100 câu hỏi kiểm tra bảo mật cho doanh nghiệp vừa và nhỏ

Câu hỏi kiểm tra	Phản hồi		
	Có	Không	N/A
1. Chính sách và quy trình bảo mật			
Bạn có thường xuyên xem xét và cập nhật chính sách và quy trình bảo mật không?			
Bạn đã xây dựng kế hoạch ứng phó sự cố chưa?			
Bạn đã xác định rõ vai trò và trách nhiệm của từng người liên quan đến bảo mật thông tin chưa?			
Bạn đã có chương trình đào tạo nhận thức an ninh mạng cho nhân viên chưa?			
Tất cả nhân viên đã ký vào biểu mẫu xác nhận chính sách bảo mật chưa?			
2. Kiểm soát quyền truy cập			
Bạn đã thiết lập chính sách mật khẩu mạnh chưa?			
Bạn có bật xác thực đa yếu tố cho các tài khoản quan trọng không?			
Quyền truy cập có được xem xét và cập nhật thường xuyên không?			
Các tài khoản không hoạt động có được vô hiệu hóa hoặc xóa chưa?			
Quyền truy cập quản trị chỉ dành cho những người được ủy quyền hay không?			
Bạn có theo dõi và ghi nhật ký truy cập và hoạt động của người dùng không?			
3. Bảo mật mạng			
Bạn đã cài đặt và cấu hình tường lửa chưa?			
Bạn đã triển khai hệ thống phát hiện và ngăn chặn xâm nhập (IDS/IPS) chưa?			

Bạn có thường xuyên quét và vá lỗi lỗ hổng mạng chưa?			
Bạn có sử dụng phân đoạn mạng (segmentation) để cô lập các hệ thống quan trọng chưa?			
Bạn có thường xuyên cập nhật và vá lỗi thiết bị và phần mềm mạng chưa?			
4. Thiết bị điểm cuối			
Bạn đã triển khai giải pháp bảo mật endpoint (chống virus, phần mềm độc hại) chưa?			
Bạn đã bật mã hóa thiết bị cho laptop và thiết bị di động khác chưa?			
Bạn có thường xuyên cập nhật và vá lỗi cho tất cả các điểm cuối không?			
Bạn có khả năng xóa dữ liệu với thiết bị bị mất hoặc bị đánh cắp không?			
Bạn có thực thi các chính sách cho phép và chặn ứng dụng không?			
5. Bảo vệ dữ liệu			
Dữ liệu nhạy cảm đã được mã hóa khi lưu trữ và truyền tải chưa?			
Bạn có sao lưu dữ liệu thường xuyên và đồng thời kiểm tra quy trình khôi phục không?			
Quyền truy cập vào dữ liệu nhạy cảm đã được giới hạn theo nguyên tắc "cần biết" (need-to-know) chưa?			
Bạn đã triển khai công nghệ ngăn ngừa mất dữ liệu (DLP) chưa?			
Bạn đã có các quy trình loại bỏ dữ liệu phù hợp chưa?			
6. Email			
Doanh nghiệp có sử dụng email gateway bảo mật hay không?			
Nhân viên đã được đào tạo để nhận biết các kỹ thuật lừa đảo phishing và social engineering chưa?			
Doanh nghiệp đã triển khai mã hóa email cho thông tin nhạy cảm chưa?			
Doanh nghiệp có thường xuyên cập nhật phần mềm và cấu hình máy chủ email không?			

