CyStack

11 RỦI RO BẢO MẬT trong Doanh nghiệp

MỤC LỤC

I. TỔNG QUAN

Theo một báo cáo tại trung tâm nghiên cứu Kaspersky Lab, Việt Nam là một trong 3 nước có nguy cơ bị tấn công mạng cao nhất thế giới. Bên cạnh đó, doanh nghiệp Việt phải chịu thiệt hại tới 10 triệu đô-la Mỹ sau mỗi cuộc tấn công - đây là mức cao nhất trong khu vực Châu Á Thái Bình Dương (Cisco, 2018).

Cho dù là người lạc quan nhất thì cũng không thể phủ nhận: **tình hình an ninh mạng ở Việt Nam đang trong trạng thái báo động**. Và các tổ chức, doanh nghiệp là mục tiêu chính của tội phạm mạng.

Xu hướng tấn công mạng có sự biến chuyển từ nhỏ lẻ sang những vụ tấn công quy mô lớn, được đầu tư bài bản. Với những thủ thuật tinh vi, tin tặc dễ dàng qua mặt các doanh nghiệp và thực hiện các vụ tấn công vi phạm dữ liệu, DDOS, tiêm nhiễm malware gây cản trở quá trình kinh doanh.

Với mục đích giúp doanh nghiệp Việt đương đầu với các cuộc tấn công mạng, chúng tôi đã biên soạn cuốn sách “11 vấn đề bảo mật doanh nghiệp cần biết”. Hy vọng, sau cuốn sách này, các CEO sẽ hiểu rõ hơn về tình hình an ninh mạng doanh nghiệp tại Việt Nam, từ đó đưa ra biện pháp phòng thủ phù hợp, giúp doanh nghiệp phát triển an toàn, bền vững trước vô vàn rủi ro của mạng internet thời kỳ 4.0.

> *... Việt Nam là một trong 3 nước có nguy cơ bị tấn công mạng cao nhất thế giới.*

II. 11 RỦI RO BẢO MẬT DOANH NGHIỆP CẦN BIẾT

1. LỖ HỔNG BẢO MẬT

Lỗ hổng bảo mật là những điểm yếu nằm trong thiết kế và cấu hình của hệ thống. Chúng cho phép kẻ tấn công đánh cắp cơ sở dữ liệu, chiếm quyền quản trị, ghi đè nội dung, và thực hiện nhiều hành vi sai trái khác. Thông thường trong một doanh nghiệp sẽ bị ảnh hưởng bởi 2 loại lỗ hổng:

- **Lỗ hổng tồn tại trong phần mềm, thiết bị mà doanh nghiệp sử dụng (khách quan):** VD lỗ hổng tồn tại trong Windows, Wordpress, Skype, phần mềm CRM, thiết bị router/modem wifi, v.v.
- **Lỗ hổng phát sinh khi doanh nghiệp thiết kế phần mềm, ứng dụng (chủ quan):** Phổ biến nhất là lỗ hổng ứng dụng web, mobile như Cross-site Scripting, SQL injection, lỗi phân quyền, lỗi misconfiguration (cấu hình sai),...

> *48% các vụ đánh cắp dữ liệu được khai thác từ các lỗ hổng bảo mật (năm 2018)*

GIẢI PHÁP

Tất cả những lỗ hổng bảo mật này sẽ nguy hiểm khi và chỉ khi tin tặc tìm thấy và khai thác chúng. Vì thế, nếu "vá" được lỗ hổng kịp thời, DN sẽ phòng tránh được các cuộc tấn công (mặc dù điều này không hề dễ dàng). Dưới đây là một vài giải pháp hữu hiệu để hạn chế lỗ hổng:

- Luôn cập nhật các phiên bản MỚI NHẤT của phần mềm, hệ điều hành, các ứng dụng của bên thứ ba để nhận được bản vá lỗi từ nhà phát hành nhanh nhất có thể.
- Không sử dụng phần mềm bẻ khóa (crack). Đôi khi, chính phần mềm crack là "cửa sau" để tin tặc tấn công DN.
- Sử dụng công cụ quét lỗ hổng & đánh giá lỗ hổng tự động cho toàn bộ hệ thống. Điều này giúp phát hiện phần lớn các lỗ hổng cơ bản.
- Thực hiện Pen-test định kỳ cho hệ thống ứng dụng, sản phẩm (website, mobile app, IoT, software...) để phát hiện ra những lỗ hổng nguy hiểm. Việc này càng cần thiết đối với các doanh nghiệp dựa vào website/mobile app để tăng lượng người dùng.

