ZERO TRUST ARCHITECTURE

Never trust - Always verify

Cyber Team

Vũ Minh Tuyến (trưởng nhóm)

Đinh Thị Thanh Huyền

Nguyễn Văn Thành

MỤC LỤC

LỜI NÓI ĐẦU

Sự tiến bộ của công nghệ và những thay đổi trong cách chúng ta làm việc đồng nghĩa các mối đe dọa an ninh mạng cũng tăng lên và chúng ta đang phải đối mặt với các mối đe dọa mới mỗi ngày. Đó có thể đến từ bên ngoài hoặc bên trong tổ chức - ví dụ: nếu một nhân viên vô tình mở một email lừa đảo hoặc để máy tính xách tay của họ không khóa và ai đó không có quyền truy cập vào nó. Để chống lại các lỗ hổng này, khi mà các cách bảo mật truyền thống đã không còn hiệu quả, bắt buộc các doanh nghiệp phải tìm ra những phương pháp mới để giải quyết vấn đề này.

Sau thời gian học tập môn Chuyên nghiệp trong Công nghệ cũng như thảo luận nhóm, chúng em đã có sự nhận thức sâu sắc về vấn đề bảo mật không chỉ ảnh hưởng tới những công ty, doanh nghiệp mà còn tác động tới cả sự phát triển của công nghệ trong tương lai. Chính vì lẽ đó, chúng em đã chọn phương pháp bảo mật Zero Trust làm đề tài nghiên cứu của nhóm.

Chúng em xin gửi lời cảm ơn tới thầy Nguyễn Nam Hoàng đã cung cấp những kiến thức cơ sở, người đã trực tiếp hướng dẫn để nhóm em có thể hoàn thành báo cáo thực tập tổng hợp này.

Báo cáo nghiên cứu tổng hợp bao gồm các phần sau:

- **Phần 1:** Tiêu đề và tóm tắt sơ lược về đề tài bài tiểu luận, giới thiệu chung về bài tiểu luận
- **Phần 2:** Định nghĩa, nguyên tắc và chức năng của Zero Trust
- **Phần 3:** So sánh và đánh giá mô hình Zero Trust với các mô hình truyền thống; đưa ra hiệu quả, các hạn chế của Zero Trust
- **Phần 4:** Kết luận, tương lai của Zero Trust
- **Phần 5:** Tài liệu tham khảo

PHẦN 1: GIỚI THIỆU CHUNG

Trong bối cảnh cả thế giới đang khủng hoảng trước làn sóng dịch Covid 19, xu hướng làm việc tại nhà ngày càng gia tăng. Đây cũng là nguyên nhân làm gia tăng các trò gian lận và lừa đảo, các cuộc tấn công nhanh và một loạt các phương thức tấn công mạng khác đang tìm cách khai thác các lỗ hổng bảo mật[1]. Theo Microsoft, 54% các nhà lãnh đạo bảo mật báo cáo rằng sự gia tăng các cuộc tấn công lừa đảo kể từ khi dịch bùng phát. Vì vậy các tổ chức, doanh nghiệp cần có một phương pháp bảo mật mới.

Bảo mật Zero Trust đã chuyển từ một lựa chọn sang ưu tiên kinh doanh trong những ngày đầu của đại dịch, khi các nhà lãnh đạo doanh nghiệp tìm cách xử lý luồng công việc mới, có khả năng không an toàn, nhiều thiết bị đăng nhập vào mạng công ty [2]từ nhà của nhân viên. Microsoft cho biết, do sự phát triển của công việc phải làm từ xa, có hơn 51% các nhà lãnh đạo doanh nghiệp đang đẩy nhanh việc triển khai các khả năng của mô hình bảo mật Zero Trust. Điều này sẽ trở thành tiêu chuẩn của an ninh mạng với 94% doanh nghiệp đang trong quá trình triển khai mô hình bảo mật Zero Trust mới.

Bài tiểu luận này sẽ đưa cho người đọc cái nhìn tổng quan nhất về mô hình bảo mật Zero Trust, từ định nghĩa, nguyên tắc cho tới hiệu quả của mô hình này, so sánh với các mô hình bảo mật truyền thống và cuối cùng là tương lai cho Zero Trust. Trước đây đã có nhiều tổ chức nghiên cứu về chủ đề này, ví dụ như Jason Gabris với cuốn sách về Zero Trust, bài báo bảo mật dữ liệu đám mây bằng Zero Trust của Researchgate[3], tuy nhiên các tài liệu này mang tính học thuật cao và đôi khi gây khó khăn cho người đọc. Nếu bạn chưa từng nghe hoặc mới chỉ biết qua về Zero Trust thì sau bài tiểu luận này các bạn sẽ có được cái nhìn rõ nét về mô hình bảo mật này, những điểm mạnh cũng như sự hạn chế, thách thức mà Zero Trust đang đối mặt và sẽ gặp phải trong tương lai.

---

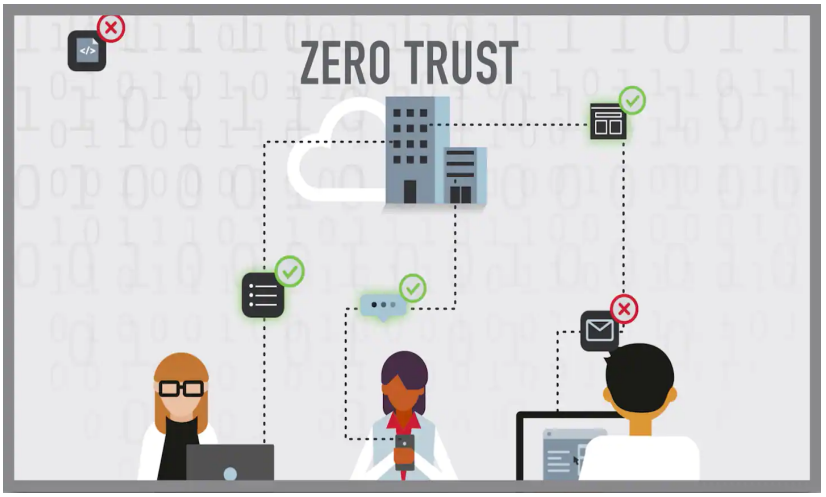
[1] "Lỗ Hổng Bảo Mật là gì? – Tìm hiểu về Lỗ Hổng Website và Phần mềm." https://cystack.net/vi/blog/lo-hong-bao-mat. Ngày truy cập 22 thg 11. 2021.
[2] "Triển khai hệ thống mạng cho doanh nghiệp, tổ chức - ITTODAY." https://ittoday.vn/trien-khai-he-thong-mang/. Ngày truy cập 22 thg 11. 2021.
[3] "Zero Trust Architecture - ResearchGate." https://www.researchgate.net/publication/335998480_Zero_Trust_Architecture. Ngày truy cập 22 thg 11. 2021.

