải bị vô hiệu hóa.

• Khai thác: Kẻ tấn công có thể sử dụng quét cổng để xác định các cổng và dịch vụ mở, có thể bị khai thác thông qua các lỗ hổng chưa được vá hoặc các vấn đề về cấu hình.

**5. Kiểm soát truy cập không đầy đủ**

• Mô tả: Kiểm soát truy cập không được xác định rõ ràng hoặc phân tách đặc quyền không đủ ('insufficient privilege separation') cho phép người dùng hoặc ứng dụng truy cập nhiều tài nguyên hơn mức cần thiết.

• Khai thác: Kẻ tấn công có thể leo thang đặc quyền để truy cập trái phép vào dữ liệu nhạy cảm hoặc vào các chức năng quản trị ('administrative functions').

**6. Phần mềm lỗi thời hoặc không được hỗ trợ**

• Mô tả: Phần mềm hoặc hệ điều hành không còn được nhà cung cấp hỗ trợ có thể không còn nhận được bản cập nhật bảo mật, khiến chúng dễ bị tấn công.

• Khai thác: Kẻ tấn công nhắm mục tiêu vào phần mềm cũ hơn có lỗ hổng chưa vá đã được công khai.

**7. Lỗ hổng 'SQL injection'**

• Mô tả: 'SQL injection' xảy ra khi kẻ tấn công có thể thao túng truy vấn cơ sở dữ liệu của máy chủ bằng cách tiêm mã SQL độc hại.

• Khai thác: Kẻ tấn công sử dụng các trường nhập liệu được thiết kế đặc biệt để thực thi các lệnh SQL tùy ý, có khả năng truy cập hoặc sửa đổi dữ liệu nhạy cảm dẫn đến vi phạm dữ liệu nghiêm trọng.

**8. Lỗ hổng XSS (Cross-Site Scripting attacks)**

• Mô tả: Lỗ hổng XSS xảy ra khi ứng dụng web cho phép thực thi các tập lệnh độc hại trong trình duyệt của người dùng cuối.

• Khai thác: Kẻ tấn công khai thác lỗ hổng bằng cách tiêm các tập lệnh độc hại có thể đánh cắp cookie phiên, mạo danh người dùng hoặc chuyển hướng họ đến các trang web độc hại, xâm phạm tài khoản người dùng.

**9. Tấn công từ chối dịch vụ (DoS)**

• Mô tả: Một cuộc tấn công DoS làm quá tải máy chủ với các yêu cầu quá mức, khiến máy chủ trở nên chậm, không phản hồi hoặc bị sập hoàn toàn.

• Khai thác: Kẻ tấn công có thể khai thác **điểm yếu** trong khả năng hoặc cấu hình máy chủ để khiến người dùng hợp pháp không thể sử dụng dịch vụ.

**10. Lỗ hổng API không an toàn**

• Mô tả: API (Giao diện lập trình ứng dụng ('Application Programming Interfaces')) thường được sử dụng để kết nối các dịch vụ, nhưng nếu không được bảo mật đúng cách, chúng có thể trở thành điểm vào cho kẻ tấn công.

• Khai thác: Kẻ tấn công có thể khai thác các điểm cuối API không an toàn bằng cách bỏ qua xác thực, lạm dụng xác thực đầu vào hoặc truy cập dữ liệu nhạy cảm khiến thông tin khách hàng bị truy cập trái phép.

**11. Điểm yếu do không đủ nhật ký và giám sát**

• Mô tả: Nếu không có nhật ký ('logging') và giám sát phù hợp, máy chủ có thể không cung cấp đủ thông tin để phát hiện và ứng phó với các sự cố bảo mật.

• Khai thác: Kẻ tấn công có thể xâm phạm hệ thống và không bị phát hiện trong thời gian dài do không đủ giám sát lưu lượng mạng và hoạt động của hệ thống, làm trầm trọng thêm thiệt hại mà chúng có thể gây ra.

**12. Tấn công kỹ thuật xã hội (Social Engineering Attacks) vào điểm yếu của người dùng**

• Mô tả: Máy chủ có thể bị xâm phạm gián tiếp khi kẻ tấn công lừa nhân viên hoặc quản trị viên cung cấp thông tin nhạy cảm, chẳng hạn như thông tin đăng nhập.

• Khai thác: Các cuộc tấn công lừa đảo và các phương pháp kỹ thuật xã hội khác có thể dẫn đến truy cập trái phép nếu quản trị viên bị lừa tiết lộ thông tin truy cập quan trọng.

**13. Điểm yếu về bảo mật vật lý**

• Mô tả: Nếu quyền truy cập vật lý vào máy chủ không được kiểm soát đúng cách, kẻ tấn công có thể truy cập vào phần cứng, dẫn đến đánh cắp dữ liệu hoặc can thiệp.

