CyStack

DATA SHEET

Ngăn ngừa thất thoát dữ liệu

Ngăn chặn việc mất dữ liệu, đảm bảo tuân thủ

Tổng quan

Ngăn ngừa thất thoát dữ liệu (DLP) là một công nghệ và tập hợp các quy trình mà các doanh nghiệp sử dụng để đảm bảo rằng thông tin bí mật hoặc nhạy cảm không bị mất, bị đánh cắp hoặc sử dụng sai mục đích.

DLP là cần thiết vì dữ liệu nhạy cảm là mục tiêu có giá trị đối với tội phạm mạng và có thể được sử dụng cho các hoạt động độc hại như ăn cắp danh tính, lừa đảo và tống tiền. Điều quan trọng đối với các doanh nghiệp là bảo vệ dữ liệu nhạy cảm để tránh tổn thất tài chính, thiệt hại về uy tín và các hình phạt pháp lý. Các giải pháp DLP có thể giúp các doanh nghiệp xác định và bảo vệ dữ liệu nhạy cảm, chặn truy cập trái phép vào dữ liệu đó và phản ứng nhanh với các vụ vi phạm dữ liệu.

Các giải pháp DLP cũng giúp các doanh nghiệp tuân thủ các quy định và tiêu chuẩn khác nhau như HIPAA, PCI-DSS và GDPR, yêu cầu các doanh nghiệp bảo vệ dữ liệu nhạy cảm. Nhiều doanh nghiệp cũng được yêu cầu thông báo cho các cá nhân và cơ quan có thẩm quyền khi xảy ra lộ lọt dữ liệu và DLP có thể giúp các tổ chức đáp ứng yêu cầu này.

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 HP, Microsoft, Sea Group, Alibaba, v.v.

Từ kinh nghiệm kiểm thử và phát triển phần mềm của mình, đội ngũ CyStack hiểu rõ nguyên nhân rò rỉ dữ liệu và cách ngăn chặn hiệu quả. Các chuyên gia sẽ giúp doanh nghiệp đưa ra các chiến lược DLP hiệu quả và quan trọng nhất là phù hợp với chính sách và stack công nghệ hiện tại của doanh nghiệp.

Lợi ích của khách hàng

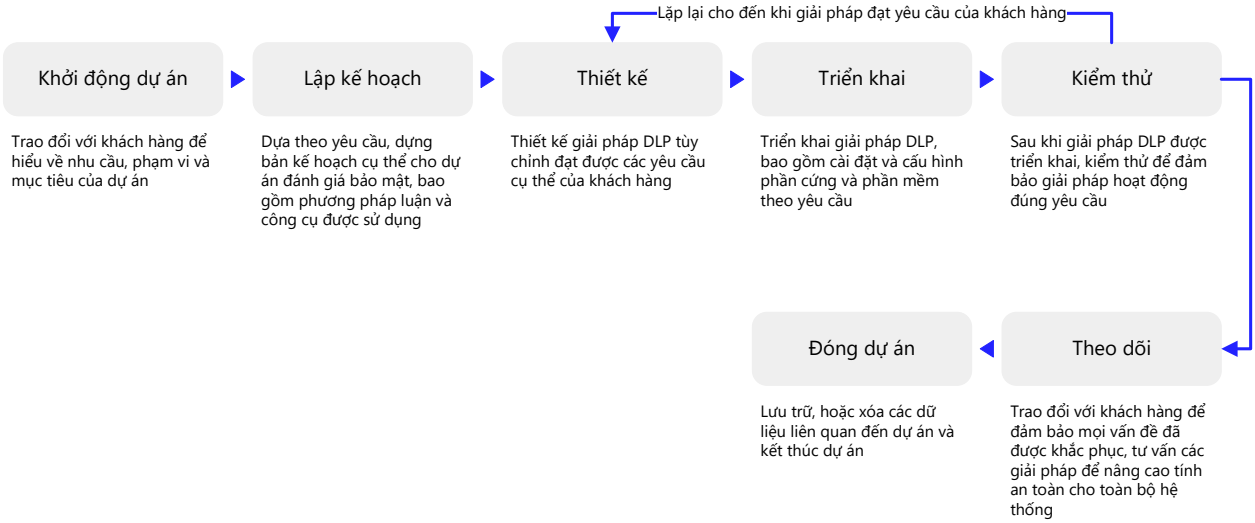
- Bảo vệ dữ liệu nhạy cảm khỏi bị mất, bị đánh cắp hoặc sử dụng sai mục đích
- Tuân thủ các quy định và tiêu chuẩn khác nhau như HIPAA, PCI-DSS và GDPR
- Giảm nguy cơ lộ lọt dữ liệu và các sự cố bảo mật khác
- Xác định và ngăn chặn việc truyền dữ liệu nhạy cảm
- Theo dõi được các hoạt động và hiệu suất của giải pháp DLP

