CẨM NANG AN NINH MẠNG

Bảo vệ Doanh nghiệp Việt từ A-Z trong Kỷ nguyên số

được biên soạn không ngoài mục đích cung cấp một lộ trình chi tiết, từ A đến Z, giúp các nhà lãnh đạo, quản lý IT và toàn thể nhân viên trong tổ chức nhận diện đúng các mối nguy, hiểu rõ các điểm yếu và trang bị những chiến lược, công cụ phòng thủ hiệu quả nhất.

Nguyễn Anh Tuấn

Cẩm nang An ninh mạng Toàn diện 2025: Bảo vệ Doanh nghiệp Việt từ A-Z trong Kỷ nguyên số

Lời Mở Đầu: Kỷ nguyên Số và Cuộc chiến Ngầm

Chúng ta đang sống trong một kỷ nguyên số đầy biến động, nơi công nghệ là động lực tăng trưởng cốt lõi của mọi doanh nghiệp. Tuy nhiên, song hành với những cơ hội to lớn là những rủi ro không hề nhỏ. Không gian mạng đã trở thành một chiến trường thực sự, nơi các cuộc tấn công ngày càng tinh vi, có tổ chức và gây ra những thiệt hại không thể lường trước.

Năm 2024 đã chứng kiến một bức tranh an ninh mạng đầy thách thức tại Việt Nam. Theo thống kê, đã có tới **hơn 659.000 vụ tấn công mạng** xảy ra, ảnh hưởng đến **hơn 46% cơ quan và doanh nghiệp**. Vấn đề lộ lọt dữ liệu cũng ở mức báo động với **hơn 14,5 triệu tài khoản** của người dùng Việt Nam bị rò rỉ, chiếm 12% tổng số toàn cầu.Bước sang năm 2025, cuộc chiến này được dự báo sẽ còn khốc liệt hơn. Sự trỗi dậy của Trí tuệ nhân tạo (AI) không chỉ hỗ trợ phòng thủ mà còn trở thành vũ khí lợi hại trong tay tội phạm mạng, giúp chúng tạo ra các chiến dịch lừa đảo và mã độc tinh vi chưa từng có. Ransomware (mã độc tống tiền), tấn công chuỗi cung ứng và lừa đảo có chủ đích sẽ tiếp tục là những mối đe dọa thường trực.

Trong bối cảnh đó, nhiều doanh nghiệp Việt Nam, đặc biệt là các doanh nghiệp vừa và nhỏ (SME), vẫn còn thiếu sự chuẩn bị, xem an ninh mạng là một khoản chi phí thay vì một khoản đầu tư chiến lược. Sự lơ là này chính là lỗ hổng chết người, có thể khiến doanh nghiệp trả giá bằng chính sự tồn tại của mình.

"Cẩm nang An ninh mạng Toàn diện 2025" được biên soạn không ngoài mục đích cung cấp một lộ trình chi tiết, từ A đến Z, giúp các nhà lãnh đạo, quản lý IT và toàn thể nhân viên trong tổ chức nhận diện đúng các mối nguy, hiểu rõ các điểm yếu và trang bị những chiến lược, công cụ phòng thủ hiệu quả nhất. An ninh mạng không còn là trách nhiệm của riêng bộ phận IT, mà là văn hóa, là ý thức của cả một tập thể. Đã đến lúc chúng ta xây dựng pháo đài số của riêng mình.

HN: 71 Trần Quốc Toản, Hoàn Kiếm
Tel: (024) 3942 6896
Hotline: 19002069
Email: e-sales@esc.vn | Website: www.esc.vn
HCM: A16 đường 18, P. HBC, Thủ Đức
Tel: (028) 6294 4808

Chương I: Toàn cảnh Chiến trường Mạng Việt Nam 2025

Để phòng thủ hiệu quả, trước hết chúng ta phải hiểu rõ kẻ thù và chiến trường. Không gian mạng Việt Nam đang đối mặt với những thách thức chưa từng có tiền lệ, đòi hỏi một cách tiếp cận chủ động và toàn diện.

1.1. Tình hình chung: Những con số biết nói

Năm 2024 là một năm đầy sóng gió đối với an ninh mạng Việt Nam. Các cuộc tấn công không chỉ tăng về số lượng mà còn nguy hiểm hơn về quy mô và mức độ phức tạp.

