Khuyến nghị giải pháp kĩ thuật

BẢO VỆ PHÒNG CHỐNG & GIẢM THIỂU THIỆT HẠI do ransomware

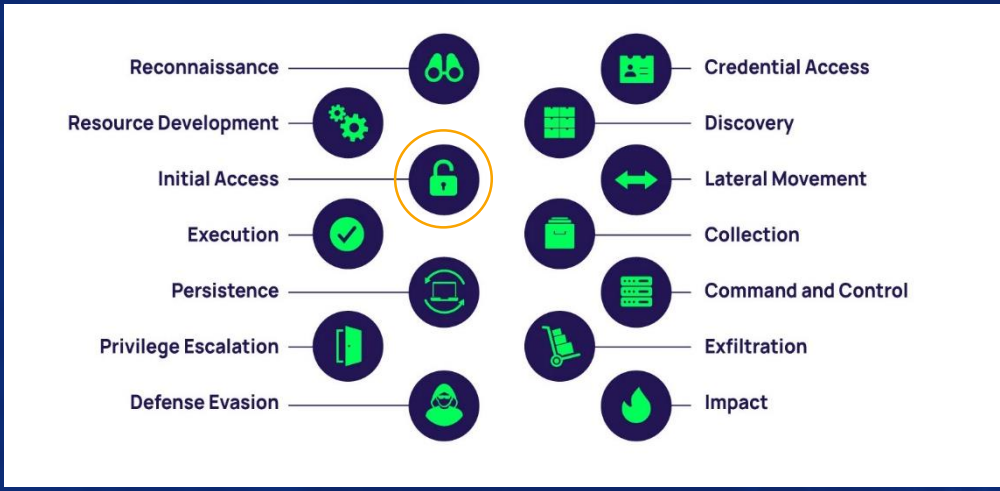
Theo ghi nhận, chỉ trong 1 tháng trở lại đây, tình hình tấn công mạng đang gia tăng với quy mô và tính chất vô cùng phức tạp, nhắm vào các hệ thống của các cơ quan, doanh nghiệp điện lực, chứng khoán, ngân hàng, viễn thông, dầu khí, y tế... Nguy hiểm và phổ biến nhất là hình thức tấn công mã hóa dữ liệu (ransomware). Hơn bao giờ hết, các tổ chức tại Việt Nam cần gấp rút củng cố hệ thống an toàn thông tin mạng, đối phó với những rủi ro về an toàn thông tin. Là đối tác tin cậy về an toàn thông tin với 30 năm kinh nghiệm đồng hành cùng 3.200+ tổ chức lớn, FPT IS xin gửi đến doanh nghiệp các khuyến nghị chung để đảm bảo an toàn thông tin, phòng chống và giảm thiểu thiệt hại do ransomware gây ra.

01 ĐỀ XUẤT MỘT SỐ GIẢI PHÁP KỸ THUẬT CHO VIỆC BẢO VỆ, PHÒNG CHỐNG VÀ GIẢM THIỂU THIỆT HẠI DO RANSOMWARE

Sẵn sàng cho tình huống xấu nhất

Hạng mục	Kết quả cần đạt	Công việc cần thực hiện
Dự phòng & Khôi phục dữ liệu	Sao lưu dữ liệu	• Phân loại mức độ quan trọng: Tuỳ thuộc vào đặc thù sản xuất kinh doanh của mỗi tổ chức, doanh nghiệp, nên phân loại dữ liệu CNTT và hệ thống CNTT theo mức độ quan trọng khác nhau. Ví dụ có thể chia thành 4 loại sau: – Mức độ 1: Không quan trọng – Mức độ 2: Bình thường – Mức độ 3: Quan trọng – Mức độ 4: Đặc biệt quan trọng • Triển khai giải pháp sao lưu dự phòng phù hợp với các mức độ quan trọng nêu trên. – Ví dụ: Đối với máy chủ đặc biệt quan trọng, thường xuyên duy trì và cập nhật một bản backup "Golden images" bao gồm: OS, cấu hình, các phần mềm được cài đặt sẵn, dữ liệu mới nhất. • Bản backup của dữ liệu và hệ thống từ mức quan trọng trở lên nên được sao lưu ra một hệ thống Backup độc lập về mặt vật lý với hệ thống đang hoạt động. • Chuẩn bị sẵn sàng các thiết bị phần cứng (máy chủ vật lý) có khả năng tương thích với các bản Backup
	Khôi phục dữ liệu	• Xây dựng kịch bản khôi phục dữ liệu từ các bản sao lưu • Diễn tập khôi phục dữ liệu để đảm bảo hệ thống có thể đưa vào hoạt động trở lại một cách nhanh nhất.
Xây dựng và diễn tập kịch bản xử lý sự cố	Kịch bản xử lý sự cố (CyberSecurity Incident Response)	• Xây dựng kịch bản xử lý sự cố ATTT do mã độc gây ra (có thể phối hợp với các đơn vị cung cấp dịch vụ SOC, Security Incident Response) • Thực hiện diễn tập định kỳ (theo quý)
	Kế hoạch quản trị khủng hoảng ATTT (CyberSecurity CRISIS Management Plan)	• Xây dựng kịch bản Kế hoạch quản trị khủng hoảng ATTT • Thực hiện diễn tập Kế hoạch quản trị khủng hoảng ATTT (tối thiểu 1 năm 1 lần)

