LÀM GÌ KHI DỮ LIỆU BỊ RÒ RỈ?

Rò rỉ thông tin nhạy cảm trong doanh nghiệp là điều rất khó tránh khỏi, ngay cả những tên tuổi lớn như Bank of America, LexisNexis, Time Warner, DSW Shoe Warehouse, T-Mobile, đại học Califonia, Berkeley gần đây đều đã bị xâm phạm dữ liệu. Trong thực tế có đến hàng trăm, h&agra
Rò rỉ thông tin nhạy cảm trong doanh nghiệp là điều rất khó tránh khỏi, ngay cả những tên tuổi lớn như Bank of America, LexisNexis, Time Warner, DSW Shoe Warehouse, T-Mobile, đại học Califonia, Berkeley gần đây đều đã bị xâm phạm dữ liệu. Trong thực tế có đến hàng trăm, hàng ngàn công ty có dữ liệu cá nhân nhạy cảm bị đột nhập nhưng không được công chúng biết nhiều. Diana McKenzie, Chủ tịch bộ phận CNTT của Công ty Neal, Gerber & Eisenberg, một hãng luật tại Chicago, nói: "Có bệnh viện vô tình cho biết thông tin về một vài bệnh nhân AIDS, hoặc có ngân hàng tình cờ tiết lộ với người gửi tiền toàn bộ thông tin về tình hình tài chính của một ai đó. Có hàng tấn ví dụ như vậy". Đối với các Giám đốc CNTT (CIO), cần phải hiểu hai sự việc sau: Vấn đề không còn là liệu công ty bạn có thể bị rò rỉ dữ liệu không mà là khi nào sẽ bị. Do vậy, bạn cần biết phải xử lý ra sao trước khi chẳng may công ty bạn nằm trong 10% có xì-căng-đan lan truyền khắp đất nước trên các phương tiện truyền thông. Một thực tế mới Scott Sobel, Phó Chủ tịch Công ty Levick Strategic Communications cho rằng lúc trước bạn còn đổ thừa là do tai nạn khách quan nhưng giờ đây mọi người sẽ tin rằng sự cố xảy ra là do ai đó cẩu thả hay cố ý phá hoại. Do vậy, bạn cần có giải pháp đối với sự việc ngay lập tức. Nhưng nếu chỉ dựa vào cách xử lý mà lâu nay bạn vẫn thường dùng để đối phó với các mối đe doạ truyền thống như virus hay tin tặc xâm nhập thì cũng chưa đủ, bởi lẽ ngày nay các nguy cơ có thể xuất hiện từ các nguồn rất đa dạng. Rich Baich, Giám đốc điều hành của Công ty PricewaterhouseCoopers, trước đây là chuyên gia về an ninh thông tin cho Công ty ChoicePoint, cho biết: "Những thất bại của các công ty khi xử lý sự cố trong năm qua bắt buộc họ phải thiết kế lại cách đối phó với những tình huống tương tự trong tương lai". Đầu năm nay, người ta phát hiện ChoicePoint đã làm lộ thông tin đóng giả là các doanh nghiệp hợp pháp. Theo Baich, các công ty cần tạo ra một cơ chế tập trung và phổ biến cho nhân viên hoặc công chúng để họ báo cáo các nguy cơ xâm phạm dữ liệu, kể cả những hành động không đòi hỏi kỹ thuật cao. Tương tự đường dây điện thoại nóng cho khách hàng, mỗi công ty phải có một đội phản ứng nhanh được đào tạo bài bản, hành động theo một sơ đồ quyết định hình cây phân cấp và đưa ra quyết định phù hợp tuỳ thuộc vào bản chất của vấn đề. Dựa vào đặc thù của mỗi tổ chức mà quy ước xử lý sự cố cụ thể được lập ra. Bạn có thể chọn báo cáo sự cố trực tiếp với người tổng cố vấn, hoặc Giám đốc an ninh CNTT (CSO), hay chủ tịch công ty. Dù bạn chọn cách nào đi nữa, quy trình báo cáo phải được định nghĩa và thống nhất trước. "Tập trung công việc xử lý về một mối sẽ giúp tránh được thói quen phổ biến là xem nhẹ báo cáo về các sự cố", McKenzie nhận xét. "Tôi không nhớ đã bao nhiêu lần nhìn thấy nhân viên quên hỏi số điện thoại hay thậm