**Phụ lục 1**

## *CÁC MỐI ĐE DỌA ĐỐI VỚI TÀI SẢN CNTT VÀ CÁC HẬU QUẢ*

Bảng dưới đây sẽ đưa ra các ví dụ về những mối đe dọa. Danh sách này có thể được sử dụng khi đánh giá các mối đe dọa. Các mối đe dọa có thể là do cố ý, vô ý hay do môi trường (tự nhiên) và có thể gây ra ví dụ như sự thiệt hại hay mất mát những dịch vụ cần thiết. Theo đó, danh sách liệt kê ra từng kiểu đe dọa như sau: C (cố ý), V (vô ý), MT (môi trường).

- C: được sử dụng cho tất cả các hành động cố ý nhằm tới các tài sản thông tin.

- V: được sử dụng cho tất cả các hành động do con người có thể vô ý gây ra thiệt hại lên các tài sản thông tin.

- MT: được sử dụng cho tất cả các sự cố không do hành động chủ quan của con người gây ra.

Các nhóm đe dọa không được sắp xếp theo thứ tự ưu tiên.

### 1. Các mối đe dọa điển hình

| Loại | Các mối đe dọa | Nguồn gốc |
|---|---|---|
| Thiệt hại về vật chất | Cháy/Hỏa hoạn | C, V, MT |
| | Thiệt hại về nguồn nước | C, V, MT |
| | Sự ô nhiễm | C, V, MT |
| | Tai nạn nghiêm trọng | C, V, MT |
| | Sự phá hủy thiết bị hoặc các phương tiện thông tin | C, V, MT |
| | Bụi, ăn mòn, đóng băng | C, V, MT |
| Các sự kiện thiên nhiên | Hiện tượng khí hậu | MT |
| | Hiện tượng địa chấn | MT |
| | Hiện tượng núi lửa | MT |
| | Hiện tượng khí tượng | MT |
| | Lũ lụt | MT |
| Thiệt hại các dịch vụ cần | Lỗi hệ thống điều hòa không khí hay hệ thống cấp nước | C, V |
| | Thất thoát trong cung cấp điện năng | C, V, MT |
| | Lỗi các trang thiết bị truyền thông | C, V |

| | | |
|---|---|---|
| thiết | | |
| Nhiễu do bức xạ | Bức xạ điện từ | C, V, MT |
| | Bức xạ nhiệt | C, V, MT |
| | Xung điện từ | C, V, MT |
| Gây hại tới thông tin | Nghe trộm các tín hiệu nhiễu gây hại tới thông tin | C |
| | Gián điệp từ xa | C |
| | Nghe trộm | C |
| | Mất trộm phương tiện thông tin hoặc tài liệu | C |
| | Mất trộm các thiết bị | C |
| | Phục hồi các phương tiện thông tin đã được tái chế hoặc đã bị loại bỏ | C |
| | Lộ thông tin | C, V |
| | Dữ liệu từ các nguồn không đáng tin cậy | C, V |
| | Giả mạo phần cứng | C |
| | Giả mạo phần mềm | C, V |
| | Phát hiện vị trí | C |
| Các lỗi kỹ thuật | Lỗi do thiết bị | V |
| | Sự cố, hỏng thiết bị | V |
| | Trạng thái bão hòa của hệ thống thông tin | C, V |
| | Sự cố phần mềm | V |
| | Vi phạm về bảo trì hệ thống thông tin | C, V |
| Các hành vi trái phép | Sử dụng trái phép thiết bị | C |
| | Sao chép gian lận phần mềm | C |
| | Sử dụng phần mềm giả mạo hoặc đã bị sao chép | C, V |
| | Sửa đổi làm sai hỏng dữ liệu | C |
| | Xử lý dữ liệu không hợp pháp | C |
| Gây hại tới các chức | Lỗi trong sử dụng | V |
| | Lạm dụng quyền | C, V |
| | Giả mạo quyền | C |
| | Từ chối hành động | C |
| | Vi phạm tính sẵn sàng của nhân viên. | C, V, MT |

| | | |
|---|---|---|
| năng | | |

**2. Các mối đe dọa do con người gây ra**

Đặc biệt phải xem xét tới các nguồn gốc mối đe dọa mà nguyên nhân là do con người. Các nguồn gốc này được ghi thành từng nhóm trong bảng dưới đây:

