|  |
| --- |
| HỌC VIỆN KỸ THUẬT MẬT MÃ  **KHOA ANTOÀN THÔNG TIN**  Logo HvKTMM  BÁO CÁO MÔN HỌC QUẢN LÍ VÀ XÂY DỰNG CHÍNH SÁCH AN TOÀN THÔNG TIN  **Đề tài: Khả năng giảm thiểu các mối đe dọa từ nội bộ doanh nghiệp của chính sách An toàn thông tin**  Nhóm sinh viên thực hiện:  TRẦN TUẤN LÂM                    AT150530  PHẠM VĂN THÁI                 AT150551  TRẦN ANH TUẤN AT150560    Giảng viên hướng dẫn: **PHẠM DUY TRUNG**  Hà Nội, 12-2021 |

MỤC LỤC

[MỤC LỤC 2](#_Toc90508684)

[DANH MỤC CÁC TỪ VIẾT TẮT 4](#_Toc90508685)

[LỜI NÓI ĐẦU 5](#_Toc90508686)

[CHƯƠNG 1. TỔNG QUAN VỀ CHÍNH SÁCH ATTT 6](#_Toc90508687)

[1.1 Khái niệm chính sách ATTT 6](#_Toc90508688)

[1.2 Mục đích của chính sách ATTT 6](#_Toc90508689)

[1.3 Chính sách ATTT bao gồm những gì 7](#_Toc90508690)

[1.4 Yêu cầu đặt ra đối với chính sách ATTT 8](#_Toc90508691)

[CHƯƠNG 2. TỔNG QUAN VỀ MỐI ĐE DỌA TRONG NỘI BỘ DOANH NGHIỆP 9](#_Toc90508692)

[2.1 Nhân viên nội bộ là gì? 9](#_Toc90508693)

[2.2 Mối đe dọa trong nội bộ là gì? 9](#_Toc90508694)

[2.3 Vì sao mối đe dọa trong nội bộ lại cực kỳ nguy hiểm? 10](#_Toc90508695)

[2.4 Các loại mối đe dọa trong nội bộ 11](#_Toc90508696)

[2.4.1 Đe dọa không chủ ý 11](#_Toc90508697)

[2.4.2 Đe doạ có chủ đích 11](#_Toc90508698)

[2.4.3 Các mối đe dọa khác 12](#_Toc90508699)

[2.5 Mối đe dọa trong nội bộ xảy ra như thế nào? 12](#_Toc90508700)

[2.5.1 Bạo lực 12](#_Toc90508701)

[2.5.2 Gián điệp 13](#_Toc90508702)

[2.5.3 Phá hoại 13](#_Toc90508703)

[2.5.4 Trộm cắp 14](#_Toc90508704)

[2.5.5 Mối đe dọa không gian mạng 14](#_Toc90508705)

[CHƯƠNG 3. CÁC PHƯƠNG PHÁP ĐÁNH GIÁ KHẢ NĂNG GIẢM THIỂU MỐI ĐE DỌA TỪ NỘI BỘ DOANH NGHIỆP CỦA CHÍNH SÁCH ATTT 15](#_Toc90508706)

[3.1 Trường hợp sơ suất trong nội bộ 15](#_Toc90508707)

[3.2 Thu thập chính sách ATTT 16](#_Toc90508708)

[3.3 Phân loại các trường hợp 17](#_Toc90508709)

[3.3.1 Động cơ 17](#_Toc90508710)

[3.3.2 Sự kiện kết tủa 18](#_Toc90508711)

[3.3.3 Mục tiêu tấn công 19](#_Toc90508712)

[CHƯƠNG 4. PHÂN TÍCH CÁC CHÍNH SÁCH ATTT TRONG VIỆC GIẢM THIỂU CÁC MỐI ĐE DỌA TỪ NỘI BỘ DOANH NGHIỆP 20](#_Toc90508713)

[4.1 Lỗi con người 21](#_Toc90508714)

[4.2 Chính sách không được tuân thủ 21](#_Toc90508715)

[4.3 Email 21](#_Toc90508716)

[4.4 Xử lý tài nguyên không đúng cách 22](#_Toc90508717)

[4.5 Vận chuyển dữ liệu 22](#_Toc90508718)

[4.6 Kỹ nghệ xã hội 23](#_Toc90508719)

[4.7 Bảo vệ chống lại vi-rút hoặc phần mềm độc hại 23](#_Toc90508720)

[4.8 Dữ liệu được bảo vệ không đúng cách 23](#_Toc90508721)

[4.9 Dữ liệu được sao chép vào thiết bị không an toàn 24](#_Toc90508722)

[4.10 Tổng hợp 24](#_Toc90508723)

[CHƯƠNG 5. KẾT LUẬN 27](#_Toc90508724)

