CÁC MẸO BẢO MẬT CHO THẾ GIỚI WEB 2.0

Phản ứ

Phản ứng của doanh nghiệp trước dòng chảy mới Web 2.0 rất khác nhau. Dưới đây là một số mẹo giúp bạn lựa chọn chính sách phát triển bảo mật và thực tiễn phù hợp nhất cho tổ chức của mình. Các mẹo này được xây dựng dựa trên giới hạn quy định của nhiều website mạng xã hội cùng quy tắc của các thiết bị mini, trình tin nhắn tức thời. Ngoài ra chúng tôi cũng cung cấp một số mẹo mức chuyên gia trong hoạt động tuyên truyền chính sách Web 2.0 mới tới nhân viên trong công ty.

Mẹo thứ nhất: "Canh giữ" các bí mật doanh nghiệp trong thế giới Web 2.0

Không có cách thức nào được gọi là hoàn hảo có thể loại trừ một trăm phần trăm nguy cơ rò rỉ thông tin trong môi trường blog. Do đó, sử dụng kết hợp nhiều phương pháp như hàng rào phòng thủ, phần mềm chủ động dò tìm xâm phạm và chương trình ngăn chặn là một lựa chọn sáng suốt.

• Chúng ta thử đánh giá lại xem liệu có cần update chương trình anti-virus, chương trình bảo vệ mã độc hại cho lưu lượng Web? Chúng ta sẽ xem xét cách thức tổng hợp, theo lời khuyên của các chuyên gia ở Gartner: phần mềm diệt virus, bộ lọc đường dẫn URL, các điều khiển ứng dụng, các dịch vụ Website nổi tiếng và kỹ thuật tìm kiếm an toàn.

• Thành lập một Uỷ ban giám sát blog, tức một nhóm nhân viên có nhiệm vụ giám sát các hoạt động viết blog bên trong công ty và quản lý phục vụ nhu cầu của nhân viên.

• Liên tục cập nhật chính sách về quyền sử dụng, nội quy thành viên, bí mật thương mại và nhiều chính sách khác để quản lý blog và các website xã hội như MySpace, YouTube.

• Cân nhắc vấn đề liệu có nên triển khai hoạt động giám sát và kỹ thuật lọc nội dung, update các công cụ lọc URL.

Mẹo thứ hai: Bảo vệ mạng và dữ liệu trước các thiết bị mini?

Một trong những đe doạ lớn nhất đối với mạng và dữ liệu bảo mật ngày nay đến từ các thiết bị siêu nhỏ gọn. Quá tinh vi ư? Đúng vậy! Không thể khắc phục được ư? Chưa hẳn! Chúng ta hãy bắt đầu với một số biên pháp phòng tránh sau đây:

• Đưa ra quy định nêu rõ ai được quyền dùng các thiết bị này và được dùng trong trường hợp nào.

• Xác định chính xác số lương thiết bị có trong tổ chức là bao nhiêu và kiểm tra xem liệu nhân viên có sử dụng thiết bị cá nhân riêng khi làm việc không. Đánh giá liệu phần mềm diệt virus đang sử dụng có thể bảo vệ thực sự an toàn mạng doanh nghiệp của mình trước các malware đến từ thiết bị bên ngoài không.

• Sao lưu chính sách, quy định với kỹ thuật, công nghệ. Chỉ cho phép thiết bị sở hữu bên trong doanh nghiệp hoạt động trên mạng. Xem xét việc dùng các ứng dụng để loại bỏ các truy cập không xác định đến từ cổng USB. Triển khai các quy định bảo vệ dữ liệu như mã hoá dữ liệu nhạy cảm để dữ liệu được an toàn cho dù thiết bị mini có bị mất. Nếu cần, nâng cấp phần mềm để loại bỏ malware từ các thiết bị như USB.

Mẹo thứ ba: Quản lý nguy cơ bảo mật từ trình tin nhắn tức thời

Hầu hết mọi tổ chức đều không hoàn toàn cấm sử dụng chương trình tin nhắn tức thời (IM) tại nơi làm việc. Các chuyên gia đưa ra lời khuyên rằng nên cân nhắc nhiều mối nguy hiểm có thể đến từ IM và triển khai quy định, chính sách bảo mật cần thiết.

