CyStack

DATA SHEET

Kiểm thử mạng nội bộ

Bảo vệ hệ thống hạ tầng mạng doanh nghiệp toàn diện

Tổng quan

Kiểm thử bảo mật mạng nội bộ là đánh giá cơ sở hạ tầng mạng và các biện pháp kiểm soát bảo mật của doanh nghiệp để xác định các lỗ hổng và đảm bảo tuân thủ các chính sách bảo mật cũng như quy định của ngành. Quá trình kiểm thử thường bao gồm các đánh giá về kiến trúc mạng, kiểm soát truy cập, bảo mật dữ liệu và quy trình ứng cứu sự cố.

Mục tiêu chính của kiểm thử bảo mật mạng nội bộ là xác định và giảm thiểu rủi ro bảo mật tiềm ẩn đối với cơ sở hạ tầng mạng của doanh nghiệp. Điều này bao gồm việc xác định các lỗ hổng trong kiến trúc và cấu hình của mạng, đánh giá hiệu quả của các biện pháp kiểm soát bảo mật và đánh giá sự tuân thủ của doanh nghiệp với các chính sách bảo mật và quy định của ngành.

Kiểm thử cũng giúp các doanh nghiệp:

- Phát hiện mọi hoạt động độc hại hoặc vi phạm bảo mật có thể đã xảy ra.
- Đánh giá mức độ sẵn sàng của quy trình ứng cứu sự cố.
- Xác minh sự tuân thủ của mạng với luật và quy định bảo vệ dữ liệu.
- Đảm bảo tính bảo mật của dữ liệu nhạy cảm được lưu trữ trên mạng.
- Cải thiện tình hình bảo mật tổng thể.
- Cung cấp cơ sở để giám sát và cải tiến liên tục.

Mục đích của kiểm thử bảo mật mạng nội bộ không phải để "tấn công" hay "xâm nhập hệ thống", mà để xác định các lỗ hổng tiềm ẩn và đưa ra các giải pháp cải thiện bảo mật.

Lợi ích của khách hàng

- Tăng cường bảo mật mạng nội bộ
- Đảm bảo tuân thủ các tiêu chuẩn và quy định của ngành
- Hiểu và quản lý rủi ro bảo mật hiệu quả hơn
- Xây dựng mô hình quản trị tốt hơn và đưa ra chiến lược quản lý rủi ro mạnh mẽ hơn
- Có xác nhận độc lập của bên thứ ba về tình hình bảo mật mạng nội bộ

Giải pháp của CyStack

Đội ngũ kiểm thử bảo mật của CyStack bao gồm những chuyên gia tài năng giàu kinh nghiệm, thành thạo các phương pháp kiểm thử bám sát mục tiêu và tối ưu nhất. Họ là những chuyên gia có nền tảng vững chắc về phát triển phần mềm và nghiên cứu an ninh mạng, giúp đội ngũ CyStack đánh giá toàn diện nhất các rủi ro bảo mật trong sản phẩm số của doanh nghiệp. Các chuyên gia tại CyStack cũng thường xuyên tham gia các hội nghị an ninh mạng lớn trên thế giới với vai trò diễn giả hàng năm, đồng thời họ là những chuyên gia săn lỗi phần mềm với nhiều thành tích phát hiện ra các lỗ hổng bảo mật nghiêm trọng và được ghi danh trên Hall of Fame của các hãng công nghệ lớn toàn cầu như IBM, HP, Microsoft, Sea Group, Alibaba, v.v.

Đội ngũ chuyên gia thực hiện đánh giá mạng nội bộ của doanh nghiệp, bao gồm máy chủ, mạng và kho lưu trữ, cũng như kiến trúc hệ thống và cách thiết lập để xác định bất kỳ lỗ hổng hoặc cấu hình sai nào có thể bị tin tặc công khai thác. Các chuyên gia cũng sẽ xem xét cài đặt, cấu hình bảo mật của mạng nội bộ và ứng dụng để đảm bảo thiết lập đúng, bao gồm việc kiểm tra mã hóa phù hợp, kiểm soát truy cập và bảo mật mạng.

