CyStack

Tổng quan về Crowdsourced Security

Giải pháp Bảo Mật Cộng Đồng và những điều cần biết để triển khai.

MỤC LỤC

Lời mở đầu

Áp lực về tốc độ và tính cạnh tranh gay gắt trong thời đại hiện nay đã buộc doanh nghiệp phải liên tục thay đổi. Vòng đời phát triển sản phẩm đang rút ngắn lại, quy trình phát triển vì vậy cũng cần phải đảm bảo tính linh hoạt trong khi vẫn đòi hỏi chất lượng không đổi.

Trước tình hình đó, một trong những yếu tố khó để duy trì chất lượng nhất chính là tính bảo mật. Chỉ tính riêng năm 2018, nhiều bê bối đã lần lượt xảy ra trong lĩnh vực an toàn thông tin đối với những đơn vị công nghệ lớn trên thế giới như Google, Facebook, Quora. Tại Việt Nam, những tin tức liên quan đến rò rỉ dữ liệu khách hàng của chuỗi cửa hàng bán lẻ Thế Giới Di Động và FPT Shop cũng khiến nhiều doanh nghiệp lo ngại về tình hình an ninh mạng.

Để bảo vệ doanh nghiệp khỏi các rủi ro về bảo mật, một trong các giải pháp tiên tiến nhất đang được áp dụng trong lĩnh vực bảo mật là Crowdsourced Security (Bảo mật dựa trên tiềm lực cộng đồng). Với hiệu quả vượt trội do tận dụng được năng lực của nhiều nhà nghiên cứu độc lập, giải pháp này đã được tin tưởng và áp dụng bởi các công ty công nghệ hàng đầu trên thế giới như Google, Facebook, Paypal, Uber hay Tesla - hứa hẹn xu hướng tất yếu trong lĩnh vực an ninh mạng trên thế giới cũng như tại Việt Nam.

Là những chuyên gia bảo mật tâm huyết, chúng tôi cùng chung một khát vọng, đó là áp dụng những công nghệ tiên tiến nhất về bảo mật & an ninh mạng vào phục vụ cho các doanh nghiệp Việt, từ đó tạo ra môi trường kinh doanh lành mạnh, trong sạch và công bằng - giúp cải thiện thứ hạng của nền kinh tế Việt trên bản đồ Năm châu. Một trong những giải pháp tiên tiến mà chúng tôi cho rằng sẽ làm thay đổi bộ mặt an ninh mạng quốc gia, chính là Bảo Mật Cộng Đồng. Cuốn sách sẽ tập trung trả lời những câu hỏi sau:

- Crowdsourced Security (Bảo Mật Cộng Đồng) là gì?
- Tại sao cần Bảo Mật Cộng Đồng?
- Bảo Mật Cộng Đồng có lợi thế gì so với các phương pháp bảo mật khác?
- Làm sao để ứng dụng phương pháp Bảo Mật Cộng Đồng cho doanh nghiệp?

Hy vọng tài liệu này sẽ giúp bạn có cái nhìn toàn diện về phương pháp Crowdsourced Security. Từ đó đưa ra những chiến thuật bảo mật hợp lí cho doanh nghiệp của mình.

Trân trọng,
WhiteHub Team

Thực trạng An toàn thông tin

An toàn thông tin là bài toán vô cùng phức tạp mà mọi doanh nghiệp đều phải đối mặt. Ngay cả những công ty công nghệ hàng đầu thế giới cũng không thể tránh khỏi gặp phải những bê bối bảo mật vô cùng nghiêm trọng trong năm 2018 vừa qua:

87 triệu
người dùng Facebook bị lộ thông tin

53 triệu
người dùng Google+ bị rò rỉ dữ liệu

10.220
cuộc tấn công mạng vào các hệ thống thông tin tại Việt Nam*

(*Theo thống kê của Trung tâm Giám sát an toàn không gian mạng quốc gia)

Ngoài ra, những tin đồn về rò rỉ dữ liệu liên quan đến các đơn vị thương mại điện tử lớn như: Thế Giới Di Động, FPTShop và Con Cưng đã gây thiệt hại hàng trăm tỉ đồng cũng như suy giảm uy tín đối với người dùng.