Crowdsourced Security là hình thức cải tiến của pen-test. Phương pháp này cung cấp cho doanh nghiệp một cộng đồng chuyên gia bảo mật sẵn sàng kiểm thử sản phẩm cho doanh nghiệp. Chi phí được tính theo lỗ hổng tìm thấy, giúp doanh nghiệp tối ưu ngân sách.

[Xem thêm: Ra mắt nền tảng Crowdsourced Security đầu tiên tại Việt Nam]

2. TẤN CÔNG PASSWORD

Đây là hình thức tấn công mà kẻ xấu tìm cách truy cập vào hệ thống hoặc các tài khoản của doanh nghiệp bằng cách cố gắng lấy được mật khẩu của quản trị viên. Có thể là mật khẩu tài khoản ngân hàng hoặc các kênh quản lý tài chính của doanh nghiệp (các cổng thanh toán, ví điện tử); cũng có thể là tài khoản của các hệ thống quản lý khách hàng (CRM), website, hệ thống thư điện tử, tài khoản mạng xã hội... hay mật khẩu của các hệ thống quản trị khác.

GIẢI PHÁP

- Xây dựng những quy ước về đặt mật khẩu trong doanh nghiệp và cho users, đặc biệt là với các tài khoản quan trọng. Cần sử dụng những mật khẩu mạnh bằng cách kết hợp chữ cái, số và các ký tự đặc biệt. VD: @nh^125& thay vì anh125
- Sử dụng xác thực hai bước (gửi mã OTP qua SMS, tạo mã token...)
- Sử dụng phần mềm diệt virus tại các máy tính trong mạng nội bộ
- Thường xuyên quét mã độc (malware) cho website, server
- Nâng cao hiểu biết của nhân viên về an ninh mạng, đặc biệt là các dấu hiệu nhận biết các file độc hại, keylogger, malware, virus...

3. TẤN CÔNG DOS/DDOS

Các cuộc **tấn công từ chối dịch vụ** (DoS hoặc DDoS) có mục đích chính là ngăn chặn người dùng truy cập vào một dịch vụ nhất định (có thể là website hoặc hệ thống mạng của doanh nghiệp). Để thực hiện được điều này, tin tặc tạo những luồng traffic và dữ liệu khổng lồ nhắm vào các hệ thống của nạn nhân, gây quá tải hệ thống. Khi đó người dùng bình thường sẽ gặp hiện tượng chậm, lag giật, hay không thể truy cập. Loại hình tấn công này đặc biệt gây hại cho các doanh nghiệp TMĐT, bán lẻ trực tuyến, Tài chính - ngân hàng, ví điện tử.

GIẢI PHÁP

Hiện nay, không có cách nào phòng tránh được 100% tấn công DDoS. Tuy nhiên, doanh nghiệp có thể hạn chế bị tấn công và giảm thiểu thiệt hại bằng cách sau:

- Sử dụng tường lửa website (WAF) để ngăn chặn traffic độc hại
- Sử dụng giải pháp giảm thiểu DDoS để hứng luồng traffic độc hại thay cho website
- Sử dụng công cụ giám sát & cảnh báo sự cố Website để phát hiện và xử lí kịp thời

Xem ngay: ***6 mẹo để chống lại tấn công DDoS***

4. MÃ ĐỘC VÀ VIRUS

Mã độc (**malware**) là vấn nạn "thế kỷ" đã gây vô số thiệt hại cho nền kinh tế toàn cầu. Chúng là những chương trình, đoạn mã độc hại được lập trình để tấn công người dùng. Có vô vàn các loại mã độc khác nhau, tuy nhiên phổ biến nhất vẫn là virus, trojan, ransomware, adware, hay gần đây nhất là cryto-miner (mã độc đào tiền ảo).