DANH MỤC CÁC TỪ VIẾT TẮT

|  |  |
| --- | --- |
| **Từ viết tắt** | **Ý nghĩa** |
| ATTT | An toàn thông tin |

LỜI NÓI ĐẦU

Trong thời kỳ chuyển đổi số, vấn đề bảo mật thông tin dữ liệu nội bộ là thách thức của mọi doanh nghiệp. Công nghệ thông tin và mạng internet là những yếu tố không thể thiếu trong việc vận hành và quản lý các doanh nghiệp, tổ chức. Tuy nhiên, nếu không kết hợp bảo mật tốt sẽ dẫn tới những rủi ro tiềm ẩn vô cùng lớn. Những dữ liệu nội bộ công ty có thể bị mất, rò rỉ thông tin khách hàng, gây tổn thất cho khách hàng, những người liên quan và cho chính doanh nghiệp đó. Khách hàng cũng dễ mất niềm tin và có thể dẫn đến những vụ kiện không mong muốn cho doanh nghiệp. Kẻ xấu có thể làm tê liệt hệ thống, kiểm soát thông tin, dữ liệu của doanh nghiệp, tạo các tin giả gây ảnh hưởng danh tiếng, hoạt động sản xuất kinh doanh. Bên cạnh đó, hacker có thể lợi dụng sự sơ hở trong việc bảo mật kém của doanh nghiệp để gửi đường link giả mạo, phần mềm độc hại, sau đó đánh cắp dữ liệu một cách dễ dàng.

Lúc này, doanh nghiệp có thể đối mặt với thông tin giả mạo, thất thoát, rò rỉ dữ liệu, hoặc bị tung tin sai sự thật về công ty và điều này có thể gây tổn hại nghiêm trọng đến hệ thống, dữ liệu và danh tiếng của một tổ chức. Vì vậy việc quản lý và xây dựng một chính sách ATTT hiệu quả trong nội bộ doanh nghiệp là một điều cực kỳ cần thiết. Nội dung dưới đây chúng em xin trình bày về khả năng mà chính sách ATTT của doanh nghiệp giảm thiểu các mối đe dọa trong nội bộ doanh nghiệp .

# CHƯƠNG 1. TỔNG QUAN VỀ CHÍNH SÁCH ATTT

## 1.1 Khái niệm chính sách ATTT

Là một tài liệu giải thích cách một doanh nghiệp hoặc tổ chức thu thập – lưu trữ – quản lý – sử dụng – chia sẻ thông tin của người dùng, đối tác, hoặc nhân viên. Chính sách ATTT phải thỏa mãn các yêu cầu về bảo mật thông tin của người dùng

Là các tuyên bố hình thức nhằm mô tả các mục tiêu, ưu tiên và mục đích quản lí an toàn hệ thống thông tin cũng như cách đạt được những mục tiêu này

Ví dụ về chính sách dọn dẹp bàn làm việc:

* Các máy tính phải được khóa khi không có người sử dụng.
* Các tủ tài liệu chứa thông tin hạn chế hoặc nhạy cảm phải được đóng và khóa khi không sử dụng.
* Mật khẩu không được ghi lên trên các tờ ghi chú được dán trên hoặc dưới máy tính, cũng như không được viết chúng ra ở một vị trí dễ tiếp cận.
* Các bản in có chứa thông tin bị hạn chế hoặc nhạy cảm phải được xóa ngay lập tức khỏi máy in.

## Mục đích của chính sách ATTT

* Bảo vệ con người và thông tin
* Đưa ra các quy tắc cho hoạt động của người dùng, quản trị hệ thống, quản lí và nhân viên an ninh
* Cho phép nhân viên an ninh giám sát, thăm dò và điều tra
* Xác định và phê chuẩn hậu quả của sự vi phạm
* Xác định quan điểm cơ sở thống nhất về AT của tổ chức
* Hỗ trợ tối thiểu hóa rủi ro
* Hỗ trợ sự tuân thủ quy định và luật lệ

## Chính sách ATTT bao gồm những gì

* Phạm vi

Đảm bảo phạm vi cần giải quyết tất cả các thông tin trong hệ thống, các chương trình, dữ liệu, mạng nội bộ và tất cả nhân viên trong tổ chức của bạn. Ngoài ra, tổ chức có thể có những chính sách riêng về phạm vi cho từng phòng, bộ phận làm việc.

* Phân loại thông tin

Người điều hành tổ chức cần cung cấp những định nghĩa, nội dung cụ thể về việc đảm bảo an ninh thông tin và những giải pháp bảo mật mạng thay vì “bí mật” hoặc “hạn chế”.

* Mục tiêu quản lý rõ ràng

Tổ chức cần phải đưa ra những mục tiêu rõ ràng trong quản lý và xử lý, khắc phục các sự cố liên quan tới an toàn thông tin trong từng phân loại (ví dụ các nghĩa vụ pháp lý, quy định và hợp đồng đối với việc đảm bảo an ninh).