| Nguồn gốc mối đe dọa | Động cơ thực hiện | Các hậu quả có thể xảy ra |
|---|---|---|
| Hacker, cracker<br>Tin tặc, người ăn trộm tin | Thách thức<br>Lòng tự trọng<br>Sự nổi loạn, chống đối<br>Địa vị/Danh tiếng<br>Tiền bạc | Tấn công máy tính<br>Kỹ thuật lừa đảo<br>Xâm phạm, tấn công hệ thống<br>Truy cập hệ thống trái phép |
| Tội phạm máy tính | Phá hủy thông tin<br>Công bố thông tin bất hợp pháp<br>Lợi ích tài chính<br>Thay đổi dữ liệu trái phép | Tội phạm máy tính (ví dụ: theo dõi trên mạng)<br>Hành động gian lận (ví dụ: tái tạo, mạo danh, nghe lén thông tin)<br>Mua chuộc thông tin<br>Giả mạo gói tin<br>Xâm nhập hệ thống |
| Khủng bố | Tống tiền<br>Phá hủy<br>Khai thác<br>Trả thù<br>Lợi ích chính trị<br>Đưa thông tin | Bom/khủng bố<br>Chiến tranh thông tin<br>Tấn công hệ thống (ví dụ: từ chối phân phối dịch vụ)<br>Xâm nhập hệ thống<br>Giả mạo hệ thống |
| Gián điệp công nghiệp (cơ quan tình báo, các công ty, chính phủ nước ngoài, | Lợi ích cạnh tranh<br>Gián điệp kinh tế | Lợi ích quốc phòng<br>Lợi ích chính trị<br>Khai thác kinh tế<br>Trộm cắp thông tin<br>Xâm phạm quyền riêng tư cá nhân<br>Kỹ thuật lừa đảo<br>Xâm nhập hệ thống<br>Truy cập trái phép hệ thống (truy cập vào các thông tin đã |

| | | |
|---|---|---|
| các tổ chức quan tâm khác) | | phân loại, độc quyền, và/hoặc các thông tin liên quan đến công nghệ) |
| Những người trong nội bộ của tổ chức (được đào tạo kém, bất mãn, có ý xấu, cẩu thả, không trung thực, hoặc thôi việc) | Tò mò<br>Lòng tự trọng<br>Tin tức tình báo<br>Lợi ích tài chính<br>Sự trả thù<br>Lỗi và thiếu sót do vô ý (ví dụ: lỗi nhập dữ liệu, lỗi lập trình) | Tấn công vào chuyên viên<br>Tống tiền<br>Xem thông tin độc quyền<br>Lạm dụng máy tính<br>Gian lận và trộm cắp<br>Mua chuộc thông tin<br>Giả mạo dữ liệu đầu vào, dữ liệu bị hỏng<br>Nghe trộm<br>Mã độc hại (ví dụ như virus, Trojan horse)<br>Bán thông tin cá nhân<br>Lỗi hệ thống<br>Xâm nhập hệ thống<br>Phá hoại hệ thống<br>Truy cập hệ thống trái phép |

## Phụ lục 2

## *DANH SÁCH CÁC ĐIỂM YẾU*

Bảng dưới đây đưa ra những ví dụ về các điểm yếu trong những khu vực khác nhau, bao gồm các ví dụ về những mối đe dọa mà có thể khai thác các điểm yếu này. Danh sách này giúp đánh giá các mối đe dọa và điểm yếu, nhằm xác định các tình huống sự cố liên quan. Cần phải nhấn mạnh rằng, trong một số trường hợp thì các mối đe dọa khác cũng có thể khai thác các điểm yếu này.

| **Kiểu** | **Những ví dụ về các điểm yếu** | **Những ví dụ về các mối đe dọa** |
|---|---|---|
| Phần cứng | Bảo trì thiết bị không đầy đủ/cài đặt lỗi các phương tiện lưu trữ | Vi phạm về bảo trì hệ thống thông tin |
| | Thiếu phương án thay thế định kỳ | Phá hủy thiết bị hoặc phương tiện thông tin |
| | Dễ ảnh hưởng bởi độ ẩm, bụi, bẩn | Bụi, ăn mòn, đóng băng |
| | Nhạy cảm với bức xạ điện từ | Bức xạ điện từ |
| | Thiếu biện pháp thay đổi cấu hình hiệu quả | Lỗi trong sử dụng |
| | Dễ ảnh hưởng bởi biến đổi điện áp | Mất nguồn cung cấp điện năng |
| | Dễ ảnh hưởng bởi thay đổi nhiệt độ | Hiện tượng khí tượng học |
| | Phần lưu trữ không được bảo vệ | Trộm cắp các phương tiện thông tin hoặc tài liệu |
| | Thiếu cẩn thận khi loại bỏ | Trộm cắp các phương tiện thông tin hoặc tài liệu |
| | Sao chép không được kiểm soát | Trộm cắp các phương tiện thông tin hoặc tài liệu |
| | **Những ví dụ về các điểm yếu** | **Những ví dụ về các mối đe dọa** |
| | Quy trình kiểm thử phần mềm | Lạm dụng quyền |