- **Tần suất tấn công dày đặc:** Hơn 46% cơ quan, doanh nghiệp tại Việt Nam thừa nhận đã bị tấn công mạng ít nhất một lần trong năm qua.
- **Thiệt hại tài chính nặng nề:** Các cuộc tấn công bằng mã độc tống tiền (ransomware) đã mã hóa tới 10 Terabyte dữ liệu, gây tổng thiệt hại ước tính gần 11 triệu USD.
- **Lừa đảo gia tăng:** Hơn 4.000 tên miền lừa đảo đã được ghi nhận, và số lượng trang giả mạo thương hiệu tăng gấp 3 lần so với năm 2023, trong đó ngành tài chính - ngân hàng là mục tiêu chính, chiếm 71% tổng số vụ tấn công.
- **Tấn công từ chối dịch vụ (DDoS) bùng nổ:** Ghi nhận hơn 924.000 cuộc tấn công DDoS, tăng 34% so với năm trước, với những cuộc tấn công có quy mô cực lớn, vượt ngưỡng 1 Tbps.

1.2. Các Xu hướng Tấn công Mạng Nổi bật năm 2025

Tội phạm mạng không ngừng "nâng cấp" vũ khí. Năm 2025 được dự báo sẽ chứng kiến sự lên ngôi của các phương thức tấn công tinh vi, tận dụng những công nghệ mới nhất.

- **Tấn công được hỗ trợ bởi AI (AI-powered Attacks):** Đây là xu hướng nguy hiểm nhất. Tội phạm mạng sẽ lạm dụng AI để :
    - Tạo ra các email lừa đảo (phishing) với nội dung và văn phong hoàn hảo, cực kỳ khó phân biệt.
    - Sản xuất các video, hình ảnh, giọng nói giả mạo (deepfake) để thực hiện các kịch bản lừa đảo tinh vi.
    - Tự động hóa việc dò tìm lỗ hổng và phát triển các loại mã độc có khả năng "học" và lẩn tránh các phần mềm bảo mật.
- **Ransomware-as-a-Service (RaaS) và Tống tiền Kép:** Mô hình "cho thuê mã độc tống tiền" (RaaS) đang bùng nổ, cho phép những kẻ tấn công ít kỹ năng cũng có thể thực hiện các vụ tấn công quy mô lớn. Hơn nữa, các nhóm hacker không chỉ mã hóa dữ liệu để đòi tiền chuộc mà còn thực hiện "tống tiền kép": đe dọa công khai dữ liệu nhạy cảm đã đánh cắp nếu nạn nhân không trả tiền. Các vụ tấn công lớn nhắm vào VNDirect, PVOIL, và Bệnh viện Mắt Trung ương trong năm 2024 là những minh chứng điển hình cho mức độ tàn phá của ransomware.
- **Tấn công vào Chuỗi cung ứng (Supply Chain Attacks):** Thay vì tấn công trực diện vào một "pháo đài" được bảo vệ tốt, tin tặc sẽ chọn con đường vòng: tấn công vào các đối tác, nhà cung cấp dịch vụ bên thứ ba có hệ thống bảo mật yếu hơn, rồi từ đó xâm nhập vào mục tiêu chính. Đây là một mối đe dọa thầm lặng nhưng cực kỳ nguy hiểm.
- **Tấn công có Chủ đích (APT) và Lừa đảo Tinh vi:** Các nhóm tin tặc chuyên nghiệp (APT) như Mustang Panda, Lazarus vẫn liên tục hoạt động, sử dụng các kỹ thuật tiên tiến để xâm nhập và nằm vùng trong hệ thống của các tổ chức tài chính, dịch vụ công và năng lượng. Các hình thức lừa đảo

HN: 71 Trần Quốc Toản, Hoàn Kiếm
Tel: (024) 3942 6896
Hotline: 19002069
Email: e-sales@esc.vn | Website: www.esc.vn
HCM: A16 đường 18, P. HBC, Thủ Đức
Tel: (028) 6294 4808

cũng được "cá nhân hóa" cao độ, nhắm vào từng cá nhân cụ thể (Spear Phishing), qua điện thoại (Vishing) hoặc tin nhắn (Smishing).