• Khai thác: Kẻ tấn công có quyền truy cập vật lý có thể cài đặt phần mềm độc hại, sao chép dữ liệu từ ổ đĩa hoặc can thiệp vào cấu hình hệ thống; ví dụ lây nhiễm phần mềm độc hại thông qua các ổ đĩa USB bị nhiễm.

## IV. CÁC ĐIỂM YẾU TRONG HỆ THỐNG LƯU TRỮ CÓ THỂ BỊ KHAI THÁC

Hệ thống lưu trữ, đặc biệt là hệ thống trong môi trường doanh nghiệp, lưu trữ dữ liệu quan trọng và do đó là mục tiêu chính của các tác nhân đe dọa. Chúng có nhiều **điểm yếu** khác nhau, nếu không được bảo mật đúng cách, có thể dẫn đến trộm cắp, mất mát hoặc thao túng dữ liệu. Dưới đây là một số **điểm yếu** phổ biến nhất của hệ thống lưu trữ có thể bị khai thác:

**1. Dữ liệu không được mã hóa khi lưu trữ**

• Mô tả: Dữ liệu được lưu trữ trên đĩa hoặc ổ đĩa mà không được mã hóa sẽ dễ bị truy cập trái phép. Mã hóa cung cấp một lớp bảo vệ ngay cả khi phương tiện lưu trữ bị xâm phạm.

• Khai thác: Các tác nhân đe dọa có được quyền truy cập vật lý hoặc logic vào dữ liệu không được mã hóa có thể đọc, sao chép hoặc thao túng thông tin được lưu trữ.

**2. Mã hóa dữ liệu không đầy đủ khi truyền tải**

• Mô tả: Khi dữ liệu di chuyển giữa các hệ thống lưu trữ, máy chủ và máy khách, dữ liệu có thể bị chặn nếu không được mã hóa đúng cách. Dữ liệu khi truyền tải phải được mã hóa bằng các giao thức bảo mật như giao thức TLS/SSL.

• Khai thác: Kẻ tấn công có thể chặn và nghe lén các dữ liệu truyền đi bằng cách sử dụng các cuộc tấn công trung gian (MITM), dẫn đến rò rỉ dữ liệu hoặc đánh cắp thông tin đăng nhập.

**3. Kiểm soát truy cập được định cấu hình sai**

• Mô tả: Cài đặt kiểm soát truy cập kém có thể cấp cho người dùng trái phép quyền truy cập, sửa đổi hoặc xóa dữ liệu quá mức trong hệ thống lưu trữ. Thiếu quyền truy cập dựa trên vai trò hoặc quyền quá rộng là những vấn đề phổ biến.

• Khai thác: Kẻ tấn công, dù là bên ngoài hay bên trong, đều có thể khai thác các cấu hình sai này để truy cập vào dữ liệu nhạy cảm mà chúng không được phép truy cập.

**4. Thông tin xác thực yếu hoặc mặc định**

• Mô tả: Các hệ thống lưu trữ dựa vào mật khẩu yếu hoặc thông tin xác thực mặc định là mục tiêu dễ dàng cho các cuộc tấn công bằng vũ lực hoặc nhồi thông tin xác thực.

• Khai thác: Kẻ tấn công có thể sử dụng các công cụ tự động để thử các mật khẩu phổ biến (như '123456') hoặc thông tin xác thực mặc định, giành được quyền truy cập trái phép vào hệ thống lưu trữ.

**5. Thiếu kiểm toán và giám sát**

• Mô tả: Nếu không có hoạt động ghi nhật ký (''logging) và giám sát, các hoạt động đáng ngờ hoặc trái phép có thể không bị phát hiện trong thời gian dài. Điều này cho phép kẻ tấn công hoạt động trong hệ thống mà không bị phát hiện.

• Khai thác: Kẻ tấn công có thể đánh cắp, thay đổi hoặc phá hủy dữ liệu mà không gây ra bất kỳ báo động nào, khiến các tổ chức khó có thể phản ứng hoặc xác định được vi phạm.

**6. Lưu trữ mạng bị lộ**

• Mô tả: Các hệ thống lưu trữ mạng như NAS ('Network attached storage') hoặc SAN ('Storage Area Network') thường được cấu hình sai để có thể truy cập qua Internet hoặc mạng lớn hơn mức cần thiết.

• Khai thác: Kẻ tấn công có thể tìm kiếm các hệ thống lưu trữ bị lộ thông qua địa chỉ IP hướng ra Internet hoặc các chia sẻ mạng không được bảo vệ, truy cập dữ liệu hoặc thậm chí kiểm soát hệ thống lưu trữ.