| | | |
|---|---|---|
| Phần mềm | thiếu hoặc không có | |
| | Lỗ hổng phổ biến trong phần mềm | Lạm dụng quyền |
| | Không "tắt máy" khi rời khỏi máy trạm | Lạm dụng quyền |
| | Loại bỏ hoặc tái sử dụng các phương tiện lưu trữ mà không xóa hết dữ liệu đúng cách | Lạm dụng quyền |
| | Thiếu kiểm định | Lạm dụng quyền |
| | Cấp sai quyền truy cập | Lạm dụng quyền |
| | Phần mềm phân phối quá rộng rãi | Sai lệch dữ liệu |
| | Áp dụng các chương trình ứng dụng cho các dữ liệu sai về mặt thời gian | Sai lệch dữ liệu |
| | Giao diện người dùng phức tạp | Lỗi trong sử dụng |
| | Thiếu tài liệu | Lỗi trong sử dụng |
| | Phạm vi thiết lập không chính xác | Lỗi trong sử dụng |
| | Ngày tháng không chính xác | Lỗi trong sử dụng |
| | Thiếu cơ chế nhận dạng và xác thực như xác thực người dùng | Giả mạo quyền |
| | Bảng mật khẩu không được bảo vệ | Giả mạo quyền |
| | Việc quản lý mật khẩu kém | Giả mạo quyền |
| | Kích hoạt dịch vụ không cần thiết | Xử lý dữ liệu bất hợp pháp |
| | Phần mềm mới hoặc chưa ổn định | Sai chức năng phần mềm |
| | **Những ví dụ về các điểm yếu** | **Những ví dụ về các mối đe dọa** |
| | Chỉ dẫn kỹ thuật không rõ ràng hoặc không đầy đủ cho những nhà phát triển phần mềm | Sai chức năng phần mềm |
| | Thiếu biện pháp thay đổi hiệu quả | Sai chức năng phần mềm |
| | Không kiểm soát được việc tải và | Giả mạo phần mềm |

| | | |
|---|---|---|
| | sử dụng phần mềm | |
| | Thiếu bản sao lưu | Giả mạo phần mềm |
| | Thiếu sự bảo vệ đối với tòa nhà, các cửa ra vào và cửa sổ | Trộm cắp các phương tiện thông tin hoặc tài liệu |
| | Lỗi khi đưa những báo cáo quản lý | Sử dụng trái phép thiết bị |
| Mạng | Thiếu bằng chứng về việc gửi hoặc nhận được một thông điệp | Từ chối hành động |
| | Đường truyền thông không được bảo vệ | Nghe trộm |
| | Luồng thông tin nhạy cảm không được bảo vệ | Nghe trộm |
| | Khớp nối cáp yếu | Lỗi các trang thiết bị viễn thông |
| | Điểm lỗi đơn | Lỗi các trang thiết bị viễn thông |
| | Thiếu nhận biết và chứng thực của người gửi và người nhận | Giả mạo quyền |
| | Kiến trúc mạng không an toàn | Gián điệp từ xa |
| | Truyền đi những mật khẩu ở dạng rõ ràng (mật khẩu không được mã hóa) | Gián điệp từ xa |
| | Quản lý mạng không thích đáng | Tình trạng bão hòa của hệ thống thông tin |
| | Các kết nối mạng công cộng không được bảo vệ | Sử dụng trang thiết bị trái phép |
| | **Những ví dụ về các Điểm yếu** | **Những ví dụ về các Mối đe dọa** |
| Nhân | Sự vắng mặt của nhân viên | Vi phạm tính sẵn sàng của nhân viên |
| | Thủ tục tuyển dụng không đầy đủ | Phá hủy trang thiết bị hay phương tiện thông tin |