Doanh nghiệp có thực thi chính sách lưu trữ email không?			
7. Bảo mật web			
Doanh nghiệp đã cài đặt và cập nhật tường lửa ứng dụng web (WAF) chưa?			
Doanh nghiệp có quét lỗ hổng bảo mật cho ứng dụng web không?			
Doanh nghiệp có tuân thủ các phương pháp viết code bảo mật không?			
Doanh nghiệp có thường xuyên theo dõi và kiểm tra log máy chủ web không?			
Doanh nghiệp có sử dụng giao thức kết nối an toàn SSL/TLS không?			
8. Bảo mật mạng không dây			
Doanh nghiệp đã bảo mật mạng Wi-Fi bằng mã hóa mạnh chưa?			
Doanh nghiệp đã thay đổi mật khẩu router mặc định chưa?			
Doanh nghiệp đã phân đoạn mạng Wi-Fi cho khách và nội bộ chưa?			
Doanh nghiệp có quét tìm các điểm truy cập trái phép không?			
Doanh nghiệp có giới hạn quyền truy cập vật lý vào cơ sở hạ tầng mạng không?			
9. Rủi ro từ nhà cung cấp và bên thứ ba			
Doanh nghiệp có đánh giá bảo mật của các bên thứ ba không?			
Doanh nghiệp đã đưa ra các yêu cầu bảo mật trong hợp đồng với nhà cung cấp chưa?			
Doanh nghiệp có thường xuyên xem xét và kiểm tra quyền truy cập của bên thứ ba không?			
Doanh nghiệp có hệ thống giám sát các vụ vi phạm hoặc sự cố dữ liệu liên quan đến nhà cung cấp không?			
Doanh nghiệp có quy trình chấm dứt hợp đồng nhanh chóng với nhà cung cấp trong trường hợp có lo ngại về bảo mật không?			
10. An ninh vật lý			

Bạn đã bảo vệ khu vực trung tâm dữ liệu và phòng máy chủ chưa?			
Bạn đã lắp đặt hệ thống giám sát và báo động chưa?			
Bạn đã có biện pháp bảo vệ laptop và thiết bị di động khỏi bị trộm cắp chưa?			
Bạn có thường xuyên kiểm kê và theo dõi thiết bị phần cứng không?			
Bạn đã thiết lập các biện pháp kiểm soát truy cập vật lý chưa?			
11. Bảo mật dịch vụ đám mây			
Bạn đã tìm hiểu kỹ về nhà cung cấp dịch vụ đám mây trước khi lựa chọn chưa?			
Bạn đã áp dụng các biện pháp bảo mật tốt nhất cho hệ thống đám mây của bạn chưa?			
Dữ liệu của bạn trên hệ thống đám mây đã được mã hóa chưa?			
Bạn có thường xuyên xem xét lại quyền truy cập vào hệ thống đám mây không?			
Bạn có theo dõi hoạt động bất thường trên hệ thống đám mây không?			
12. Nhận thức và kĩ năng nhân viên			
Bạn đã tổ chức đào tạo về an ninh mạng thường xuyên cho nhân viên chưa?			
Bạn đã thực hiện các bài kiểm tra giả mạo phishing cho nhân viên chưa?			
Bạn đã xây dựng văn hóa bảo mật trong doanh nghiệp chưa?			
Bạn đã tạo các kênh để nhân viên có thể báo cáo các vấn đề về an ninh mạng chưa?			
Bạn đã cập nhật tài liệu đào tạo dựa trên các mối đe dọa mới nhất chưa?			
13. Xử lý sự cố			
Bạn đã có kế hoạch xử lý sự cố với vai trò rõ ràng cho từng bộ phận/cá nhân chưa?			
Bạn đã thiết lập quy trình liên lạc khi xảy ra sự cố an ninh chưa?			