**7. Phần mềm lưu trữ lỗi thời hoặc chưa được vá**

• Mô tả: Các hệ thống lưu trữ, giống như bất kỳ phần mềm nào, cần được cập nhật và vá lỗi thường xuyên để khắc phục các lỗ hổng bảo mật. Không áp dụng các bản vá này sẽ khiến các lỗ hổng đã biết bị khai thác.

• Khai thác: Kẻ tấn công có thể khai thác các lỗ hổng đã biết trong phần mềm quản lý lưu trữ hoặc hệ điều hành cơ bản để giành quyền kiểm soát hoặc tăng đặc quyền trong hệ thống - ví dụ: Các lỗ hổng trong chương trình cơ sở lưu trữ hoặc giao diện quản lý (như CVE-2019-1649 trong Cisco UCS) là mục tiêu chính của kẻ tấn công.

**8. Quản lý dự phòng dữ liệu không đúng cách**

• Mô tả: Quản lý dự phòng và sao lưu không đúng cách, chẳng hạn như lưu trữ bản sao lưu ở cùng vị trí với dữ liệu chính, có thể dẫn đến mất dữ liệu hoàn toàn nếu xảy ra tấn công hoặc lỗi phần cứng.

• Khai thác: Trong các cuộc tấn công bằng phần mềm tống tiền ('ransomware attacks'), nếu bản sao lưu được lưu trữ trên cùng một mạng hoặc ổ đĩa với dữ liệu chính, kẻ tấn công có thể mã hóa hoặc phá hủy cả hai bản sao, khiến nạn nhân không có tùy chọn khôi phục.

**9. Xóa dữ liệu không đầy đủ ('Insufficient Data Sanitization')**

• Mô tả: Khi các thiết bị lưu trữ đã ngừng sử dụng hoặc được sử dụng lại, việc không xóa hoặc hủy dữ liệu đúng cách sẽ khiến thông tin có thể khôi phục được, ngay cả khi có vẻ như đã bị xóa.

• Khai thác: Kẻ tấn công có thể khôi phục dữ liệu nhạy cảm từ ổ cứng hoặc ổ đĩa thể rắn (SSD) bị xóa không đúng cách và sử dụng cho mục đích xấu.

**10. Điểm yếu về bảo mật vật lý**

• Mô tả: Các thiết bị và hệ thống lưu trữ có thể bị truy cập vật lý và bị can thiệp nếu không được bảo mật đầy đủ. Điều này bao gồm phòng máy chủ, trung tâm dữ liệu hoặc các thiết bị riêng lẻ như ổ cứng ngoài.

• Khai thác: Kẻ tấn công có quyền truy cập vật lý có thể đánh cắp phương tiện lưu trữ, cài đặt phần cứng độc hại (như phần mềm ghi phím hoặc trình đánh hơi dữ liệu) hoặc phá hủy dữ liệu; ví dụ: kẻ tấn công có thể chỉ cần đi vào một trung tâm dữ liệu không an toàn, cắm USB độc hại vào hệ thống lưu trữ và trích xuất thông tin nhạy cảm.

**11. Truy cập API không an toàn vào bộ nhớ đám mây ('Insecure API Access to Cloud Storage')**

• Mô tả: Nhiều hệ thống lưu trữ, đặc biệt là hệ thống lưu trữ dựa trên đám mây, để lộ API tương tác với dữ liệu. Nếu các API này không được bảo mật đúng cách (ví dụ: thông qua xác thực mạnh hoặc giới hạn tốc độ), chúng có thể bị lạm dụng.

• Khai thác: Kẻ tấn công có thể lạm dụng API không an toàn để truy cập hoặc thao túng dữ liệu, bỏ qua các cơ chế bảo mật truyền thống như tường lửa hoặc VPN.

**12. Thiếu kiểm tra tính toàn vẹn của dữ liệu**

• Mô tả: Nếu không có cơ chế đảm bảo tính toàn vẹn của dữ liệu ('Data Integrity Checks'), chẳng hạn như tổng kiểm tra hoặc xác minh băm, kẻ tấn công có thể sửa đổi hoặc làm hỏng dữ liệu mà không bị phát hiện.

• Khai thác: Kẻ tấn công có thể thay đổi dữ liệu đã lưu trữ (ví dụ: trong bối cảnh tài chính hoặc y tế), dẫn đến gian lận tài chính hoặc hậu quả có hại nếu dữ liệu bị hỏng là đáng tin cậy; ví dụ: các cuộc tấn công toàn vẹn trong lĩnh vực tài chính có thể liên quan đến việc thay đổi hồ sơ để tạo ra các giao dịch gian lận hoặc can thiệp vào bằng chứng trong cơ sở dữ liệu pháp lý.