* Bối cảnh

Một chính sách an toàn thông tin phải được đặt trong trong bối cảnh cụ thể, có hướng dẫn quản lý và tài liệu bổ sung theo sát bối cảnh (ví dụ: được tất cả các cấp quản lý chấp thuận, tất cả các tài liệu xử lý thông tin khác phải phù hợp với nó).

* Có tài liệu hỗ trợ

Bao gồm các tài liệu hỗ trợ (ví dụ: vai trò và trách nhiệm, quá trình, tiêu chuẩn công nghệ, thủ tục, hướng dẫn, cách khắc phục và ứng cứu sự cố).

* Hướng dẫn cụ thể

Bao gồm các tài liệu hướng dẫn về phương pháp an ninh cho hệ thống nội bộ, phương pháp sử dụng internet an toàn trên mạng xã hội hay những yêu cầu trong bảo mật cho toàn bộ tổ chức (ví dụ: tất cả quyền truy cập vào bất kỳ hệ thống máy tính đều phải yêu cầu xác minh danh tính và xác thực, không chia sẻ cơ chế xác thực cá nhân).

* Có trách nhiệm rõ ràng

Tổ chức cần đưa ra những trách nhiệm cụ thể được xác lập (ví dụ: bộ phận công nghệ là nhà cung cấp duy nhất các đường dây viễn thông, bộ phận kỹ thuật là chuyên bảo mật hệ thống mạng, website và khắc phục sự cố).

* Hậu quả

Bao gồm các hậu quả cho sự không tuân thủ theo chính sách an toàn thông tin của tổ chức (ví dụ sa thải hoặc chấm dứt hợp đồng làm việc).

## Yêu cầu đặt ra đối với chính sách ATTT

* Kiểm soát được mọi mối đe dọa đối với hệ thống
* Bao gồm việc bảo vệ con người và thông tin
* Thiết lập luật lệ cho người dùng
* Xác định hậu quả của các vi phạm
* Tối thiểu hóa rủi ro cho tổ chức

# TỔNG QUAN VỀ MỐI ĐE DỌA TRONG NỘI BỘ DOANH NGHIỆP

## Nhân viên nội bộ là gì?

Nhân viên nội bộ là bất kỳ người nào có quyền truy cập hoặc có kiến ​​thức về các nguồn lực của tổ chức, bao gồm nhân sự, cơ sở vật chất, thông tin, thiết bị, mạng và hệ thống.

Ví dụ về nhân viên nội bộ có thể bao gồm:

* Một người mà tổ chức tin cậy, bao gồm nhân viên, thành viên tổ chức và những người mà tổ chức đã cung cấp thông tin nhạy cảm và quyền truy cập.
* Một người được cấp huy hiệu hoặc thiết bị truy cập xác định họ là người có quyền truy cập thường xuyên hoặc liên tục (ví dụ: nhân viên hoặc thành viên của tổ chức, nhà thầu, nhà cung cấp, người giám sát hoặc người sửa chữa).
* Một người mà tổ chức đã cung cấp máy tính hoặc quyền truy cập mạng.
* Một người phát triển các sản phẩm và dịch vụ của tổ chức; nhóm này bao gồm những người biết bí mật của các sản phẩm cung cấp giá trị cho tổ chức.
* Một người hiểu biết về các nguyên tắc cơ bản của tổ chức, bao gồm sự định giá, chi phí, điểm mạnh và điểm yếu của tổ chức.
* Một người hiểu biết về chiến lược và mục tiêu kinh doanh của tổ chức, được giao phó các kế hoạch trong tương lai hoặc các phương tiện để duy trì tổ chức và cung cấp phúc lợi cho mọi người của tổ chức.
* Trong phạm vi chức năng của chính phủ, nhân viên nội bộ có thể là người có quyền truy cập vào thông tin được bảo vệ, nếu bị xâm phạm, có thể gây thiệt hại cho an ninh quốc gia và an toàn công cộng.

## Mối đe dọa trong nội bộ là gì?

Mối đe dọa trong nội bộ là khả năng nhân viên nội bộ sử dụng quyền truy cập hoặc hiểu biết được ủy quyền của họ về một tổ chức để gây hại cho tổ chức đó. Tác hại này có thể bao gồm các hành vi có chủ đích xấu, tự mãn hoặc vô ý ảnh hưởng tiêu cực đến tính toàn vẹn, tính bảo mật và tính sẵn có của tổ chức, dữ liệu, nhân sự hoặc cơ sở của tổ chức.