02 NGĂN CHẶN VÀ HẠN CHẾ MỨC ĐỘ ẢNH HƯỞNG CỦA RANSOMWARE



MITRE ATT&CK Tatics in the enterprise matrix

2.1. Giảm thiểu rủi ro từ các mối đe doạ ngoài Internet

Initial Access Vector:
Internet-Facing Vulnerabilities and Misconfigurations

Hạng mục	Kết quả cần đạt	Công việc cần thực hiện
Kiểm soát truy cập	KHÔNG MỞ CÁC DỊCH VỤ KHÔNG CẦN THIẾT RA VÙNG MẠNG BIÊN (internet, partner, ...) • Chỉ cho phép người dùng bên ngoài tổ chức truy cập tới các ứng dụng cần thiết, liên quan tới hoạt động sản xuất – kinh doanh của đơn vị. • Ngăn chặn triệt để các truy cập từ xa, không an toàn vào trong hệ thống, thiết bị như: Các giao thức quản trị hệ thống và thiết bị (Remote desktop, ssh, telnet,...), giao thức chia sẻ file (smb, tftp, ftp, ..).	1. Rà soát chính sách cấu hình trên Router, Firewall và các thiết bị bảo mật vùng biên (Internet, đối tác): Loại bỏ 100% các Rule (NAT, Firewall rule) cho phép người dùng bên ngoài khởi tạo các kết nối quản trị (Remote desktop, ssh, telnet, ứng dụng chia sẻ file SMB, ..) hoặc sử dụng các giao thức không an toàn vào trong hệ thống (telnet, ftp, tftp,...) 2. Chỉ cho phép người dùng bên ngoài khởi tạo kết nối tới các ứng dụng, dịch vụ cần thiết liên quan tới hoạt động thương mại, sản xuất, kinh doanh. Khuyến nghị sử dụng các giao thức an toàn, có mã hoá 3. Khai thác triệt để các hệ thống bảo vệ vùng biên (bao gồm nhưng không giới hạn): – Hệ thống chống tấn công DDOS – Hệ thống tường lửa NetGen Firewall – Hệ thống tường lửa ứng dụng: Web Application Firewall – Hệ thống IPS, IDS, NTA để phát hiện bất thường mức mạng
	Không sử dụng các phần mềm điều khiển từ xa như: Teamviewer, Remote Utilities, UltraVNC, AnyDesk, AeroAdmin, RemotePC, Chrome Remote Desktop, Logmein, ...	• Cấu hình hệ thống firewall ngăn chặn triệt để các phần mềm điều khiển máy tính, máy chủ từ xa. • Rà soát 100% máy tính cá nhân, máy chủ; loại bỏ hoàn toàn việc cài đặt các phần mềm điều khiển từ xa.