Hậu quả do malware gây ra cũng vô cùng đa dạng: từ việc mở file chậm, máy tính chạy chậm, tới việc bị mất password, bị khóa file đòi tiền chuộc, hiển thị quảng cáo, mất dữ liệu quan trọng, hoặc máy tính trở thành công cụ đào tiền ảo của hacker...

GIẢI PHÁP

- Sử dụng một phần mềm diệt virus/malware bản trả phí để đạt hiệu quả cao nhất. Tuyệt đối không sử dụng crack
- Cẩn trọng với các thiết bị ngoại vi: USB, CD, ổ cứng,... Đảm bảo các thiết bị được quét Virus trước khi kết nối với máy tính doanh nghiệp
- Đào tạo kiến thức an ninh mạng cho nhân viên: cách nhận biết tấn công Phishing, file nguy hiểm, email giả mạo, thận trọng khi lướt web,...

Xem ngay: ***Bảo mật Website A - Z: Từ chiến lược đến thực thi***

5. TẤN CÔNG GIẢ MẠO PHISHING

Phishing (hay tấn công giả mạo) là hành vi giả dạng thành một cá nhân hay đơn vị tin cậy (gmail, ngân hàng, cổng thanh toán...) nhằm đánh lừa người dùng. Nạn nhân của phishing thường tự giác cung cấp các thông tin mà Phisher nhắm tới mà không hề nghi ngờ: thẻ tín dụng, mật khẩu thanh toán, các thông tin nội bộ doanh nghiệp... Đôi khi, kẻ tấn công lợi dụng hình thức này để lây nhiễm malware vào thiết bị của nạn nhân, gây nhiều hậu quả khôn lường.

Ở Việt Nam, rất nhiều tổ chức đã trở thành nạn nhân của hình thức tấn công này như Bkav (2011), VCCorp (2014), Bộ tài nguyên và môi trường (2014), VNG (2015), Vietnam Airline (2016).

GIẢI PHÁP

Để giải giảm thiểu rủi ro từ các cuộc tấn công lừa đảo, doanh nghiệp cần thực hiện 3 việc chính như sau:

- Triển khai các chương trình đào tạo về nhận thức cho nhân viên, đặc biệt là cấp bậc quản lý - những người có vai trò quan trọng nhất định đối với các doanh nghiệp
- Luôn cẩn trọng khi thực hiện các giao dịch trực tuyến, kiểm tra kỹ các email nhận được: tên người gửi, tổ chức của người gửi đã đúng chưa, link có an toàn không...
- Kết hợp triển khai các giải pháp phòng chống mã độc dựa trên công nghệ AI, đây là giải pháp tốt nhất dựa trên việc phát hiện các hành vi bất thường

Chi tiết: ***Phishing là gì? Giải pháp chống phishing hiệu quả***

6. MÃ ĐỘC TỐNG TIỀN (RANSOMWARE)

Mã độc tống tiền (Ransomware) là một loại phần mềm độc hại được tin tặc sử dụng nhằm mục đích mã hóa hoặc đánh cắp dữ liệu của người dùng, và sử dụng chính dữ liệu đó để tống tiền các nạn nhân. Thông thường là qua các mạng tiền ảo như Bitcoin hay Ethereum.

Hiện nay các mã độc tống tiền đã chuyển sang sử dụng những thuật toán mã hóa bậc cao, khiến quá trình phục hồi dữ liệu vô cùng khó khăn và gần như là không thể nếu không có khóa giải mã do tin tặc cung cấp. Tin tặc sử dụng các kênh thanh toán ẩn danh qua các loại tiền ảo khiến cho việc truy tìm kẻ chủ mưu gần như không thể thực hiện.