Cơ quan An ninh mạng và Cơ sở hạ tầng (CISA) định nghĩa mối đe dọa nội bộ là mối đe dọa mà nhân viên nội bộ sẽ sử dụng quyền truy cập được ủy quyền của họ, dù cố ý hoặc không cố ý, để làm tổn hại đến nhiệm vụ, tài nguyên, nhân sự, cơ sở vật chất, thông tin, thiết bị, mạng của cơ, hoặc các hệ thống. Mối đe dọa này có thể biểu hiện thành thiệt hại thông qua các hành vi nội bộ sau:

* Gián điệp
* Khủng bố
* Làm tổn hại trái phép
* Tham nhũng, bao gồm tham gia vào tội phạm có tổ chức xuyên quốc gia
* Sự phá hoại
* Bạo lực nơi làm việc
* Sự mất mát hoặc suy giảm có chủ ý hoặc không cố ý của các nguồn lực hoặc năng lực của bộ phận

## Vì sao mối đe dọa trong nội bộ lại cực kỳ nguy hiểm?

Trong báo cáo SANS năm 2019 về các mối đe dọa nâng cao, các chuyên gia bảo mật đã xác định những lỗ hổng lớn trong phòng thủ mối đe dọa nội bộ do thiếu tầm nhìn về baseline của hành vi người dùng thông thường cũng như quản lý tài khoản người dùng đặc quyền, khiến cho chúng trở thành mục tiêu hấp dẫn hơn trong các trường hợp lừa đảo hoặc xâm phạm thông tin đăng nhập.

Phát hiện các mối đe dọa trong nội bộ không phải là nhiệm vụ dễ dàng đối với các đội an ninh. Nhân viên nội bộ đã có quyền truy cập hợp pháp vào tổ chức và thông tin, tài sản của tổ chức và việc phân biệt giữa người dùng bình thường và có chủ đích xấu là một thách thức. Họ là những người biết nơi đặt các vị trí nhạy cảm và cũng thường có level truy cập cao. Do đó, việc vi phạm dữ liệu do nhân viên nội bộ gây ra sẽ gây tốn kém hơn đáng kể cho các tổ chức so với việc gây ra bởi kẻ tấn công bên ngoài.

Trong nghiên cứu Cost of Insider Threats vào năm 2018 của viện Ponemon, các chuyên gia nhận thấy rằng tổn thất trung bình hàng năm của một mối đe dọa trong nội bộ là 8,76 triệu đô la, trong khi chi phí trung bình của một vụ vi phạm dữ liệu trong cùng kỳ là 3,86 triệu đô la.

## Các loại mối đe dọa trong nội bộ

Mối đe dọa nội bộ có thể là vô tình hoặc cố ý.

### Đe dọa không chủ ý

#### Sơ suất

Nhân viên nội bộ thuộc loại này khiến tổ chức bị đe dọa do sự bất cẩn. Những nhân viên nội bộ không cẩn thận thường quen thuộc với các chính sách ATTT hoặc CNTT nhưng lại chọn phớt lờ chúng, tạo ra rủi ro cho tổ chức. Các ví dụ bao gồm việc cho phép ai đó “Piggybacking” thông qua một lối vào được bảo mật, đặt sai vị trí hoặc làm mất thiết bị lưu trữ di động có chứa thông tin nhạy cảm và bỏ qua các thông báo cài đặt các bản cập nhật và bản vá bảo mật mới.

#### Tình cờ

Nhân viên nội bộ kiểu này nhầm lẫn gây ra rủi ro ngoài ý muốn cho tổ chức. Các tổ chức có thể làm việc thành công để giảm thiểu tai nạn, nhưng chúng sẽ xảy ra; chúng không thể được ngăn chặn hoàn toàn, nhưng những trường hợp xảy ra có thể được giảm thiểu. Các ví dụ bao gồm nhập sai địa chỉ email và vô tình gửi tài liệu kinh doanh nhạy cảm cho đối thủ cạnh tranh, vô tình hoặc vô tình nhấp vào siêu liên kết, mở tệp đính kèm chứa vi-rút trong email lừa đảo hoặc vứt bỏ tài liệu nhạy cảm không đúng cách.

### Đe doạ có chủ đích

Đe doạ có chủ ý là những hành động được thực hiện để gây tổn hại cho tổ chức vì lợi ích cá nhân hoặc hành động vì bất bình cá nhân. Nhân viên nội bộ có chủ đích thường được coi là “nhân viên nội bộ có chủ đích xấu”. Động cơ là lợi ích cá nhân hoặc gây hại cho tổ chức. Ví dụ, nhiều nhân viên nội bộ có động cơ “trả đũa” do những kỳ vọng chưa được đáp ứng liên quan đến việc không được công nhận (ví dụ: thăng chức, tiền thưởng, chuyến du lịch mong muốn) hoặc thậm chí là chấm dứt hợp đồng. Các hành động của họ bao gồm làm rò rỉ thông tin nhạy cảm, quấy rối cộng sự, phá hoại thiết bị hoặc gây bạo lực. Những người khác đã đánh cắp dữ liệu độc quyền hoặc tài sản trí tuệ với hy vọng hão huyền là thăng tiến sự nghiệp của họ.