2.1. Giảm thiểu rủi ro từ các mối đe doạ ngoài Internet

Initial Access Vector: Internet-Facing Vulnerabilities and Misconfigurations

Hạng mục	Kết quả cần đạt	Công việc cần thực hiện
Kiểm soát truy cập	Nhận diện lỗ hổng bảo mật trên các thiết bị & hệ thống ứng dụng. Triển khai phương án khắc phục triệt để.	**1. Bắt buộc:** • Rà soát lỗ hổng bảo mật – VA (Vulnerability Assessment): định kỳ hàng tháng đối với các máy chủ, thiết bị vùng ngoài (DMZ, đối tác), các máy chủ và thiết bị quan trọng trong hệ thống. – Phối hợp với các bộ phận liên quan, triển khai các hành động khắc phục lỗ hổng bảo mật sau rà quét – 100% các thiết bị, máy chủ vùng biên (ưu tiên thiết bị trong vùng có nguy cơ cao như: Internet, DMZ, đối tác...): sử dụng phần mềm có bản quyền, cập nhật liên tục hệ điều hành, các bản vá bảo mật, phần mềm ứng dụng, phần mềm từ các hãng thứ ba. • 100% hệ thống ứng dụng trước khi phơi ra ngoài Internet cần được rà soát bảo mật lớp ứng dụng (Pentest, ScanCode) để loại bỏ các điểm yếu bảo mật **2. Khuyến nghị:** • VA và khắc phục lỗ hổng bảo mật định kỳ hàng Quý đối với 100% các thiết bị CNTT trong hệ thống. • Bất cứ có sự thay đổi nào về code ứng dụng (cập nhật version, sửa lỗi) đều phải có báo cáo đánh giá an toàn source code (Pentest, ScanCode)
	Tăng cường bảo mật trên máy tính & và máy chủ (Hardening)	• Cấu hình/kích hoạt tính năng Firewall (Host Firewall) trên máy tính, máy chủ & các thiết bị trong hệ thống. • Cấu hình (Host Firewall) chỉ cho phép địa chỉ dải địa chỉ IP tin cậy (từ dải IP của bộ phận vận hành hệ thống, địa chỉ IP từ hệ thống PAM/PIM, địa chỉ IP từ các phần mềm quản trị tập trung...) để tránh tấn công ngang hàng hoặc truy cập không mong muốn từ địa chỉ IP không tin cậy trong hệ thống. • Disable/vô hiệu hoá các cổng kết nối (service port) không cần thiết trên thiết bị • Cài đặt & cập nhật phần mềm Antivirus • Cài đặt phần mềm EDR • Cài đặt và tích hợp log về hệ thống SIEM • Hardening (tăng cường bảo mật) cho các thiết bị theo: – Chính sách ATTT của tổ chức – Khuyến nghị của hãng – Best Practices của các tổ chức bảo mật độc lập: NIST, CIS
	Đảm bảo SMB protocol an toàn khi đưa vào sử dụng	• Vô hiệu hoá (Disable) SMBv1 (cả server và client), trường hợp cần sử dụng thì cập nhật lên SMBv3 đối với tất cả các server và máy trạm. Sử dụng phiên bản tối thiểu là SMBv 3.1.1 trở lên. • Hạn chế tới mức tối đa việc sử dụng giao thức SMB trong hệ thống: – Ngăn chặn triệt để kết nối TỚI & TỪ vùng biên sử dụng giao thức SMB (chặn TCP port 137, 138, 139) – Chặn hoặc giới hạn tới mức tối đa việc sử dụng giao thức SMB trong nội bộ tổ chức, doanh nghiệp. Trên hệ thống Firewall chỉ mở kết nối tới các dịch vụ cần thiết như Share File server, Domain controler. Các máy chủ còn lại không có chức năng chia sẻ file thì vô hiệu hóa tính năng SMB Server Service. – Đối với máy tính người dùng, vô hiệu hoá tính năng SMB Server Services để chia sẻ ngang hàng. • Cấu hình yêu cầu bắt buộc sử dụng Kerberos-based IP Security (Ipsec) cho SMB để Chặn hành vi các máy không tham gia AD brute-force SMB • Cấu hình SMB signing để chặn một số tấn công MITM và PTH