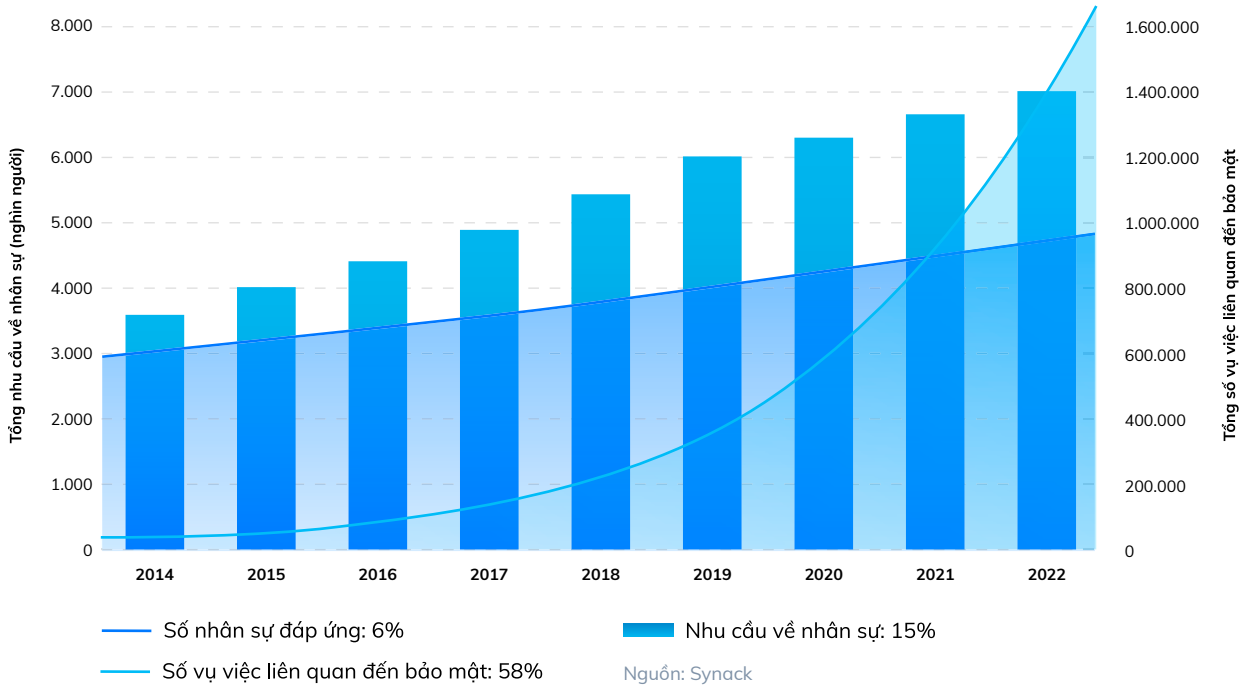
Những nguyên nhân

Dù sở hữu đội ngũ bảo mật riêng hay đã sử dụng dịch vụ kiểm thử của một đơn vị bên ngoài, rất nhiều hệ thống của doanh nghiệp vẫn trở thành nạn nhân của tin tặc. Trước tình hình đó, câu hỏi được đặt ra là: Có những nguyên nhân nào khiến cho các doanh nghiệp ngày càng đối diện nhiều nguy cơ mất an toàn thông tin mạng trong thời đại ngày nay?

Trên thực tế, có nhiều nguyên nhân dẫn tới việc một hệ thống bị tin tặc tấn công. Tuy nhiên, 2 lí do cơ bản nhất giải thích cho tình trạng trên là bài toán về nhân lực và động lực.

1. Thiếu hụt nhân lực có trình độ cao trong ngành an toàn thông tin

Biểu đồ so sánh mức tăng trưởng hàng năm giữa nhu cầu nhân sự, số lượng nhân sự đáp ứng và số cuộc tấn công mạng có chủ đích



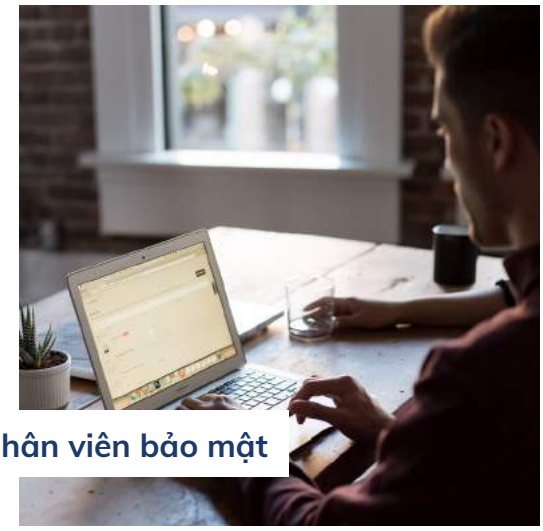
Nguồn: Synack

Theo khảo sát của PwC và Cybersecurity Ventures thực hiện, số lượng các vụ tấn công mạng sẽ tăng hơn 50% trong năm 2019, trong khi số lượng nhân sự bảo mật có trình độ cao chỉ tăng 6%. Với mức tăng trưởng này, số lao động chất lượng cao trong ngành bảo mật sẽ không đủ để đáp ứng nhu cầu về bảo mật của các doanh nghiệp hiện nay.