Các lĩnh vực thiệt hại nặng nề khi bị tấn công ransomware: chăm sóc sức khỏe, tài chính & ngân hàng, thương mại điện tử...

GIẢI PHÁP

Để phòng chống mã độc tống tiền, doanh nghiệp cần kết hợp đồng thời nhiều phương pháp:

- Cài đặt các phần mềm Antivirus/Anti-malware hoặc các giải pháp Endpoint Security tiên tiến
- Liên tục nâng cấp và cập nhật các phiên bản, bản vá mới nhất của các phần mềm đang sử dụng, đặc biệt là hệ điều hành Windows, office, phần mềm kế toán
- Ưu tiên lưu trữ các dữ liệu quan trọng trên các hệ thống cloud (Google Drive, Dropbox, Onedrive...)
- Đào tạo nhân viên về việc sử dụng máy tính, mạng xã hội, email và duyệt web để tránh bị lây nhiễm các loại mã độc nguy hiểm này
- Sử dụng các giải pháp phát hiện và ngăn chặn mã độc tiên tiến dựa trên trí tuệ nhân tạo và được quản lý tập trung

7. THIẾT BỊ IOT KHÔNG AN TOÀN

The Internet of Things - IoT là mạng lưới bao gồm tất cả mọi vật dụng, thiết bị có kết nối với internet nhằm phục vụ con người tốt hơn. Một vài thiết bị IoT phổ biến: camera an ninh, router Internet, loa thông minh, hệ thống định vị trên xe và các thiết bị y tế hiện đại... Chính khả năng kết nối và điều khiển từ xa thông minh của các thiết bị IoT đã mở ra một con đường mới để tin tặc chiếm đoạt các thông tin nhạy cảm của cá nhân và doanh nghiệp.

Các điểm yếu phổ biến về bảo mật của các hệ thống IoT đang được sử dụng gồm có: lỏng lẻo trong quy trình xác thực (sử dụng thông tin đăng nhập mặc định), truyền tải thông tin không mã hóa, các lỗ hổng SQL Injection và sự sơ suất của nhà cung cấp trong việc xác minh và mã hóa bản cập nhật phần mềm. Dựa vào việc lợi dụng các điểm yếu này, tin tặc có thể dễ dàng chiếm đoạt dữ liệu cá nhân, thông tin đăng nhập và cài đặt mã độc vào hệ thống của thiết bị.

GIẢI PHÁP

Đối với doanh nghiệp, quá trình đánh giá và lựa chọn đơn vị cung cấp thiết bị là một trong những yếu tố quan trọng nhất cần cân nhắc để đảm bảo tính bảo mật cho hệ thống IoT nội bộ. Các chủ doanh nghiệp cần chắc chắn đối tác có thể đáp ứng các yêu cầu về bảo mật và có các hình thức hỗ trợ để khắc phục ngay các vấn đề bảo mật thiết bị có thể xuất hiện trong quá trình vận hành.

Ngoài ra, đơn vị cần tự thực hiện kiểm tra, đánh giá bảo mật thiết bị với các bước cơ bản sau:

- Không sử dụng các thiết bị không hỗ trợ nâng cấp phần mềm, firmware hoặc thay đổi mật khẩu
- Thay tên đăng nhập mặc định và mật khẩu trước khi kết nối thiết bị vào mạng Internet
- Mật khẩu sử dụng trên mỗi thiết bị IoT đều phải là duy nhất, đặc biệt đối với các thiết bị có kết nối Internet trực tiếp
- Luôn luôn cài đặt bản vá mới nhất cho các thiết bị này thông qua việc cập nhật phần mềm và firmware để giảm thiểu nguy cơ thiết bị bị tấn công
- Kiểm tra tính bảo mật và chính sách sử dụng dữ liệu của ứng dụng (application) được sử dụng để điều khiển thiết bị
- Cài đặt hệ thống thiết bị IoT trên một mạng riêng, thiết lập tường lửa (Firewall) và liên tục theo dõi để phát hiện các dấu hiệu bất thường
- Tắt thiết bị hoặc tính năng của thiết bị khi không sử dụng đến

8. BYOD (BRING YOUR OWN DEVICE)

Sử dụng thiết bị cá nhân, hay Bring your own device (BYOD) là chính sách đang được áp dụng tại nhiều doanh nghiệp hiện nay. Các doanh nghiệp này cho phép nhân viên mang thiết bị công nghệ cá nhân do chính họ sở hữu (laptop, máy tính bảng và điện thoại thông minh) đến chỗ làm và sử dụng chúng để truy cập vào các thông tin và ứng dụng nội bộ của công ty.