HN: 71 Trần Quốc Toản, Hoàn Kiếm
Tel: (024) 3942 6896
Hotline: 19002069
Email: e-sales@esc.vn | Website: www.esc.vn
HCM: A16 đường 18, P. HBC, Thủ Đức
Tel: (028) 6294 4808

Chương II: Giải phẫu Lỗ hổng - Những Điểm yếu Chết người của Doanh nghiệp

Một chuỗi dây xích chỉ mạnh bằng mắt xích yếu nhất của nó. Tương tự, một hệ thống phòng thủ dù hiện đại đến đâu cũng có thể sụp đổ chỉ vì một lỗ hổng, dù là kỹ thuật hay con người.

2.1. Lỗ hổng Kỹ thuật

Đây là những "cửa ngõ" mà tin tặc thường xuyên nhắm tới để xâm nhập vào hệ thống.

- **SQL Injection & Cross-Site Scripting (XSS):** Đây là hai trong số những lỗ hổng ứng dụng web phổ biến và nguy hiểm nhất. Chúng cho phép kẻ tấn công chèn các đoạn mã độc hại vào website, từ đó có thể đánh cắp dữ liệu người dùng, chiếm quyền điều khiển phiên đăng nhập, hoặc thay đổi nội dung trang web.
- **Lỗ hổng Zero-day và Phần mềm chưa vá lỗi:** Lỗ hổng "zero-day" là những lỗ hổng mới được phát hiện và chưa có bản vá chính thức từ nhà sản xuất. Đây là vũ khí cực kỳ nguy hiểm trong tay tin tặc. Bên cạnh đó, việc chậm trễ trong việc cập nhật, vá các lỗ hổng đã được công bố trên các phần mềm thông dụng (hệ điều hành, trình duyệt, VPN, tường lửa) cũng là một sai lầm chết người, tạo điều kiện cho hacker khai thác.
- **Sai cấu hình trên nền tảng Đám mây (Cloud Misconfigurations):** Việc dịch chuyển lên đám mây mang lại nhiều lợi ích nhưng cũng đi kèm các rủi ro mới nếu không được cấu hình đúng cách. Các lỗi phổ biến bao gồm: để lộ các cổng quản trị, đặt mật khẩu mặc định yếu, quản lý quyền truy cập lỏng lẻo, và các giao diện lập trình ứng dụng (API) không an toàn.

2.2. Lỗ hổng Con người - Mắt xích Yếu nhất

Thực tế phũ phàng là, yếu tố con người thường là nguyên nhân chính gây ra phần lớn các sự cố an ninh mạng.

- **Tấn công Phi kỹ thuật (Social Engineering):** Đây là nghệ thuật thao túng tâm lý để lừa nạn nhân tự nguyện tiết lộ thông tin nhạy cảm hoặc thực hiện một hành động có hại. Các hình thức phổ biến bao gồm :
    - **Phishing (Lừa đảo qua email):** Gửi email giả mạo các tổ chức uy tín để lừa người dùng nhấp vào link độc hại hoặc cung cấp thông tin đăng nhập.
    - **Vishing (Lừa đảo qua giọng nói):** Gọi điện thoại, giả danh nhân viên ngân hàng, cơ quan chức năng để yêu cầu cung cấp thông tin.
    - **Smishing (Lừa đảo qua tin nhắn SMS):** Gửi tin nhắn SMS chứa link độc hại.
- **Mối đe dọa từ Nội bộ (Insider Threats):** Đây là một trong những rủi ro khó phòng chống nhất, bao gồm hai dạng chính :
    - **Vô ý (Unintentional):** Nhân viên vô tình làm lộ dữ liệu do bất cẩn, gửi nhầm email, sử dụng Wi-Fi công cộng không an toàn, hoặc bị lừa bởi các chiêu trò phishing.
    - **Cố ý (Malicious):** Nhân viên bất mãn hoặc bị mua chuộc chủ động đánh cắp, phá hoại dữ liệu của công ty.
- **Thiếu Nhận thức và Cảnh giác:** Việc xem nhẹ các mối đe dọa, thiếu cảnh giác và thiếu kiến thức về các quy trình bảo mật cơ bản của nhân viên chính là "lỗi mở" lớn nhất, tạo điều kiện cho mọi hình thức tấn công khác thành công.

