BÁO CÁO AN NINH MẠNG

GÓC NHÌN & GIẢI PHÁP TỪ CHUYÊN GIA ESC

(Tài liệu lưu hành nội bộ)

Quý 3/2025

Contents

Báo Cáo An Ninh Mạng Tháng 9/2025: Góc nhìn & Giải pháp từ Chuyên gia ESC

Với hơn 20 năm kinh nghiệm trong lĩnh vực cung cấp tài nguyên Internet và các giải pháp chuyển đổi số, đội ngũ chuyên gia tại ESC liên tục theo dõi và phân tích bối cảnh an ninh mạng tại Việt Nam. Báo cáo này là tổng hợp những quan sát, phân tích chuyên sâu và khuyến nghị chiến lược của chúng tôi, nhằm giúp các doanh nghiệp và tổ chức nhận diện đúng rủi ro và xây dựng một hệ thống phòng thủ vững chắc trong bối cảnh kỹ thuật số đầy biến động của năm 2025.

Phần 1: Bối Cảnh An Ninh Mạng Việt Nam Quý 3/2025: Thách Thức và Thực Trạng

1.1. Tổng quan Tình hình: Tấn công Leo thang, Năng lực Phòng thủ Theo sau

Bước vào quý 3 năm 2025, từ góc nhìn của chúng tôi, bối cảnh an ninh mạng tại Việt Nam tiếp tục cho thấy những diễn biến phức tạp. Sự tăng trưởng không ngừng của nền kinh tế số và sự mở rộng của các hạ tầng công nghệ thông tin, dù mang lại nhiều cơ hội, cũng đã biến các tổ chức và doanh nghiệp Việt Nam thành mục tiêu hấp dẫn hơn đối với tội phạm mạng. Dữ liệu từ các hệ thống giám sát quốc gia trong năm 2024 đã cho thấy một bức tranh đáng báo động khi ghi nhận hơn 659.000 sự kiện tấn công mạng, một con số phản ánh quy mô và tần suất của các mối đe dọa mà khách hàng của chúng tôi phải đối mặt.

Tuy nhiên, thách thức lớn nhất mà chúng tôi nhận thấy không chỉ nằm ở số lượng, mà còn ở sự gia tăng về mức độ tinh vi. Các xu hướng tấn công trong năm 2025 cho thấy sự thay đổi rõ rệt về chất. Tội phạm mạng ngày càng tận dụng các công nghệ tiên tiến như trí tuệ nhân tạo (AI-generated malware), công nghệ deepfake để mạo danh, và các mô hình mã độc tống tiền dưới dạng dịch vụ (Ransomware-as-a-Service - RaaS). Những công nghệ này đang đặt ra những thách thức chưa từng có cho các hệ thống phòng thủ truyền thống.

Đối mặt với một môi trường đe dọa ngày càng leo thang, năng lực phòng thủ của nhiều tổ chức tại Việt Nam lại cho thấy một "khoảng trống sẵn sàng" đáng lo ngại. Mặc dù có những tín hiệu tích cực khi tỷ lệ doanh nghiệp được xếp loại "Trưởng thành" trong năng lực ứng phó sự cố đã tăng từ 6% năm 2024 lên 11% năm 2025, con số này vẫn thấp hơn đáng kể so với mức trung bình của khu vực và toàn cầu. Qua kinh nghiệm làm việc với hàng ngàn doanh nghiệp, chúng tôi nhận thấy tốc độ cải thiện năng lực phòng thủ trong nước vẫn chưa bắt kịp với tốc độ phát triển của các mối đe dọa, tạo ra một môi trường thuận lợi cho các cuộc tấn công thành công.

1.2. Các Mắt xích Yếu Cố hữu: Con người, Ngân sách và Hạ tầng

Phân tích sâu hơn về "khoảng trống sẵn sàng" này, các chuyên gia của chúng tôi đã chỉ ra ba mắt xích yếu kém mang tính hệ thống trong nhiều tổ chức: nhân lực, ngân sách và hạ tầng công nghệ. Ba yếu tố này tạo

ra một vòng luẩn quẩn của sự yếu kém, khiến các tổ chức liên tục ở trong thế bị động thay vì chủ động phòng ngừa.

