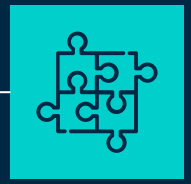
BÀI TẬP BUỔI 4

Môn: An toàn mạng máy tính

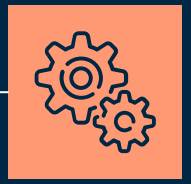
GVHD: ThS. Lê Đức Thịnh

--- Nhóm 10 ---
Nguyễn Chí Toàn - 19522361
Nguyễn Hoàng Hiệu - 19521503
Cao Thị Bích Phượng - 19522058
Đoàn Thị Thanh Nhàn - 19521929

NỘI DUNG TÌM HIỂU



01 Khái niệm về Zero Trust



02 Mô hình bảo mật cơ bản

03 Ưu điểm và nhược điểm

04 Tính ứng dụng

Khái niệm về Zero Trust

01

1 . Khái niệm về Zero Trust

Zero Trust là gì?

Zero Trust là mô hình tập trung vào bảo mật dựa trên ý tưởng rằng doanh nghiệp ***không nên*** có tùy chọn tin cậy mặc định cho bất kỳ thứ gì bên ngoài hoặc bên trong ranh giới của họ. Thay vào đó, họ phải xác thực mọi thứ cố gắng giành quyền truy cập và kết nối với hệ thống trước khi quyền truy cập được cấp.

1 . Khái niệm về Zero Trust

- 3 nguyên lý của mô hình bảo mật Zero Trust

Xác thực đối tượng truy cập

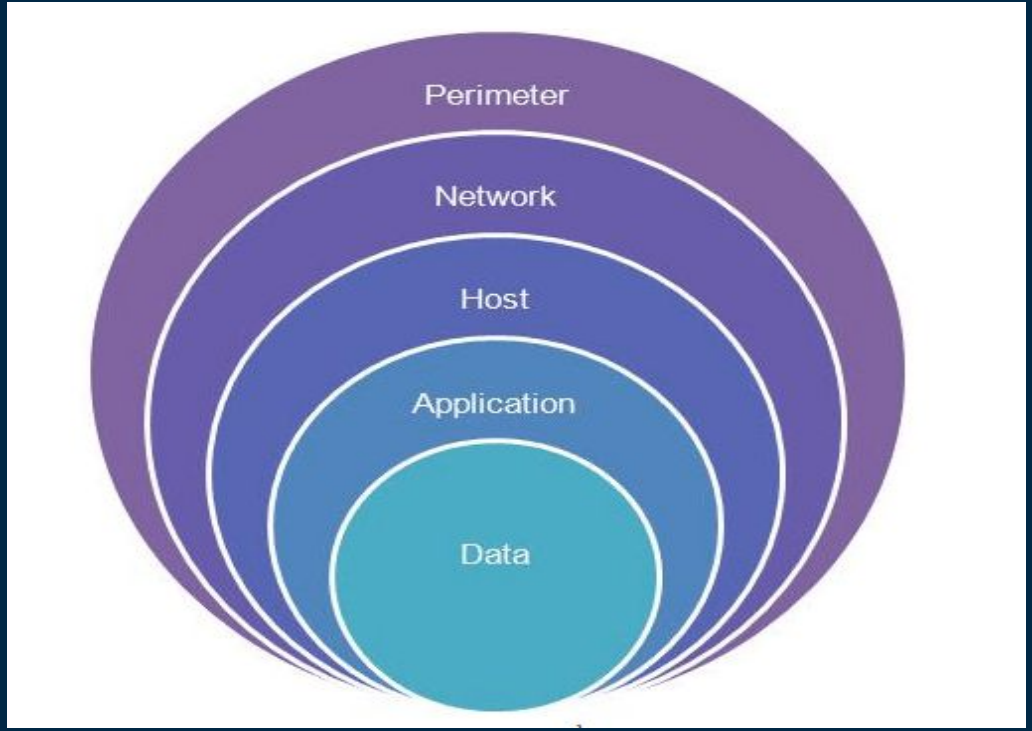
Giới hạn cấp phép truy cập độc quyền

Giả định trường hợp vi phạm

Mô hình bảo mật cơ bản

02

2 . Mô hình bảo mật cơ bản:



2 . Mô hình bảo mật cơ bản:

IDENTITY	Zero Trust bắt đầu với việc xác định danh tính, xác minh rằng chỉ những người, thiết bị được cấp quyền mới được phép truy cập vào hệ thống.
PERIMETER	Được bảo vệ chủ yếu bằng Firewall và router, thiết lập những quy tắc chung để quản lý mà hạn chế sự tấn công từ các attacker.
NETWORK	Thiết kế, quản lý mạng nội bộ một cách chặt chẽ, có các biện pháp bảo vệ lớp mạng để truy cập vào các tài nguyên, đặc biệt là tài nguyên quan trọng.
HOST	Cập nhật hệ điều hành và các ứng dụng, đánh giá mức độ bảo mật của các thiết bị, hạn chế trao đổi trực tiếp giữa host và các thiết bị ngoại vi.
APPLICATION	Zero Trust giám sát các ứng dụng của bạn dù là trong cục bộ hay ở đám mây vì khi cập nhập hay cài đặt phần mềm, nó sẽ trỏ đến thông tin của bạn.
DATA	Bảo vệ dữ liệu trên các tệp của bạn, cũng như các dữ liệu có cấu trúc và phi cấu trúc ở bất kì đâu trong CSDL của bạn bằng cách mã hóa chúng.

Ưu điểm và nhược điểm

03

3 . Ưu và nhược điểm

Ưu điểm

Chính sách xác thực và truy cập của người dùng

Nó dựa trên việc triển khai chính xác xác thực đa yếu tố kết hợp với cấu trúc các chính sách bảo mật để xác nhận những tài nguyên nào người dùng có thể truy cập. Có trường hợp các công ty lựa chọn SSO (Đăng nhập một lần hoặc thu nhập đơn giản) được quản lý bởi các nhà cung cấp dịch vụ đám mây. Cái sau được gọi là IDaaS, nghĩa là, nhận dạng như một dịch vụ . Trong mô hình Zero-Trust, quyền truy cập vào tài nguyên được bảo vệ theo các điều sau: bối cảnh của yêu cầu và rủi ro mà nó tạo ra trong trường hợp cấp phép. Việc cấp các quyền này có thể có nghĩa là quyền truy cập hạn chế vào các chức năng của tài nguyên chúng tôi đang quản lý, một lớp xác thực khác được thêm vào trước khi cấp quyền hoặc định nghĩa về thời gian cụ thể khi kết nối với mạng sẽ tự động kết thúc.

3 . Ưu và nhược điểm

Ưu điểm

Phân đoạn dữ liệu và tài tài nguyên

Phân chia nguồn lực phù hợp giữa các người dùng khác nhau sẽ cho phép các chính sách bảo mật được triển khai trở nên hữu ích. Không còn đáng tin cậy để cung cấp quyền truy cập duy nhất và bất kỳ người dùng nào trong mạng có thể truy cập bất kỳ tài nguyên nào mà không có bất kỳ hạn chế nào. Điều này sẽ đại diện cho vô số rủi ro, đặc biệt là lọc dữ liệu cá nhân.

Điều tương tự áp dụng cho dữ liệu cá nhân. Bản thân chúng tôi đại diện cho rủi ro lớn nhất cho dữ liệu của chúng tôi. Chúng được phơi bày mọi lúc, đặc biệt là khi chúng ta thao tác chung từ điện thoại di động. Nếu chúng tôi không thực hiện các biện pháp bảo mật chính xác, có thể trong vài giây, dữ liệu của chúng tôi bị xâm phạm hoặc chúng tôi mất hoàn toàn.

3 . Ưu và nhược điểm

Ưu điểm

Bảo mật dữ liệu

Một trong những trọng tâm của mô hình Zero Trust là bảo mật dữ liệu. Ứng dụng mã hóa End-to-End là một trong những biện pháp bảo mật ngày càng cần thiết để áp dụng. Nó không còn đủ để mã hóa dữ liệu khi gửi hoặc nhận nó. Ngoài ra trong quá trình vận chuyển và tại thời điểm được xử lý, chúng không nên được coi là văn bản đơn giản vì điều này sẽ bật đèn xanh cho các rò rỉ không mong muốn.

- Sao lưu tự động đảm bảo dữ liệu sẵn có tại thời điểm chúng tôi cần chúng. Điều quan trọng là những bản sao này được tạo ra ít nhất trên cơ sở hàng tuần. Nếu có bất kỳ vấn đề nào với máy tính tại nơi làm việc của chúng tôi và các tệp của chúng tôi bị ảnh hưởng, bản sao lưu cuối cùng có thể cứu chúng tôi khỏi nhiều vấn đề. Không ai thích phải bắt đầu bất kỳ tài liệu nào từ đầu.