HN: 71 Trần Quốc Toản, Hoàn Kiếm
Tel: (024) 3942 6896
Hotline: 19002069
Email: e-sales@esc.vn | Website: www.esc.vn
HCM: A16 đường 18, P. HBC, Thủ Đức
Tel: (028) 6294 4808

Chương III: Xây dựng Pháo đài Phòng thủ - Chiến lược Bảo mật Toàn diện

Đối mặt với một chiến trường phức tạp, chúng ta không thể phòng thủ một cách manh mún. Doanh nghiệp cần một chiến lược bảo mật đa lớp, toàn diện, kết hợp giữa pháp lý, công nghệ và quy trình.

3.1. Nền tảng Pháp lý: Tuân thủ để Bảo vệ

Luật An ninh mạng của Việt Nam đã quy định rõ trách nhiệm của các doanh nghiệp trong việc bảo vệ không gian mạng. Việc tuân thủ không chỉ là nghĩa vụ pháp lý mà còn là bước đi cơ bản để tự bảo vệ. Các doanh nghiệp cần đặc biệt lưu ý các yêu cầu về:

- Xây dựng phương án ứng phó và báo cáo sự cố an ninh mạng.
- Bảo mật thông tin và tài khoản người dùng.
- Lưu trữ một số loại dữ liệu người dùng tại Việt Nam và đặt chi nhánh hoặc văn phòng đại diện (đối với doanh nghiệp nước ngoài có liên quan).

3.2. Phòng thủ theo Chiều sâu (Defense-in-Depth)

Đây là triết lý xây dựng nhiều lớp phòng thủ độc lập. Nếu một lớp bị xuyên thủng, các lớp khác vẫn sẽ đứng vững để bảo vệ tài sản cốt lõi.

Lớp 1: Bảo mật Vành đai Mạng (Network Security)

- **Tường lửa Ứng dụng Web (WAF - Web Application Firewall):** WAF hoạt động như một người lính gác cổng cho website và ứng dụng của bạn. Nó giám sát và lọc tất cả lưu lượng truy cập HTTP/HTTPS, giúp ngăn chặn hiệu quả các cuộc tấn công phổ biến như SQL Injection và Cross-Site Scripting (XSS) trước khi chúng tiếp cận máy chủ.
- **Giải pháp Chống tấn công DDoS:** Trước sự bùng nổ của các cuộc tấn công từ chối dịch vụ, việc trang bị một giải pháp chống DDoS chuyên dụng là yêu cầu bắt buộc để đảm bảo tính liên tục của hoạt động kinh doanh.

Lớp 2: Bảo mật Điểm cuối (Endpoint Security)

- **Giải pháp Phát hiện và Phản hồi tại Điểm cuối (EDR - Endpoint Detection and Response):** Các phần mềm diệt virus truyền thống đã không còn đủ sức chống lại các mối đe dọa tinh vi. EDR là giải pháp thế hệ mới, hoạt động bằng cách liên tục giám sát mọi hành vi trên các thiết bị đầu cuối (máy tính, máy chủ). Nhờ ứng dụng AI và Machine Learning, EDR có thể phát hiện các hành vi bất thường, các mã độc chưa từng được biết đến và tự động phản ứng để cô lập mối đe dọa, cung cấp cho quản trị viên cái nhìn toàn cảnh về cuộc tấn công.

Lớp 3: Bảo mật Dữ liệu (Data Security)

- **Mã hóa Dữ liệu (Encryption):** Mọi dữ liệu nhạy cảm, từ thông tin khách hàng đến tài sản trí tuệ, phải được mã hóa cả khi đang được lưu trữ (at rest) và khi đang được truyền đi (in transit). Mã hóa

HN: 71 Trần Quốc Toản, Hoàn Kiếm
Tel: (024) 3942 6896
Hotline: 19002069
Email: e-sales@esc.vn | Website: www.esc.vn
HCM: A16 đường 18, P. HBC, Thủ Đức
Tel: (028) 6294 4808

là lớp phòng thủ cuối cùng, đảm bảo rằng kể cả khi tin tặc đánh cắp được dữ liệu, chúng cũng không thể đọc được.

- **Quy tắc Sao lưu 3-2-1:** Đây là quy tắc vàng trong việc bảo vệ dữ liệu, đặc biệt là để chống lại ransomware. Quy tắc này yêu cầu :
  - Có ít nhất **3 bản sao** của dữ liệu.
  - Lưu trữ trên **2 loại phương tiện** lưu trữ khác nhau (ví dụ: ổ cứng ngoài và đám mây).
  - Giữ **1 bản sao ở một địa điểm khác** (off-site), tách biệt hoàn toàn với hệ thống chính.