Phương pháp luận

Nội dung kiểm thử bảo mật nội bộ của CyStack thường bao gồm:

1. **Đánh giá kiến trúc mạng**: Dịch vụ này sẽ liên quan đến việc đánh giá kiến trúc mạng của doanh nghiệp và xác định bất kỳ lỗ hổng nào có thể bị tin tặc khai thác, bao gồm đánh giá việc sử dụng tường lửa, hệ thống ngăn chặn và phát hiện xâm nhập cũng như các thiết bị bảo mật khác.
2. **Đánh giá kiểm soát truy cập**: Dịch vụ này sẽ đánh giá hiệu quả kiểm soát truy cập của doanh nghiệp, ví dụ cơ chế xác thực và ủy quyền, đồng thời xác định bất kỳ điểm yếu tiềm ẩn nào.
3. **Đánh giá bảo mật dữ liệu**: Dịch vụ này sẽ xem xét các biện pháp bảo mật dữ liệu của doanh nghiệp và đánh giá tính bảo mật, tính toàn vẹn và tính khả dụng của dữ liệu nhạy cảm được lưu trữ trên mạng.
4. **Đánh giá khả năng phản hồi sự cố**: Dịch vụ này sẽ đánh giá các quy trình ứng cứu sự cố của doanh nghiệp và đánh giá hiệu quả của các quy trình ứng cứu sự cố trong việc phát hiện và phản ứng với các sự cố bảo mật.
5. **Đánh giá tuân thủ**: Dịch vụ này sẽ xem xét sự tuân thủ của doanh nghiệp với các chính sách, tiêu chuẩn và quy định bảo mật có liên quan.
6. **Cung cấp một báo cáo toàn diện** tóm tắt các phát hiện của cuộc kiểm thử và đưa ra các khuyến nghị để cải thiện.

CyStack cũng cung cấp hỗ trợ bổ sung như hướng dẫn khắc phục, đào tạo bảo mật cũng như giám sát và quản lý liên tục.

Trong quá trình kiểm thử bảo mật mạng nội bộ, các mục tiêu hoặc đối tượng cụ thể sẽ được kiểm thử phụ thuộc vào phạm vi kiểm thử. Phạm vi đề cập đến các yếu tố cụ thể của cơ sở hạ tầng mạng và cơ chế kiểm soát bảo mật sẽ được đánh giá. Các mục tiêu sẽ được kiểm tra có thể bao gồm:

1. **Thiết bị mạng**: bộ định tuyến, bộ chuyển mạch và tường lửa, cũng như các điểm truy cập không dây và thiết bị mạng khác.
2. **Máy chủ**: máy chủ web, máy chủ cơ sở dữ liệu và các loại máy chủ khác.
3. **Thiết bị đầu cuối**: máy tính xách tay, máy trạm và thiết bị di động, bao gồm hệ điều hành, phần mềm và ứng dụng.
4. **Cơ sở hạ tầng đám mây**: IaaS, PaaS và SaaS.
5. **Truy cập từ xa**: kết nối mạng riêng ảo (VPN), giao thức máy tính từ xa (RDP) và các giải pháp truy cập từ xa khác.
6. **Các dịch vụ và giao thức mạng**: hệ thống tên miền (DNS), giao thức cấu hình động máy chủ (DHCP), các dịch vụ và giao thức khác được sử dụng để hỗ trợ các hoạt động mạng.
7. **Các cơ chế kiểm soát truy cập**: các giao thức xác thực và phân quyền, xác thực đa yếu tố và các quyền truy cập của người dùng.
8. **Các biện pháp bảo mật dữ liệu**: mã hóa dữ liệu, sao lưu dữ liệu và ngăn ngừa thất thoát dữ liệu.
9. **Quy trình ứng phó sự cố**: phát hiện và phản ứng sự cố, quy trình xử lý sự cố và các giao thức giao tiếp.
10. **Đáp ứng tuân thủ**: với các chính sách, tiêu chuẩn và quy định bảo mật có liên quan như HIPAA, PCI-DSS, SOC2.

Tính năng chính

- Đảm bảo rằng hạ tầng mạng an toàn
- Đánh giá toàn diện hạ tầng mạng về các cấu hình, kiến trúc, chính sách và quy trình
- Quản lý, theo dõi, đánh giá mức độ ưu tiên và khắc phục những phát hiện trong nền tảng quản lý lỗ hổng của CyStack
- Nhận các khuyến nghị phù hợp để tăng cường bảo mật hệ thống
- Giảm thiểu các rủi ro và nâng cao hiệu quả vận hành