Nhân lực và Ngân sách: Thiếu hụt nguồn nhân lực an ninh mạng có chuyên môn là một trong những rào cản lớn nhất. Dữ liệu cho thấy có tới 56.16% doanh nghiệp chưa có đủ nhân sự chuyên trách. Tình hình càng trở nên nghiêm trọng hơn khi 35.56% tổ chức chỉ có dưới 5 nhân viên phụ trách an ninh mạng, một con số quá nhỏ bé so với yêu cầu vận hành một trung tâm giám sát an ninh (SOC) cơ bản. Song song với đó, hơn 50% tổ chức thừa nhận rằng ngân sách dành cho bảo mật không theo kịp nhu cầu thực tế. Điều này dẫn đến một hệ quả tất yếu: các giải pháp bảo mật bị cắt xén, rời rạc và thiếu tính tích hợp.

Hạ tầng Phân mảnh: Sự thiếu hụt về ngân sách và nhân lực trực tiếp dẫn đến một vấn đề nghiêm trọng khác là hạ tầng bảo mật phân mảnh. Có tới 84% doanh nghiệp tại Việt Nam đang vận hành trên 10 công cụ bảo mật khác nhau, phần lớn không được đồng bộ hóa. Việc triển khai nhiều giải pháp điểm từ các nhà cung cấp khác nhau tạo ra một môi trường quản lý phức tạp, nơi các công cụ hoạt động không ăn khớp. Điều này không chỉ gây khó khăn cho việc giám sát toàn diện mà còn tạo ra những "lỗ hổng giữa các lỗ hổng" – những điểm mù an ninh mà kẻ tấn công có thể khai thác.

Rò rỉ Dữ liệu và Mối đe dọa Nội bộ: Hệ quả của những yếu kém trên là sự gia tăng đáng báo động về các sự cố rò rỉ dữ liệu. Trong năm 2024, Việt Nam chiếm tới 12% tổng số tài khoản bị lộ lọt trên toàn cầu. Con số này cho thấy dữ liệu của người dùng và doanh nghiệp Việt Nam đang là mục tiêu hàng đầu. Thêm vào đó, các mối đe dọa không chỉ đến từ bên ngoài. Các sự cố rò rỉ dữ liệu nội bộ, phần lớn xuất phát từ yếu tố con người, đã tăng khoảng 30% trong bối cảnh làm việc từ xa ngày càng phổ biến.

Những yếu tố này kết hợp lại tạo thành một chu kỳ tự duy trì của sự yếu kém. Ngân sách hạn hẹp và nhân sự thiếu hụt dẫn đến việc mua sắm các công cụ rời rạc. Hạ tầng phức tạp này lại quá sức quản lý đối với đội ngũ mỏng, dẫn đến các lỗ hổng chưa được vá. Kẻ tấn công sau đó dễ dàng khai thác những điểm yếu này, buộc các tổ chức phải liên tục "chữa cháy". Để thoát khỏi vòng luẩn quẩn này, các doanh nghiệp cần một sự thay đổi cơ bản trong cách tiếp cận, không chỉ về công nghệ mà còn về chiến lược đầu tư và phát triển con người.

Phần 2: Phân Tích Chuyên Sâu Các Hình Thức Tấn Công Website Phổ Biến

Để xây dựng một chiến lược phòng thủ hiệu quả, việc hiểu rõ cơ chế, mục tiêu và tác động của các hình thức tấn công phổ biến là yêu cầu tiên quyết. Dưới đây là phân tích của đội ngũ chuyên gia ESC về các loại hình tấn công mà chúng tôi thường xuyên ghi nhận và xử lý cho khách hàng trong năm 2025.

Bảng 1: Tóm tắt các Hình thức Tấn công Website Phổ biến tại Việt Nam (Theo phân tích của ESC)

Hình thức Tấn công	Cơ chế Hoạt động	Mục tiêu Chính	Tác động Kinh doanh
SQL Injection	Chèn mã SQL độc hại vào các trường nhập liệu của website để thao túng cơ sở dữ liệu.	Cơ sở dữ liệu (dữ liệu khách hàng, tài chính).	Mất cắp/thay đổi dữ liệu, chiếm quyền