### Các mối đe dọa khác

#### Đe dọa thông đồng

Một tập hợp con các mối đe dọa nội bộ có chủ đích xấu là các mối đe dọa thông đồng, trong đó một hoặc nhiều nhân viên nội bộ cộng tác với một tác nhân đe dọa bên ngoài để xâm phạm tổ chức. Những sự cố này thường liên quan đến việc tội phạm mạng tuyển dụng một nhân viên nội bộ hoặc một số nhân viên nội bộ để thực hiện hành vi gian lận, trộm cắp tài sản trí tuệ, gián điệp hoặc kết hợp cả ba.

#### Các mối đe dọa từ bên thứ ba

Ngoài ra, các mối đe dọa của bên thứ ba thường là các nhà thầu hoặc nhà cung cấp không phải là thành viên chính thức của một tổ chức nhưng đã được cấp một số cấp quyền truy cập vào các cơ sở, hệ thống, mạng hoặc con người để hoàn thành công việc của họ. Các mối đe dọa này có thể là mối đe dọa trực tiếp hoặc gián tiếp.

* Các mối đe dọa trực tiếp là những cá nhân hành động theo cách làm tổn hại đến tổ chức đã được chọn làm mục tiêu.
* Các mối đe dọa gián tiếp nói chung là các lỗ hổng trong hệ thống để lộ tài nguyên cho các tác nhân đe dọa không chủ ý hoặc có chủ đích xấu.

## Mối đe dọa trong nội bộ xảy ra như thế nào?

Các mối đe dọa nội bộ biểu hiện theo nhiều cách khác nhau: bạo lực, gián điệp, phá hoại, trộm cắp và các hành vi trên mạng. Các biểu hiện của mối đe dọa nội bộ được xác định cụ thể dưới đây.

Biểu hiện của mối đe dọa từ nhân viên nội bộ

### Bạo lực

Hành động này bao gồm đe dọa bạo lực, cũng như các hành vi đe dọa khác tạo ra môi trường đe dọa, thù địch hoặc lạm dụng.

* Bạo lực tại nơi làm việc hoặc tổ chức bất kỳ hành động hoặc đe dọa bạo lực thể chất, quấy rối, quấy rối tình dục, đe dọa, bắt nạt, đùa cợt xúc phạm hoặc hành vi đe dọa khác của đồng nghiệp hoặc cộng sự xảy ra tại nơi làm việc của một người hoặc trong khi một người đang làm việc .
* Khủng bố trong một hình hài mối đe dọa nội bộ là việc nhân viên, thành viên hoặc những người khác có liên kết chặt chẽ với một tổ chức sử dụng bạo lực bất hợp pháp hoặc đe dọa bạo lực để chống lại tổ chức đó. Mục tiêu của chủ nghĩa khủng bố là thúc đẩy một mục tiêu chính trị hoặc xã hội.

### Gián điệp

Gián điệp là hoạt động bí mật hoặc bất hợp pháp do thám một chính phủ, tổ chức, thực thể hoặc cá nhân nước ngoài để lấy thông tin bí mật nhằm phục vụ lợi ích quân sự, chính trị, chiến lược hoặc tài chính.

* Gián điệp kinh tế là hoạt động bí mật để lấy bí mật thương mại từ nước ngoài (ví dụ: tất cả các hình thức và loại thông tin tài chính, kinh doanh, khoa học, kỹ thuật, kinh tế hoặc kỹ thuật và các phương pháp, kỹ thuật, quy trình, thủ tục, chương trình hoặc mã để sản xuất ).
* Gián điệp chính phủ là các hoạt động thu thập thông tin tình báo bí mật của một chính phủ chống lại chính phủ khác để đạt được lợi thế chính trị hoặc quân sự. Nó cũng có thể bao gồm (các) chính phủ theo dõi các tổ chức doanh nghiệp như các công ty hàng không, công ty tư vấn, các tổ chức tư vấn hoặc các công ty vũ khí. Hoạt động gián điệp của chính phủ còn được gọi là thu thập thông tin tình báo.
* Gián điệp hình sự liên quan đến một công dân của một nước tiết lộ bí mật của chính phủ nước đó cho nước ngoài.

### Phá hoại

Phá hoại mô tả các hành động cố ý gây hại cho cơ sở hạ tầng vật lý hoặc ảo của tổ chức, bao gồm cả việc không tuân thủ các quy trình bảo trì hoặc CNTT, làm ô nhiễm không gian sạch, cơ sở vật chất bị hư hại hoặc xóa mã để ngăn chặn các hoạt động thường xuyên.