PHẦN 2: HIỂU VỀ ZERO TRUST

I. Định nghĩa:

Hệ thống Zero Trust là 1 nền tảng bảo mật tích hợp sử dụng thông tin tóm lược từ danh tính, bảo mật và cơ sở hạ tầng của hệ thống, cũng như các công cụ phân tích và rủi ro để thông báo và cho phép kích hoạt biện pháp đối phó đối với toàn bộ doanh nghiệp. Zero Trust chuyển đổi từ mô hình lớp rìa thành mô hình coi trọng sâu hơn vào bảo mật tài nguyên và danh tính. Kết quả là, các tổ chức có thể liên tục thích nghi với quyền điều khiển mặc cho sự thay đổi của yếu tố bên ngoài, đạt được bảo mật cấp cao hơn, giảm thiểu rủi ro, đồng thời tăng cường sự nhanh nhạy trong kinh doanh.

Thay vì giả định mọi thứ sau tường lửa công ty là an toàn, mô hình Zero Trust giả định vi phạm và xác minh từng yêu cầu như thể yêu cầu đó bắt nguồn từ mạng mở. Bất kể yêu cầu đó bắt nguồn từ đâu hay truy nhập vào tài nguyên nào thì Zero Trust cũng luôn nhắc nhở chúng ta "không bao giờ tin cậy, luôn xác minh". Mỗi yêu cầu truy nhập đều được xác thực, ủy quyền và mã hóa đầy đủ trước khi cấp quyền truy nhập. Các nguyên tắc phân vùng cực nhỏ và quyền truy nhập đặc quyền tối thiểu được áp dụng để giảm thiểu hành vi xâm nhập mạng. Thông tin và phân tích phong phú được sử dụng để phát hiện cũng như ứng phó với những bất thường trong thời gian thực[4].



Hình 3.1. Tổng quan về mô hình Zero Trust

[4] "Thời gian thực (Real-time) là gì? So sánh với báo giá chứng khoán ...." 23 thg 6. 2020, https://vietnambiz.vn/thoi-gian-thuc-real-time-la-gi-so-sanh-voi-bao-gia-chung-khoan-bi-tri-hoan-20200622112313195.htm. Ngày truy cập 9 thg 11. 2021.

* trích trong Zero Trust Security: An Enterprise Guide. Jason Garbis, Jerry W. Chapman (21/306)

II. Bản chất:

Bản chất của phương pháp Zero Trust là không tin tưởng bất cứ ai, ngay cả khi đó là một nhân viên. Mỗi khi ai đó cố gắng truy cập vào mạng của bạn, bạn phải xác minh rằng họ đáng tin cậy thông qua thông tin thời gian thực từ nhiều nguồn trước khi cấp cho họ quyền truy cập, bất kể vị trí của họ. Giả định là các mối đe dọa tồn tại bên trong và bên ngoài ranh giới mạng truyền thống, và vi phạm là không thể tránh khỏi hoặc đã xảy ra.

III. Nguyên tắc:

Hình 3.2. Ba nguyên tắc của Zero Trust

- **Xác minh rõ ràng:**

Luôn xác thực và ủy quyền dựa trên tất cả các điểm dữ liệu có sẵn, bao gồm danh tính người dùng, vị trí, tình trạng thiết bị, dịch vụ hoặc khối lượng công việc, phân loại dữ liệu và các hành vi bất thường.

- **Sử dụng quyền truy cập đặc quyền tối thiểu:**

Hạn chế quyền truy nhập của người dùng bằng quyền truy nhập vừa đúng lúc và vừa đủ (JIT/JEA[5][6]), các chính sách dựa trên rủi ro và bảo vệ dữ liệu để giúp bảo vệ dữ liệu cũng như hiệu suất.

- **Giả định vi phạm:**

[5] "Overview of Just Enough Administration (JEA) - PowerShell." 11 thg 10. 2021, https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/overview. Ngày truy cập 8 thg 11. 2021.
[6] "Implement JIT and JEA Administration in Windows Server 2019." 22 thg 1. 2021, https://www.pluralsight.com/courses/implement-jit-jea-administration-windows-server-2019. Ngày truy cập 8 thg 11. 2021.

Giảm thiểu việc truy nhập phân đoạn và bán kính ảnh hưởng. Xác minh mã hóa đầu cuối và sử dụng phân tích để có được khả năng quan sát, thúc đẩy việc phát hiện mối đe dọa và cải thiện khả năng phòng thủ.

IV. Khu vực phòng vệ Zero Trust:

- **Danh tính:**

Xác minh và bảo mật từng danh tính bằng hoạt động xác thực mạnh mẽ trên toàn bộ tài sản kỹ thuật số của bạn.

- **Điểm cuối:**

Tăng khả năng quan sát các thiết bị đang truy nhập mạng. Đảm bảo trạng thái tuân thủ và tình trạng thích ứng trước khi cấp quyền truy nhập.

- **Ứng dụng:**

Khám phá công nghệ thông tin ngoài luồng, đảm bảo các quyền trong ứng dụng thích hợp, cấp quyền truy nhập dựa trên phân tích trong thời gian thực, đồng thời giám sát và kiểm soát hành động của người dùng.

- **Dữ liệu:**

Chuyển từ bảo vệ dữ liệu dựa trên vành đai sang bảo vệ dựa trên dữ liệu. Sử dụng thông tin để phân loại và đánh nhãn dữ liệu. Mã hóa và hạn chế quyền truy nhập dựa trên các chính sách của tổ chức.

- **Hạ tầng:**

Sử dụng phép đo từ xa để phát hiện các cuộc tấn công và sự bất thường, tự động chặn cũng như gắn cờ hành vi rủi ro, đồng thời áp dụng các nguyên tắc quyền truy nhập đặc quyền tối thiểu.

- **Mạng:**

Hãy đảm bảo không tin cậy các thiết bị và người dùng chỉ vì các thiết bị và người dùng đó đang ở trong mạng nội bộ. Mã hóa tất cả các thông tin liên lạc nội bộ, giới hạn quyền truy nhập theo chính sách, đồng thời sử dụng chức năng phân vùng cực nhỏ và phát hiện mối đe dọa trong thời gian thực.

