KPMG 30+ YEARS IN VIETNAM & CAMBODIA

Hồi chuông cảnh tỉnh từ sự cố CrowdStrike

BÀI HỌC KINH NGHIỆM VỀ PHỤC HỒI VÀ DUY TRÌ HOẠT ĐỘNG KINH DOANH TRONG MỌI TÌNH HUỐNG

Ngày nay, công nghệ là nền tảng cho hầu hết mọi khía cạnh của hoạt động kinh doanh, sự ổn định và liên tục của hệ thống CNTT trở thành một yếu tố sống còn trước mọi gián đoạn đột ngột.

Với sự phổ biến rộng rãi của hệ điều hành Microsoft Windows trong môi trường doanh nghiệp, sự cố ngừng hoạt động hàng loạt do bản cập nhật bảo mật của CrowdStrike đã gây ra những hậu quả nghiêm trọng trên toàn cầu. Bắt đầu xuất hiện ở Úc, sự cố này nhanh chóng lan rộng, ảnh hưởng đến nhiều lĩnh vực quan trọng như tài chính, y tế, vận tải và hàng không.

Điều đáng chú ý là sự cố này không phải do một cuộc tấn công mạng gây ra, mà lại xuất phát từ một bản vá lỗi phần mềm, nhằm mục đích phát hiện và phân tích các mối đe dọa.

Và giờ đây nhiều đơn vị đang bắt đầu rà soát lại ***Quy trình phát triển phần mềm (SDLC) của các đối tác bên thứ ba***, cũng như đánh giá lại ***Kế hoạch kinh doanh liên tục (BCP)*** của mình.

PHÂN TÍCH SỰ CỐ

Các tệp dữ liệu bị lỗi được chạy ở cấp độ của trình điều khiển (*driver-level*), làm MS Windows bị treo và hiển thị "màn hình xanh chết chóc" *(blue screen of dea*th).

Cách khắc phục đơn giản, chỉ là khởi động máy vào chế độ "**Safe mode**", xóa các tập tin bị lỗi và khởi động lại lần nữa.

Tuy nhiên, hầu hết các hệ thống Microsoft hiện nay đều được mã hóa bằng BitLocker và cần nhập mã khôi phục (*recovery key*), còn các mã này thì rất dài.

Hậu quả là các quản trị viên hệ thống phải vào từng máy chủ, máy trạm; có trường hợp còn phải mang theo ổ đĩa USB chứa recovery key, di chuyển từ cơ sở này sang cơ sở khác, để lần lượt khôi phục thủ công hệ thống. Quá trình này tốn rất nhiều thời gian và công sức.

Sự cố này không chỉ đơn thuần là một vấn đề kỹ thuật, mà là một hồi chuông để các doanh nghiệp nhìn nhận một cách nghiêm túc về tầm quan trọng của việc xây dựng một quy trình SDLC chặt chẽ, cũng như một kế hoạch kinh doanh liên tục một cách toàn diện.

Lập kế hoạch dự phòng và phục hồi

Song song với việc khắc phục sự cố cấp bách, các doanh nghiệp cần xây dựng một nền tảng vững chắc cho tương lai bằng cách tích hợp các kế hoạch dự phòng toàn diện. Không chỉ tập trung vào hạ tầng công nghệ thông tin, các kế hoạch này còn phải bao quát các hoạt động kinh doanh cốt lõi, nhằm đảm bảo sự liên tục và ổn định trong mọi tình huống. Bền vững không đồng nghĩa với việc loại bỏ hoàn toàn rủi ro, mà là khả năng thích ứng và phục hồi nhanh chóng trước các sự cố. Các doanh nghiệp cần chuẩn bị sẵn sàng các phương án ứng phó để giảm thiểu tối đa tác động đến hoạt động kinh doanh.

Mặc dù không thể kiểm soát hoàn toàn các yếu tố bên ngoài, các doanh nghiệp hoàn toàn có thể chủ động tăng cường khả năng sẵn sàng để đối phó với mọi tình huống.