* Phá hoại vật chất là thực hiện các hành động có chủ ý nhằm gây hại cho cơ sở hạ tầng vật chất của tổ chức (ví dụ: cơ sở vật chất hoặc thiết bị).
* Phá hoại ảo đang thực hiện các hành động có chủ đích xấu thông qua các phương tiện kỹ thuật để làm gián đoạn hoặc ngừng hoạt động kinh doanh bình thường của tổ chức.

### Trộm cắp

Trộm cắp là hành động đơn giản của hành vi ăn cắp, cho dù là tiền hay tài sản trí tuệ.

* Tội phạm tài chính là hành vi lấy hoặc sử dụng trái phép hoặc bất hợp pháp tiền hoặc tài sản của một người, doanh nghiệp hoặc tổ chức với mục đích thu lợi từ đó.
* Trộm cắp tài sản trí tuệ là hành vi trộm cắp hoặc cướp ý tưởng, phát minh hoặc các sáng tạo của cá nhân hoặc tổ chức, bao gồm cả bí mật thương mại và sản phẩm độc quyền, ngay cả khi các khái niệm hoặc vật phẩm bị đánh cắp có nguồn gốc từ kẻ trộm.

### Mối đe dọa không gian mạng

Các mối đe dọa kỹ thuật số bao gồm trộm cắp, gián điệp, bạo lực và phá hoại bất kỳ thứ gì liên quan đến công nghệ, thực tế ảo, máy tính, thiết bị hoặc internet.

* Các mối đe dọa không chủ ý là sự phô bày không có chủ đích xấu(thường là do ngẫu nhiên hoặc không cố ý) đối với cơ sở hạ tầng CNTT, hệ thống và dữ liệu của tổ chức gây ra tổn hại không mong muốn cho tổ chức. Ví dụ bao gồm email lừa đảo, phần mềm giả mạo và “quảng cáo độc hại” (nhúng nội dung độc hại vào quảng cáo trực tuyến hợp pháp).
* Đe dọa có chủ ý là các hành động có chủ đích xấu được thực hiện bởi những người bên trong thù địch sử dụng các phương tiện kỹ thuật để làm gián đoạn hoặc tạm dừng hoạt động kinh doanh thường xuyên của tổ chức, xác định điểm yếu CNTT, lấy thông tin được bảo vệ hoặc nói cách khác là một kế hoạch tấn công thông qua quyền truy cập vào hệ thống CNTT. Hành động này có thể liên quan đến việc thay đổi dữ liệu hoặc chèn phần mềm độc hại hoặc các phần mềm gây khó chịu khác để làm gián đoạn hệ thống và mạng.

# CÁC PHƯƠNG PHÁP ĐÁNH GIÁ KHẢ NĂNG GIẢM THIỂU MỐI ĐE DỌA TỪ NỘI BỘ DOANH NGHIỆP CỦA CHÍNH SÁCH ATTT

Chương này sẽ mô tả các phương pháp thu thập và đánh giá hiệu quả của các chính sách ATTT trong doanh nghiệp trong việc đối phó với việc sơ suất làm tổn hại trong nội bộ bằng cách thảo luận về phương pháp thu thập các trường hợp sơ suất làm tổn hại trong nội bộ, sau đó nêu chi tiết về các chính sách đã được thu thập và cuối cùng là đánh giá các trường hợp (dựa trên mô hình mô tả đặc tính tấn công).

## Trường hợp sơ suất trong nội bộ

Khái niệm về một nhân viên nội bộ vừa rõ ràng vừa dễ hiểu. Mô tả này được cải tiến bởi Grietzer et al. để đưa ra định nghĩa về ý nghĩa của một mối đe dọa sơ suất (hoặc không cố ý) trong nội bộ. Việc sử dụng chính định nghĩa này đã hỗ trợ các chuyên gia trong việc thu thập thông tin về các trường hợp sơ suất trong nội bộ.

Diagram

Description automatically generated

*Hình 1. Một mô hình để nắm bắt các mối đe dọa nội bộ có chứa một số yếu tố chính: “Catalyst” đề cập đến lý do bao quát cho sự cố, "Actor Characteristics” nắm bắt trạng thái của tác nhân, “Attack Characteristics” trình bày chi tiết các yếu tố liên quan đến cuộc tấn công và cuối cùng là “Organisation Characteristics” bao gồm tài sản tổ chức và lỗ hổng bảo mật.*

Các chuyên gia đã thu thập được 60 trường hợp sự cố đáp ứng mô tả đặc điểm của một mối đe dọa sơ suất trong nội bộ từ một số từ các nguồn khác nhau, bao gồm: các bài viết, báo cáo chính thứcvà các bài viết có liên quan khác. Các chuyên gia không đặt ra hạn chế trên quy mô của các trường hợp đã được thu thập, việc đó đồng nghĩa với việc các chuyên gia đã xác định và thu thập các trường hợp mà kích thước và phạm vi của sự cố không phải là một trong những tiêu chí lựa chọn của các chuyên gia. Các chuyên gia đã thu thập các trường hợp với mục đích đưa ra các bộ phận tiêu biểu về các loại sự cố và cũng trong một loạt các ngành công nghiệp bị ảnh hưởng bởi mối đe dọa trong nội bộ. Những trường hợp mà các chuyên gia có thu thập tất cả các sự cố phản ánh đã được phát hiện và được báo cáo trong vòng 10 năm qua.

