Khung tiền thưởng cho chương trình Bug Bounty

“Thưởng bao nhiêu tiền cho một lỗ hổng?” là câu hỏi của nhiều CTO/CISO trước khi triển khai chương trình bảo mật Bug Bounty trên WhiteHub. Quả thực, không có một mức giá cố định nào có thể áp dụng cho mọi trường hợp. Mỗi lỗ hổng khác nhau có ý nghĩa và tác động khác nhau lên hệ thống và công việc kinh doanh, vì thế chúng nên được định giá khác nhau.

Với kinh nghiệm triển khai chương trình bug bounty cho hơn 30 doanh nghiệp lớn nhỏ tại Việt Nam, đội ngũ chuyên gia của chúng tôi đã đưa ra một mức khung tiền thưởng tiêu chuẩn cho chương trình bug bounty. Bao gồm những yếu tố mà doanh nghiệp cần cân nhắc trước khi quyết định mức thưởng như quy mô bảo mật của công ty, mức độ ưu tiên của các loại lỗ hổng, bảng giá tham khảo và các yếu tố khác cần xem xét.

Mặc dù khung tham chiếu này không phải tiêu chuẩn có thể áp dụng với mọi chương trình bug bounty, mọi doanh nghiệp. Chúng tôi hy vọng đây là một tài liệu tham khảo giúp bạn hình dung được giá trị của một bug phụ thuộc vào những yếu tố nào, và làm sao để xác định khung tiền thưởng cho chương trình bug bounty để đạt được mục tiêu bảo mật.

Quy mô bảo mật của công ty

Ngân sách cho bug bounty phụ thuộc vào quy mô hệ thống của công ty

Quy mô hệ thống thông tin và bảo mật của công ty là yếu tố quan trọng nhất để xác định mức thưởng cho các lỗ hổng trong chương trình bug bounty. Một tổ chức sở hữu hệ thống thông tin lớn và yêu cầu bảo mật cao thường tồn tại các lỗ hổng khó tìm. Các lỗ hổng này đòi hỏi nhiều thời gian và công sức hơn nên chúng có giá trị lớn hơn.

Mặc dù có nhiều yếu tố khác nhau ảnh hưởng tới độ phức tạp của hệ thống doanh nghiệp, bảng dưới đây sẽ giúp đánh giá sơ bộ mức độ lớn mạnh của hệ thống bảo mật trong doanh nghiệp của bạn.

	CƠ BẢN	TRUNG BÌNH	CHUYÊN NGHIỆP
Triết lý	Cho rằng an ninh mạng là điều gì đó đáng sợ.	Cho rằng an ninh mạng cần được tích hợp sâu vào công việc kinh doanh.	An ninh mạng là một phần của văn hóa.
Con người	- CISO báo cáo với IT. - Không có hoặc có đội ngũ Security nhỏ (1-2 người). - Thường team IT kiêm security.	- CISO báo cáo cho COO hoặc giám đốc khác ngoài IT. - Đội ngũ Security lớn hơn (3 - 5 người)	- CISO báo cáo trực tiếp cho CEO và là một thành viên ban lãnh đạo. - Đội ngũ security lớn, được đào tạo theo quy trình.
Quy trình	- Tùy cơ ứng biến - Phụ thuộc vào team IT.	Phối hợp tốt hơn với team IT. Tuy nhiên quy trình vẫn còn thủ công và phụ thuộc vào sự tỏa sáng cá nhân.	Có quy trình làm việc rõ ràng. Có khả năng tự động hóa và scale-up cùng doanh nghiệp.
Công nghệ	- Sử dụng các công nghệ bảo mật cơ bản với các thiết lập đơn giản. - Hệ thống bảo mật rời rạc, không có sự liền mạch. - Tập trung vào phòng ngừa và tuân thủ quy định, chính sách.	- Sử dụng các công nghệ bảo mật tiên tiến hơn. - Có sử dụng thêm các công cụ thu thập và phân tích sự kiện an ninh.	- Xây dựng kiến trúc công nghệ bảo mật cho doanh nghiệp - Tập trung vào phòng ngừa, phát hiện và phản ứng sự cố. - Phát triển Identity management và data security để đối phó với các vấn đề bảo mật từ môi trường cloud computing & mobile security.

