

Bản tin nhanh về Pháp luật

Tháng 9 năm 2025

CẦN LÀM GÌ KHI TỔ CHỨC THÔNG TIN TÍN DỤNG BỊ TẤN CÔNG MẠNG

Ngày 10 tháng 9 năm 2025, Trung tâm Ứng cứu khẩn cấp không gian mạng quốc gia (VNCERT) xác nhận một vụ tấn công mạng nghiêm trọng nhằm vào Trung tâm Thông tin Tín dụng Quốc gia Việt Nam (CIC), đơn vị trực thuộc Ngân hàng Nhà nước Việt Nam. Cuộc tấn công có dấu hiệu truy cập trái phép với mục đích đánh cắp dữ liệu cá nhân.

Ngay sau đó, VNCERT đã triển khai các biện pháp kỹ thuật và điều tra khẩn cấp, phối hợp cùng các công ty an ninh mạng hàng đầu, CIC và các cơ quan chức năng của Ngân hàng Nhà nước. Mức độ ảnh hưởng của vụ vi phạm dữ liệu vẫn đang được điều tra, tuy nhiên cảnh báo đã được phát đi trên toàn hệ thống tài chính nhằm giảm thiểu rủi ro tiềm ẩn.

Tại Sao Vấn Đề Này Quan Trọng

Theo quy định pháp luật bảo vệ dữ liệu cá nhân tại Việt Nam, các tổ chức cung cấp thông tin tín dụng như CIC thường đóng vai trò là **Bên Xử lý Dữ liệu (Data Processor)**, trong khi các ngân hàng là **Bên Kiểm soát Dữ liệu (Data Controller)**.

Sự phân biệt này đặc biệt quan trọng trong các tình huống vi phạm dữ liệu:

- CIC phải thông báo cho các ngân hàng đối tác.
- Các ngân hàng phải đánh giá rủi ro và thông báo cho cơ quan chức năng có thẩm quyền.
- Tùy vào mức độ nghiêm trọng của vụ việc, ngân hàng có thể phải thông báo cho các cá nhân bị ảnh hưởng.

Điều này tạo ra một chuỗi thông báo nhiều tầng, làm tăng yêu cầu tuân thủ và vận hành.

Khuyến Nghị Dành Cho Các Ngân Hàng và Tổ Chức Tài Chính

Trước sự việc này, các ngân hàng cần nhanh chóng thực hiện:

1. **Đánh giá mức độ ảnh hưởng** – Xác minh xem dữ liệu khách hàng do mình quản lý có bị ảnh hưởng hay không.
2. **Phối hợp với CIC** – Đảm bảo chia sẻ thông tin kịp thời và chính xác.
3. **Thực hiện đánh giá rủi ro** – Xác định khả năng và mức độ ảnh hưởng đến cá nhân.
4. **Chuẩn bị thông báo** – Thông báo cho Bộ Công an (MPS) trong trường hợp cần thiết.
5. **Hướng dẫn khách hàng** – Cảnh báo về nguy cơ lừa đảo, giả mạo hoặc đánh cắp danh tính từ dữ liệu bị rò rỉ.

Sự kiện này nhấn mạnh tầm quan trọng của việc sẵn sàng ứng phó sự cố, giám sát nhà cung cấp và phối hợp xử lý trong ngành tài chính Việt Nam.

KPMG Luôn Sẵn Sàng Hỗ Trợ

Trong bối cảnh rủi ro an ninh mạng ngày càng gia tăng, phản ứng kịp thời và phối hợp hiệu quả là yếu tố then chốt. **KPMG sẵn sàng hỗ trợ** các ngân hàng và tổ chức tài chính trong việc:

- Tư vấn quy trình thông báo theo quy định pháp luật
- Đánh giá tác động của sự cố vi phạm dữ liệu
- Nâng cao năng lực an ninh mạng và giám sát nhà cung cấp
- Tăng cường khả năng ứng phó sự cố

Với đội ngũ chuyên gia đa ngành, KPMG hỗ trợ doanh nghiệp quản lý rủi ro, tăng cường tuân thủ và xây dựng niềm tin thông qua sự kết hợp giữa hiểu biết pháp luật chuyên sâu và năng lực kỹ thuật toàn diện.

Liên hệ với chúng tôi ngay để được hỗ trợ và tư vấn.

Liên hệ với chúng tôi

Email: info@kpmg.com.vn

Mọi thông tin trong tài liệu này đều là thông tin chung và không nhằm mục đích cung cấp tư vấn cho trường hợp cụ thể của bất kỳ tổ chức hay cá nhân nào. Mặc dù chúng tôi cố gắng cung cấp thông tin chính xác và cập nhật nhất một cách có thể, chúng tôi không thể đảm bảo rằng những thông tin này còn chính xác lúc người đọc nhận được hoặc sẽ duy trì tính chính xác này trong tương lai. Bất cứ ai cũng không nên quyết định hành động dựa trên những thông tin trong tài liệu này nếu không có sự tư vấn phù hợp từ các chuyên gia sau khi xem xét từng tình huống cụ thể.

© 2025 Công ty TNHH KPMG, Công ty TNHH Thuế và Tư vấn KPMG, Công ty Luật TNHH KPMG, Công ty TNHH Dịch vụ KPMG, đều là công ty trách nhiệm hữu hạn một thành viên được thành lập tại Việt Nam và là công ty thành viên trong tổ chức toàn cầu của các công ty KPMG độc lập, liên kết với KPMG International Limited, một công ty trách nhiệm hữu hạn theo bảo lãnh được thành lập tại Vương Quốc Anh. Tất cả các quyền được bảo hộ.

Tên và biểu tượng KPMG là nhãn hiệu thương mại được cấp phép sử dụng cho các công ty thành viên độc lập của tổ chức các công ty KPMG toàn cầu.



Quét mã QR để truy cập website:
kpmg.com.vn