Kế hoạch sao lưu và phục hồi

Một chiến lược sao lưu và phục hồi hữu hiệu là thiết yếu đối với các đơn vị, nhằm giảm thiểu tác động từ các sự cố tương tự, bao gồm cả việc đánh giá khả năng khôi phục với quy mô lớn và nhiều áp lực. Các bước quan trọng cần thực hiện như sau:

1. Xây dựng một **chiến lược** sao lưu và phục hồi bám sát theo quy mô của tổ chức.
2. Thực hiện kiểm tra định kỳ để đảm bảo chiến lược sao lưu và phục hồi luôn được **bảo trì và cập nhật.**
3. Đánh giá **khả năng triển khai** chiến lược ở **quy mô** tương ứng với các **mục tiêu** khôi phục đã đề ra.
4. Tích hợp các **kịch bản sự cố mất khả năng truy cập** vào kế hoạch phục hồi sự cố, bao gồm cả tình huống mất truy cập vật lý, cũng như mất kết nối mạng đối với hệ thống đám mây, và bên thứ ba.
5. Thực hiện **đánh giá tác động** định kỳ để hiểu rõ hơn phạm vi ảnh hưởng khi một dịch vụ, ứng dụng cụ thể gặp sự cố hoặc mạng lưới bị xâm nhập.
6. **Rà soát danh sách** nhà cung cấp phần mềm và các bên thứ ba quan trọng để tránh phụ thuộc quá mức vào một số ít nhà cung cấp. Đồng thời, thực hiện **đánh giá định kỳ** về các biện pháp kiểm soát tại các bên thứ ba quan trọng.
7. Rà soát lại **chính sách bảo hiểm** (nếu có) liên quan đến các gián đoạn từ bên thứ ba để xác định khả năng giảm thiểu tác động tài chính thông qua bảo hiểm gián đoạn kinh doanh.

Tầm quan trọng của quản lý rủi ro đối tác thứ ba

Công tác thẩm định khi lựa chọn và giám sát các nhà cung cấp, đặc biệt là những bên có ảnh hưởng trọng yếu đến cơ sở hạ tầng CNTT cần được thực hiện cẩn thận. Bên cạnh đó, việc chọn lựa các nhà cung cấp có Quy trình phát triển phần mềm (**SDLC**) và Quản lý thay đổi (**change management**) nghiêm ngặt cũng là một yêu cầu thiết yếu. Các doanh nghiệp có thể bổ các hoạt động như sau:

1. **Đánh giá rủi ro theo thông lệ:** cần duy trì bao quát một danh mục các bên thứ ba; và thực hiện đánh giá đối với các bên thứ ba cung cấp phần mềm nghiệp vụ và dịch vụ kinh doanh. Đánh giá này cần xem xét khả năng doanh nghiệp có thể tiếp tục hoạt động, tình hình tài chính, cách thực hành bảo mật, lịch sử tuân thủ và các sự cố trước đây.
2. **Bảo vệ thông qua hợp đồng:** Xác định các Thỏa thuận Mức độ Dịch vụ (**SLA**) rõ ràng, bao gồm các yêu cầu về hiệu suất, thời gian hoạt động, và chế tài nếu không tuân thủ.
3. **Kiểm toán và giám sát:** Thực hiện rà soát thường xuyên các biện pháp kiểm soát của các bên thứ ba, bao gồm kiểm toán định kỳ, xem xét các báo cáo SOC1/SOC2, và duy trì liên lạc thường xuyên với các nhà cung cấp quan trọng để nhanh chóng giải quyết các vấn đề và mối lo ngại. Đặc biệt, cần chú trọng đến quy trình cập nhật và chứng nhận phần mềm, yêu cầu các nhà cung cấp kiểm tra và thẩm định kỹ lưỡng trước khi triển khai bất kỳ cập nhật nào là rất quan trọng.

KPMG có thể hỗ các doanh nghiệp như thế nào?

KPMG có thể giúp doanh nghiệp xây dựng một môi trường số an toàn, đáng tin cậy và vững chắc trước những rủi ro và mối đe dọa ngày càng gia tăng.

- **Rà soát và kiểm nghiệm các kế hoạch phục hồi dữ liệu (*data recovery*) và kinh doanh liên tục (*business continuity*).**
- **Rà soát và kiểm nghiệm chiến lực chống chịu trong bảo mật CNTT (*cyber resiliency*).**
- **Rà soát chiến lược quản lý chuỗi cung ứng và quản lý rủi ro bên thứ ba.**
- **Tăng cường nguồn lực và hỗ trợ khắc phục sự cố CrowdStrike hiện tại.**
- **Tối ưu hóa hoạt động bảo mật và công nghệ thông qua dịch vụ duy trì nguồn lực thuê ngoài (retainer), giúp doanh nghiệp nhanh chóng ứng phó với các tình huống bảo mật bất ngờ và giảm thiểu thiệt hại.**

Liên hệ với chúng tôi

Triệu Thị Thu Lan
Thành viên điều hành, Bộ phận Tư vấn CNTT

Ngũ Thái Ngọc Khiêm
Giám đốc kỹ thuật, Bộ phận Tư vấn CNTT

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