MƯỜI KHUYNH HƯỚNG BẢO MẬT HIỆN NAY

Trong một bài phát biểu quan trọng tại Hội nghị bảo mật Hack in the Box diễn ra tại Kuala Lampua (Malaysia) hồi tháng trước, Bruce Schneiver – trưởng phòng công nghệ của hãng cung cấp dịch vụ bảo mật quản lý Counterpane Internet Security đã xác định 10 khuynh hướng tác động đến bảo mật thông tin ngày nay.

1. Thông tin có giá trị hơn.

Amazon.com tin tưởng vào thông tin để thực hiện mua bán sách trực tuyến dễ dàng qua hệ thống mua bán "một cú click". Tương tự, hoạt động kinh doanh của Pets.com cũng phát triển nhanh chóng với quan điểm cơ sở dữ liệu khách hàng của công ty "là thứ quý giá nhất mà họ có", Bruce nói.

Thông tin cũng có giá trị trong điều khiển truy cập như cung cấp chức năng đăng nhập đơn và thẩm định cho người dùng, buộc thực thi các điều luật đã quy định, sử dụng thông tin giúp tìm ra tội phạm và thu thập chứng cứ.

2. Mạng trở thành cơ sở hạ tầng then chốt.

Internet vốn không được xây dựng để trở thành cơ sở hạ tầng then chốt. "Điều này chỉ mới xảy ra gần đây". Các hệ thống có tầm quan trọng cao không ngừng chuyển sang khung thiết kế cho Internet.

Internet đã giúp các công ty vận hành hiệu quả hơn, dễ dàng trong giao tuyếp giữa người với người. Nhưng cũng có những mối nguy hiểm kinh tế đe doạ thực sự trong đó. "Nếu mức sử dụng Internet giảm, hay một bộ phận của Internet giảm hiệu suất, nó thực sự ảnh hưởng rất lớn tới nền kinh tế".

3. Người dùng không tự kiểm soát thông tin của mình một cách phù hợp

Chẳng hạn các hãng cung cấp dịch vụ Internet kiểm soát thông tin người dùng qua bản ghi lưu lại trên website người đó ghé thăm và thư điện tử gửi - nhận của họ. Cũng như thế một số hãng phân phối di động lưu lại bản copy số điện thoại khách hàng trên server của họ.

"Có nhiều giá trị trong thông tin về bạn. Nhưng bạn không kiểm soát được tính bảo mật của nó thậm chí với những thông tin cá nhân nguy hiểm nhất".

4. Hoạt động hacking mang tính chất tội phạm chuyên nghiệp ngày càng tăng

Hacking không còn là hoạt động "doạ ma" nữa. Những cuộc tấn công mang tính tổ chức do tội phạm chuyên nghiệp đứng đầu ngày càng tăng theo khuynh hướng lợi nhuận. "Tính chất tự nhiên

của các cuộc tấn công đã thay đổi, vì đối thủ chúng nhắm tới đang thay đổi".

Những cuộc khai thác liên quan đến kiểu tấn công DoS (denial of server) và phishing là hai ví dụ điển hình của hình thức tấn công tội phạm. Hơn nữa, có hẳn một thị trường đen cho các cuộc khai thác, cho phép kẻ tấn công thâm nhập vào các hệ thống IT tổng hợp đầu não.

5. Tính phức tạp là kẻ thù của bạn

"Các hệ thống ngày càng phức tạp hơn thì mức an toàn càng giảm đi". Schneirer còn gọi Internet là "bộ máy phức tạp nhất chưa từng được xây dựng".

Tính năng nâng cao trong công nghệ bảo mật đơn giản không theo kịp sự phát triển của Internet. "Bảo mật ngày càng tốt hơn, nhưng tính phức tạp là nguyên nhân cho những điều tồi tệ nhất còn phát triển nhanh hơn".

6. Tấn công nhanh hơn vá lỗi

Các lỗ hổng và điểm yếu bị khai thác được phát hiện nhanh hơn khả năng vá lỗi của các nhà sản xuất. Ở những trường hợp khác, các lỗ hổng trong hệ thống nhúng như router của Cisco System không thể được vá lỗi, để lại lỗ hổng nghiêm trọng cho các công ty.

7. Các loại sâu sinh ra tinh vi chưa từng có

Chúng bao gồm các công cụ đánh giá lỗ hổng, rà soát các hàng rào bảo vệ tổng hợp để tìm ra điểm yếu, dùng Google để thu thập thông tin một cách thông minh. "Khuynh hướng này là kết quả của các sâu đang chuyển mình thành tội phạm".

8. Điểm cuối là liên kết yếu nhất

"Sẽ không có vấn đề gì đối với kế hoạch thẩm định của bạn nếu chiếc máy từ xa không đáng tin cậy". Trong nhiều trường hợp máy tính nằm ngoài khả năng bảo mật của công ty là mắt xích yếu nhất. Các máy tính này thường bị tấn công bởi sâu, phần mềm gián điệp… là cơ hội cho những kẻ tấn công tận dụng.

9. Người dùng cuối có thể là mối đe doạ

Các công ty phát triển phần mềm có xu hướng bảo vệ chống người dùng cuối ngày càng tăng. Phần mềm DRM (digital rights management) là một ví dụ. "Như chúng ta đang thấy, bảo mật không bảo hộ người dùng mà là bảo vệ chống lại người dùng".

Một ví dụ điển hình là trường hợp của DRM, được cài đặt bởi Sony Corp. mà không cần sự cho phép của người dùng, phần mềm trở thành nguyên nhân đe doạ máy tính người dùng cuối. "Nguyên tắc và điều lệ quanh vấn đề này là một chiến trường lớn", Schneiver còn dự đoán cuộc chiến này sẽ diễn ra giữa phần mềm máy tính bảo vệ người dùng và phần mềm được thiết kế để

bảo vệ chống lại người dùng.

10. Các điều lệ sẽ chuyển hướng kiểm soát bảo mật

Không thiếu nguyên tắc chỉ dẫn một công ty nên điều khiển dữ liệu như thế nào. Các điều luật như Sarbanes – Oxley Act sẽ buộc mọi người phải tuân thủ chế độ kiểm soát bảo mật tổng hợp.

T.Thu