3.3. Mô hình Zero Trust: "Không bao giờ Tin tưởng, Luôn luôn Xác minh"

- Mô hình bảo mật truyền thống dựa trên vành đai (tin tưởng mọi thứ bên trong mạng) đã lỗi thời. Zero Trust là một khung kiến trúc bảo mật hiện đại, hoạt động dựa trên triết lý "giả định rằng hệ thống đã bị xâm phạm".**Nguyên tắc cốt lõi:**
  - **Xác minh một cách tường minh (Verify Explicitly):** 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, và loại dữ liệu.
  - **Sử dụng quyền truy cập đặc quyền tối thiểu (Use Least Privileged Access):** Cấp cho người dùng quyền truy cập vừa đủ (just-in-time và just-enough-access) để thực hiện công việc của họ.
  - **Giả định có vi phạm (Assume Breach):** Giảm thiểu bán kính ảnh hưởng của các cuộc tấn công bằng cách phân đoạn mạng và mã hóa toàn bộ phiên làm việc từ đầu đến cuối.
- **Các bước triển khai thực tế:**
  - **Xác thực đa yếu tố (MFA):** Bắt buộc MFA cho tất cả người dùng, đặc biệt là các tài khoản quản trị.
  - **Quản lý thiết bị:** Đảm bảo tất cả các thiết bị truy cập vào tài nguyên của công ty đều tuân thủ các chính sách bảo mật.
  - **Phân đoạn mạng:** Chia nhỏ mạng lưới thành các vùng nhỏ hơn để ngăn chặn sự lây lan của các cuộc tấn công.

3.4. Vai trò của AI trong Phòng thủ

Trí tuệ nhân tạo không chỉ là công cụ tấn công mà còn là một đồng minh đắc lực trong phòng thủ. AI giúp các hệ thống bảo mật trở nên thông minh và chủ động hơn bằng cách :

- **Phát hiện mối đe dọa thông minh:** AI có khả năng phân tích một lượng dữ liệu khổng lồ từ lưu lượng mạng, nhật ký hệ thống để phát hiện các hành vi bất thường, các mẫu tấn công mới mà con người có thể bỏ sót.
- **Tự động hóa phản ứng:** Khi phát hiện mối đe dọa, AI có thể tự động thực hiện các hành động ngăn chặn tức thời như cô lập một thiết bị bị nhiễm, chặn một địa chỉ IP độc hại, giúp giảm thiểu thời gian phản ứng và hạn chế thiệt hại.
- **Phân tích và dự báo:** AI giúp phân tích các lỗ hổng, xếp hạng mức độ ưu tiên và thậm chí dự báo các cuộc tấn công tiềm ẩn trong tương lai, cho phép doanh nghiệp phòng thủ một cách chủ động.

HN: 71 Trần Quốc Toản, Hoàn Kiếm
Tel: (024) 3942 6896
Hotline: 19002069
Email: e-sales@esc.vn | Website: www.esc.vn
HCM: A16 đường 18, P. HBC, Thủ Đức
Tel: (028) 6294 4808

Chương IV: Con người - Bức tường Lửa Vững chắc nhất

Công nghệ dù tiên tiến đến đâu cũng không thể thay thế được yếu tố con người. Một đội ngũ nhân viên được trang bị đầy đủ nhận thức và kỹ năng chính là tuyến phòng thủ quan trọng và hiệu quả nhất.

4.1. Xây dựng Văn hóa An ninh mạng

An ninh mạng phải trở thành một phần trong DNA của doanh nghiệp, bắt đầu từ ban lãnh đạo và lan tỏa đến từng nhân viên.

- **Đào tạo Nhận thức (Awareness Training):**
  - **Nội dung thực tế:** Các chương trình đào tạo cần tập trung vào các tình huống thực tế mà nhân viên thường gặp, như cách nhận diện email phishing, cách tạo và quản lý mật khẩu mạnh, các quy tắc an toàn khi sử dụng Wi-Fi công cộng và mạng xã hội.
  - **Đào tạo liên tục:** Thay vì chỉ đào tạo một lần mỗi năm, hãy tổ chức các buổi cập nhật kiến thức, gửi các bản tin cảnh báo định kỳ để nhận thức của nhân viên luôn được làm mới trước các mối đe dọa mới.
- **Diễn tập Tấn công Giả lập (Simulated Attacks):**
  - Thường xuyên gửi các email phishing giả lập đến nhân viên để kiểm tra mức độ cảnh giác và củng cố kiến thức đã học. Đây là cách hiệu quả nhất để biến lý thuyết thành phản xạ thực tế.