Hình 3.3. Khu vực an ninh bảo vệ bởi Zero Trust

V. Zero Trust là thiết kế, không phải sản phẩm:

Zero Trust không phải là một giải pháp công nghệ thông tin có thể được cung cấp bởi một nhà cung cấp duy nhất trên thị trường. Thay vào đó, đó là một hệ thống các nguyên tắc thiết kế kết hợp biện pháp bảo mật công nghệ thông tin dựa trên các nguyên lý cụ thể. .

Mỗi người có trách nhiệm trong một tổ chức phải hiểu cách thức hoạt động của Zero Trust và cam kết thực hiện nó. Zero Trust nên thâm nhập vào mọi khía cạnh hoạt động của nó, đặc biệt là những khía cạnh liên quan đến dữ liệu. Có một số chiến lược có thể được sử dụng để thực hiện Zero Trust, tùy thuộc vào quy mô, cấu trúc của tổ chức và mức độ nhạy cảm của dữ liệu mà nó xử lý, cùng với các yếu tố khác.

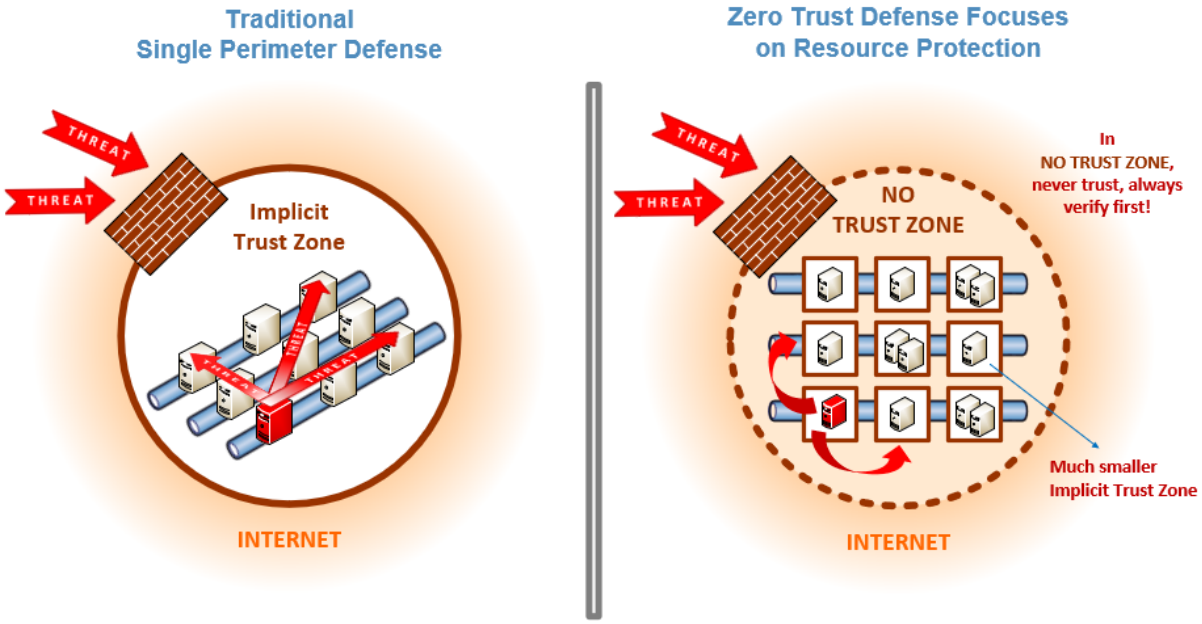
VI. Tại sao nên chọn Zero Trust?

Ngày nay, các tổ chức cần có một mô hình bảo mật mới thích ứng hiệu quả hơn với sự phức tạp của môi trường hiện đại, thân thiện với nơi làm việc kết hợp và bảo vệ con người, thiết bị, ứng dụng cũng như dữ liệu ở mọi nơi.

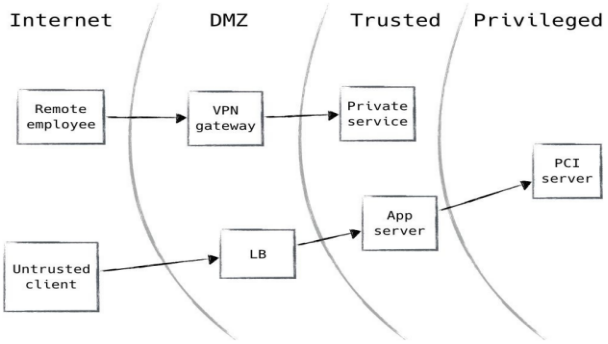
- **Năng suất ở mọi nơi:** Cho phép người dùng của bạn làm việc an toàn hơn mọi lúc, mọi nơi, trên mọi thiết bị.
- **Di chuyển đám mây:** Hỗ trợ chuyển đổi kỹ thuật số bằng tính năng bảo mật thông minh dành cho môi trường phức tạp hiện nay.
- **Giảm thiểu rủi ro:** Lấp đầy lỗ hổng bảo mật và giảm thiểu nguy cơ xâm nhập mạng.

PHẦN 3: ĐÁNH GIÁ

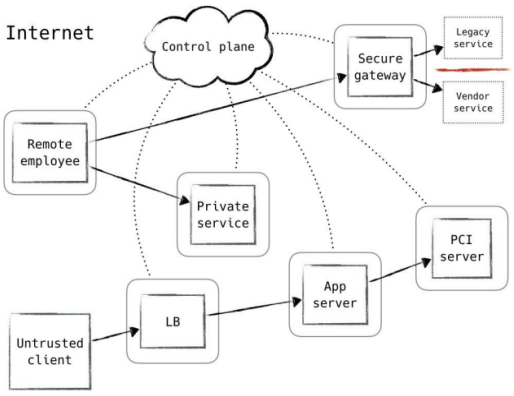
I. So sánh thực nghiệm - Tuyên bố rõ ràng mục tiêu thực nghiệm



Hình 4.1: So sánh giữa mô hình bảo mật truyền thống và Zero Trust



Hình 4.2. Mô hình bảo mật truyền thống



Hình 4.3. Mô hình Zero Trust

Các mô hình bảo mật truyền thống hiện tại được xây dựng theo cách thức thiết lập một hàng rào cứng, phân chia mạng nội bộ và mạng internet bằng các thiết bị như: Firewall[7], IPS, IDS[8]... Bên trong hàng rào là vùng tin tưởng (Trusted Zone), bên