			quản trị, tổn hại uy tín.
DDoS	Sử dụng mạng botnet để tạo ra một lượng truy cập khổng lồ, làm quá tải và sập máy chủ.	Tính sẵn sàng của dịch vụ.	Gián đoạn hoạt động kinh doanh, mất doanh thu, giảm uy tín.
Phishing	Giả mạo các trang web hoặc email uy tín để lừa người dùng cung cấp thông tin nhạy cảm.	Thông tin đăng nhập, tài chính của người dùng.	Đánh cắp danh tính, lừa đảo tài chính, lây nhiễm mã độc.
Cross-Site Scripting (XSS)	Chèn mã độc (thường là JavaScript) vào website, mã này sẽ thực thi trên trình duyệt của người dùng.	Người dùng của website (đánh cắp session, cookie).	Chiếm phiên đăng nhập, chuyển hướng người dùng, phá hoại giao diện.
Ransomware & Malware	Mã hóa dữ liệu của nạn nhân và đòi tiền chuộc, hoặc cài cắm phần mềm độc hại để đánh cắp thông tin.	Dữ liệu và hệ thống của tổ chức.	Mất dữ liệu vĩnh viễn, tống tiền, gián đoạn hoạt động nghiêm trọng.

2.1. Tấn công Chèn mã SQL (SQL Injection): Đánh cắp "Mỏ vàng" Dữ liệu

SQL Injection vẫn là một trong những hình thức tấn công ứng dụng web nguy hiểm và phổ biến nhất, nhắm trực tiếp vào "trái tim" của website là cơ sở dữ liệu.

- **Cơ chế hoạt động:** Kẻ tấn công lợi dụng các lỗ hổng trong khâu xử lý dữ liệu đầu vào của ứng dụng web. Bằng cách chèn các đoạn mã SQL độc hại vào các trường nhập liệu như ô tìm kiếm hoặc biểu mẫu đăng nhập, kẻ tấn công có thể lừa máy chủ thực thi các truy vấn ngoài ý muốn.
- **Tác động kinh doanh:** Hậu quả của một cuộc tấn công SQL Injection thành công là vô cùng nghiêm trọng. Kẻ tấn công có thể đánh cắp toàn bộ thông tin nhạy cảm, bao gồm dữ liệu khách hàng, mật khẩu, chi tiết thẻ tín dụng; sửa đổi hoặc xóa dữ liệu; và thậm chí chiếm toàn quyền kiểm soát website.

2.2. Tấn công Từ chối Dịch vụ Phân tán (DDoS): "Bóp nghẹt" Hoạt động Kinh doanh

Tấn công DDoS không nhằm mục đích đánh cắp dữ liệu mà là làm tê liệt hoàn toàn khả năng hoạt động của một website.

- **Cơ chế hoạt động:** Kẻ tấn công sử dụng một mạng lưới máy tính bị nhiễm mã độc (botnet) để đồng loạt gửi một lượng yêu cầu truy cập khổng lồ đến máy chủ mục tiêu, làm cạn kiệt tài nguyên và khiến website không thể truy cập.

- **Tác động kinh doanh:** Tại Việt Nam, DDoS là một mối đe dọa hiện hữu. Năm 2024 ghi nhận hơn 924.000 cuộc tấn công DDoS, tăng 34% so với năm trước. Tác động của DDoS là ngay lập tức: gián đoạn hoạt động, thiệt hại tài chính trực tiếp và tổn hại nghiêm trọng đến uy tín thương hiệu.

2.3. Tấn công Lừa đảo (Phishing) và Kỹ thuật Xã hội: Khai thác Lỗ hổng Con người

Phishing là nghệ thuật lừa đảo, khai thác yếu tố tâm lý và sự tin tưởng của con người.

- **Cơ chế hoạt động:** Kẻ tấn công tạo ra các email, tin nhắn hoặc website giả mạo, có giao diện giống hệt các tổ chức uy tín để thúc ép nạn nhân nhấp vào một liên kết độc hại hoặc cung cấp thông tin nhạy cảm.
- **Sự tiến hóa với AI:** Trong năm 2025, mối đe dọa từ phishing đã trở nên nguy hiểm hơn với sự hỗ trợ của AI. Các công cụ AI cho phép kẻ tấn công tạo ra các email lừa đảo gần như hoàn hảo về mặt ngôn ngữ, thậm chí tạo ra các nội dung giả mạo giọng nói và video (deepfake), khiến các chiến dịch lừa đảo trở nên cực kỳ thuyết phục.
- **Tác động kinh doanh:** Phishing thường là bước đầu tiên trong một chuỗi tấn công phức tạp hơn, dẫn đến việc đánh cắp tài khoản và lây nhiễm các loại mã độc khác, đặc biệt là ransomware.

