CƠ SỞ AN TOÀN THÔNG TIN

Bài 10. Một số vấn đề khác

1. An toàn vật lý
2. Nhân lực an toàn thông tin
3. Đảm bảo an toàn liên tục

An toàn vật lý

- Một trong những cách đơn giản nhất nhưng hiệu quả nhất để bảo vệ tài sản thông tin
- phụ thuộc vào ngân sách, kích thước, loại hình kinh doanh và sự nhạy cảm của thông tin
- bảo vệ ba loại tài sản chính: con người, trang thiết bị và dữ liệu

- Các hiểm họa:
  - Nhiệt độ quá cao
  - Các chất khí
  - Các chất lỏng
  - Sinh vật sống
  - Các vật phóng đi tự động như tên lửa…
  - Các chuyển động
  - Các bất thường về năng lượng
  - Con người
  - Các chất độc
  - Khói và lửa

- việc sao lưu dữ liệu, loại bỏ các dữ liệu nhạy cảm khi không cần dùng nữa (làm cho dữ liệu không thể truy cập khi không còn cần thiết: cắt nhỏ một tập giấy có chứa dữ liệu nhạy cảm trước khi vất đi)…

- Các bước…
  - Khảo sát các tòa nhà và giải quyết các vấn đề rõ ràng. Đặt ổ khóa bền vững trên cửa ra vào, lắp đặt các cửa sổ tốt, và chắc chắn rằng mọi người ngừng hoạt động vào cuối ngày
  - Đặt máy chủ và các thiết bị chuyên môn quan trọng khác trong phòng chuyên dụng với khóa cửa bên trong và không có cửa sổ
  - Cài đặt hệ thống điều hòa không khí và phát hiện lửa thích hợp trong các phòng đặc biệt

- Các bước…
  - Tránh để các thiết bị quan trọng gần lỗ thông hơi, đường ống, nhà bếp, nhà vệ sinh, bộ tản nhiệt và các mối nguy hiểm tương tự khác
  - Tắt màn hình vào ban đêm (điều này ngăn cản việc ánh sáng làm lộ)
  - Giữ một danh sách (hoặc kiểm kê tài sản) của tất cả các hệ thống, bộ nhớ, bộ xử lý, số seri, vị trí và ngày mua

- Các bước…
  - Gắn nhãn vĩnh viễn trên thiết bị có giá trị => có thể giúp tìm lại các thiết bị bị đánh cắp
  - Giữ các bản sao lưu cách xa các hệ thống nguồn, và nếu có thể tắt trang web
  - Trong khu vực chia sẻ, các khu vực công cộng hoặc mở (ví dụ như phòng tiếp khách) sử dụng khóa Kensington (cáp) để gắn các thiết bị có giá trị với bàn

- Các bước…
  - Giảm thiểu số lượng giấy và các thông tin nhạy cảm để lại trên bàn làm việc. Khóa tài liệu trong tủ (thiết lập chính sách “bàn sạch" nếu có thể)
  - Nếu công ty bao gồm khoảng hơn 15-20 người, nên sử dụng biển hiệu khách truy cập và khuyến khích nhân viên kiểm tra những khách không có người đi kèm

- Các bước:
  - Hộ tống tất cả các khách - không để cho họ đi lang thang xung quanh mà không có sự giám sát.
  - Duy trì sổ nhật ký khách truy cập và thời gian khi khách truy cập vào và rời trụ sở. Duy trì một sổ nhật ký khác cho việc vào ra đối với khu vực nhạy cảm, chẳng hạn như phòng máy tính.
  - Xem xét các camera quan sát trong lĩnh vực CNTT quan trọng (ví dụ như phòng máy chủ) và các khu vực tiếp tân
  - Thực hiện việc bảo hiểm thích hợp cho tổ chức ngay cả khi đó là một tổ chức nhỏ.

Nhân lực an toàn thông tin

- Bản mô tả công việc
- Phỏng vấn
- Thẩm tra lý lịch
  - Kiểm tra định danh: Xác nhận số định danh và số an sinh xã hội
  - Kiểm tra bằng cấp: Xác nhận của tổ chức liên quan, bằng cấp và chứng chỉ đạt được, và trạng thái chứng nhận
  - Xác minh việc làm trước đây: Xác nhận của nơi ứng viên đã làm việc, tại sao rời đi, đã làm gì, và trong bao lâu
  - Kiểm tra tham khảo: Xác nhận tham chiếu và tính toàn vẹn của các nguồn tham khảo
  - Lịch sử bồi thường của người lao động: Điều tra các khiếu nại từ bồi thường của nhân viên
  - Hồ sơ xe cơ giới: Điều tra hồ sơ lái xe, đình chỉ và DUI
  - Lịch sử ma túy: sàng lọc ma túy và sử dụng ma túy, quá khứ và hiện tại
  - Lịch sử tín dụng: Điều tra các vấn đề về tín dụng, các vấn đề tài chính và phá sản
  - Lịch sử tòa án dân sự: Điều tra sự tham gia của nguyên đơn hoặc bị đơn trong vụ án dân sự
  - Lịch sử tòa án hình sự: Điều tra về tình trạng hình sự, bắt giữ, kết án, và thời gian thụ án
- Hợp đồng tuyển dụng
- Định hướng cho nhân viên mới
- Đào tạo an toàn tại chỗ
- Đánh giá hiệu suất
- Chấm dứt/ rời khỏi tổ chức:
  - Quyền truy cập vào các hệ thống của tổ chức phải bị loại bỏ
  - Phải trả lại các thiết bị di động
  - Ổ đĩa cứng phải được an toàn
  - Phải thay đổi khóa tủ tập tin
  - Phải thu hồi quyền truy cập thẻ chìa khóa
  - Hộ tống ra khỏi cơ sở của tổ chức

- Cân nhắc an toàn đối với những người không phải là nhân viên:
  - Nhân viên tạm thời/ thời vụ

Tài liệu tham khảo

1. Whitman, Mattord, **Principles of Information Security** (5e), Cengage Learning, 2014


Q&A