[7] "What Is a Firewall? - Cisco." https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html. Ngày truy cập 8 thg 11. 2021.
[8] "IDS vs. IPS: What is the Difference? - Varonis." 29 thg 3. 2020, https://www.varonis.com/blog/ids-vs-ips/. Ngày truy cập 8 thg 11. 2021.

ngoài là vùng không tin tưởng (Untrusted Zone). Theo mô hình này, việc truy cập vùng tin tưởng từ bên ngoài hàng rào là rất khó, nhưng việc truy cập hệ thống sẽ trở nên dễ dàng khi đã ở trong hàng rào. Tại vùng Trusted, hệ thống mặc định tin tưởng mục đích truy cập hệ thống là đúng khi xác thực thành công. Khi đó, người dùng có thể thực hiện mọi thao tác với tài khoản hiện có. Người dùng hay tin tặc đều có mức độ tin tưởng như nhau khi đã ở trong vùng Trusted. Đây chính là lỗ hổng của cách xây dựng hệ thống hiện tại: tin tưởng quá dễ dàng.

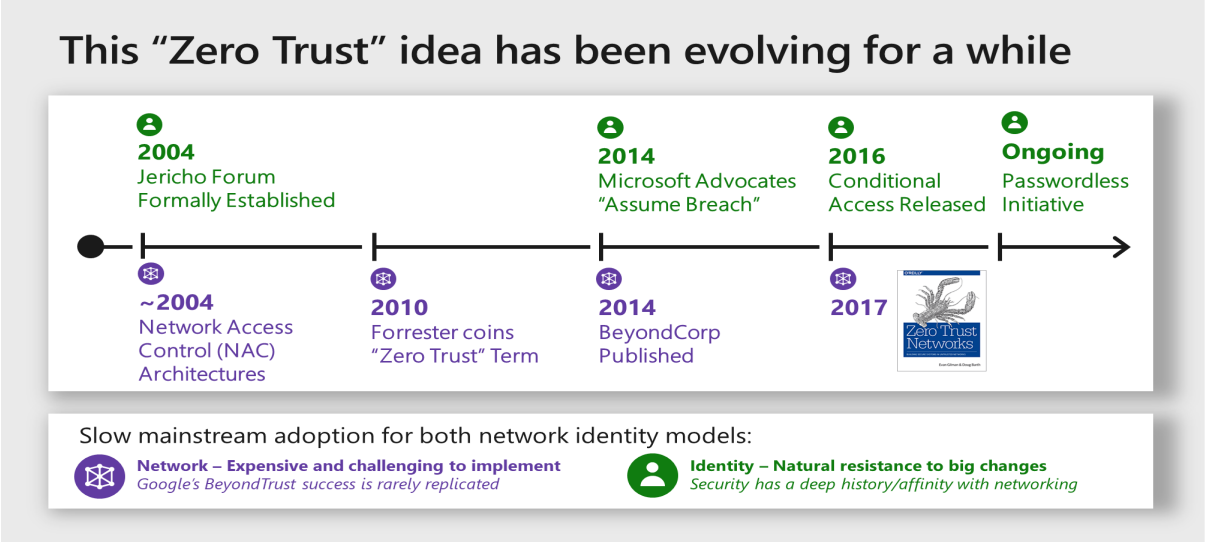
Để khắc phục lỗ hổng trên, Zero Trust đã được nghiên cứu và áp dụng với hướng đi hoàn toàn khác trong mô hình bảo mật truyền thống trên. Zero Trust được định nghĩa là sự kết hợp giữa các ứng dụng, dữ liệu và danh tính, hoàn toàn phù hợp với bối cảnh công nghệ thông tin hiện nay. Nguyên lý của Zero-Trust đi ngược lại hướng tiếp cận truyền thống: mặc định coi tất cả các vùng là Untrusted và mọi truy cập vào hệ thống là không tin tưởng, không an toàn. Không một người, thiết bị, phiên truy cập nào là tin cậy (dù trong nội mạng hay ngoài Internet), mặc định từ chối mọi truy cập từ người dùng, thiết bị đến tài nguyên của doanh nghiệp và chỉ cho phép kết nối khi người dùng, thiết bị có thể chứng minh được sự tin cậy của mình. Như vậy, kể cả người dùng bình thường hay tin tặc khi truy cập vào hệ thống, ứng dụng cũng đều mặc định bị coi là không tin tưởng.

Mô hình bảo mật truyền thống	**Mô hình bảo mật Zero Trust**
Giả định rằng tất cả người dùng trong vùng mạng đều là tin cậy.	Chia ra nhiều nhánh và yêu cầu xác nhận tại nhiều điểm trong vùng mạng.
Usernames và passwords là chìa khóa và người dùng phải nhớ chúng; chỉ cần đưa ra 1 lần là được cấp quyền truy cập vào hệ thống.	Sử dụng các phương pháp xác thực thay thế, và xác thực là bắt buộc đối với mọi thứ bạn muốn truy cập.
Tự do truy cập khi vượt qua firewall.[9]	Hạn chế quyền truy cập vì mỗi xác thực chỉ cung cấp quyền truy cập vào một khía cạnh của mạng.

Bảng 4.4: So sánh chi tiết giữa mô hình truyền thống và Zero Trust

[9] "What Is a Firewall? - Cisco." https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-firewall.html. Ngày truy cập 22 thg 11. 2021.