Bạn đã diễn tập kế hoạch xử lý sự cố bằng cách mô phỏng các tình huống khác nhau chưa?			
Bạn đã có nhật ký sự cố để phân tích sau khi sự cố kết thúc chưa?			
Bạn đã có kế hoạch xử lý sự cố cho các loại cảnh báo an ninh khác nhau chưa?			
14. Tuân thủ quy định			
Bạn đã xác định được các quy định về bảo mật dữ liệu liên quan đến hoạt động của mình chưa?			
Bạn đã tuân thủ các quy định như GDPR, HIPAA hoặc các luật khác chưa?			
Bạn có tài liệu hóa các hoạt động liên qua đến bảo mật để phục vụ cho việc kiểm tra tuân thủ không?			
Bạn có tìm kiếm hướng dẫn pháp lý và tuân thủ chúng để đáp ứng các quy định mới không?			
Bạn có thường xuyên cập nhật các biện pháp bảo mật để phù hợp với những thay đổi trong quy định không?			
15. Giám sát và cảnh báo			
Bạn đã triển khai hệ thống SIEM (Security Information and Event Management - quản lý thông tin và sự kiện bảo mật) chưa?			
Bạn có đang theo dõi log mạng và hệ thống để phát hiện hoạt động bất thường không?			
Bạn có thiết lập cảnh báo tự động cho các sự cố an ninh tiềm ẩn không?			
Bạn có thường xuyên xem xét và phân tích log bảo mật không?			
Bạn đã có kế hoạch xử lý sự cố cho các loại cảnh báo an ninh khác nhau chưa?			
16. Phát triển phần mềm an toàn			
Doanh nghiệp đã triển khai các kĩ thuật viết phần mềm an toàn chưa?			
Doanh nghiệp đã tiến hành kiểm tra và đánh giá bảo mật mã nguồn?			
Các ứng dụng phần mềm được cập nhật và vá lỗi thường xuyên hay không?			

Các ứng dụng có được kiểm tra lỗ hổng bảo mật đã biết hay chưa?			
Doanh nghiệp đã có quy trình SDLC (secure development lifecycle - quy trình phát triển phần mềm an toàn) hay chưa?			
17. Sao lưu và khôi phục dữ liệu			
Dữ liệu và hệ thống quan trọng có được sao lưu thường xuyên?			
Bản sao lưu được lưu trữ ở đâu? Trên máy chủ khác hay trên cloud?			
Quy trình khôi phục dữ liệu đã được kiểm tra chưa?			
Các hạ tần quan trọng có hệ thống dự phòng không?			
Doanh nghiệp đã có kế hoạch khôi phục sau thảm họa?			
18. Bảo mật thiết bị di động			
Doanh nghiệp đã triển khai giải pháp quản lý thiết bị di động (MDM)?			
Thiết bị di động có được bật mã hóa không?			
Nhân viên được đào tạo về các biện pháp bảo mật thiết bị di động?			
Phần mềm trên thiết bị di động được cập nhật thường xuyên?			
Các thiết bị đó có khả năng xóa dữ liệu từ xa hay không?			
19. Bảo mật thiết bị IoT			
Bạn đã thiết lập mật khẩu mạnh và mã hóa cho thiết bị IoT chưa?			
Bạn đã tách biệt thiết bị IoT khỏi mạng lưới quan trọng của doanh nghiệp chưa?			
Bạn có thường xuyên cập nhật firmware cho thiết bị IoT không?			
Bạn đã tắt các tính năng không cần thiết trên thiết bị IoT chưa?			
Bạn có theo dõi và đánh giá hoạt động, bảo mật của thiết bị IoT không?			
20. Sử dụng mạng xã hội an toàn			
Bạn đã đào tạo nhân viên về cách sử dụng mạng xã hội an toàn chưa?			

Doanh nghiệp đã có hướng dẫn về việc chia sẻ thông tin công ty trên mạng xã hội chưa?			
Bạn có theo dõi hoạt động mạng xã hội để nắm bắt các thông tin liên quan đến công ty không?			
Bạn có thường xuyên cập nhật cài đặt quyền riêng tư cho tài khoản mạng xã hội của công ty không?			
Bạn đã có kế hoạch ứng phó với các sự cố an ninh mạng xã hội chưa?			
21. Bảo hiểm an ninh mạng			
Bạn đã xem xét sử dụng bảo hiểm an ninh mạng để giảm thiểu rủi ro tài chính chưa?			
Bạn đã xem xét kỹ các điều khoản và phạm vi bảo hiểm chưa?			
Bạn có cập nhật gói bảo hiểm phù hợp với tình hình an ninh mạng của doanh nghiệp không?			
Bạn đã thông báo về chính sách bảo hiểm an ninh mạng đến các bên liên quan chưa?			
Bạn có hợp tác với bên cung cấp bảo hiểm trong việc đảm bảo an ninh mạng và ứng phó sự cố không?			