2.2. Giảm thiểu rủi ro lộ lọt thông tin đăng nhập hệ thống

Initial Access Vector:
Compromised Credentials

Hạng mục	Kết quả cần đạt	Công việc cần thực hiện
Triển khai Xác thực đa nhân tố (MFA)	Cấu hình xác thực đa nhân tố (MFA) đối với các ứng dụng trong tổ chức. Đặc biệt, ưu tiên triển khai MFA với các dịch vụ quan trọng, có nguy cơ cao bị tấn công, như: - Dịch vụ VPN - Dịch vụ Email - Hệ thống quản lý tài khoản đặc quyền IAM/PAM (nếu có) - Các hệ thống đặc biệt quan trọng	• Đảm bảo các User Azure đều sử dụng MFA -> Kiểm tra đã cấu hình Azure AD Condition Access đối với các dịch vụ trên Azure như Exchange O365 • Đảm bảo các User PAM đều sử dụng MFA • Đảm bảo các User VPN đều sử dụng MFA • Đảm bảo các User mail On-premise sử dụng MFA
Triển khai hệ thống quản lý tài khoản đặc quyền và định danh người dùng như PAM/IAM	Ưu tiên triển khai hệ thống IAM/PAM để quản lý tài khoản đặc quyền, phân quyền và giám sát người dùng trong quá trình vận hành	• 100% hệ thống, dịch vụ cần tích hợp với hệ thống PAM, IAM cho quá trình quản trị, vận hành và khai thác dịch vụ.
	Đối với đơn vị sử dụng hệ thống quản lý tài khoản đặc quyền (PAM)	• Tích hợp hệ thống PAM với hệ thống xác thực đa nhân tố MFA. • Đảm bảo 100% các phiên quản trị tới các thiết bị & ứng dụng (ví dụ như remote desktop, SSH...) phải đi qua PAM. Triển khai cấu hình trên hệ thống Firewall và Firewall mức host: Chỉ cho phép PAM truy cập vào thiết bị, hệ thống ứng dụng. Không cho phép người dùng truy cập trực tiếp để quản trị và vận hành. • Cấu hình PAM ghi lại toàn bộ quá trình truy cập thiết bị. • Định nghĩa các truy cập bất thường (ví dụ truy cập thiết bị ngoài giờ làm việc). Đối với các truy cập bất thường, tạo luồng phê duyệt của cấp cao hơn thì cán bộ vận hành mới truy cập được vào thiết bị.
Chính sách quản lý tài khoản	Thay đổi mật khẩu mặc định (default username/password)	• Rà soát và thay đổi mật khẩu mặc định cho 100% các thiết bị và ứng dụng trong hệ thống.
	Không sử dụng tài khoản đặc quyền như root, administrator vào quá trình vận hành, quản trị hàng ngày.	• Rà soát tài khoản đặc quyền: root/administrator. • Thu hồi 100% tài khoản đặc quyền. Cán bộ nhận tài khoản đặc quyền tiến hành đổi mật khẩu cho các tài khoản nêu trên. • Tạo User Group (Nhóm người dùng) có quyền khác nhau phù hợp với vị trí làm việc • Tạo User: – Mỗi cá nhân có một tài khoản riêng. Tuyệt đối không sử dụng chung tài khoản – Tài khoản User được gắn vào User Group tương ứng

2.2. Giảm thiểu rủi ro lộ lọt thông tin đăng nhập hệ thống

Initial Access Vector:
Compromised Credentials

Hạng mục	Kết quả cần đạt	Công việc cần thực hiện
Chính sách quản lý tài khoản	Chính sách về mật khẩu	• Mật khẩu dài tối thiểu 15 ký tự bao gồm: Chữ thường, chữ hoa, số và ký tự đặc biệt • Tối thiểu 03 tháng phải thay đổi mật khẩu một lần • Thiết lập chế độ cho phép tự động khoá tài khoản sau khi đăng nhập nhiều lần liên tiếp trong một khoảng thời gian nhất định. Và chỉ có Admin mới có quyền kích hoạt lại tài khoản bị khoá. Ví dụ đăng nhập sai 10 lần liên tiếp trong 10 phút. • Không lưu giữ mật khẩu dưới dạng clear-text • Trường mật khẩu trong CSDL phải được mã hoá • Tuyệt đối không lưu tài khoản và mật khẩu đăng nhập trên các nền tảng và ứng dụng trực tuyến để tránh nguy cơ lộ lọt dữ liệu • Vô hiệu hóa tính năng ghi nhớ mật khẩu trên các trình duyệt web
Truy cập an toàn	Cấu hình Remote Access an toàn	• Thay đổi port mặc định của các dịch vụ nhạy cảm như SSH, RDP... • Cấu hình ẩn bớt các banner hoặc các message có chứa thông tin về dịch vụ (tên OS, tên phần mềm, phiên bản phần mềm) để giảm hiệu quả quá trình rà quét của hacker • Ưu tiên sử dụng phương pháp xác thực bằng private key/dongle/certificate đối với các hệ thống có hỗ trợ
	Truy cập quản trị an toàn tới các hệ thống và thiết bị	• Access Control List (ACL): Xây dựng một danh sách sách các địa chỉ IP tin cậy (ví dụ như dải IP nội bộ của bộ phận vận hành) và giao thức quản trị (mức OS, ứng dụng) được phép truy cập vào các thiết bị, hệ thống ứng dụng. • Triển khai cấu hình này trên các thiết bị: – Firewall – Cấu hình mức host (trên bản thân thiết bị) để chống tấn công ngang hàng
	Tránh trường hợp tài khoản bị tấn công Lateral movement PTH	• Đưa các user admin đặc quyền vào group Protected User (tính năng: chặn NTML...)