**13. Lỗ hổng trong quy trình sao lưu và khôi phục**

• Mô tả: Bản thân các hệ thống sao lưu có thể là mục tiêu nếu chúng không được bảo mật đúng cách hoặc quy trình khôi phục không được xác minh. Kẻ tấn công có thể lây nhiễm phần mềm độc hại vào các bản sao lưu hoặc đảm bảo tổ chức không thể khôi phục dữ liệu của mình sau một cuộc tấn công.

• Khai thác: Kẻ tấn công có thể làm hỏng hoặc xóa dữ liệu sao lưu, khiến các tổ chức không thể khôi phục sau các sự cố như tấn công bằng phần mềm tống tiền.

## V. CÁC ĐIỂM YẾU TRONG HỆ THỐNG SAO LƯU CÓ THỂ BỊ KHAI THÁC

Hệ thống sao lưu rất cần thiết cho việc khôi phục dữ liệu và duy trì hoạt động kinh doanh, nhưng chúng cũng có một số lỗ hổng có thể bị các tác nhân đe dọa khai thác nếu không được bảo mật đúng cách. Sau đây là một số **điểm yếu** phổ biến trong hệ thống sao lưu và cách kẻ tấn công có thể khai thác chúng:

**1. Dữ liệu sao lưu không an toàn (thiếu mã hóa)**

• Mô tả: Nếu các bản sao lưu không được mã hóa, dữ liệu dễ bị truy cập trái phép. Các bản sao lưu không được mã hóa sẽ để lộ thông tin nhạy cảm, bao gồm dữ liệu cá nhân, hồ sơ tài chính hoặc sở hữu trí tuệ.

• Khai thác: Kẻ tấn công có quyền truy cập vào bộ lưu trữ sao lưu có thể đánh cắp, sao chép hoặc thao túng dữ liệu. Điều này đặc biệt rủi ro trong các bản sao lưu trên đám mây hoặc ngoài trang web có thể đi qua các mạng không đáng tin cậy.

**2. Kiểm soát truy cập không đầy đủ**

• Mô tả: Kiểm soát truy cập yếu, bao gồm chính sách mật khẩu kém, thiếu xác thực đa yếu tố (MFA) hoặc quyền người dùng quá mức, giúp người dùng trái phép (người trong cuộc hoặc kẻ tấn công bên ngoài) dễ dàng truy cập và thao túng dữ liệu sao lưu.

• Khai thác: Kẻ tấn công truy cập các tệp sao lưu và xóa, thay đổi hoặc đánh cắp dữ liệu. Người dùng được cấp quyền với quyền quá mức gây ra rủi ro đáng kể về việc vô tình hoặc cố ý làm hỏng tính toàn vẹn của bản sao lưu.

**3. Dữ liệu sao lưu được kết nối với mạng chính ('Primary Network')**

• Mô tả: Khi các bản sao lưu được lưu trữ trên cùng một mạng với các hệ thống chính, đặc biệt là trong môi trường lưu trữ trực tuyến, phần mềm tống tiền hoặc phần mềm độc hại có thể lây lan sang hệ thống sao lưu, xâm phạm cả dữ liệu chính và dữ liệu sao lưu.

• Khai thác: Trong các cuộc tấn công bằng phần mềm tống tiền, kẻ tấn công cố tình nhắm mục tiêu vào các bản sao lưu để đảm bảo rằng nạn nhân không thể khôi phục hệ thống của họ mà không trả tiền chuộc.

**4. Thiếu các bản sao lưu ngoại vi hoặc không có khoảng cách an toàn**

• Mô tả: Nếu các bản sao lưu không được lưu trữ ngoại vi hoặc không có khoảng cách an toàn (cách ly vật lý), chúng sẽ dễ bị tấn công giống như các cuộc tấn công ảnh hưởng đến hệ thống chính, chẳng hạn như thiên tai, hỏa hoạn hoặc các cuộc tấn công mạng có mục tiêu.

• Khai thác: Kẻ tấn công có thể phá hủy cả dữ liệu chính và các bản sao lưu nếu chúng được lưu trữ ở cùng một vị trí, dẫn đến mất dữ liệu hoàn toàn; ví dụ: Một vụ hỏa hoạn ở trung tâm dữ liệu hoặc một cuộc tấn công mạng phối hợp sẽ xóa sổ cả các hệ thống chính và các bản sao lưu được lưu trữ trong cùng một cơ sở, khiến tổ chức không thể khôi phục dữ liệu của mình.