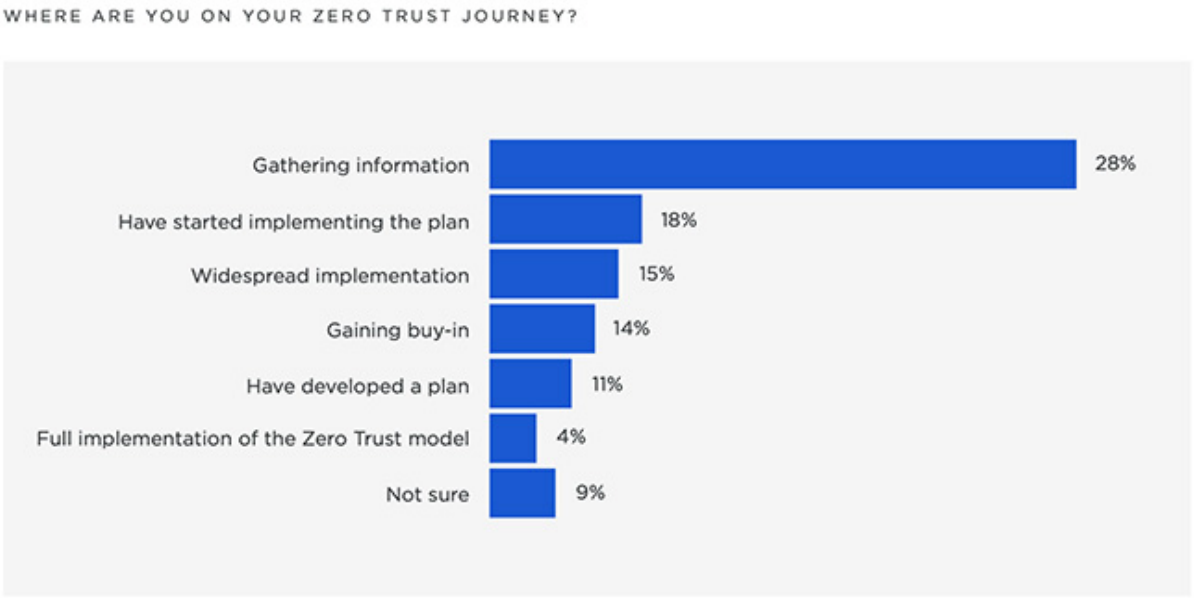
II. Kết luận từ kết quả thực nghiệm (Hướng nghiên cứu này khẳng định/phủ định giả thiết đã đặt ra không?)



Bảng 4.5: Sự phát triển trong quá khứ

Các mô tả mạch lạc sớm nhất về ý tưởng Zero Trust có thể được bắt nguồn từ các đề xuất sau làn sóng tấn công an ninh mạng lớn. Bắt đầu từ đầu những năm 2000, các doanh nghiệp và tổ chức công nghệ thông tin đã bị rung chuyển bởi các loại sâu như ILOVEYOU, Nimda[10] và SQL Slammer[11]. Mặc dù thiệt hại nhưng những trải nghiệm này là chất xúc tác cho các sáng kiến bảo mật tích cực như Vòng đời phát triển bảo mật của Microsoft (SDL) và bắt đầu các cuộc thảo luận nghiêm túc về việc cải thiện bảo mật máy tính. Các cuộc thảo luận về chiến lược trong khung thời gian này đã hình thành hai trường phái tư tưởng chính - mạng và danh tính: Mạng - Trường phái suy nghĩ này đã nhân đôi việc sử dụng các điều khiển mạng để bảo mật bằng cách tạo ra các phân đoạn mạng nhỏ hơn và đo lường độ tin cậy của các thiết bị trước khi các điều khiển mạng cho phép truy cập vào tài nguyên. Mặc dù đầy hứa hẹn, cách tiếp cận này rất phức tạp và cho thấy sự tiếp nhận hạn chế bên ngoài một số điểm sáng như Google's BeyondCorp. Identity - Một cách tiếp cận khác, được Diễn đàn Jericho ủng hộ, được thúc đẩy để loại bỏ hoàn toàn các biện pháp kiểm soát an ninh mạng bằng cách tiếp cận "de-perimeterisation[12]". Cách tiếp cận này phần lớn nằm ngoài tầm với của công nghệ có sẵn vào thời điểm đó nhưng đã gieo mầm quan trọng cho Zero Trust ngày nay.

[10] "Nimda - Wikipedia." https://en.wikipedia.org/wiki/Nimda. Ngày truy cập 8 thg 11. 2021.
[11] "SQL Slammer - Wikipedia." https://en.wikipedia.org/wiki/SQL_Slammer. Ngày truy cập 8 thg 11. 2021.
[12] "De-perimeterization - Wikipedia." https://en.wikipedia.org/wiki/De-perimeterisation. Ngày truy cập 8 thg 11. 2021.



Bảng 4.6: Sự quan trọng của Zero Trust trong tương lai

Theo Illumio, mặc dù hầu hết các chuyên gia bảo mật và công nghệ thông tin đều coi Zero Trust là một phần quan trọng trong phương pháp tiếp cận an ninh mạng, nhưng vẫn còn một chặng đường dài để triển khai.

Đặc biệt là khi người dùng tiếp tục di chuyển mạng ngoài khuôn viên sang mô hình phân tán làm việc tại nhà và đối mặt với các đe dọa mới và đang mở rộng, các tổ chức phải nhanh chóng áp dụng tư duy bảo mật "không bao giờ tin tưởng, luôn xác minh" để giảm thiểu vi phạm bằng cách hạn chế tiếp cận và ngăn cản chuyển động.

Đáng chú ý, 49% những người tham gia được khảo sát cho rằng Zero Trust là yếu tố quan trọng đối với mô hình bảo mật tổ chức của họ. Chỉ có 2% các nhà lãnh đạo doanh nghiệp tin rằng Zero Trust là không cần thiết.

"Zero Trust là sứ mệnh quan trọng đối với bất kỳ chiến lược an ninh mạng nào. Đối thủ không dừng lại ở điểm vi phạm - họ di chuyển khắp các môi trường để đạt được mục tiêu đã định hoặc tiếp cận những món trang sức quý giá của bạn ", Matthew Glenn, phó chủ tịch cấp cao quản lý sản phẩm của Illumio cho biết.

"Trong thế giới ngày nay, việc ngăn chặn sự di chuyển qua lại của những kẻ tấn công đã trở thành công việc cơ bản đối với công việc của một người phòng thủ. Hơn nữa, khi nhân viên tiếp tục làm việc từ xa trên quy mô lớn, điều cần thiết là phải mở rộng độ tin cậy bằng không tới điểm cuối để giảm thiểu bề mặt tấn công hơn nữa và bảo mật cho doanh nghiệp. "

**** Việc áp dụng Zero Trust chỉ mới bắt đầu***

Trong khi các tổ chức coi trọng Zero Trust là một phần cần thiết trong chiến lược an ninh mạng của họ, thì việc áp dụng rộng rãi vẫn còn thiếu. Trong số những người được hỏi cho rằng zero trust là cực kỳ quan trọng hoặc rất quan trọng đối với tình hình an ninh của họ, chỉ có 19% đã thực hiện đầy đủ hoặc thực hiện rộng rãi kế hoạch zero trust của họ.