3 . Ưu và nhược điểm

Ưu điểm

Điều phối bảo mật

Cuối cùng, việc vẽ một luồng thông qua tất cả các trụ cột này là tầm quan trọng của việc điều phối bảo mật. Ngay cả khi không có hệ thống quản lý bảo mật, các tổ chức sử dụng Zero Trust vẫn cần đảm bảo rằng các giải pháp bảo mật hoạt động tốt cùng nhau và bao gồm tất cả các vectơ tấn công có thể xảy ra. Bản thân sự chồng chéo không phải là một vấn đề, nhưng có thể khó để tìm ra các cài đặt phù hợp để tối đa hóa hiệu quả và giảm thiểu xung đột.

3 . Ưu và nhược điểm

Nhược điểm

Zero Trust được coi là một phương pháp tiếp cận toàn diện để đảm bảo quyền truy cập trên các mạng, ứng dụng và môi trường từ người dùng, thiết bị người dùng cuối, API, IoT, dịch vụ vi mô, vùng chứa, v.v. Trong khi hướng tới mục tiêu bảo vệ lực lượng lao động, khối lượng công việc và nơi làm việc, Zero Trust thực sự gặp phải một số thách thức.
Bao gồm các:

- ➔ Ngày càng có nhiều loại người dùng khác nhau (trong văn phòng và từ xa)
- ➔ Ngày càng có nhiều loại thiết bị khác nhau (di động, IoT, công nghệ sinh học)
- ➔ Ngày càng có nhiều loại ứng dụng khác nhau (CMS, mạng nội bộ, nền tảng thiết kế)
- ➔ Nhiều cách khác để truy cập và lưu trữ dữ liệu (drive, cloud, edge)

Tính ứng dụng

04

4. Tính ứng dụng

- **Bảo mật danh tính với Zero Trust:** Khi một danh tính cố gắng truy cập một tài nguyên, cần xác minh danh tính đó bằng cách xác thực mạnh và đảm bảo quyền truy cập tuân thủ và điển hình cho danh tính đó. Tuân theo các nguyên tắc truy cập đặc quyền ít nhất

- **Điểm cuối an toàn với Zero Trust:** Sau khi danh tính đã được cấp quyền truy cập vào tài nguyên, dữ liệu có thể chuyển đến nhiều điểm cuối khác nhau — từ thiết bị IoT đến điện thoại thông minh, BYOD đến thiết bị do đối tác quản lý và khối lượng công việc tại chỗ tới các máy chủ được lưu trữ trên đám mây. Sự đa dạng này tạo ra một diện tích bề mặt tấn công lớn.

4. Tính ứng dụng

- **Ứng dụng an toàn với Zero Trust:** Áp dụng các biện pháp kiểm soát và công nghệ để khám phá CNTT ẩn, đảm bảo quyền thích hợp trong ứng dụng, truy cập cổng dựa trên phân tích thời gian thực, giám sát hành vi bất thường, kiểm soát hành động của người dùng và xác thực các tùy chọn cấu hình an toàn.

- **Bảo mật dữ liệu với Zero Trust:** Cuối cùng, các nhóm bảo mật đang bảo vệ dữ liệu. Khi có thể, dữ liệu phải vẫn an toàn ngay cả khi dữ liệu đó rời khỏi các thiết bị, ứng dụng, cơ sở hạ tầng và mạng mà tổ chức kiểm soát. Phân loại, gắn nhãn và mã hóa dữ liệu cũng như hạn chế quyền truy cập dựa trên các thuộc tính đó.

4. Tính ứng dụng

- **Cơ sở hạ tầng an toàn với Zero Trust:** Sử dụng phép đo từ xa để phát hiện các cuộc tấn công và sự bất thường, đồng thời tự động chặn và gắn cờ các hành vi nguy hiểm và thực hiện các hành động bảo vệ.
- **Mạng an toàn với Zero Trust:** Phân đoạn mạng (và thực hiện phân đoạn vi mô trong mạng sâu hơn) và triển khai bảo vệ mối đe dọa theo thời gian thực, mã hóa đầu cuối, giám sát và phân tích.
- **Khả năng hiển th, tự động hóa và điều phối với Zero Trust:** Xác định cách tiếp cận để triển khai phương pháp luận Zero Trust từ đầu đến cuối trên danh tính, điểm cuối và thiết bị, dữ liệu, ứng dụng, cơ sở hạ tầng và mạng.

THANKS FOR WATCHING