Các chuyên gia đã sử dụng mô hình đặc điểm của mối đe dọa trong nội bộ trước đây để cung cấp cơ sở cho việc phân tích các trường hợp đã thu thập được . Mô hình đã được tạo ra để nắm bắt tất cả các điểm dữ liệu quan trọng được liên kết với các trường hợp các mối đe dọa trong nội bộ (cả chủ đích xấu và không chủ đích xấu). Mô hình này tạo điều kiện thuận lợi cho việc nắm bắt các điểm chính trong một sự cố, và đã làm nổi bật các yếu tố thích hợp nhất liên quan đến những trường hợp mà các chuyên gia đã thu thập được. Điều này đã cung cấp cho các chuyên gia một tập dữ liệu nhất quán trên tất cả các trường hợp đã thu thập được. Một ví dụ của mô hình có thể được nhìn thấy trong Hình 1. Mô hình đặc điểm đã được sử dụng để mã hóa tập hợp các trường hợp được thu thập của các chuyên gia, bằng cách sử dụng một lập trình viên duy nhất.

## Thu thập chính sách ATTT

Các chuyên gia đã thu thập một mẫu 10 chính sách ATTT đã được công bố công khai trên Internet, qua một loạt các lĩnh vực khác nhau: học thuật (3 chính sách), chính quyền địa phương (3 chính sách), y tế (1 chính sách), tài chính (1 chính sách), khoa học và công nghệ (1 chính sách) và thực thi pháp luật (1chính sách). Các chính sách ATTT đã được chọn để đưa ra cái nhìn về các ngành phân phối trong các trường hợp thu thập được của mối đe dọa nội bộ. Ngoài các chính sách trong thực tế đã được thu thập, các chuyên gia cũng đã sử dụng các chính sách mẫu,công khai trên mạng. Lý do cho việc bao gồm chính sách mẫu trong mẫu phân tích của các chuyên gia là bởi vì việc những mẫu chính sách này sẽ được một số tổ chức sử dụng trong thực tế là điều có thể thấy trước được.Do thiếu tính khả dụng, các chính sách đã chọn không liên kết với các tổ chức được đại diện bởi các trường hợp sơ suất nội bộ của các chuyên gia. Tất cả các chính sách ATTT sử dụng trong nghiên cứu của các chuyên gia đã được ẩn danh.

## Phân loại các trường hợp

Mô hình trong Hình 1 được thiết kế để nắm bắt cả hai sự cố nội bộ chủ đích xấu và không chủ đích xấu. Việc ánh xạ các trường hợp thu được và thông qua thông tin trong tài liệu,cho thấy sự cần thiết phải mở rộng phạm vi của một số thành phần trong mô hình. Điều này nhằm đảm bảo rằng tất cả thông tin liên quan đã được thu thập cho các trường hợp mối đe dọa trong nội bộ. Dưới đây các chuyên gia thảo luận ngắn gọn về các sửa đổi được yêu cầu.

### **Động cơ**

Một trong những thay đổi rõ ràng nhất đó là được xác định là không có ý đồ xấu ở sự cố trong tất cả các trường hợp đã được phân tích. Điều này sau đó đã được nhấn mạnh bởi Jones và Ashenden, người chỉ ra rằng

Diagram

Description automatically generated

*Hình 2. Phân tích lý do, hành động và tác động của mối đe dọa trong nội bộ*

việc không có chủ đích xấu hoặc động cơ là một trong những yếu tố chính giúp tách các sự cố sơ suất trong nội bộ ra khỏi các hành vi cố ý của mối đe dọa trong nội bộ.

### Sự kiện kết tủa

Công việc trước đây của các chuyên gia mô tả sự kiện kết tủa như là một sự kiện quan trọng có khả năng khiến một nhân viên nội bộ trở thành mối đe dọa cho sếp của họ. Khái niệm về 'điểm tới hạn' không áp dụng trực tiếp khi chúng ta xem xét sự cố làm tổn hại nội bộ. Các trường hợp nghiên cứu tiết lộ rằng rất hiếm khi có một sự kiện duy nhất khiến một cá nhân tác động tiêu cực đến tổ chức của họ.Magklaras và Furnell đề xuất lý do cho sự sơ suất là sử dụng sai hệ thống máy tính: kiến ​​thức hệ thống không đầy đủ,các yếu tố có thể ảnh hưởng đến công việc liên quan đến hiệu suất (ví dụ: khối lượng công việc quá tải), và cuối cùng là thiếu nhận thức về đào tạo bảo mật. Khi xem xét về sự cố lộ thông tin nội bộ, chúng ta càng quan tâm đến lý do tại sao nhân viên mắc lỗi ở lần đầu tiên và do đó các chuyên gia mở rộng sự kiện kết tủa để xem xét lý do chung của sự cố, ví dụ như rò rỉdữ liệu nhạy cảm qua email có thể do được đào tạo không đầy đủ hoặc nhận thức chưa đúng đắn về chính sách.