**** Các công nghệ thúc đẩy Zero Trust***

Không một sản phẩm hay giải pháp nào có thể giúp các tổ chức đạt được niềm tin bằng không, vì vậy Illumio đã hỏi các công ty công nghệ nào đã triển khai trên hành trình đạt được niềm tin bằng không. Không có gì ngạc nhiên khi các giải pháp có rào cản gia nhập thấp hơn, như xác thực đa yếu tố (MFA)[13] và đăng nhập một lần (SSO)[14], được áp dụng rộng rãi hơn.

Tuy nhiên, 32% số người được hỏi đã áp dụng phân đoạn trong toàn khuôn viên trường, 30% khác đã kết hợp các công nghệ theo chu vi do phần mềm xác định (SDP) và 26% đang tận dụng phân đoạn vi mô, một công nghệ không tin cậy quan trọng để ngăn chặn sự di chuyển theo chiều của những kẻ tấn công.

Sau sáu tháng, hầu hết những người được hỏi có kế hoạch thực hiện phân khúc vi mô và SDP, điều này sẽ mở đường cho việc áp dụng zero trust trên quy mô lớn. Trên thực tế, 51% người được hỏi có kế hoạch triển khai phân đoạn vi mô như một trong những biện pháp kiểm soát độ tin cậy chính của họ, do tính hiệu quả và tầm quan trọng của nó trong việc ngăn chặn các vi phạm cao cấp bằng cách ngăn chặn chuyển động bên.

Cuối cùng, trong sáu tháng tới, 23% tổ chức có kế hoạch triển khai MFA và 18% có kế hoạch triển khai SSO.

---

[13] "Xác thực đa yếu tố (MFA) - Microsoft Security." https://www.microsoft.com/vi-vn/security/business/identity-access-management/mfa-multi-factor-authentication. Ngày truy cập 8 thg 11. 2021.

[14] "Single sign-on (SSO) - Đăng nhập một lần và những điều bạn chưa ...." 26 thg 6. 2019, https://bizflycloud.vn/tin-tuc/single-sign-on-sso-dang-nhap-mot-lan-va-nhung-dieu-ban-chua-biet-20190626110743015.htm. Ngày truy cập 8 thg 11. 2021.

III. Ứng dụng

1. Zero Trust so với VPN:

Mô hình Zero Trust thay thế VPN[15] được các công ty sử dụng truyền thống để nhân viên của họ truy cập tài sản kỹ thuật số của họ từ xa. VPN đang được thay thế vì chúng có một lỗ hổng lớn mà mạng không tin cậy có thể giải quyết. Trong VPN, bất kỳ vi phạm nào xảy ra trong kênh được mã hóa kết nối người dùng với mạng của tổ chức sẽ cấp cho những kẻ tấn công tiềm năng quyền truy cập không giới hạn vào tất cả các tài nguyên của công ty được kết nối với mạng.

Trên các cơ sở hạ tầng cũ, tại chỗ, VPN hoạt động tốt, nhưng chúng tạo ra nhiều rủi ro hơn so với các giải pháp trên đám mây hoặc cơ sở hạ tầng hỗn hợp.

Zero Trust đã khắc phục được khuyết điểm này của VPN nhưng lại thêm một nhược điểm tiềm ẩn: chúng có thể dẫn đến phức tạp hơn về mặt triển khai và bảo trì, vì các ủy quyền phải được cập nhật cho tất cả người dùng, thiết bị và tài nguyên. Điều này đòi hỏi phải làm việc thêm, nhưng các bộ phận công nghệ thông tin đạt được khả năng kiểm soát tốt hơn đối với tài nguyên và bù lại giảm được các lỗ hổng bảo mật.

May mắn thay, những lợi ích của Zero Trust có thể được thực hiện mà không cần thêm nỗ lực bảo trì và triển khai, nhờ vào các công cụ tự động hóa và hỗ trợ trong các nhiệm vụ quản trị mạng. Các công cụ được thảo luận dưới đây giúp bạn áp dụng các chính sách không tin cậy với nỗ lực và chi phí tối thiểu.

2. Hysolate:

Hysolate chia thiết bị của người dùng thành hai vùng riêng biệt, mỗi vùng chạy trong hệ điều hành riêng, tận dụng các công nghệ bảo mật dựa trên siêu giám sát và ảo hóa mới nhất. Một hệ điều hành là hệ điều hành không được quản lý / không đáng tin cậy / cá nhân của người dùng và một hệ điều hành khác là hệ điều hành công ty đáng tin cậy chạy trong máy ảo.

Máy ảo công ty chạy một hệ điều hành bị khóa hoàn toàn có thể chứa chứng chỉ máy khách không thể truy cập được để đảm bảo tính toàn vẹn của máy ảo. Nhà môi giới Zero Trust sẽ chỉ cho phép máy ảo công ty chạy trên Hysolate[16] có quyền

---

[15] "VPN là gì? Các giao thức thường dùng, ưu và nhược điểm của VPN." 3 thg 5. 2021, https://www.dienmayxanh.com/kinh-nghiem-hay/vpn-la-gi-cac-giao-thuc-thuong-dung-uu-va-nhuoc-di-1126993. Ngày truy cập 9 thg 11. 2021.

[16] "Hysolate - Restoring Trust in User Endpoints." https://www.hysolate.com/. Ngày truy cập 10 thg 11. 2021.

truy cập vào các ứng dụng doanh nghiệp nhạy cảm. Người dùng cuối sẽ không thể truy cập các ứng dụng này từ bất kỳ môi trường / thiết bị không đáng tin cậy nào khác.

Với Hysolate, công nghệ thông tin có thể cách ly máy ảo nhạy cảm của công ty khỏi Hệ điều hành "vùng năng suất rủi ro hơn" của người dùng, bao gồm các điều khiển chi tiết đối với khay nhớ tạm, USB, mạng, ứng dụng và hơn thế nữa. Với kiến trúc Zero Trust này, các doanh nghiệp thực sự có thể chuyển sang kiến trúc an toàn theo từng thiết kế.

3. Dữ liệu và Dịch vụ được Phân phối

Môi trường dựa trên đám mây được phân phối trên toàn cầu và có thể truy cập từ mọi nơi, điều này vừa là ưu điểm vừa là nhược điểm. Các công ty đang lưu trữ nhiều tài nguyên, dữ liệu và ứng dụng nhạy cảm hơn trên đám mây và mô hình bảo mật cũ, trong đó các điểm cuối do công ty kiểm soát và mạng công ty có thể được bảo mật chặt chẽ, không còn bị giữ lại.