2.4. Cross-Site Scripting (XSS): Biến Người dùng thành Đồng phạm Bất đắc dĩ

Khác với SQL Injection, XSS nhắm vào người dùng của website, biến trình duyệt của họ thành công cụ thực thi mã độc.

- **Cơ chế hoạt động:** Kẻ tấn công tìm cách chèn các đoạn mã độc hại (thường là JavaScript) vào các trang của một website đáng tin cậy. Khi một người dùng khác truy cập vào trang này, trình duyệt của họ sẽ tự động thực thi đoạn mã đó.
- **Tác động kinh doanh:** Một khi mã độc được thực thi, kẻ tấn công có thể đánh cắp phiên đăng nhập của người dùng (Session Hijacking), thay đổi nội dung trang web, hoặc chuyển hướng người dùng đến các trang lừa đảo khác.

2.5. Mã độc Tống tiền (Ransomware) và các Mã độc khác (Malware)

Ransomware là một trong những mối đe dọa gây thiệt hại tài chính nặng nề nhất cho các tổ chức.

- **Cơ chế hoạt động:** Ransomware là một loại phần mềm độc hại, sau khi xâm nhập vào hệ thống sẽ tiến hành mã hóa tất cả các tệp dữ liệu quan trọng và đòi tiền chuộc để đổi lấy khóa giải mã.
- **Sự bùng nổ của "Ransomware-as-a-Service" (RaaS):** Sự phát triển của mô hình RaaS đã hạ thấp rào cản kỹ thuật, cho phép những kẻ tấn công không có kỹ năng cao vẫn có thể thuê hoặc mua các bộ công cụ ransomware từ các nhóm tội phạm mạng chuyên nghiệp.
- **Tác động kinh doanh và chiến thuật "Tống tiền kép":** Tác động của ransomware là vô cùng tàn khốc. Hơn nữa, các nhóm tấn công hiện đại thường áp dụng chiến thuật "tống tiền kép": chúng không chỉ mã hóa dữ liệu mà còn đánh cắp một bản sao trước đó và đe dọa công khai nếu nạn nhân từ chối trả tiền chuộc.

Phân tích của chúng tôi cho thấy các hình thức tấn công này không hoạt động độc lập mà thường được kết hợp trong một chiến dịch tinh vi. Do đó, một chiến lược phòng thủ hiệu quả phải là một chiến lược đa lớp, có khả năng bảo vệ trên nhiều mặt trận khác nhau.

Phần 3: Hệ Sinh Thái Phòng Thủ Toàn Diện Của Chúng Tôi

Tại ESC, chúng tôi không chỉ nhận diện các mối đe dọa mà còn xây dựng một hệ sinh thái các giải pháp bảo mật toàn diện để bảo vệ khách hàng. Với hơn 22 năm kinh nghiệm, chúng tôi cung cấp một loạt các giải pháp từ nền tảng hạ tầng đến các lớp bảo mật chuyên dụng, được thiết kế để đối phó trực tiếp với các hình thức tấn công đã nêu.

Bảng 2: Sơ đồ Đối chiếu Mối đe dọa và Giải pháp từ ESC

Mối đe dọa	eCloud Hosting & Server	Chứng chỉ SSL	F1-UWSS Suite (WAF, WSFinder, WMDS)	Email Security (Anti-Spam/Virus, 2FA)
SQL Injection	Bảo vệ gián tiếp	Không áp dụng	**Bảo vệ cao** (thông qua WebCastle WAF)	Không áp dụng
XSS	Bảo vệ gián tiếp	Không áp dụng	**Bảo vệ cao** (thông qua WebCastle WAF)	Không áp dụng
DDoS	Bảo vệ hạn chế	**Không bảo vệ trực tiếp**	Bảo vệ hạn chế (Layer 7)	Không áp dụng
Phishing	Không áp dụng	Bảo vệ gián tiếp (tăng uy tín)	Không áp dụng	**Bảo vệ cao** (lọc email, 2FA)
Ransomware	Bảo vệ gián tiếp (qua backup)	Không áp dụng	Bảo vệ gián tiếp (WMDS)	**Bảo vệ cao** (ngăn chặn vector lây nhiễm)

3.1. Nền tảng Bảo mật Cơ bản: Hosting, Máy chủ và Chứng chỉ SSL

Tại ESC, chúng tôi tin rằng mọi chiến lược bảo mật website phải bắt đầu từ một nền tảng hạ tầng vững chắc.