**5. Dữ liệu sao lưu được lưu trữ mà không có chính sách lưu giữ**

• Mô tả: Nếu không có chính sách lưu giữ phù hợp, các bản sao lưu có thể lưu trữ dữ liệu quá lâu hoặc không đủ lâu. Việc lưu trữ dữ liệu lỗi thời hoặc không liên quan có thể khiến tổ chức phải chịu rủi ro theo quy định, trong khi việc lưu trữ không đầy đủ có thể dẫn đến mất dữ liệu quan trọng.

• Khai thác: Kẻ tấn công có quyền truy cập vào bản sao lưu có thể lấy thông tin lỗi thời nhưng vẫn có giá trị, chẳng hạn như hồ sơ khách hàng cũ hoặc chiến lược kinh doanh bí mật.

**6. Phần mềm sao lưu dễ bị tấn công**

• Mô tả: Phần mềm sao lưu có thể có lỗ hổng hoặc lỗi mà kẻ tấn công có thể khai thác. Điều này bao gồm phần mềm lỗi thời, hệ thống chưa vá hoặc giao diện không an toàn được sử dụng để quản lý quy trình sao lưu.

• Khai thác: Việc khai thác lỗ hổng trong phần mềm sao lưu có thể cung cấp cho kẻ tấn công quyền truy cập trái phép vào môi trường sao lưu, cho phép chúng thay đổi hoặc phá hủy dữ liệu sao lưu hoặc truy cập vào thông tin nhạy cảm.

**7. Thiếu kiểm tra tính toàn vẹn của bản sao lưu thường xuyên**

• Mô tả: Nếu không kiểm tra và xác minh tính toàn vẹn của bản sao lưu thường xuyên, các tổ chức có thể thấy rằng bản sao lưu của họ không đầy đủ, bị hỏng hoặc không sử dụng được khi họ cố gắng khôi phục dữ liệu sau một cuộc tấn công hoặc thảm họa.

• Khai thác: Kẻ tấn công có thể phá hoại bản sao lưu bằng cách đưa mã độc hại hoặc giả mạo dữ liệu, đảm bảo rằng ngay cả khi bản sao lưu được khôi phục, dữ liệu vẫn không sử dụng được hoặc bị xâm phạm.

**8. Lưu trữ sao lưu không an toàn (Đám mây hoặc vật lý)**

• Mô tả: Lưu trữ sao lưu, dù trên ổ đĩa vật lý hay trên đám mây, đều có thể dễ bị tấn công nếu không được bảo mật đúng cách. Sao lưu dựa trên đám mây có thể có API không an toàn và phương tiện sao lưu vật lý (ví dụ: băng hoặc ổ đĩa ngoài) có thể thiếu bảo vệ vật lý.

• Khai thác: Kẻ tấn công có thể truy cập dữ liệu sao lưu được lưu trữ trên bộ lưu trữ đám mây không được bảo vệ đầy đủ thông qua API không an toàn, cấu hình sai hoặc đánh cắp thông tin đăng nhập. Tương tự như vậy, việc đánh cắp vật lý phương tiện sao lưu có thể dẫn đến vi phạm dữ liệu.

**9. Tần suất sao lưu không đủ**

• Mô tả: Sao lưu không thường xuyên có thể khiến các tổ chức dễ bị mất dữ liệu nếu xảy ra sự kiện quan trọng giữa các khoảng thời gian sao lưu. Nếu chỉ sao lưu hàng tuần hoặc hàng tháng, dữ liệu quan trọng từ khoảng thời gian tạm thời có thể bị mất trong một cuộc tấn công hoặc thảm họa.

• Khai thác: Kẻ tấn công có thể gây mất dữ liệu đáng kể bằng cách nhắm mục tiêu vào các hệ thống giữa các lần sao lưu, biết rằng tổ chức sẽ không thể khôi phục dữ liệu gần đây.

**10. Phân chia nhiệm vụ không đủ (Quản lý sao lưu)**

• Mô tả: Nếu các tác vụ quản lý sao lưu không được phân chia hợp lý, một người dùng duy nhất có thể kiểm soát cả việc tạo và xóa bản sao lưu. Điều này làm tăng nguy cơ bị tấn công nội gián hoặc vô tình xóa bản sao lưu.

• Khai thác: Một người dùng nội gián độc hại hoặc tài khoản quản trị viên bị xâm phạm có thể xóa hoặc phá hoại bản sao lưu mà không có sự giám sát, dẫn đến mất dữ liệu hoặc không khả dụng trong quá trình xảy ra sự cố;

ví dụ: Một nhân viên bất mãn có quyền truy cập quản trị xóa các bản sao lưu quan trọng, dẫn đến mất hoàn toàn dữ liệu có thể khôi phục được.