Lộ thông tin là bài toán nan giải dành cho các đơn vị áp dụng chính sách BYOD do các thiết bị này không đảm bảo các tiêu chuẩn về bảo mật dữ liệu, gây ra nguy cơ bị rò rỉ thông tin. Rất khó để đảm bảo quyền kiểm soát và truy cập dữ liệu nội bộ khi truyền tải, lưu trữ và xử lý dữ liệu trên thiết bị cá nhân của nhân viên. Xác suất thiết bị bị kẻ xấu đánh cắp và dữ liệu bên trong bị lợi dụng cũng rất cao so với các doanh nghiệp không áp dụng chính sách này.

Ngoài ra, các thiết bị cá nhân có nguy cơ bị lây nhiễm mã độc cao hơn do không thể kiểm soát các mạng mà thiết bị được kết nối: mạng gia đình, mạng wifi công cộng,... Khi một nhân viên kết nối với mạng wifi công cộng, thông tin nội bộ có nguy cơ bị lộ do tin tặc tấn công man-in-the-middle hoặc bị theo dõi.

GIẢI PHÁP

Các tổ chức áp dụng chính sách BYOD cần đảm bảo quy trình bảo mật bắt buộc đối với các thiết bị có thực hiện kết nối vào hạ tầng mạng và truy cập các thông tin nhạy cảm của công ty. Chính sách BYOD cần đi kèm với các điều khoản để đảm bảo:

- Thiết bị được sử dụng được cập nhật các bản vá bảo mật liên tục để hạn chế tin tặc tấn công thiết bị thông qua các lỗ hổng mới được công bố
- Áp dụng các hình thức bảo mật thông tin như quản trị thiết bị di động (MDM), app virtualization và containerization
- Hạn chế IP truy cập: chỉ cấp quyền truy cập vào trang quản trị cho địa chỉ IP ở công ty. Như vậy, nhân viên sẽ không thể truy cập vào trang quản trị từ xa
- Phân quyền truy cập dữ liệu rõ ràng, đúng mục đích. Mỗi chức vụ khác nhau cần truy cập những loại dữ liệu khác nhau. Tránh cấp quyền truy cập dữ liệu nhạy cảm khi không cần thiết

9. RÒ RỈ DỮ LIỆU (DATA BREACH)

Rò rỉ dữ liệu (data breach) xảy ra khi dữ liệu nhạy cảm, thông tin mật và các loại dữ liệu cần được bảo vệ khác của doanh nghiệp bị sao chép, truy cập hoặc sử dụng bởi các cá nhân và tổ chức bên ngoài. Những thông tin nhạy cảm thường xuyên bị nhắm tới gồm thông tin thẻ tín dụng, thông tin y tế (PHI), thông tin cá nhân, bí mật kinh doanh và tài sản trí tuệ.

Xem chi tiết: ***Lộ thông tin khách hàng, doanh nghiệp chịu hậu quả gì?***

Tội phạm mạng thường tìm kiếm các lỗ hổng bảo mật trong hệ thống lưu trữ thông tin của doanh nghiệp, qua đó chiếm quyền kiểm soát, điều chỉnh, copy dữ liệu. Những ngành bị ảnh hưởng nặng nề nhất bao gồm: y tế & chăm sóc sức khỏe, tài chính - ngân hàng, thương mại điện tử, bán lẻ trực tuyến, phần mềm...