Trước tình hình đó, các doanh nghiệp đang phải đối diện bài toán khó khăn: làm thế nào để tiếp cận được với các chuyên gia bảo mật có năng lực nhằm tăng cường tính bảo mật cho hệ thống và sản phẩm của công ty. Để giải quyết vấn đề này, rất cần có một giải pháp thực sự hiệu quả với chi phí phù hợp để doanh nghiệp ở mọi giai đoạn phát triển đều có thể sử dụng.

2. Động cơ hành động: Tin tặc vs Nhân viên bảo mật

So với các lực lượng bảo mật truyền thống, tin tặc có động cơ hành động mạnh mẽ và cách tiếp cận tự do hơn, tạo điều kiện cho sức sáng tạo:

	 **Tin tặc**	 **Nhân viên bảo mật**
Động cơ chính	Tại sao tin tặc tấn công? • Sở thích phá hoại • Thử thách/thể hiện bản thân • Thể hiện quan điểm cá nhân (tôn giáo, chính trị, etc.) • Tiền ...	Tại sao nhân viên bảo mật bảo vệ hệ thống website? • Được trả lương
Cách thực hiện	Liên tục tìm kiếm những lỗ hổng bảo mật nguy hiểm	Chạy những phần mềm, ứng dụng được lập trình tự động
Mục tiêu cuối cùng	Phá hoại hoặc xâm nhập sâu vào hệ thống	Đảm bảo an toàn cho toàn bộ hệ thống
Thành quả	Hưởng lợi tùy theo kết quả của quá trình tấn công	Hưởng lương cố định theo thời gian làm việc

Bảng so sánh trên cho thấy rõ ràng sự khác biệt trong động cơ hành động của tin tặc so với các lực lượng bảo mật. Nếu như tin tặc phải tấn công thành công vào hệ thống mới có cơ hội kiếm lời, thì hầu như mức lương thưởng dành cho nhân sự bảo mật đều được quyết định từ trước. Việc này không thể thúc đẩy các chuyên gia bảo mật đạt được hiệu suất cao nhất, cũng như tạo ra điều kiện để một vài cá nhân hay đơn vị có các hành vi thiếu trách nhiệm trong công việc.

Không chỉ vậy, mục tiêu cuối cùng giữa hoạt động của tin tặc và các lực lượng bảo mật cũng hoàn toàn khác biệt. Tin tặc có thể thoải mái sáng tạo nhằm tìm ra các lỗ hổng nghiêm trọng và chiếm đoạt hệ thống, do đó có thể liên tục tìm ra nhiều hướng tấn công ngày một khó đoán. Trong khi đó, các lực lượng bảo mật có xu hướng tuân thủ theo các khung tiêu chuẩn truyền thống về bảo mật và dựa vào các giải pháp công nghệ để tiết kiệm thời gian - vốn không thể so sánh với sức sáng tạo của con người, đặc biệt trong lĩnh vực bảo mật.

> *Trong bối cảnh thiếu nguồn nhân lực có trình độ chuyên sâu và chênh lệch trong động cơ làm việc giữa đội ngũ bảo mật truyền thống và tin tặc, Crowdsourced Security ra đời nhằm giải quyết bài toán hóc búa về an toàn thông tin mà các doanh nghiệp hiện nay đang phải đối mặt.*

Crowdsourced Security là gì?