2.3. Giảm thiểu rủi ro tấn công Phishing

Initial Access Vector: Phishing

Hạng mục	Kết quả cần đạt	Công việc cần thực hiện
Nâng cao nhận thức ATTT cho người dùng	Triển khai các chương trình đào tạo, nâng cao nhận thức ATTT cho 100% cán bộ nhân viên trong tổ chức kể cả đội ngũ vận hành CNTT	• Đào tạo nhận thức ATTT • Triển khai các chương trình đánh giá nhận thức ATTT như: Email Phishing
Gửi & nhận email an toàn	Ngăn chặn và loại bỏ email không an toàn	• Kích hoạt tính năng ngăn chặn email độc hại trên hệ thống email-gateway để loại bỏ trước khi gửi tới người dùng trong tổ chức: – Chặn lọc theo tiêu đề email – Chặn lọc theo nội dung trong email – Chặn lọc dựa trên địa chỉ IP của mail-gateway (IP độc hại) – Chặn domain giả mạo (kẻ tấn công thường sử dụng để tiến hành các chiến dịch email phishing) • Đảm bảo Email GW được cấu hình: SPF, DKIM (must), DMARC (optional) đầy đủ • Không sử dụng các port legacy như IMAP SMTP OWA. Chuyển sang sử dụng OAuth2 (Modern Auth Exchange On Prem) (không mất tiền, nhưng không có MFA builtin) / Hybrid Modern Auth (mất tiền, nhưng có MFA builtin) • Cấu hình email-gateway chặn brute-force password • Đối với file đính kèm trong email: Xem xét không cho gửi file nén đặt mật khẩu để có thể tận dụng tính năng EOP của Micrsoft khi rà quét file đính kèm

2.4. Giảm thiểu rủi ro nhiễm mã độc

Initial Access Vector: Precursor Malware Infection

Hạng mục	Kết quả cần đạt	Công việc cần thực hiện
Phòng ngừa lây nhiễm mã độc	Phòng chống mã độc	• Rà soát và tiến hành cài đặt phần mềm Antivirus trên 100% máy chủ, máy trạm • Bật tính năng tự động cập nhật để đảm bảo phần mềm Antivirus luôn được cập nhật phiên bản mới nhất • Tích hợp hệ thống Antivirus với hệ thống SIEM để giám sát 24/7
	Phát hiện hành vi bất thường	• Rà soát và tiến hành cài đặt phần mềm EDR trên 100% máy chủ, máy trạm để phát hiện các hành vi bất thường (các tiến trình bất thường, không được phép thực thi trên máy chủ, máy trạm) • Tích hợp hệ thống EDR với hệ thống SIEM để giám sát 24/7 • Xem xét phương án triển khai IPS/IDS để phát hiện hành vi bất thường trên hệ thống mạng

2.4. Giảm thiểu rủi ro nhiễm mã độc

Initial Access Vector: Precursor Malware Infection

Hạng mục	Kết quả cần đạt	Công việc cần thực hiện
Phòng ngừa lây nhiễm mã độc	Thu thập log tập trung phục vụ cho điều tra trong trường hợp có sự cố	• 100% máy chủ và các thiết bị quan trọng được tích hợp và đẩy log về hệ thống SIEM nhằm phát hiện sớm các hành vi bất thường hoặc phục vụ công tác điều tra số.
Săn tìm mối đe dọa trên hệ thống	Compromise assessment/ Threathunt Định kỳ	• Chủ động săn tìm dấu hiệu máy chủ bị tấn công, cô lập và xử lý sớm đối với máy chủ bị lây nhiễm mã độc

2.5. Giảm thiểu rủi ro từ đối tác cung cấp dịch vụ

Initial Access Vector:
Third Parties and Managed Service Providers

Hạng mục	Kết quả cần đạt	Công việc cần thực hiện
Quản lý rủi ro từ đối tác cung cấp dịch vụ cho tổ chức	Xác định rõ vai trò và trách nhiệm của đối tác khi xảy ra sự cố ATTT	• Xây dựng ma trận trách nhiệm, xác định rõ vai trò, nhiệm vụ của đối tác cung cấp dịch vụ cho tổ chức, doanh nghiệp. • Xác định mức độ đền bù thiệt hại khi sự cố xảy ra • Ban hành tiêu chuẩn ATTT mà đối tác bắt buộc phải tuân thủ, tổ chức kiểm tra mức độ tuân thủ của đối tác.
	Phân quyền tối thiểu cho đối tác cung cấp dịch vụ	• Các bên thứ ba và MSP chỉ được phép truy cập vào các thiết bị và máy chủ nằm trong vai trò hoặc trách nhiệm của họ. • Đối tác được cấp phát tài khoản theo đúng vai trò, chức năng của họ.