| | | |
|---|---|---|
| sự | Đào tạo về an toàn không đầy đủ | Lỗi trong sử dụng |
| | Việc sử dụng phần mềm và phần cứng không đúng | Lỗi trong sử dụng |
| | Thiếu nhận thức về bảo mật | Lỗi trong sử dụng |
| | Thiếu cơ chế giám sát | Xử lý dữ liệu bất hợp pháp |
| | Thiếu giám sát công việc của nhân viên | Trộm cắp các phương tiện thông tin hoặc tài liệu |
| | Thiếu chính sách cho việc sử dụng đúng phương tiện thông tin viễn thông và thông điệp | Sử dụng trang thiết bị trái phép |
| Địa điểm | Không cẩn thận khi kiểm soát hay kiểm soát không đầy đủ sự vào ra tại các toà nhà hay văn phòng | Phá hủy trang thiết bị hoặc phương tiện thông tin |
| | Vị trí ở một khu vực dễ bị lũ lụt | Lũ lụt |
| | Lưới điện không ổn định | Mất điện |
| | Thiếu sự bảo vệ đối với tòa nhà, các cửa ra vào và cửa sổ | Trộm cắp các trang thiết bị |
| Tổ chức | Thiếu thủ tục chính thức cho việc đăng ký và hủy đăng ký người dùng | Lạm dụng quyền |
| | Thiếu quy trình chính thức để xem xét (giám sát) quyền truy cập | Lạm dụng quyền |
| | **Những ví dụ về các điểm yếu** | **Những ví dụ về các mối đe dọa** |
| | Thiếu hoặc không có đầy đủ các quy định (liên quan đến an toàn) trong các hợp đồng với khách hàng và/hoặc các bên thứ ba | Lạm dụng quyền |
| | Thiếu thủ tục giám sát các phương tiện xử lý thông tin | Lạm dụng quyền |
| | Việc kiểm tra (giám sát) nội bộ thiếu thường xuyên | Lạm dụng quyền |
| | Thiếu thủ tục nhận biết và đánh giá rủi ro | Lạm dụng quyền |

| | | |
|---|---|---|
| | Thiếu ghi chép báo cáo khuyết điểm trong quản trị và vận hành | Lạm dụng quyền |
| | Việc đáp ứng bảo trì dịch vụ không thỏa đáng | Vi phạm về bảo trì hệ thống thông tin |
| | Thiếu hoặc không có đầy đủ các thỏa thuận mức độ dịch vụ | Vi phạm về bảo trì hệ thống thông tin |
| | Thiếu thủ tục kiểm soát sự thay đổi | Vi phạm về bảo trì hệ thống thông tin |
| | Thiếu thủ tục chính thức về kiểm soát ghi chép tài liệu ISMS | Sai lệch dữ liệu |
| | Thiếu thủ tục chính thức để giám sát bản ghi ISMS | Sai lệch dữ liệu |
| | Thiếu thủ tục chính thức cho việc xác thực các thông tin công khai sẵn có | Dữ liệu từ các nguồn không đáng tin |
| | Thiếu phân bố trách nhiệm an toàn thông tin phù hợp | Từ chối hành động |
| | Thiếu kế hoạch liên tục trong nghiệp vụ | Lỗi trang thiết bị |
| | Thiếu chính sách sử dụng e-mail | Lỗi trong sử dụng |
| | Thiếu thủ tục giới thiệu phần mềm trong hệ thống vận hành | Lỗi trong sử dụng |
| | **Những ví dụ về các Điểm yếu** | **Những ví dụ về các Mối de dọa** |
| | Thiếu ghi chép bản ghi quản trị và vận hành | Lỗi trong sử dụng |
| | Thiếu thủ tục xử lý thông tin đã được phân loại | Lỗi trong sử dụng |
| | Thiếu trách nhiệm an toàn thông tin trong mô tả công việc | Lỗi trong sử dụng |
| | Thiếu hoặc không có đầy đủ những điều khoản (liên quan đến an toàn thông tin) trong các hợp đồng với người lao động | Xử lý dữ liệu bất hợp pháp |
| | Thiếu hoạt động xử lý kỷ luật trong trường hợp xảy ra sự cố an | Trộm cắp các trang thiết bị |

| | | |
|---|---|---|
| | toàn thông tin | |
| | Thiếu chính sách chính thức đối với việc sử dụng thiết bị máy tính di động | Trộm cắp các trang thiết bị |
| | Thiếu quyền kiểm soát các tài sản bên ngoài tổ chức | Trộm cắp các trang thiết bị |
| | Thiếu hoặc không có đầy đủ các chính sách đối với bàn làm việc và máy tính của nhân viên | Trộm cắp các phương tiện thông tin hoặc tài liệu |
| | Thiếu giấy phép của các tổ chức xử lý thông tin | Trộm cắp các phương tiện thông tin hoặc tài liệu |
| | Thiếu cơ chế giám sát đối với các vi phạm an toàn thông tin | Trộm cắp các phương tiện thông tin hoặc tài liệu |
| | Việc xem xét quản lý thiếu thường xuyên | Sử dụng trang thiết bị trái phép |
| | Thiếu thủ tục cho việc báo cáo các điểm yếu về an toàn | Sử dụng trang thiết bị trái phép |
| | Thiếu các thủ tục và điều khoản liên quan đến quyền sở hữu trí tuệ (bản quyền) | Sử dụng phần mềm giả mạo hoặc đã bị sao chép |