**11. Sao lưu không quét phần mềm độc hại**

• Mô tả: Các bản sao lưu không được quét thường xuyên để tìm phần mềm độc hại (‘malware’) hoặc kiểm tra tính toàn vẹn có thể lưu trữ các tệp bị nhiễm, dẫn đến tái nhiễm trong quá trình khôi phục dữ liệu.

• Khai thác: Kẻ tấn công có thể lây nhiễm phần mềm độc hại vào dữ liệu sao lưu, đảm bảo rằng bất kỳ dữ liệu nào được khôi phục đều đưa phần mềm độc hại trở lại môi trường.

**12. Không có bản sao lưu bất biến**

• Mô tả: Một số hệ thống sao lưu không có tính bất biến (‘immutable’), nghĩa là sau khi tạo bản sao lưu, bản sao lưu đó có thể bị sửa đổi hoặc xóa. Điều này cho phép kẻ tấn công xâm phạm hoặc xóa bản sao lưu sau một cuộc tấn công.

• Khai thác: Kẻ tấn công nhắm mục tiêu cụ thể vào các bản sao lưu có thể bị xóa hoặc thay đổi để đảm bảo rằng tổ chức không thể khôi phục dữ liệu sau một cuộc tấn công, buộc họ phải trả tiền chuộc.

**13. Các cửa sổ sao lưu chồng chéo**

• Mô tả: Nếu lịch trình sao lưu chồng chéo với các cửa sổ sản xuất (ví dụ: trong giờ làm việc), điều này có thể làm chậm hệ thống, khiến người quản trị vô hiệu hóa các bản sao lưu hoặc hoãn chúng, điều này có thể dẫn đến bỏ lỡ các cơ hội sao lưu và tăng rủi ro.

• Khai thác: Kẻ tấn công có thể khai thác các khoảng thời gian hoạt động sao lưu bị giảm hoặc bị đình chỉ để phát động một cuộc tấn công, biết rằng hệ thống không được bảo vệ đầy đủ.

## VI. CÁC ĐIỂM YẾU TRONG QUẢN LÝ DỮ LIỆU CÓ THỂ BỊ KHAI THÁC

**Điểm yếu** trong quản lý dữ liệu, nếu không được giải quyết đúng cách, có thể khiến các tổ chức phải đối mặt với nhiều cuộc tấn công từ các tác nhân đe dọa. Dưới đây là các lỗ hổng chính trong hoạt động quản lý dữ liệu mà kẻ tấn công có thể khai thác:

**1. Kiểm soát truy cập dữ liệu yếu hoặc không nhất quán**

• Mô tả: Việc thiếu các biện pháp kiểm soát truy cập được thực thi đúng cách có thể cho phép người dùng trái phép truy cập, sửa đổi hoặc xóa dữ liệu. Điều này thường xảy ra do các quyền được xác định không rõ ràng, cơ chế xác thực yếu hoặc không áp dụng nguyên tắc đặc quyền tối thiểu.

• Khai thác: Kẻ tấn công khai thác các quyền quá mức hoặc cấu hình sai để truy cập dữ liệu nhạy cảm hoặc sử dụng các tài khoản bị xâm phạm để điều hướng hệ thống và đánh cắp dữ liệu.

**2. Dữ liệu nhạy cảm chưa được mã hóa**

• Mô tả: Không mã hóa dữ liệu nhạy cảm khi lưu trữ và khi truyền tải sẽ khiến dữ liệu đó bị truy cập trái phép. Dù kẻ tấn công truy cập được vào hệ thống, mã hóa vẫn đóng vai trò là biện pháp bảo vệ để bảo vệ dữ liệu.

• Khai thác: Kẻ tấn công xâm phạm hệ thống có thể đánh cắp dữ liệu nhạy cảm, chưa được mã hóa, dẫn đến vi phạm thông tin bí mật.

**3. Phân loại dữ liệu kém**

• Mô tả: Không phân loại và dán nhãn dữ liệu đúng cách dựa trên mức độ nhạy cảm của dữ liệu có thể dẫn đến việc xử lý dữ liệu hoặc các biện pháp bảo mật không phù hợp. Dữ liệu có độ nhạy cao có thể được lưu trữ hoặc xử lý với mức độ bảo mật tương tự như dữ liệu ít quan trọng hơn.

• Khai thác: Kẻ tấn công có thể dễ dàng truy cập thông tin nhạy cảm hơn khi thông tin đó không được phân loại hoặc bảo vệ theo giá trị của dữ liệu, làm tăng khả năng thiệt hại do vi phạm.