Nguồn tham chiếu thông tin:

- https://www.cisa.gov/sites/default/files/2023-10/StopRansomware-Guide-508C-v3_1.pdf
- https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf

FPT IS - ĐỐI TÁC TIN CẬY VỀ AN NINH AN TOÀN THÔNG TIN

cho hệ thống công nghệ thông tin
của tổ chức, doanh nghiệp

Giám sát và phản ứng sự cố ATTT

↓10X
Thời gian phản hồi (MTTR)

↓90%
Rủi ro trên các Endpoint toàn thời gian

85%
Độ bao phủ ma trận vector tấn công mạng (MITRE ATT & CK®)

Điều hành An ninh mạng tập trung

Cảnh báo bảo mật chính xác và sớm nhất
99%

<30 phút
Thời gian ghi nhận sự cố (TTA)

Phản hồi sự cố kể từ khi sự cố bảo mật được xác nhận với mức nghiêm trọng nhất
<1 giờ

Giải pháp bảo mật do FPT IS phát triển:

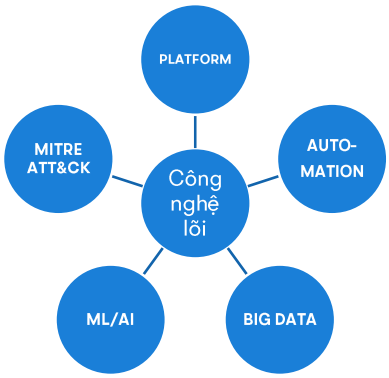
- FPT.EagleEye malBot - Phần mềm phát hiện và giám sát bảo mật lớp mạng - NTA
- FPT.EagleEye mGuard - Phần mềm giám sát và quản lý sự kiện an ninh tập trung - SIEM

Dịch vụ bảo mật:

- Tư vấn tuân thủ Bảo mật chuẩn quốc tế ISO27001, PCI DSS
- Tư vấn và triển khai hạ tầng bảo mật
- Dịch vụ kiểm thử xâm nhập - Pentest
- Dịch vụ đánh giá Bảo mật hạ tầng - VA
- Dịch vụ Audit và tối ưu hạ tầng network & security
- Dịch vụ Threat Hunting – Săn tìm mối nguy, săn tìm mã độc

Dịch vụ Giám sát an toàn thông tin (CSOC)

- FPT.EagleEye MDR - Dịch vụ giám sát an toàn thông tin lớp Endpoint (dành cho doanh nghiệp vừa và nhỏ)
- FPT.EagleEye mSOC - Dịch vụ Giám sát an toàn thông tin 24/7 mSOC



Sát cánh cùng tổ chức, doanh nghiệp chuyển đổi số an toàn

Cam kết có mặt trong vòng 1 giờ sau khi phát hiện sự cố để cùng xử lý

Báo cáo thời gian thực toàn bộ tiến trình với cổng thông tin trực tuyến

Phát hiện cảnh báo, xử lý ngay

Ứng dụng công nghệ phòng vệ an ninh mạng tiên tiến nhất thế giới

Chuyên gia bảo mật được chứng nhận chuẩn quốc tế

Giám sát 24/7

Công ty TNHH FPT IS

Trụ sở: Số 10 phố Phạm Văn Bạch, Phường Dịch Vọng, Quận Cầu Giấy, TP. Hà Nội, Việt Nam

Văn phòng Hà Nội: Tầng 22 tòa nhà Keangnam Landmark72, E6 đường Phạm Hùng, Phường Mễ Trì, Quận Nam Từ Liêm, TP. Hà Nội, Việt Nam

Chi nhánh TP. Hồ Chí Minh: Lô B3, Đường Sáng tạo, Khu E-Office, Khu chế xuất Tân Thuận, Phường Tân Thuận Đông, Quận 7, TP. Hồ Chí Minh, Việt Nam

024 3562 6000 - 024 7300 7373

contact@fpt.com

fpt-is.com