Nguồn: *Enterprise Strategy Group*

Một lưu ý quan trọng là mỗi tổ chức có thể sở hữu các mục tiêu cần bảo mật (target) khác nhau với mức độ phức tạp khác nhau. Mô hình này có thể áp dụng để so sánh tương quan giữa các doanh nghiệp, cũng như giữa các target với nhau.

Mức độ ưu tiên của lỗ hổng

Các loại lỗ hổng có ưu tiên cao nhất

Khi đã xác định được mức độ lớn mạnh của hệ thống bảo mật DN, bạn có thể xây dựng một bảng giá cho các lỗ hổng. Việc đầu tiên là xác định được mức độ ưu tiên cho từng loại lỗ hổng khác nhau. Việc này rất quan trọng bởi vì các lỗi ưu tiên cao hơn xứng đáng nhận phần thưởng cao hơn - chúng đòi hỏi nhiều thời gian, nỗ lực và kỹ năng hơn để tìm thấy.

Để xác định được mức độ ưu tiên, chúng ta phải đánh giá lỗ hổng qua 2 tiêu chí:

- Tác động về mặt kỹ thuật
- Tác động tới kinh doanh.

Khi WhiteHub nhận được một lỗ hổng có thể tái hiện lại, các Kỹ sư bảo mật sẽ tiến hành 1) đánh giá tác động kỹ thuật và 2) gán mức độ ưu tiên cho lỗ hổng. Thông tin này sau đó được gửi cho khách hàng để đánh giá tác động kinh doanh và xác nhận lại mức độ ưu tiên của lỗ hổng. Mức độ ưu tiên này có thể được điều chỉnh theo ngữ cảnh của ứng dụng, các điều kiện bảo mật bên ngoài hoặc quy trình của tổ chức.

Thang đánh giá bao gồm 5 mức độ khác nhau cho tất cả các lỗ hổng: Critical, High, Medium, Low, Risk. Các lỗ hổng được gán nhãn “Critical” là các lỗ hổng có nguy cơ cao nhất. Ngược lại, nhãn “Risk” được gán cho các lỗ hổng mà rủi ro của nó có thể chấp nhận được.

Dưới đây là bảng ưu tiên cơ bản. Bạn có thể tham khảo để làm điểm khởi đầu, hoặc tự điều chỉnh cho phù hợp với nhu cầu của mình.

MỨC ƯU TIÊN	ẢNH HƯỞNG	LOẠI LỖ HỔNG
Rất nguy hiểm - Critical	- Khai thác lỗ hổng có thể chiếm được quyền điều khiển của máy chủ hoặc thiết bị hạ tầng khác mà ứng dụng hoạt động trên đó - Lỗ hổng cho phép leo thang đặc quyền, từ anonymous hoặc normal user lên administrator - Lỗ hổng cho phép đánh cắp dữ liệu nhạy cảm như tài chính, thông tin cá nhân của người dùng, các loại mật khẩu, token, API key - Việc tấn công là hoàn toàn trực tiếp, không cần sử dụng các hình thức lừa đảo, social engineering để thu thập thông tin từ con người	- Remote Code Execution - Authentication Bypass - XML External Entities Injection - SQL Injection - Database leaking
Nguy hiểm - High	- Việc khai thác lỗ hổng có thể dẫn đến leo thang đặc quyền, từ anonymous user lên normal user - Lỗ hổng có thể dẫn đến mất mát dữ liệu hoặc gây gián đoạn truy cập - Lỗ hổng gây thay đổi đến các tính năng được thiết kế trong sản phẩm	- Stored XSS - CSRF tại những trang nhạy cảm - IDOR - SSRF
Trung bình - Medium	- Thông thường, kẻ tấn công phải sử dụng các hình thức lừa đảo, social engineering để thu thập thông tin từ con người để tiếp cận nạn nhân - Việc khai thác yêu cầu kẻ tấn công phải hoạt động trên một vùng mạng nội bộ với mục tiêu - Việc khai thác chỉ mang lại một lượng thông tin rất hạn chế - Các lỗ hổng đòi hỏi quyền người dùng cao hơn để khai thác thành công	- Reflective XSS - URL redirect - CSRF tại những trang ít nhạy cảm
Thấp - Low	Các lỗ hổng không thể khai thác về mặt chức năng. Lỗ hổng đó là theo thiết kế hoặc rủi ro nó gây ra được coi là chấp nhận được.	- SSL misconfigurations - SPF misconfiguration - Self-XSS
Nguy cơ - Risk	- Cuộc tấn công có tác động rất thấp đến hoạt động và dữ liệu của mục tiêu - Việc khai thác thường đòi hỏi truy cập ở mức vật lý hoặc local	- Debug information - Sử dụng CAPTCHAs - Code obfuscation - Rate limiting.