**4. Thiếu kiểm tra tính toàn vẹn của dữ liệu**

• Mô tả: Nếu không có các cơ chế như tổng kiểm tra, xác minh băm hoặc kiểm soát phiên bản, các tổ chức không thể đảm bảo dữ liệu không bị giả mạo, dẫn đến khả năng thao túng hoặc làm hỏng dữ liệu.

• Khai thác: Kẻ tấn công có thể sửa đổi dữ liệu mà không bị phát hiện, gây ra gian lận tài chính, thay đổi hồ sơ hoặc chèn mã độc.

**5. Chính sách lưu giữ dữ liệu không đủ**

• Mô tả: Chính sách lưu giữ dữ liệu yếu hoặc không tồn tại dẫn đến việc lưu trữ dữ liệu không cần thiết hoặc lỗi thời, làm tăng bề mặt tấn công (‘attack surface’). Ngoài ra, dữ liệu quan trọng có thể bị xóa quá sớm.

• Khai thác: Kẻ tấn công có quyền truy cập vào dữ liệu cũ hoặc được lưu giữ không đúng cách có thể lợi dụng dữ liệu đó để thực hiện kỹ thuật xã hội, lợi ích tài chính hoặc bị phạt theo quy định nếu tổ chức không tuân thủ luật lưu giữ dữ liệu.

**6. Hệ thống sao lưu được quản lý không đúng cách**

• Mô tả: Nếu quy trình sao lưu được quản lý kém, dữ liệu có thể không được sao lưu thường xuyên hoặc hệ thống sao lưu có thể không an toàn. Điều này có thể dẫn đến việc sao lưu không đầy đủ hoặc không thể truy cập trong thảm họa hoặc cuộc tấn công.

• Khai thác: Kẻ tấn công có thể xóa, mã hóa hoặc làm hỏng các bản sao lưu, khiến tổ chức không thể khôi phục dữ liệu quan trọng sau một cuộc tấn công mạng.

**7. Truyền dữ liệu không an toàn**

• Mô tả: Khi dữ liệu nhạy cảm được truyền qua mạng mà không được mã hóa hoặc sử dụng các giao thức không an toàn (ví dụ: FTP), dữ liệu đó có thể bị kẻ tấn công chặn lại.

• Khai thác: Các cuộc tấn công trung gian (MITM) có thể chặn các lần truyền dữ liệu, cho phép kẻ tấn công đánh cắp, thay đổi hoặc can thiệp vào thông tin đang truyền; ví dụ: Trong một giao dịch tài chính, kẻ tấn công chặn và sửa đổi dữ liệu, thay đổi thông tin chi tiết về thanh toán để chuyển hướng tiền vào tài khoản của chính chúng.

**8. Cơ sở dữ liệu cấu hình sai**

• Mô tả: Cơ sở dữ liệu cấu hình sai (ví dụ: thiếu danh sách kiểm soát truy cập phù hợp, mở trên Internet hoặc có thông tin xác thực mặc định) rất dễ bị tấn công.

• Khai thác: Kẻ tấn công có thể tìm kiếm cơ sở dữ liệu mở hoặc dễ bị tấn công bằng các công cụ (như Shodan), cho phép chúng dễ dàng truy cập dữ liệu nhạy cảm hoặc thực hiện các truy vấn SQL độc hại.

**9. Tài khoản có đặc quyền quá mức**

• Mô tả: Việc cấp cho người dùng quyền truy cập quá mức hoặc đặc quyền quản trị làm tăng nguy cơ vi phạm dữ liệu vì những tài khoản này có thể bị kẻ tấn công nhắm tới.

• Khai thác: Kẻ tấn công có thể chiếm đoạt các tài khoản có đặc quyền quá mức để có quyền truy cập rộng rãi vào các hệ thống và dữ liệu nhạy cảm; ví dụ: Kẻ tấn công xâm phạm tài khoản của nhân viên bằng các quyền quản trị, giành quyền truy cập không hạn chế vào các cơ sở dữ liệu nhạy cảm nhất của tổ chức.

**10. Cơ chế xác thực yếu hoặc lỗi thời**

• Mô tả: Mật khẩu yếu, xác thực một yếu tố hoặc hệ thống xác thực lỗi thời không có nhiều khả năng bảo vệ chống lại truy cập trái phép.

• Khai thác: Kẻ tấn công sử dụng các kỹ thuật như ‘credential stuffing’, tấn công bằng vũ lực hoặc kỹ thuật xã hội (‘brute-force attacks, or social engineering’) để có quyền truy cập vào tài khoản người dùng.

**11. Thực hành xử lý dữ liệu không đầy đủ**

• Mô tả: Không xử lý hoặc xóa dữ liệu (‘sanitize data’) đúng cách sau khi không còn cần thiết (ví dụ: xóa ổ cứng, hủy hồ sơ giấy) khiến dữ liệu có thể khôi phục được và dễ bị truy cập trái phép.