• Kiểm tra công nghệ sử dụng trong doanh nghiệp và cân bằng với các yếu tố khác trước khi quyết định có cấm sử dụng IM hay không.

• Xem xét vấn đề kết hợp chặt chẽ IM với các quy định đã được xây dựng trong sử dụng e-mail ở giai đoạn đầu thông qua IM và thực hiện theo trường hợp thực tế tốt nhất.

• Xác định trước các quy định công nghiệp và quy định nội bộ đặt ra cho hoạt động lưu trữ IM và xây dựng kế hoạch tương ứng cho phù hợp.

• Đình chỉ ngay lập tức các tin nhắn IM vi phạm quy định công nghiệp và thông báo cho người lãnh đạo hoặc nhân viên uỷ quyền.

Mẹo thứ tư: Nói cho nhân viên hiểu, làm cho nhân viên theo

Tất cả công nghệ hiện đại nhất trên thế giới không thể giúp bạn đảm bảo an toàn thông tin nếu nhân viên của chính bạn không hiểu và tuân theo các quy định đã đặt ra. Vậy thì:

• Đầu tiên, cần phải hiểu nhân viên của mình, sử dụng phương tiện truyền thông hiệu quả nhất để tiến hành hội thảo hay đưa ra các thông điệp cụ thể về quy tắc, quy định tới từng nhân viên. Bà mẹ của những đứa trẻ thường thích cái gì càng đơn giản càng tốt, như các bản ghi nhớ ngắn gọn, mạch lạc dễ nghe, dễ đọc và dễ nhớ. Còn các quý ông lại thường thích tin nhắn hay e-mail vì nó nhanh và chi tiết.

• Sử dụng kỹ thuật truyền thông tương tác, như video game, các câu hỏi trắc nghiệm thử tài

nhanh. Phương pháp này đơn giản mà hiệu quả, gây được hứng thú cho nhân viên vì nó mang tính giải trí, nhưng vẫn đem lại tác dụng giáo dục.

• Tránh sử dụng theo kiểu ra lệnh, cấp trên bảo cấp dưới phải tuân theo, vì rất dễ gây phản ứng ngược đối với nhân viên trẻ. Tuyên truyền với tấn suất mỗi năm một lần sẽ không đem lại hiệu quả gì, vì thời gian như vậy không đủ nhiều để các quy định còn đọng lại trong đầu nhân viên.

• Cố gắng đưa ra các thư tin hoặc e-mail hài hước, vui nhộn và đặc sắc như gửi thư với một loại cum từ "Bạn có biết?" ở đầu mỗi đoạn, vừa mang tính giải trí, vừa có tác dụng giáo dục.

• Với các buổi gặp trực tiếp nhân viên, đừng nên chỉ nói cái gì được thực hiện và tiến hành (như mã hoá máy tính để bàn) mà còn phải giải thích tại sao càn làm như vậy. Khuyến khích câu hỏi từ phía nhân viên và đưa ra câu trả lời càng súc tích, ngắn gọn nhưng chính xác càng tốt. Như thế không chỉ làm thoả mãn trí óc nhân viên, khiến họ cảm thấy được tôn trọng, được lắng nghe mà ngay những người quản lý cũng học hỏi thêm được nhiều ý tưởng để nâng cao chính sách, quy định và hành động sao cho đặt hiệu quả cao nhất.

• Đưa ra thông tin cảnh báo liên quan đến bảo mật nhưng có thể áp dụng được cho các thiết bị bên ngoài nơi làm việc. Như các rủi ro có thẻ gặp phải khi chia sẻ bài hát trên iPod mức ngang hàng là một ví dụ. Ai cũng sẽ quan tâm đến những điều có thể giúp ích cho cuộc sống cá nhân trước tiên.

• Tổ chức các bài nói chuyên của chuyên gia bảo mật hoặc nhân viên kinh doanh về tầm quan trọng của bảo mật thông tin. Điều đó sẽ có sức thuyết phục với nhân viên quan tâm đến các vấn đề kinh doanh chứ không phải theo cách nghĩ thông thường của họ là đánh đồng cùng với các vấn đề IT.