Bảng Giá tham khảo

Ngân sách hàng năm, phạm vi phần thưởng và giá cho mỗi lỗ hổng.

Tại WhiteHub, chúng tôi tham khảo giá thị trường của các nền tảng Bug Bounty quốc tế và Việt Nam. WhiteHub thực hiện một số điều chỉnh để đảm bảo mức thưởng cơ bản phù hợp với cả doanh nghiệp Việt và không làm mất quyền lợi của Nhà nghiên cứu.

Mức thưởng cơ bản

Độ lớn của hệ thống bảo mật doanh nghiệp và mức độ ưu tiên của lỗ hổng là hai yếu tố quan trọng nhất khi xác định giá trị của mỗi lỗi. Xác định tương đối hai giá trị này sẽ giúp doanh nghiệp đưa ra bảng giá bounty thích hợp.

Dưới đây là mô hình mức thưởng tham khảo dành cho các doanh nghiệp.

	QUY MÔ BẢO MẬT CỦA CÔNG TY		
	Cơ bản	**Trung bình**	**Chuyên nghiệp**
Khoảng thưởng mỗi lỗi	0 - 6M	1M - 12M	3M - 50M
Thưởng trung bình mỗi lỗi	3M	6M	23M
Critical	6M	12M	50M
High	4M	8M	30M
Medium	1M	3M	10M
Low	0	1M	3M

Xin lưu ý rằng bảng giá trên chỉ mang tính tham khảo. (1M = 1.000.000 VNĐ)

Một số tổ chức có thể bắt đầu với mức thưởng thấp và tăng dần mức thưởng theo thời gian. Lựa chọn mức thưởng thấp có thể mang lại thành công ban đầu và tiết kiệm ngân sách. Tuy nhiên cần lưu ý rằng phần thưởng là yếu tố chính cho phép các tổ chức cạnh tranh với nhau để giành lấy nhân tài trong thị trường. Và để thành công bền vững, chúng tôi khuyên bạn nên bắt đầu với các phạm vi trên.

Những yếu tố khác ảnh hưởng tới mức thưởng

Mục tiêu quan trọng

Nếu tổ chức của bạn xử lý các thông tin quan trọng, rất nhạy cảm hoặc có giá trị (ví dụ: PII, PHI, dữ liệu tài chính, v.v.), thì việc thận trọng xem xét tăng các khoản thưởng sẽ giúp DN thu hút và giữ chân nhân tài một cách nhanh chóng.

Khả năng tiếp cận mục tiêu

Nếu mục tiêu của bạn yêu cầu nhiều thiết lập để có thể tiếp cận, kiểm tra; hoặc yêu cầu nhiều kiến thức đặc thù để kiểm tra, thì việc tăng mức thưởng sẽ khiến chương trình bug bounty hấp dẫn hơn.

An ninh mạng đẳng cấp thế giới

Nếu chức của bạn có hệ thống bảo mật cực kỳ tiên tiến và (hoặc) bạn mong muốn thu hút những tài năng bảo mật tốt nhất, bạn có thể nâng gấp đôi các khoản thưởng để nhận lại những kết quả quan trọng. Điều này sẽ giúp bạn ngang hàng với một số thương hiệu nổi bật nhất hiện đang chạy các chương trình tiền thưởng trên thị trường.

Chứng tỏ mức độ an toàn của ứng dụng

Nhiều tổ chức có mong muốn sử dụng chương trình bug bounty để chứng tỏ khả năng đáp ứng bảo mật cao của sản phẩm. Trong trường hợp này, việc tăng lượng tiền thưởng cũng là một cách hiệu quả để nâng cao hiệu quả marketing cho mức độ an toàn của ứng dụng trong mắt người dùng và nhà đầu tư.

Hỗ trợ

Với các yêu cầu hỗ trợ trong việc định giá mức thưởng cho các chương trình bug bounty trên WhiteHub, vui lòng liên hệ với chuyên gia CyStack tại:

Đăng ký tư vấn (miễn phí): https://cystack.net/vi/contact

Email: contact@cystack.net