- **eCloud Hosting & Servers:** Các dịch vụ này được chúng tôi xây dựng trên nền tảng đám mây, mang lại hiệu suất và độ tin cậy cao. Chúng tôi chịu trách nhiệm bảo mật ở cấp độ hạ tầng vật lý và mạng lưới, giảm bớt gánh nặng cho khách hàng. Hơn nữa, các dịch vụ như sao lưu dữ liệu định kỳ (snapshot)

cung cấp một lớp phòng thủ cuối cùng, cho phép khôi phục hoạt động nhanh chóng sau một sự cố nghiêm trọng như tấn công ransomware.
- **Chứng chỉ SSL:** Chúng tôi cung cấp đa dạng các loại chứng chỉ SSL, một thành phần không thể thiếu. Chức năng chính của SSL là mã hóa dữ liệu truyền tải giữa trình duyệt của người dùng và máy chủ website (giao thức HTTPS), ngăn chặn các cuộc tấn công nghe lén. Ngoài ra, việc sử dụng HTTPS còn là một yếu tố quan trọng để xây dựng uy tín với người dùng và được các công cụ tìm kiếm đánh giá cao.

Tuy nhiên, chúng tôi luôn nhấn mạnh với khách hàng rằng các giải pháp nền tảng này chỉ là lớp bảo vệ cơ bản và cần được tăng cường bằng các lớp bảo mật chuyên sâu hơn.

3.2. Lá chắn Chủ động cho Website: Phân tích bộ giải pháp F1-UWSS

Để giải quyết các mối đe dọa ở tầng ứng dụng, chúng tôi cung cấp bộ giải pháp bảo mật web hợp nhất F1-UWSS, một sản phẩm mà ESC là đối tác ủy quyền chính hãng của F1Security. Đây là lớp phòng thủ chủ động và quan trọng nhất của chúng tôi dành cho website.

- **WebCastle (Tường lửa ứng dụng web - WAF):** Đây là công cụ phòng thủ trực tiếp và hiệu quả nhất chống lại các cuộc tấn công như SQL Injection và Cross-Site Scripting (XSS). WebCastle hoạt động như một bộ lọc thông minh, kiểm tra và chặn đứng các yêu cầu chứa mã độc trước khi chúng kịp gây hại cho máy chủ web.
- **WSFinder (Công cụ phát hiện Web Shell):** Web shell là một loại mã độc mà tin tặc thường cài cắm lên máy chủ để duy trì quyền truy cập từ xa. WSFinder giải quyết vấn đề này bằng cách liên tục quét máy chủ để phát hiện và cảnh báo về sự hiện diện của các "cửa hậu" này.
- **WMDS (Hệ thống phát hiện Mã độc trên Web):** Một website bị xâm nhập có thể bị lợi dụng để phát tán mã độc cho người dùng. WMDS quét các tệp tin của website để tìm kiếm và phát hiện các đoạn mã độc đã bị chèn vào, từ đó bảo vệ người dùng cuối và giữ gìn uy tín cho website.

Bộ giải pháp F1-UWSS thể hiện năng lực phòng thủ mạnh mẽ của chúng tôi ở tầng ứng dụng, trực tiếp đối phó với các kỹ thuật tấn công nguy hiểm nhất.

3.3. Bảo mật Cổng Giao tiếp Doanh nghiệp: Giải pháp Email An toàn

Chúng tôi hiểu rằng email là cửa ngõ chính cho các cuộc tấn công lừa đảo (Phishing) và là phương tiện lây nhiễm ransomware phổ biến nhất. Do đó, việc bảo vệ kênh giao tiếp này là một trụ cột quan trọng.

- **Các tính năng bảo mật chính:** Các gói dịch vụ email doanh nghiệp của ESC (Mail Pro, Mail Business) được trang bị các cơ chế phòng thủ đa lớp, bao gồm hệ thống chống thư rác (Anti-Spam), diệt virus (Anti-Virus) và tường lửa, giúp lọc bỏ phần lớn các email độc hại.
- **Xác thực hai yếu tố (2FA):** Đây là một trong những tính năng bảo mật quan trọng nhất mà chúng tôi cung cấp. 2FA yêu cầu người dùng cung cấp một yếu tố xác thực thứ hai bên cạnh mật khẩu. Ngay cả khi mật khẩu bị đánh cắp, kẻ tấn công vẫn không thể truy cập vào tài khoản.