Phương pháp luận

Giải pháp DLP của CyStack bao gồm các bước sau:

1. **Đánh giá**: Trong bước này, CyStack tiến hành đánh giá kỹ lưỡng môi trường dữ liệu hiện tại của khách hàng để xác định dữ liệu nhạy cảm và các lỗ hổng tiềm ẩn. Điều này bao gồm:
    - Xác định các loại dữ liệu cần được bảo vệ như thông tin cá nhân, dữ liệu tài chính và tài sản trí tuệ.
    - Xác định vị trí của dữ liệu đó, ví dụ trên các thiết bị đầu cuối, trên đám mây hoặc trên máy chủ email..
    - Xác định đối tượng có quyền truy cập vào dữ liệu và cách dữ liệu được truyền đi.
    - Phân tích các biện pháp kiểm soát bảo mật hiện tại của khách hàng và xác định bất kỳ sơ suất hoặc lỗ hổng nào.
    - Xác định các yêu cầu và quy định cần tuân thủ của khách hàng cũng như cách áp dụng cho môi trường dữ liệu.
2. **Thiết kế**: Dựa trên đánh giá, một giải pháp DLP được thiết kế để giải quyết các nhu cầu cụ thể của khách hàng. Điều này bao gồm:
    - Xác định các công nghệ và quy trình phù hợp sẽ được sử dụng để bảo vệ dữ liệu, ví dụ các phương pháp dành cho hệ thống mạng, thiết bị đầu cuối hay đám mây lưu trữ.
    - Xác định vị trí các công nghệ DLP sẽ được triển khai trong mạng.
    - Thiết lập cấu hình các chính sách và quy tắc DLP để phát hiện và bảo vệ dữ liệu nhạy cảm.
    - Xác định các thủ tục và quy trình công việc cần thiết để ứng phó sự cố và khôi phục dữ liệu.
    - Thiết kế bảng điều khiển quản lý và báo cáo để cung cấp khả năng hiển thị về hiệu suất của giải pháp DLP.
3. **Triển khai**: Sau khi thiết kế hoàn tất, giải pháp DLP sẽ được triển khai. Quá trình có thể bao gồm:
    - Cài đặt phần cứng và phần mềm, ví dụ phần mềm DLP và phần mềm giám sát thiết bị đầu cuối, hoặc xây dựng giải pháp tùy chỉnh cho khách hàng.
    - Cấu hình mạng và thiết bị đầu cuối, như tường lửa và hệ thống phát hiện xâm nhập.
    - Thiết lập các chính sách và quy trình bảo vệ dữ liệu, bao gồm các quy trình ứng phó sự cố và khôi phục dữ liệu.
    - Thử nghiệm giải pháp DLP để đảm bảo cấu hình đúng và hoạt động như dự định.
4. **Giám sát và quản lý**: Sau khi triển khai giải pháp DLP, cần phải liên tục giám sát và quản lý để đảm bảo rằng giải pháp này đang bảo vệ hiệu quả dữ liệu nhạy cảm. Điều này bao gồm:
    - Giám sát vi phạm dữ liệu và các sự cố bảo mật khác, như nỗ lực đánh cắp dữ liệu.
    - Cập nhật các chính sách và quy trình khi cần để thích ứng với những thay đổi trong môi trường dữ liệu hoặc để cải thiện hiệu suất của giải pháp DLP.
    - Cung cấp báo cáo và phân tích thường xuyên cho khách hàng để cung cấp khả năng hiển thị về hiệu suất của giải pháp DLP.
5. **Ứng phó sự cố**: Trong trường hợp xảy ra lộ lọt dữ liệu hoặc sự cố bảo mật khác, các dịch vụ khắc phục và ứng phó sự cố được cung cấp để giúp khách hàng ứng phó sự cố nhanh chóng và hiệu quả. Điều này bao gồm:
    - Xác định nguyên nhân của sự cố (tấn công lừa đảo hoặc nhiễm phần mềm độc hại).
    - Ngăn lại sự cố để tránh mất thêm dữ liệu.
    - Xóa mã độc hại hoặc tác nhân khỏi môi trường.
    - Khôi phục hoạt động bình thường, ví dụ trả lại dữ liệu bị lấy mất.
6. **Báo cáo**: Cung cấp bảng điều khiển quản lý tập trung để giám sát và báo cáo, cho phép khách hàng thấy các hoạt động và hiệu suất của giải pháp DLP: Điều này bao gồm:
    - Báo cáo về các loại dữ liệu đã được bảo vệ và số lượng sự cố đã được phát hiện và ngăn chặn.
    - Báo cáo về hiệu suất của hệ thống DLP, ví dụ số lượng báo động giả và cảnh báo đã bị bỏ qua.
    - Báo cáo về hiệu quả của giải pháp DLP, ví dụ số vụ vi phạm dữ liệu đã được ngăn chặn.

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