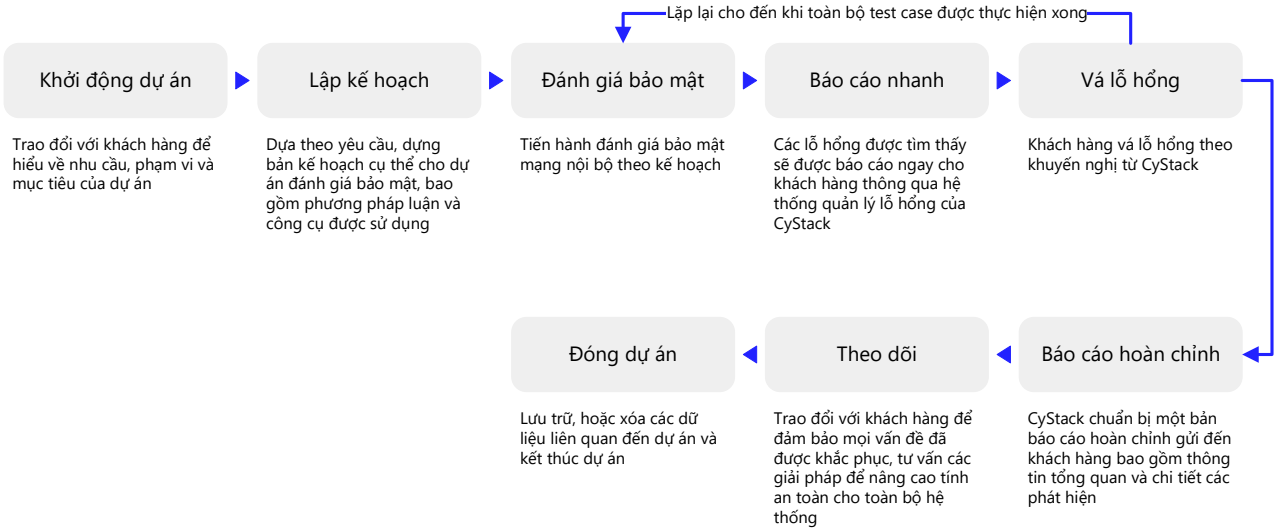
Các tiêu chuẩn

CyStack sử dụng các tiêu chuẩn ngành khác nhau và các khuyến nghị bảo mật được cập nhật mới nhất để tiến hành kiểm thử bảo mật mạng nội bộ. Các tiêu chuẩn mà CyStack sử dụng phụ thuộc vào nhu cầu và yêu cầu cụ thể của khách hàng, cũng như lĩnh vực hay môi trường pháp lý của doanh nghiệp. Một số tiêu chuẩn chung thường được sử dụng bao gồm:

- NIST SP 800-53: Tiêu chuẩn này cung cấp hướng dẫn kiểm thử bảo mật cho các hệ thống thông tin liên bang và thường được sử dụng làm khuôn khổ cho kiểm thử bảo mật mạng nội bộ.
- ISO/IEC 27001: Tiêu chuẩn quốc tế này cung cấp khuôn khổ cho việc quản lý bảo mật thông tin và được các tổ chức trên toàn thế giới áp dụng rộng rãi.
- PCI DSS: Tiêu chuẩn bảo mật dữ liệu thẻ thanh toán cung cấp khuôn khổ bảo mật các giao dịch thẻ tín dụng, là yêu cầu đối với bất kỳ tổ chức nào xử lý, lưu trữ hoặc truyền tải thông tin thẻ tín dụng.
- SOC 2: Báo cáo Kiểm Soát Tổ Chức Dịch Vụ 2 cung cấp một khuôn khổ để đánh giá mức độ an toàn, tính khả dụng, tính toàn vẹn, tính bảo mật và quyền riêng tư của hệ thống các tổ chức dịch vụ.
- OWASP (Open Web Application Security Project): Hướng dẫn cung cấp một bộ hướng dẫn và các khuyến nghị được cập nhật mới nhất để bảo mật các ứng dụng web.

CyStack cũng sử dụng các tiêu chuẩn bổ sung và các khuyến nghị bảo mật khác được cập nhật mới nhất như Top 10 của OWASP, Bộ kiểm soát các vấn đề bảo mật tối quan trọng của CIS và khung kiểm thử riêng tự xây dựng. Cần lưu ý rằng, bên cạnh việc đối chiếu theo các tiêu chuẩn đã liệt kê, CyStack cũng xem xét các chính sách và quy định trong doanh nghiệp mà công ty phải tuân thủ. Một dự án kiểm thử lý tưởng nhất sẽ được điều chỉnh theo các mục tiêu và kết quả mong muốn cụ thể của doanh nghiệp.

Quy trình làm việc với khách hàng



Về CyStack

CyStack là một công ty đổi mới sáng tạo trong lĩnh vực an ninh mạng tại Việt Nam, chúng tôi tiên phong xây dựng các sản phẩm bảo mật thế hệ mới cho cả doanh nghiệp và cá nhân. Các giải pháp của CyStack tập trung vào bảo vệ dữ liệu, phòng chống tấn công mạng và quản lý lỗ hổng bảo mật.

Để biết thêm chi tiết, liên lạc tới hotline **(+84) 247 109 9656** hoặc gửi mail tới **contact@cystack.net** để trao đổi cùng các chuyên gia bảo mật tại CyStack.
cystack.net