Các giải pháp email của chúng tôi cung cấp một lớp phòng thủ thiết yếu, trực tiếp giảm thiểu rủi ro từ các cuộc tấn công kỹ thuật xã hội.

3.4. Tư vấn về Chống Tấn công DDoS: Một Cách tiếp cận Chuyên biệt

Hệ sinh thái sản phẩm của ESC thể hiện năng lực mạnh mẽ trong việc bảo vệ tầng ứng dụng và kênh giao tiếp email. Tuy nhiên, chúng tôi luôn tư vấn rõ ràng cho khách hàng về việc chống lại các cuộc tấn công từ chối dịch vụ phân tán (DDoS) quy mô lớn ở tầng mạng.

- **Làm rõ về SSL:** Trong tài liệu của mình, chúng tôi đã nêu rõ: "Chứng chỉ SSL có bảo vệ khỏi tấn công DDoS không? Không. SSL chỉ mã hóa dữ liệu truyền tải, không bảo vệ website khỏi các cuộc tấn công từ chối dịch vụ (DDoS)".
- **Đặc thù của giải pháp chống DDoS:** Các cuộc tấn công DDoS quy mô lớn, với lưu lượng lên tới hàng trăm Gbps hoặc thậm chí Terabits mỗi giây (Tbps), đòi hỏi một loại hạ tầng phòng thủ chuyên biệt với năng lực mạng lưới khổng lồ và các "trung tâm lọc rửa" (Scrubbing Centers) chuyên dụng.

Danh mục của ESC tập trung mạnh vào bảo mật tầng ứng dụng (Application Layer Security). Đây là định vị chiến lược của chúng tôi với tư cách là một nhà cung cấp chuyên sâu về bảo mật ứng dụng. Đối với các doanh nghiệp mà tính sẵn sàng của dịch vụ là yếu tố sống còn, chúng tôi khuyến nghị một chiến lược phòng thủ bổ sung cho tầng mạng.

Phần 4: Lộ Trình Bảo Mật do Chuyên gia ESC Khuyến nghị

Dựa trên phân tích toàn diện về bối cảnh đe dọa và năng lực của các giải pháp từ ESC, đội ngũ chuyên gia của chúng tôi đề xuất một lộ trình chiến lược đa lớp. Một công nghệ tốt là chưa đủ; nó phải được kết hợp với các quy trình chặt chẽ và yếu tố con người được nâng cao nhận thức.

4.1. Xây dựng Lộ trình Bảo mật Đa lớp với Giải pháp của ESC

Để tối ưu hóa hiệu quả phòng thủ, chúng tôi khuyến nghị các tổ chức triển khai các giải pháp của ESC theo một cấu trúc đa lớp.

- **Lớp 1 - Nền tảng (Foundation Layer):** Đây là lớp cơ bản nhất, đảm bảo hạ tầng hoạt động trên một môi trường an toàn.
  - **Hành động:** Sử dụng các dịch vụ lưu trữ đám mây hiện đại như eCloud Hosting hoặc máy chủ ảo eCloud VPS của chúng tôi. Đồng thời, triển khai chứng chỉ SSL cho tất cả các tên miền để mã hóa toàn bộ lưu lượng truy cập.
- **Lớp 2 - Ứng dụng (Application Layer):** Lớp này tập trung bảo vệ chính website khỏi các cuộc tấn công khai thác lỗ hổng phần mềm.
  - **Hành động:** Triển khai bộ giải pháp F1-UWSS. Trong đó, Tường lửa Ứng dụng Web (WebCastle) sẽ là lá chắn chủ động chống lại các cuộc tấn công SQL Injection và XSS. Các công cụ WSFinder và WMDS sẽ giúp phát hiện và loại bỏ mã độc.
- **Lớp 3 - Giao tiếp (Communication Layer):** Email là vector tấn công phổ biến, việc bảo vệ kênh này là tối quan trọng.
  - **Hành động:** Sử dụng các gói email doanh nghiệp của ESC, tận dụng các tính năng lọc thư rác và quét virus. Quan trọng nhất, thực thi chính sách bắt buộc sử dụng Xác thực Hai yếu tố (2FA) cho toàn bộ tài khoản email.
- **Lớp 4 - Con người (Human Layer):** Công nghệ chỉ hiệu quả khi người dùng sử dụng đúng cách.
  - **Hành động:** Thiết lập và thực thi các chính sách mật khẩu mạnh. Chúng tôi luôn khuyến khích người dùng tạo mật khẩu ngẫu nhiên có độ khó cao khi tạo tài khoản email.