GIẢI PHÁP

Để chống lại các cuộc tấn công vi phạm dữ liệu, doanh nghiệp cần xây dựng một chiến lược bảo mật thông tin tổng thể thay vì trông chờ vào một công cụ “toàn năng” nào đó. Tham khảo các bước sau đây:

- Xây dựng chính sách bảo mật thông tin
- Bảo mật hệ thống website
- Bảo mật hệ thống CRM
- Bảo mật máy chủ & hệ thống đám mây
- Nâng cao kiến thức an ninh mạng cho nhân viên

Tham khảo: ***Giải pháp bảo mật thông tin cho doanh nghiệp***

10. TẤN CÔNG CHUỖI CUNG ỨNG

Tấn công chuỗi cung ứng (supply chain attack) là một hình thức phổ biến, thường xảy ra với các doanh nghiệp có nhiều nhà cung cấp (third-party providers/ vendors) khác nhau. Khi tin tặc không thể tấn công doanh nghiệp một cách trực tiếp, chúng sẽ tấn công các nhà cung cấp này để làm cầu nối, gián tiếp tấn công doanh nghiệp. Tấn công chuỗi cung ứng gây ra không ít rắc rối và thiệt hại cho doanh nghiệp, từ rò rỉ dữ liệu tới những hậu quả nặng nề hơn như hoạt động kinh doanh bị ngưng trệ.

Các ngành dễ bị tấn công chuỗi cung ứng: công nghiệp sản xuất, gia công sản phẩm, cung cấp phần cứng, phần mềm, nhà cung cấp đám mây... hoặc bất kỳ doanh nghiệp nào có nhiều đối tác cung cấp các thành phần trong cấu tạo sản phẩm.

GIẢI PHÁP

- Lựa chọn các vendors một cách kỹ càng, ưu tiên những vendors có uy tín trong ngành
- Quy định rõ các điều khoản bảo mật thông tin trong hợp đồng hoặc phụ lục
- Sử dụng những sản phẩm an ninh mạng giúp phát hiện hành vi bất thường xảy ra với dữ liệu doanh nghiệp (anomaly detection)

Đọc thêm về: ***Tấn công chuỗi cung ứng***

11. RỦI RO TỪ NHÂN VIÊN

Cho dù có thực hiện các biện pháp chống lại tin tặc thế nào, thì doanh nghiệp vẫn khó có thể an toàn nếu như bị chính nhân viên trong nội bộ đánh cắp dữ liệu. Đặc biệt là các nhân viên có vai trò quan trọng, có thể can thiệp trực tiếp vào cơ sở dữ liệu, hệ thống công nghệ thông tin, dữ liệu và các tài sản số khác của doanh nghiệp.

GIẢI PHÁP

Để giảm thiểu các rủi ro này, các chủ doanh nghiệp nên thực hiện đồng thời các phương án sau đây:

- Triển khai các bộ quy định, chính sách, yêu cầu cam kết về bảo mật dữ liệu, cam kết không tiết lộ và những ràng buộc khác về mặt pháp lý đối với nhân viên của công ty
- Lưu ý về việc phân quyền trong công ty đổi với các dữ liệu nhạy cảm, tài sản của công ty khi sử dụng các hệ thống tập trung hoặc các hệ thống quản lý dữ liệu trực tuyến
- Xây dựng văn hóa để nhân viên gắn bó và trung thực với công ty, với lý tưởng và tầm nhìn của doanh nghiệp, đặc biệt là đội ngũ quản lý và nhân viên quản trị hệ thống
- Triển khai các giải pháp giám sát đối với các dữ liệu quan trọng và để phát hiện các hành vi bất thường trong hệ thống. Ví dụ triển khai các giải pháp theo dõi các hành vi liên quan đến dữ liệu khách hàng (có thể lưu trữ trong CSDL, các phần mềm CRM, ERP...), hệ thống này có thể phát hiện sớm các hành vi truy xuất số lượng lớn dữ liệu khách hàng hay các hành vi chỉnh sửa bất thường