Với việc chuyển dần sang điện toán biên, các nhóm công nghệ thông tin cũng sẽ phải đọc sơ đồ từ cơ sở hạ tầng bảo mật tập trung từ trên xuống sang các mô hình tin cậy phi tập trung. Các hệ thống dựa trên biên thể hiện một rủi ro lớn đối với mô hình không tin cậy và phải được coi như các mạng riêng lẻ, với các chính sách và kiểm soát không tin cậy của riêng chúng

IV. Đề xuất cải tiến

**** Trước hết là những khó khăn trong mô hình bảo mật Zero Trust:***

1. Cách tiếp cận từng phần có thể tạo ra lỗ hổng

An ninh mạng không tin cậy cuối cùng có thể dẫn đến bảo mật vượt trội, nhưng trên đường đi, nó có thể khiến các công ty gặp nhiều rủi ro hơn.

Hầu hết các công ty tùy chỉnh các chiến lược của riêng họ bằng cách tiếp cận từng phần, nhưng các lỗ hổng hoặc vết nứt có thể phát triển khiến cho sự tin tưởng của zero kém hơn so với quảng cáo. Đồng thời, việc gỡ bỏ một giải pháp cũ có thể tạo ra lỗi bảo mật không mong muốn.

2. Yêu cầu cam kết quản lý liên tục

Một trở ngại khác thường bị bỏ qua khi chuyển sang mô hình an ninh mạng không tin cậy là nhu cầu quản lý liên tục. Mô hình Zero-Trust dựa trên một mạng lưới rộng lớn các quyền được xác định nghiêm ngặt, nhưng các công ty luôn phát triển.

Mọi người chuyển sang các vai trò mới và thay đổi địa điểm. Các biện pháp kiểm soát truy cập phải được cập nhật mỗi lần để đảm bảo đúng người có quyền truy cập vào thông tin cụ thể. Việc giữ các quyền chính xác và cập nhật đòi hỏi phải có đầu vào liên tục.

Có một vấn đề đặt ra là: nếu các biện pháp kiểm soát không được cập nhật ngay lập tức, các bên trái phép có thể có quyền truy cập vào thông tin nhạy cảm. Ví dụ, hãy tưởng tượng rằng ai đó đã bị sa thải nhưng vẫn có thể truy cập thông tin nội bộ trong một tuần. Người đó có thể có động cơ mạnh mẽ để lừa đảo, nhấn mạnh vai trò của tốc độ trong chiến lược không tin tưởng. Nếu các công ty không thể hành động nhanh chóng trong những tình huống này, dữ liệu sẽ gặp rủi ro.

3. Năng suất

Việc đưa ra phương pháp tiếp cận an ninh mạng không tin cậy cũng có thể ảnh hưởng đến năng suất. Thách thức cốt lõi của không tin tưởng là khóa quyền truy cập mà không làm cho quy trình công việc tạm dừng. Mọi người yêu cầu quyền truy cập vào dữ liệu nhạy cảm để làm việc, giao tiếp và cộng tác. Nếu các cá nhân thay đổi vai trò và thấy mình bị khóa khỏi các tệp hoặc ứng dụng trong một tuần, năng suất của họ có thể giảm mạnh. Trong những trường hợp xấu nhất, năng suất bị mất sẽ trở thành một vấn đề lớn hơn chính an ninh mạng.

Ngoài ra Zero Trust còn yêu cầu phần cứng an toàn và phần mềm phải linh hoạt.

**** Cách vượt qua thử thách***

Mạng không tin cậy có những sai sót của nó, nhưng nó vẫn là tư thế ưa thích của các công ty có ý thức bảo mật. Cách tốt nhất để giảm thiểu rủi ro cố hữu là tránh nghĩ về sự tin cậy bằng không đối với các điều khoản nhị phân.

Các công ty có thể áp dụng kiến trúc Zero Trust mà không phải từ bỏ các hệ thống kế thừa của họ. Bắt đầu bằng cách xác định dữ liệu nhạy cảm nhất và quy trình công việc quan trọng. Chúng có thể phải chịu các kiểm soát truy cập chặt chẽ hơn, chẳng hạn như xác thực đa yếu tố , truy cập đặc quyền và quản lý phiên. Dữ liệu còn lại tuân theo các điều khiển chu vi tiêu chuẩn, trong khi chỉ những thông tin quan trọng nhất mới tuân theo tiêu chuẩn không tin cậy.

Việc dần dần giới thiệu bảo mật không tin cậy là có lợi vì nó không làm gián đoạn tính liên tục của chiến lược an ninh mạng. Các công ty bắt đầu khóa các tài sản

quan trọng, nhưng vì họ không hoàn toàn từ bỏ hệ thống này cho hệ thống khác, nên họ phải đối mặt với ít mối đe dọa hơn.

Bất chấp những nỗ lực của cộng đồng an ninh mạng rộng lớn, các vụ vi phạm dữ liệu vẫn tiếp diễn. Để chống lại điều này, an ninh mạng không tin cậy tập trung vào việc bảo mật tài sản của chính nó, thay vì chỉ là các điểm vào. Miễn là các công ty nhận ra những thách thức của sự tin tưởng bằng không, họ có thể chuyển vị trí bảo mật của mình về phía trước.

PHẦN 4: KẾT LUẬN

Như đã phân tích, mô hình Zero Trust dựa vào 3 nguyên tắc cơ bản, một là xác minh danh tính, sử dụng quyền truy cập tối thiểu, gia định phạm vi. Có thể thấy với ba nguyên tắc chính này, zero trust mang lại tính bảo mật vô cùng tốt, tuy nhiên nếu không được sử dụng đúng cách trong nhiều trường hợp tạo nên sự rườm rà cho công đoạn xác thực, từ đó mất đi tính realtime trong nhiều xử lý quan trọng. Cụ thể, với rất nhiều ứng dụng nhúng, iot, realtime hay delay là một phần rất quan trọng, liên quan đến hiệu quả làm việc của ứng dụng. Ví dụ, một hệ thống nhúng điều khiển từ xa, thông thường thì chỉ cần lần đầu tiên xác minh, nếu áp dụng mô hình zero trust vào để bảo mật tương tác giữa người và hệ thống cũng như hệ thống này với hệ thống khác thì rất dễ dẫn đến mất ổn định, từ đó mất đi tính hiệu quả của hệ thống. Một giải pháp được đặt ra là thay vì luôn xác minh, xác thực mọi hành động ta có thể áp dụng mô hình zero trust là tầng bảo mật cuối cùng. Cụ thể ta vẫn áp dụng bảo mật truyền thống (là tầng bảo mật thứ nhất) cho các ứng dụng, tầng bảo mật thứ hai là zero trust, tuy nhiêu tầng bảo mật hai chỉ kích hoạt khi tầng bảo mật thứ nhất phát sinh vấn đề hay sau một khoảng thời gian cố định nào đó.