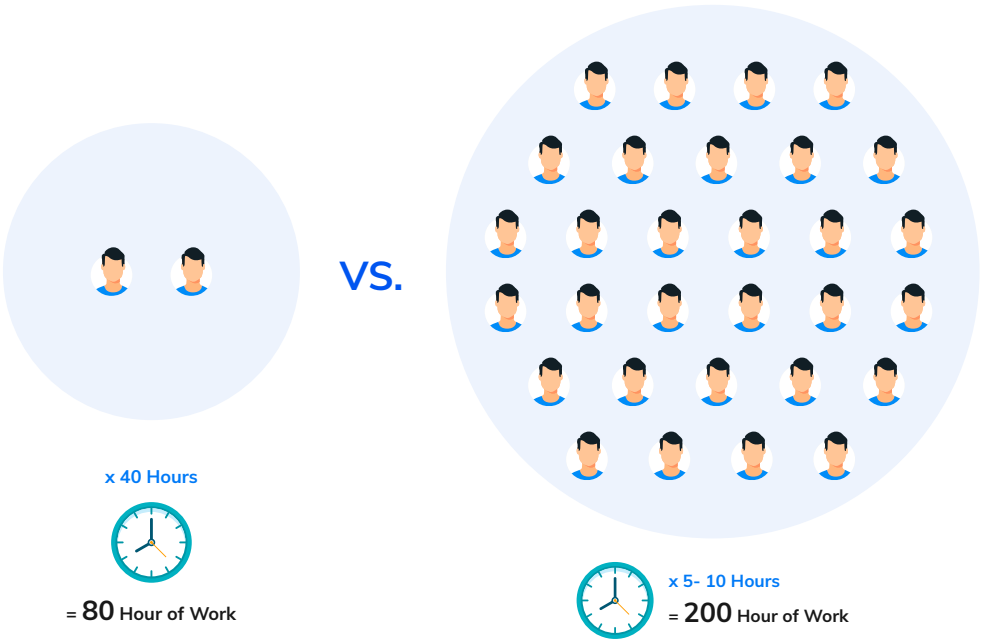
Crowdsourced Security (Bảo Mật Cộng Đồng) là phương pháp bảo mật tận dụng nguồn lực của cộng đồng các nhà nghiên cứu bảo mật độc lập và hacker mũ trắng để tăng cường bảo mật cho các sản phẩm của doanh nghiệp.

Không phải 1, 2 hay 3, mà là hàng trăm nhân lực có trình độ chuyên môn cao sẽ thực hiện kiểm thử xâm nhập (pentesting) vào sản phẩm ứng dụng web hoặc mobile app của doanh nghiệp. Từ đó tìm ra những điểm yếu bảo mật của ứng dụng và thông báo lại để doanh nghiệp kịp thời khắc phục.

Một cách tự nhiên, Crowdsourced Security đã giải quyết được bài toán về động lực sáng tạo trong vấn đề bảo mật của doanh nghiệp. Bằng cách hợp tác với một nhóm hacker mũ trắng, doanh nghiệp có thể tận dụng nguồn lực dồi dào, phù hợp với từng tình hình cụ thể và giai đoạn phát triển riêng.

Ưu điểm của Crowdsourced Security

1. Sức mạnh đám đông



Pentest truyền thống **Crowdsourced Security**

Sự độc đáo của phương pháp Crowdsourced Security nằm ở việc tận dụng sức mạnh số đông. Nếu sử dụng phương pháp bảo mật truyền thống, một doanh nghiệp sẽ có từ 2-4 nhân sự thực hiện các biện pháp bảo mật. Trong khi đó, số chuyên gia cùng dò tìm lỗ hổng có thể tăng lên tới hàng trăm người nếu doanh nghiệp chọn phương pháp Crowdsourced Security.

2. Hiệu quả bảo mật tối đa

Việc tìm kiếm lỗ hổng bảo mật cần sự đa dạng trong kinh nghiệm, kiến thức, tư duy. Do đó, 100 chuyên gia cùng tham gia bảo mật sẽ hiệu quả hơn 2-5 người.

3. Tiết kiệm thời gian, chi phí

Nhờ nguồn lực dồi dào, phương pháp Crowdsources Security giúp doanh nghiệp tìm kiếm lỗ hổng nhanh hơn & tiết kiệm chi phí nhân sự.

Những lầm tưởng về phương pháp Crowdsourced Security

Đối với nhiều doanh nghiệp, Crowdsourced Security vẫn còn là một khái niệm tương đối mới mẻ. Đó là lý do dẫn tới một số hiểu lầm đáng tiếc và nhiều đơn vị vẫn chưa thể đưa vào triển khai hình thức bảo mật tiên tiến này.

Một trong những hiểu lầm thường thấy là: **Có khi nào chính những chuyên gia tìm lỗ hổng bảo mật sẽ "khai thác" nó thay vì báo cáo lại cho doanh nghiệp không?**

Để trả lời cho vấn đề này, chúng ta hãy phân tích 2 khía cạnh: chủ quan và khách quan.