• Khai thác: Kẻ tấn công có thể khôi phục dữ liệu nhạy cảm từ phương tiện lưu trữ không được xử lý đúng cách (ví dụ: ổ cứng hoặc ổ đĩa flash) hoặc từ môi trường đám mây nơi dữ liệu không được xóa an toàn.

**12. Rủi ro tổng hợp dữ liệu**

• Mô tả: Việc tổng hợp dữ liệu từ nhiều nguồn vào một vị trí (ví dụ: hồ dữ liệu) mà không có biện pháp kiểm soát bảo mật đầy đủ có thể tạo ra một điểm lỗi duy nhất có giá trị cao đối với kẻ tấn công.

• Khai thác: Kẻ tấn công tập trung vào dữ liệu tổng hợp để đánh cắp khối lượng lớn thông tin nhạy cảm cùng một lúc, tối đa hóa tác động của vi phạm; ví dụ: Trong môi trường đám mây, lượng lớn dữ liệu khách hàng nhạy cảm từ nhiều hệ thống khác nhau được tập hợp thành một kho lưu trữ không an toàn, nơi mà kẻ tấn công nhắm tới để đánh cắp một lượng lớn dữ liệu.

**13. Không áp dụng bản vá bảo mật**

• Mô tả: Hệ thống quản lý dữ liệu lỗi thời hoặc phần mềm có lỗ hổng đã biết nhưng chưa được vá là mục tiêu dễ dàng cho kẻ tấn công.

• Khai thác: Kẻ tấn công khai thác các lỗ hổng đã biết trong phần mềm quản lý dữ liệu lỗi thời để truy cập trái phép, nâng cao đặc quyền hoặc thực thi mã độc.

**14. Shadow IT (Hệ thống dữ liệu không được giám sát)**

• Mô tả: 'Shadow IT' đề cập đến các hệ thống dữ liệu hoặc ứng dụng được triển khai mà không có sự hiểu biết hoặc chấp thuận của bộ phận CNTT; ví dụ một nhân viên lạm dụng quyền hạn của mình lén cài đặt một phần mềm chụp màn hình có nhiều tính năng vào máy tính của mình. Các hệ thống hay ứng dụng này thường thiếu các biện pháp bảo mật và tuân thủ phù hợp.

• Khai thác: Kẻ tấn công nhắm mục tiêu vào các hệ thống không chính thức này, biết rằng chúng ít có khả năng có các biện pháp kiểm soát bảo mật mạnh mẽ tại chỗ.

**15. Quản trị dữ liệu không nhất quán**

• Mô tả: Quản trị dữ liệu kém, chẳng hạn như các chính sách không nhất quán về quyền sở hữu, xử lý và trách nhiệm giải trình dữ liệu, có thể dẫn đến trách nhiệm bảo mật dữ liệu không rõ ràng.

• Khai thác: Kẻ tấn công khai thác các cấu trúc quản trị yếu để truy cập dữ liệu không được bảo vệ đầy đủ do thiếu sự giám sát hoặc trách nhiệm.

**16. Giám sát và ghi nhật ký không đầy đủ**

• Mô tả: Nếu không giám sát và ghi nhật ký ('logging') hiệu quả về hoạt động và quyền truy cập dữ liệu, hành vi bất thường hoặc truy cập trái phép có thể không bị phát hiện.

• Khai thác: Kẻ tấn công có thể di chuyển qua mạng, truy cập dữ liệu và leo thang các cuộc tấn công của chúng mà không kích hoạt báo động hoặc cảnh báo; ví dụ: Vi phạm dữ liệu không được phát hiện trong nhiều tháng vì không có cơ chế ghi nhật ký đầy đủ để theo dõi quyền truy cập trái phép vào các hệ thống nhạy cảm.

**17. Không bảo vệ dữ liệu bằng biện pháp che giấu dữ liệu hoặc 'tokenization'**

• Mô tả: Lưu trữ dữ liệu nhạy cảm ở dạng thô, thay vì sử dụng các kỹ thuật như che giấu dữ liệu hoặc mã hóa ('data masking or tokenization'), khiến dữ liệu dễ bị lộ - (*'Tokenization is the process of substituting a sensitive data element with a non-sensitive equivalent, referred to as a token'*)

• Khai thác: Kẻ tấn công truy cập dữ liệu có thể sử dụng hoặc bán dữ liệu ngay lập tức, trong khi dữ liệu được che giấu hoặc mã hóa sẽ vô dụng nếu không có khóa giải mã thích hợp./.