Chỉ nên triển khai dần dần Zero Trust. Điều này giúp bạn xác định các khu vực chính cần chú ý ngay lập tức và cũng giúp bạn ngăn chặn các lỗ hổng không được chú ý hoặc trở thành lỗ hổng nghiêm trọng, bên cạnh đó bạn có thể dễ dàng xem và giải quyết các vấn đề khi chúng phát sinh, đặc biệt nếu đang khôi phục các giải pháp cũ.

Ngoài ra, chúng ra nên triển khai các nhiệm vụ bảo trì và kiểm tra định kỳ vào các quy trình của mình. Đây là nơi các công cụ tự động hóa có thể hữu ích để kiểm tra liên tục các bản nâng cấp chương trình cơ sở hoặc hỗ trợ thay đổi cấu hình bảo mật. Bạn cũng có thể sử dụng các công cụ giám sát, cảnh báo và thông báo để giúp bạn vượt qua các cuộc tấn công.

Chống lại các lỗ hổng này bằng cách chọn phần cứng có CPU đáng tin cậy, như CPU của Intel®, giúp dễ dàng duy trì tính toàn vẹn của hệ thống. Một cách để vượt qua thử thách này là sử dụng một công cụ hoàn chỉnh như ZPE Cloud[17]. Nền tảng đám mây trung lập với nhà cung cấp này cung cấp cho bạn quyền truy cập từ xa an toàn vào cả lớp giải pháp và lớp cơ sở hạ tầng của bạn - bất kể bạn triển khai giải pháp của nhà cung cấp nào trên mạng của mình.

Các tổ chức hiểu được những lợi ích to lớn cần đạt được và quyết tâm triển khai kiến trúc Zero Trust có thể gặp phải một số thách thức trong quá trình này, bao gồm:

- **Kho công nghệ:** Hệ điều hành và ứng dụng cũ, các công cụ và nền tảng phát triển, các ứng dụng và dịch vụ của bên thứ ba cùng với các ứng dụng "cây nhà lá vườn" và nhiều ứng dụng khác
- **Thiếu tích hợp công nghệ:** Các rào cản có thể xuất hiện với các nền tảng thuộc sở hữu và bên thứ ba - bất kỳ vấn đề nào với các tích hợp này đều có thể dễ dàng khiến việc triển khai Zero Trust
- **Bề mặt mối đe dọa thay đổi nhanh chóng và bối cảnh mối đe dọa:** Điều này có thể dẫn đến những thách thức với các công nghệ bị hạn chế về phương thức triển khai

** Zero Trust - chiến lược an ninh mạng mạnh mẽ cho hiện tại và tương lai*

Nhìn chung, để được trang bị thích hợp cho công việc và bình thường mới, các doanh nghiệp nên thực hiện phương pháp Zero Trust để trao quyền cho đội công nghệ thông tin và bảo mật của họ. Bằng cách cung cấp cho họ khả năng hiển thị cần thiết để giữ an toàn cho các điểm cuối của doanh nghiệp và mạng, toàn bộ doanh nghiệp được thiết lập để thành công.

Mức độ hiển thị ngày càng tăng cung cấp bởi kiến trúc zero-trust giúp các tổ chức giải quyết nhiều thách thức bảo mật mà làm việc từ xa đã tạo ra. Bây giờ họ có thể xác minh tất cả các điểm cuối cho các mối đe dọa; trước khi mở dịch vụ kinh doanh cho nhân viên - một khả năng rất quan trọng để thực hiện các biện pháp phòng ngừa chống lại các cuộc tấn công mạng. Điều này có thể thực hiện được bất kể vị trí của nhân viên, khiến zero trust trở thành mô hình lý tưởng cho một thế giới làm việc kết hợp. Sự linh hoạt như vậy sẽ tiếp tục là yếu tố quan trọng để đảm bảo các biện pháp phòng thủ an ninh có thể thích ứng, cho phép doanh nghiệp luôn được bảo vệ bất kể điều gì xảy ra tiếp theo.

---

[17] "Cloud-Based Network Management | ZPE Cloud | ZPE Systems." https://www.zpesystems.com/products/software-cloud/zpe-cloud/. Ngày truy cập 12 thg 11. 2021.

PHẦN 5: TÀI LIỆU THAM KHẢO

- **Books:**
  - Zero Trust Security: An Enterprise Guide. *Jason Garbis, Jerry W. Chapman*
    Zero Trust security - An enterprise guide.pdf
  - Zero trust networks : building secure systems in untrusted networks. Barth, Doug, Gilman, Evan
    Zero trust networks - building secure systems in untrusted netwo…
  - Zero Trust Architecture: August 10, 2020. Scott W. Rose, Oliver Borchert, Stuart Mitchell, Sean Connelly
    Zero Trust Architecture - August 10, 2020.pdf

- **Journal Articles:**
  - A zero trust hybrid security and safety risk Analysis Method. Nikolaos Papakonstantinou, Bryan O'Halloran, May 13, 2021.
    A zero trust hybrid security and safety risk Analysis Method..pdf
  - The zero trust supply chain: Managing supply chain risk in the absence of trust. Zachary A. Collier & Joseph Sarkis, pp 3430 - 3445, 17 Feb 2021
    The zero trust supply chain Managing supply chain risk in the abs…
  - How a zero trust approach can help to secure your AWS environment. Scott, Barry

- **Conference Papers:**
  - The state of zero trust in the age of fluid working. Olie Sheridan, 23 Feb 2021
  - The Emergence of Post Covid-19 Zero Trust Security Architectures. David Haddon, Philip Bennett. 30 July 2021

- **Technical Reports:**
  - Beyond Zero Trust: Trust Is a Vulnerability. M Campell. October 2020
    Beyond_Zero_Trust_Trust_Is_a_Vulnerability.pdf
  - Survivable zero trust for cloud computing environments. Luca Ferretti. November 2020

- **Internet Sources:** ASME Digital Collection, Taylor & Francis Online, NIST, Springer Link