1. Sự khác biệt về tư duy

Về khía cạnh chủ quan, tồn tại sự khác nhau rất lớn về tư duy (mindset) giữa tin tặc (hacker mũ đen) và các nhà nghiên cứu bảo mật độc lập (hacker mũ trắng)

Tin tặc

- Lấy phá hoại làm niềm vui
- Coi thường luật pháp
- Muốn được nổi tiếng (infamous)
- Cần rất nhiều tiền để sống xa hoa

Nhà nghiên cứu bảo mật độc lập

- Mong muốn giúp đỡ
- Tôn trọng luật pháp
- Thầm lặng đóng góp cho xã hội
- Cần sự động viên tinh thần & duy trì cuộc sống

Trong khi cả tin tặc và nhà nghiên cứu bảo mật độc lập đều là những con người hết sức tài năng trong lĩnh vực CNTT, thì vẫn có những sự khác biệt cơ bản về tư duy giữa 2 đối tượng trên.

Tin tặc, những "thiên tài" trong việc xâm nhập vào hệ thống, thường được lớn lên trong sự giáo dục không đầy đủ về đạo đức và có những tư duy lệch lạc. Một số tin tặc cảm thấy thỏa mãn khi "phá hoại" website của các tổ chức lớn, một số khác ăn cắp dữ liệu để tống tiền doanh nghiệp. Cũng chính vì những sở thích quái đản như vậy, họ trở nên nổi tiếng (infamous) và xuất hiện tràn lan trên khắp các mặt báo - điều khiến họ cảm thấy tự mãn.

Những nhà nghiên cứu bảo mật độc lập (hacker mũ trắng) có tài năng không thua kém tin tặc, họ luôn tò mò, học hỏi, trau dồi và cập nhật kiến thức mới nhất. Sự khác biệt nằm ở chỗ, hacker mũ trắng tin vào những giá trị tốt đẹp & việc tôn trọng luật pháp. Họ mong muốn được cống hiến cho xã hội, họ hiểu hành động của mình giúp cho các doanh nghiệp phát triển, tạo động lực cho nền kinh tế đi lên. Việc các doanh nghiệp thưởng nóng cho các hacker mũ trắng khi báo cáo lỗ hổng không còn xa lạ. Điều này giúp tạo động lực cho hacker mũ trắng tiếp tục đóng góp tích cực cho xã hội. Thâm chí, nhiều hacker mũ trắng có thể kiếm sống bằng việc giúp các doanh nghiệp bảo mật sản phẩm của mình.

2. Quản lý nghiêm ngặt

Thông thường, phương pháp Crowdsourced Security yêu cầu một "Chính sách Thông Báo Lỗ Hổng" (đề cập ở phần sau) trong đó quy định nghiêm ngặt về quy trình bảo mật mà các chuyên gia bảo mật phải thực hiện theo. Đồng thời, bên cung cấp dịch vụ Crowdsourced Security sẽ lựa chọn và quản lý hồ sơ chuyên gia chặt chẽ, dưới sự bảo hộ của pháp luật nước sở tại. Đó là lí do khiến cho Crowdsourced Security trở nên an toàn đối với các doanh nghiệp áp dụng.

Ứng dụng phương pháp Crowdsourced Security vào bảo mật doanh nghiệp

Để hiểu rõ các ứng dụng của Crowdsourced Security trong thực tế, trước tiên cần hiểu khái niệm sau:

Thông Báo Lỗ Hổng

Thông Báo Lỗ Hổng (tiếng Anh: Vulnerability Disclosure) là các hình thức mà lỗ hổng bảo mật trên sản phẩm được thông báo tới doanh nghiệp chủ sở hữu hoặc công chúng. Có 4 hình thức Thông Báo Lỗ Hổng:

01 **Tự thông báo (Self-disclosure)**
Chính các tổ chức chủ sở hữu phát hiện ra lỗ hổng bảo mật trên sản phẩm của mình, sau đó gửi thông báo chính thức tới công chúng, đồng thời phát hành bản cập nhật vá lỗi.

02 **Thông báo bởi bên thứ ba (Third-party disclosure)**
Đơn vị thông báo lỗ hổng tới quần chúng không phải là chủ sở hữu của sản phẩm. Thông thường, bên thứ ba ở đây bao gồm các nhà nghiên cứu độc lập, hacker mũ trắng, chuyên gia bảo mật.

03 **Thông báo riêng tư (Vendor disclosure)**
Là khi những nhà nghiên cứu phát hiện ra lỗ hổng bảo mật của sản phẩm và thông báo riêng cho bên phát hành, không public tới công chúng. Theo đó, 2 bên sẽ làm việc tích cực để cho ra bản vá bảo mật.

04 **Thông báo toàn bộ (Full disclosure)**
Lỗ hổng được thông báo trực tiếp, chi tiết tới công chúng ngay khi được phát hiện, thường nhằm mục đích gây sức ép lên nhà phát hành. Trong trường hợp này, uy tín và giá trị của doanh nghiệp sẽ bị ảnh hưởng.