4.2. Bổ sung các Năng lực Bảo mật Thiết yếu: Giải quyết Vấn đề DDoS

Như đã phân tích, các giải pháp của chúng tôi tập trung mạnh vào bảo mật ứng dụng. Đối với các cuộc tấn công DDoS quy mô lớn ở tầng mạng, một chiến lược bổ sung là cần thiết.

- **Hành động:** Đối với các doanh nghiệp hoạt động trong các lĩnh vực có rủi ro cao bị tấn công DDoS như thương mại điện tử, tài chính, báo chí điện tử, việc đầu tư vào một giải pháp chống DDoS chuyên dụng là **bắt buộc**. Chúng tôi tư vấn khách hàng áp dụng một chiến lược đa nhà cung cấp:
  - Sử dụng ESC cho các dịch vụ hosting, bảo mật ứng dụng (WAF) và bảo mật email.
  - Bổ sung bằng cách đăng ký dịch vụ chống DDoS từ một nhà cung cấp chuyên biệt có hạ tầng mạng lưới toàn cầu và năng lực xử lý lưu lượng lớn.

Cách tiếp cận này cho phép doanh nghiệp tận dụng thế mạnh chuyên môn của từng nhà cung cấp, tạo ra một hệ thống phòng thủ toàn diện hơn.

4.3. Tăng cường Phòng thủ từ Yếu tố Con người và Quy trình: Công nghệ là Chưa đủ

Cuối cùng, tại ESC, chúng tôi luôn nhấn mạnh rằng an ninh mạng là một **trách nhiệm chung**. Việc triển khai các giải pháp của chúng tôi là bước khởi đầu, không phải là điểm kết thúc. Các tổ chức phải chủ động xây dựng một văn hóa an ninh mạng từ bên trong.

- **Đào tạo và Nâng cao Nhận thức:**
  - **Hành động:** Tổ chức các chương trình đào tạo nhận thức về an ninh mạng định kỳ cho toàn bộ nhân viên. Nội dung cần được cập nhật liên tục để phản ánh các kỹ thuật tấn công mới, đặc biệt là phishing sử dụng AI, nhằm xây dựng một "bức tường lửa người" (human firewall).
- **Chính sách và Quy trình Vận hành:**
  - **Hành động:** Xây dựng và thực thi các chính sách an ninh thông tin rõ ràng, bao gồm:
    - **Quản lý truy cập:** Áp dụng nguyên tắc đặc quyền tối thiểu.
    - **Quản lý bản vá:** Thiết lập một quy trình cập nhật và vá lỗi phần mềm thường xuyên.
    - **Sao lưu dữ liệu:** Thực hiện chiến lược sao lưu dữ liệu mạnh mẽ theo quy tắc 3-2-1 (3 bản sao, trên 2 loại phương tiện khác nhau, và 1 bản sao lưu ngoài văn phòng).
- **Lập kế hoạch Ứng phó Sự cố:**
  - **Hành động:** Xây dựng một kế hoạch ứng phó sự cố chi tiết, được văn bản hóa và diễn tập thường xuyên. Kế hoạch này phải xác định rõ vai trò và các bước cần thực hiện khi một sự cố xảy ra.

Tóm lại, để đạt được một trạng thái an ninh mạng vững chắc, các doanh nghiệp Việt Nam cần áp dụng một cách tiếp cận toàn diện. Việc hợp tác với một nhà cung cấp có năng lực như ESC để triển khai các công cụ công nghệ tiên tiến là một bước đi quan trọng. Tuy nhiên, sự thành công thực sự phụ thuộc vào việc doanh nghiệp chủ động nắm lấy vai trò của mình trong mô hình trách nhiệm chung: cấu hình đúng công cụ, quản lý chặt chẽ người dùng, và quan trọng nhất là đầu tư vào con người và quy trình để xây dựng một hệ thống phòng thủ có chiều sâu và bền bỉ.