chí tên người đã gọi". Tinh thần đồng đội/hợp tác Thời mà việc khắc phục sự cố an ninh thông tin chỉ một mình bộ phận CNTTT thực hiện nay đã qua rồi. Ngày nay, bộ phận giao tế (PR) và pháp lý cần tham gia càng nhanh càng tốt, ngay cả khi bạn vẫn đang xem xét mức độ của vấn đề. McKenzie nói: "Trong lúc bạn bắt đầu sửa chữa, ghi nhận và hiểu được vấn đề, phải có ngay luật sư bắt tay vào việc giảm rủi ro và bộ phận PR chuẩn bị công việc phát ngôn với bên ngoài". Ví dụ như tại công ty cung cấp dịch vụ Vanguard Managed Solutions, khi xảy ra sự cố an ninh được xem là nghiêm trọng, bộ phận tiếp thị, pháp lý và CNTT phải cùng nhau nghiên cứu xác định sẽ thông báo vụ việc với khách hàng như thế nào. Việc công khai thông tin cũng phải phù hợp với luật định. Baich khuyên: "Nếu cảnh sát yêu cầu bạn giữ kín miệng vì sợ rằng tiết lộ với

công chúng sẽ cản trở việc điều tra, bạn hãy lấy cho bằng được văn bản yêu cầu đó nhằm tránh các rắc rối sau này". Một số chuyên gia cho rằng các công ty cần xây dựng các biện pháp xử lý thống nhất để phản ứng nhanh hơn. "Việc công khai thông tin đôi khi cần được thực hiện nhanh chóng, và sẽ chẳng hay ho gì nếu bắt đầu bằng một mẩu giấy trắng", Peter Gregory, nhà chiến lược an ninh của VantagePoint Security LLC, nói. Tốc độ có tính toán Nhưng đừng hấp tấp. "Có thể bạn không muốn chờ hai ngày, nhưng bạn có thể chờ 20 phút", Gregory khuyên. "Bạn cần làm theo trình tự các thủ tục trong trường hợp khẩn cấp để trước khi người phụ trách PR đứng trước micrô thì dòng thông tin đã chảy đúng lộ trình từ nơi phát hiện rò rỉ đến bộ phận CNTT và ghé qua bộ phận PR và pháp lý". McKenzie cũng nhận xét rằng chúng ta nên phản ứng với tốc độ thận trọng. Mặc dù xử lý chậm trễ rất nguy hại nhưng cũng phải xem xét thực hiện cho hợp lý vì có thể cả nước sẽ biết đến vụ việc này. Để tránh cáo buộc rằng bạn đã không ra tay đủ nhanh để giải quyết vấn đề, McKenzie gợi ý thuê một chuyên gia tư vấn điều tra CNTT - ngay cả khi bạn cho rằng đội ngũ CNTT của mình đủ khả năng phân tích các nhật ký web và các dữ liệu khác một cách có hiệu quả. Điều này sẽ chứng tỏ bạn đang xem xét vấn đề một cách nghiêm túc. Nếu ai đó kiện bạn vì bị thiệt hại thì nhân viên PR cũng đưa ra một lý lẽ tốt rằng bạn đã thuê một ai đó ngay lập tức. "Chúng tôi đã thuê sát thủ này để giúp giải quyết vấn đề nhanh gọn". Bạn nên ghi nhật ký theo dõi bất kỳ hành động nào mà đội ngũ an ninh thực hiện và bất kỳ người nào có liên lạc với họ. "Khi tất cả đều được ghi vào nhật ký, sẽ dễ dàng hơn khi có ai đó hỏi điều gì đã xảy ra", Baich nói. Cuối cùng, khi đến thời điểm cần phải thông báo với khách hàng hay công chúng về vụ việc, hãy tỏ ra đồng cảm và trấn an mọi người. Những người bị thiệt hại do những sự cố này thường cảm thấy thiếu sự đồng cảm trong tình cảnh của mình. Nếu bạn không có thái độ quan tâm tử tế thì khả năng kiện tụng rất cao. Một sự cố an ninh thông tin xảy ra sẽ làm nhiều người nghi ngờ khả năng của công ty liệu có tiếp tục hoạt động tốt được không. Do vậy, bạn phải suy nghĩ kỹ trước khi phát ngôn nhằm làm cho giới truyền thông và khách hàng tin tưởng bạn đang kiểm soát được tình hình và đang giải quyết vụ việc.