Thông thường, doanh nghiệp nào cũng muốn các lỗ hổng của mình được thông báo dưới dạng Vendor Disclosure - tức là nếu nhà nghiên cứu tìm ra lỗ hổng bảo mật, thì thông báo cho doanh nghiệp đầu tiên thay vì công bố với công chúng. Điều này không những làm giảm thiểu rủi ro bị tin tặc tấn công và khai thác điểm yếu của sản phẩm, mà còn giúp doanh nghiệp giữ vững uy tín với khách hàng và các cổ đông.

Đó là lí do doanh nghiệp nên xây dựng một Chính sách Thông Báo Lỗ Hổng.

Chính sách Thông Báo Lỗ Hổng (Vulnerability Disclosure Policy)

Chính sách Thông báo lỗ hổng (VDP) là cần thiết đối với các doanh nghiệp cung cấp phần mềm, ứng dụng website, mobiles hay các thiết bị IoT. Chính sách này khuyến khích & ràng buộc bên thứ 3 (bao gồm những chuyên gia bảo mật độc lập và hacker) thông báo lỗ hổng cho doanh nghiệp dưới sự bảo hộ của luật pháp. Các điều lệ chi tiết sẽ tùy thuộc vào từng doanh nghiệp với các đặc trưng khác nhau, tuy nhiên đều phải có các thông tin cơ bản sau:

01 **Cam kết bảo mật**

Doanh nghiệp thực hiện VDP cần cam kết tuyệt đối đứng về phía người dùng, coi việc bảo mật cho khách hàng là kim chỉ nam cho mọi hoạt động diễn ra trong khuôn khổ VDP.

02 **Phạm vi thực hiện**

Khoanh vùng phạm vi mà doanh nghiệp muốn thực hiện VDP. VD sản phẩm laptop, điện thoại mới ra mắt, hoặc ứng dụng web hiện tại của doanh nghiệp. Thậm chí là toàn bộ các sản phẩm của doanh nghiệp.

03 **Cam kết với chuyên gia bảo mật**

Việc các chuyên gia bảo mật tự do thực hiện xâm nhập vào website, ứng dụng của doanh nghiệp là trái pháp luật. Vì thế, doanh nghiệp cần bảo đảm an toàn về mặt pháp lí dành cho các chuyên gia trong quá trình tổ chức VDP.

04 **Phương thức thông báo & Quy trình thực hiện**

Doanh nghiệp phải cung cấp 1 phương thức để giao tiếp với các chuyên gia bảo mật và thông báo 1 quy trình rõ ràng.

05 **Hướng dẫn về mức độ ưu tiên**

Doanh nghiệp cần cho các nhà nghiên cứu biết những lỗ hổng hay điểm yếu hệ thống nào là ưu tiên hàng đầu.

Một số các đơn vị đã tổ chức thành công VDP bao gồm: Google, Facebook, Apple, hay Dell inc. Thông thường, để tổ chức thành công VDP, doanh nghiệp cần có danh tiếng trên thế giới hoặc trong khu vực. Điều đó chính là chìa khóa để thu hút thêm nhiều nhà nghiên cứu độc lập, hacker mũ trắng tham gia chương trình. Ngược lại, nếu doanh nghiệp chưa xây dựng được hình ảnh thương hiệu rộng khắp, việc thực hiện chương trình Báo Cáo Lỗ Hổng dường như là vô ích do không thu hút được nhân tài tham gia. Khi đó, tổ chức Chương trình Bug Bounty sẽ là một lựa chọn phù hợp.

Chương trình Bug Bounty

Chương trình Trao Thưởng Tìm Lỗi (Bug Bounty) đang là hình thức Bảo Mật Cộng Đồng được các doanh nghiệp ưa chuộng nhất. Cơ bản, doanh nghiệp sẽ trao phần thưởng (chủ yếu là tiền thưởng, cũng có thể là hiện vật hoặc sự công nhận khác) cho các nhà nghiên cứu độc lập dựa trên các lỗ hổng họ tìm thấy. Nhờ đó, Bug Bounty huy động được một cộng đồng rất lớn các hackers mũ trắng đến từ nhiều nơi để nhanh chóng phát hiện ra các lỗ hổng tồn tại trên nhiều bề mặt tấn công.