4.2. Quy trình và Chính sách Rõ ràng

- **Xây dựng chính sách:** Doanh nghiệp cần xây dựng và ban hành các chính sách an ninh mạng rõ ràng, dễ hiểu, bao gồm các quy định về việc sử dụng thiết bị, quản lý dữ liệu, và truy cập hệ thống.
- **Quy trình báo cáo sự cố:** Thiết lập một kênh và quy trình đơn giản để nhân viên có thể báo cáo ngay lập tức bất kỳ hoạt động đáng ngờ nào mà không sợ bị khiển trách. Phản ứng nhanh chóng với các báo cáo này là chìa khóa để ngăn chặn một sự cố nhỏ leo thang thành một thảm họa.

HN: 71 Trần Quốc Toản, Hoàn Kiếm
Tel: (024) 3942 6896
Hotline: 19002069
Email: e-sales@esc.vn | Website: www.esc.vn
HCM: A16 đường 18, P. HBC, Thủ Đức
Tel: (028) 6294 4808

Chương V: Kế hoạch Hành động & Kết luận

An ninh mạng là một hành trình, không phải là đích đến. Để bắt đầu hành trình này, các doanh nghiệp có thể thực hiện ngay những bước đi đầu tiên.

5.1. Checklist Hành động Nhanh cho Doanh nghiệp

- **[ ] Đánh giá Rủi ro:** Thực hiện một cuộc đánh giá toàn diện để xác định các tài sản thông tin quan trọng nhất và các lỗ hổng bảo mật hiện có.
- **[ ] Bật Xác thực Đa yếu tố (MFA):** Kích hoạt MFA cho tất cả các tài khoản, đặc biệt là email, tài khoản quản trị và các ứng dụng quan trọng. Đây là biện pháp đơn giản nhưng hiệu quả nhất để chống lại việc đánh cắp tài khoản.
- **[ ] Đào tạo Nhân viên:** Tổ chức ngay một buổi đào tạo nhận thức về an ninh mạng cho toàn bộ nhân viên, tập trung vào lừa đảo phishing.
- **[ ] Kiểm tra Sao lưu:** Rà soát lại quy trình sao lưu dữ liệu. Đảm bảo bạn đang tuân thủ quy tắc 3-2-1 và đã thử nghiệm việc khôi phục dữ liệu từ các bản sao lưu.
- **[ ] Rà soát và Cập nhật:** Đảm bảo tất cả các hệ điều hành, phần mềm và ứng dụng trên máy chủ và thiết bị của nhân viên đều được cập nhật bản vá bảo mật mới nhất.
- **[ ] Triển khai các giải pháp bảo mật cơ bản:** Ít nhất phải có tường lửa (Firewall) và các giải pháp chống virus/mã độc thế hệ mới (EDR).

5.2. Kết luận

Trong thế giới kết nối ngày nay, không có doanh nghiệp nào là "quá nhỏ để bị tấn công". Việc đầu tư vào an ninh mạng không còn là một lựa chọn, mà là một yêu cầu bắt buộc để tồn tại và phát triển. Đó là sự đầu tư vào niềm tin của khách hàng, vào sự ổn định của hoạt động kinh doanh và vào chính tương lai của doanh nghiệp.

Bằng cách kết hợp các giải pháp công nghệ tiên tiến như WAF, EDR, AI với một chiến lược phòng thủ chiều sâu, áp dụng mô hình Zero Trust và quan trọng nhất là xây dựng một văn hóa an ninh mạng vững chắc với con người làm trung tâm, doanh nghiệp Việt Nam hoàn toàn có thể tự tin đối mặt và chiến thắng trong cuộc chiến trên không gian mạng. Hãy bắt đầu hành động ngay hôm nay.

BAN BIÊN TẬP ESC

HN: 71 Trần Quốc Toản, Hoàn Kiếm
Tel: (024) 3942 6896
Hotline: 19002069
Email: e-sales@esc.vn | Website: www.esc.vn
HCM: A16 đường 18, P. HBC, Thủ Đức
Tel: (028) 6294 4808