III. LỜI KẾT

Trên đây là một số rủi ro bảo mật phổ biến mà các doanh nghiệp Việt đang phải đối mặt. Trong thực tế, tùy từng tình hình cụ thể mà mỗi doanh nghiệp có thể gặp **một hay nhiều** trong số các vấn đề trên. Điều đó phụ thuộc vào mô hình kinh doanh, hệ thống Công nghệ thông tin, hệ thống vận hành, phương tiện lưu trữ của mỗi doanh nghiệp. Ví dụ, những công ty Thương Mại Điện Tử sẽ đặc biệt nhạy cảm với tấn công D-DOS, trong khi đối với các công ty kinh doanh offline thì việc website bị "hack" không phải vấn đề nghiêm trọng.

> *Doanh nghiệp cần xây dựng chiến lược bảo mật tổng thể để giảm thiểu rủi ro bảo mật*

Để giảm thiểu các rủi ro bảo mật này, mỗi doanh nghiệp cần xây dựng một **chiến lược bảo mật tổng thể** phù hợp với những đặc thù riêng của mình. Chiến lược phải bao gồm các bước: đánh giá an ninh mạng - đề xuất giải pháp - các công cụ sẽ sử dụng - chi phí thực hiện. Quan trọng nhất là cải thiện nhận thức của nhân viên đối với các rủi ro an ninh mạng thông qua các buổi training, đào tạo online - offline. Bằng cách này, doanh nghiệp sẽ tiết kiệm được nhiều chi phí mà vẫn đạt được hiệu quả cao trong vấn đề bảo mật của mình.

VỀ CYSTACK

CyStack là công ty đi đầu trong việc ứng dụng công nghệ vào giải quyết bài toán an ninh mạng doanh nghiệp. Chúng tôi tập trung vào 3 vấn đề chính mà các doanh nghiệp gặp phải:

- Chống tấn công mạng (Cyber-attack defense)
- Bảo vệ dữ liệu (Data protection)
- Phòng ngừa rủi ro từ bên trong (inside-threats prevention)

Với công nghệ trí thông minh nhân tạo AI & Bảo Mật Cộng Đồng, nền tảng CyStack Platform giúp giải quyết triệt để bài toán trên bằng các sản phẩm phù hợp với nhu cầu riêng của từng doanh nghiệp:

- **CyStack WhiteHub:** Giải pháp **Pentest** thế hệ mới - kết nối doanh nghiệp với cộng đồng 500+ nhà nghiên cứu (pentesters & hacker mũ trắng) để tìm lỗ hổng bảo mật trong sản phẩm (website, mobile app, IoT). Ứng dụng phương pháp Bảo Mật Cộng Đồng (Crowdsourced Security).
- **CyStack WebShield:** Giải pháp **Bảo mật website** tự động & không cần cài đặt. WebShield giúp người quản trị web thoát khỏi nỗi lo website bị tấn công bằng 4 công cụ mạnh mẽ: Tường lửa - Quét mã độc - Tìm lỗ hổng bảo mật web - Giám sát 24/7.
- **CyStack SaaS:** Giải pháp **Bảo vệ dữ liệu trên mây** với trí thông minh AI. Bằng cách phân tích những hành vi truy xuất dữ liệu bất thường, CyStack SaaS giúp chủ doanh nghiệp phát hiện và ngăn chặn các rủi ro thất thoát dữ liệu từ bên trong. Phần mềm hỗ trợ tích hợp API vào các dịch vụ SaaS như: G-suite, Office 365, Salesforce...
- **CyStack Server:** Giải pháp **Bảo vệ dữ liệu trong máy chủ** với trí thông minh AI.
- **CyStack Enterprise:** Giải pháp **Bảo vệ dữ liệu trong PC và LAN** với trí thông minh AI.

LIÊN HỆ

CTCP An ninh mạng CyStack Việt Nam - CyStack., JSC

Địa chỉ: Bigwin Tower, Số 23 Lê Văn Lương, phường Nhân Chính, quận Thanh Xuân, Hà Nội.

Email: contact@cystack.net

Hotline: (+84) 247 109 9656

Website: **https://cystack.net**