Đây là giải pháp vượt trội so với VDP vì tính hấp dẫn và thực tế của nó. Về phía doanh nghiệp, không cần có danh tiếng hay thương hiệu mà vẫn có thể thu hút được nhiều nhà nghiên cứu. Đặc biệt, doanh nghiệp chỉ phải chi 1 khoản phí thưởng cho những lỗ hổng/điểm yếu hệ thống nghiêm trọng.

Chương trình Bug Bounty thường diễn ra dưới 2 hình thức:

Chương trình Bug bounty không công khai

Những chương trình dạng này được thực hiện trong môi trường kiểm thử được kiểm soát chặt chẽ và do các nhà nghiên cứu có kinh nghiệm và năng lực thực hiện. Hầu hết các chương trình này đều cho phép doanh nghiệp kiểm soát số lượng nhà nghiên cứu tham gia cũng như quy mô kiểm thử. Đối với các sản phẩm chưa ra mắt hoặc không công khai, đây sẽ là giải pháp phù hợp nhất.

Chương trình Bug bounty công khai

Công khai chương trình Bug bounty là cách để tăng quy mô chương trình và cơ hội tiếp cận đến các nhà nghiên cứu với nhiều kỹ năng, kinh nghiệm và thế mạnh khác nhau. Đặc biệt, một lợi thế khác mà doanh nghiệp thường không để ý đến là ảnh hưởng về mặt thương hiệu - minh bạch trong chính sách bảo mật là cách các doanh nghiệp hàng đầu trên thế giới tạo uy tín với khách hàng và nhà đầu tư. Tuy nhiên, hình thức này thường chỉ phù hợp với các sản phẩm công khai như website hoặc ứng dụng di động.

Quản lý chương trình Bug Bounty

1. Do doanh nghiệp tự quản lý

Đối với các đơn vị lớn như Facebook hay Google, toàn bộ các chương trình báo cáo lỗ hổng và Bug bounty đều được tự xây dựng và quản lý bởi các đội ngũ chuyên gia bảo mật riêng thuộc nhân sự công ty. Tuy nhiên đối với các doanh nghiệp vừa và nhỏ, việc có một cộng đồng nhà nghiên cứu sẵn sàng tham gia kiểm thử cho doanh nghiệp đó và xây dựng một nền tảng giao tiếp riêng là hết sức phi thực tế.

Lựa chọn thường thấy của các đơn vị này là sử dụng các giải pháp do bên thứ 3 cung cấp. Các giải pháp này được cung cấp dưới hình thức một nền tảng với các tính năng và cộng đồng có sẵn. Doanh nghiệp sẽ có quyền quản lý chương trình của chính công ty mình - tự thực hiện các thao tác đặt hạn mức, mức thưởng, quy mô,... và duy trì giao tiếp hiệu quả với nhà nghiên cứu. Một nền tảng Crowdsourced Security sẽ cung cấp các tính năng chính sau:

Tạo và quản lý chương trình Bug bounty

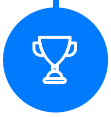
Định nghĩa phạm vi và mức thưởng tùy theo nhu cầu và ngân sách của doanh nghiệp qua từng giai đoạn phát triển

Nhận báo cáo lỗ hổng liên tục từ chuyên gia

Quá trình kiểm thử diễn ra song song với phát triển sản phẩm để kịp thời phát hiện các lỗ hổng mới

Tương tác trực tiếp với các chuyên gia bảo mật

Đảm bảo tính riêng tư và liền mạch cho quá trình liên lạc với các nhà nghiên cứu



Trao thưởng và thống kê chi phí

Theo dõi hiệu quả đầu tư và duy trì mô hình hợp tác bền vững với cộng đồng nhà nghiên cứu

Để tối ưu hiệu quả của quá trình bảo mật - thể hiện qua số lượng những báo cáo được trình bày chi tiết về những lỗ hổng thực sự nguy hại - doanh nghiệp bắt buộc phải bổ nhiệm một đội ngũ bảo mật đủ năng lực để chịu trách nhiệm cho công tác đánh giá báo cáo và khắc phục vấn đề trên sản phẩm.

Giá trị mang lại của Crowdsourced Security sẽ không đáng kể nếu hoạt động quản lý không tối ưu được 3 yếu tố sau cho chương trình: **dễ tiếp cận, bảo mật và tiết kiệm**. Để đạt được 3 yếu tố đó, đội ngũ quản lý cần đáp ứng được những tiêu chuẩn sau:

01 **Năng lực chuyên môn trong lĩnh vực bảo mật**

Công tác đánh giá lỗ hổng do các nhà nghiên cứu độc lập báo cáo đòi hỏi rất nhiều kĩ năng và kinh nghiệm. Khả năng tái hiện các lỗ hổng phức tạp trên nhiều nền tảng và hệ thống là điều kiện cần đối với mọi đội ngũ quản lý.

02 **Kỹ năng giao tiếp với nhà nghiên cứu**

Việc báo cáo lỗ hổng được trình bày hiệu quả hay không phụ thuộc hoàn toàn vào tiêu chuẩn cá nhân của mỗi nhà nghiên cứu. Do đó, việc áp dụng Crowdsourced Security hiệu quả hay không phụ thuộc rất lớn vào cách doanh nghiệp trao đổi thông tin hai chiều với các thành viên của cộng đồng bảo mật.

03 **Khả năng điều phối và tính nhẫn nại**

Không phải mọi chương trình Crowdsourced Security đều thu hút những nhà nghiên cứu xuất sắc và không phải tất cả các bản báo cáo đều đáng tin cậy. Kiên nhẫn sàng lọc và khéo léo tạo động lực cho các nhà nghiên cứu là trách nhiệm của đội ngũ quản lý.

Để tiếp cận với Crowdsourced Security một cách đơn giản hơn, nhiều doanh nghiệp đã và đang chuyển sang lựa chọn các giải pháp được vận hành hoàn toàn bởi một đơn vị bên ngoài.

2. Do đơn vị cung cấp quản lý

Cốt lõi của các chương trình này hoàn toàn tương đồng với các chương trình do doanh nghiệp tự quản lý, do đó cũng tận dụng được các lợi thế của Crowdsourced Security so với kiểm thử bảo mật truyền thống như: Tối ưu ROI thông qua mô hình trả phí dựa trên kết quả đầu ra; tăng chất lượng kiểm thử bằng cách tạo ra động lực sáng tạo cho các nhà nghiên cứu; tích hợp dễ dàng vào vòng đời phát triển sản phẩm;...

Không chỉ thế, các giải pháp được quản lý bởi đơn vị cung cấp còn giải quyết được nhiều vấn đề vô cùng khó khăn cho doanh nghiệp gồm có:

01 **Không có nhân sự bảo mật**

Đơn vị cung cấp có thể trực tiếp làm việc cùng doanh nghiệp và nhà nghiên cứu nhằm đảm bảo giao tiếp thông suốt giữa hai bên, đồng thời xác minh chất lượng của các báo cáo lỗ hổng được gửi về.

02 **Giao tiếp với nhà nghiên cứu không hiệu quả**

Bất kỳ sự gián đoạn nào, dù do phía doanh nghiệp hay nhà nghiên cứu, đều có thể ảnh hưởng đến kết quả của chương trình Bug bounty. Đơn vị cung cấp sẽ nhận trách nhiệm duy trì giao tiếp liên lạc giữa các bên liên quan cũng như đảm bảo các bên nhận đầy đủ, chính xác thông tin để quá trình kiểm thử diễn ra thuận lợi.

03 **Tối ưu chi phí**

Sử dụng các dữ liệu thu thập được trong quá trình vận hành, đơn vị cung cấp sẽ có thể đưa ra các mức thưởng phù hợp nhất cho chương trình Bug bounty để doanh nghiệp ở mọi giai đoạn phát triển đều có thể áp dụng Crowdsourced Security và đạt hiệu quả cao.

Bắt đầu với WhiteHub

Tại Việt Nam, WhiteHub đang là đơn vị đầu tiên cung cấp giải pháp Crowdsourced Security dành cho doanh nghiệp tại địa chỉ: whitehub.net
Những thông số nổi bật của WhiteHub gồm có

20	500+	400+	500M+
chương trình đã được tạo	nhà nghiên cứu tham gia	lỗ hổng được phát hiện	Đã trao thưởng

WhiteHub hiện đang cung cấp các giải pháp Crowdsourced Security sau đây:

WhitePentest+

Cung cấp nền tảng giúp doanh nghiệp tiếp cận cộng đồng hơn 500 chuyên gia an ninh mạng thông qua các chương trình Bug Bounty.

>> Xem chi tiết

WhiteBounty

Cung cấp dịch vụ bảo mật toàn diện cho doanh nghiệp ứng dụng phương pháp Crowdsourced Security.

>> Xem chi tiết

Để bắt đầu sử dụng các giải pháp Crowdsourced Security do WhiteHub cung cấp, vui lòng liên lạc với chúng tôi qua biểu mẫu đăng ký tại địa chỉ: https://cystack.net/contact

Hoặc liên lạc trực tiếp với đội ngũ kinh doanh tại CyStack qua địa chỉ email:
contact@cystack.net