### Mục tiêu tấn công

Khi xem xét một mối đe dọa có chủ đích xấu trong nội bộ , mục tiêu tấn công được vạch ra rất rõ ràng. Ví dụ, một nhân viên sao chép dữ liệu tổ chức nhạy cảm để chuyển cho một đối thủ cạnh tranh có mục tiêu xác định là làm rò rỉ thông tin của tổ chức đối thủ. Ngược lại với sự kiện kết tủa, khi xem xét mục tiêu tấn công của sự cố, các chuyên gia quan tâm đến việc nhân viên nội bộ đã muốn gì khi sự cố xảy ra (ví dụ: người dùng cố tải dữ liệu đến máy chủ tệp an toàn). Phân loại về các trường hợp được thu thập cung cấp cơ sở để so sánh phát hiện về một số các chính sách ATTT hiện có. Trong quá trình phân loại, rõ ràng có một số chủ đề lặp lại, trên tất cả các trường hợp đe dọa trong nội bộ. Hình 2 minh họa việc cô đọng lại các trường hợp thu thập được, chúng sẽ được sử dụng để phân tích phạm vi và tiện ích của các chính sách ATTT hiện có, được chia nhỏ thành ba loại chính:

* + Lý do - Nguyên nhân của sự cố là gì?
  + Hành động - Điều gì đã được thực hiện không chính xác?
  + Tác động - Tác động của sự cố là gì?

Sự phân loại, được liệt kê ở trên, cung cấp thông tin trọng tâm liên quan trực tiếp đến các loại điều khoản được quy định trong chính sách ATTT. Lấy ví dụ, các chuyên gia xem xét sự tác động của việc mất dữ liệu vật lý và điện tử vì một tổ chức thường sẽ có các phần riêng biệt của chính sách để kiểm soát việc quản lý dữ liệu được lưu trữ trong phần cứng hoặc trên phương tiện điện tử.

# PHÂN TÍCH CÁC CHÍNH SÁCH ATTT TRONG VIỆC GIẢM THIỂU CÁC MỐI ĐE DỌA TỪ NỘI BỘ DOANH NGHIỆP

Kết quả trong Bảng I cung cấp một cái nhìn tổng quan về phạm vi của mỗi chính sách ATTT khi so sánh với lý do và hành động của mối đe dọa trong nội bộ, như đã thấy trong trường hợp phân tích của các chuyên gia. Ở đây, Lý do là nguyên nhân của sự cố(ví dụ: sử dụng phần mềm không chính xác) và Hành động là điều đó đã được thực hiện không chính xác (ví dụ: một email đã bị gửi nhầm người nhận). Trong Bảng 1, các số chính sách tương ứng với các ngành sau: 1–3 Viện hàn lâm, 4–6 Chính quyền địa phương, 7 Y tế, 8 Tài chính, 9 Khoa học và công nghệ, 10 Thực thi pháp luật và 11–15 Chính sách mẫu. Dấu tích màu xanh lá cây cho biết

Table

Description automatically generated

*Bảng 1: Việc đảm bảo các chính sách ATTT khi so sánh với các lý do và hành động của mối đe dọa nội bộ*

rằng chính sách có chứa các điều khoản để giảm thiểu lý do hoặc hành động được liệt kê và dấu thập đỏ biểu thị việc thiếu độ bao quát trong một chính sách. Phần còn lại của mục này sẽ cung cấp một cái nhìn chi tiết hơn về việc phân tích chính sách của các chuyên gia, bao gồm thảo luận về các điều khoản liên quan từ các chính sách ATTT thu thập được.

## Lỗi con người

80% các chính sách bảo mật được phân tích chứa các điều khoản mà được coi là rủi ro của các sự cố trong đó lỗi của con người là yếu tố chính và đưa ra một số hình thức kiểm soát tại chỗ để chống lại nó. Ví dụ, một trong những chính sách học thuật được khảo sát có chứa một điều khoản nêu rõ các biện pháp kiểm soát phải được áp dụng để bảo vệ khỏi “lỗ hổng bảo mật, ví dụ: đánh địa chỉ không chính xác hoặc chuyển hướng sai, độ tin cậy chung và tính khả dụng của dịch vụ ”. Điều này trái ngược với kiểm soát về việc ngăn chặn việc sử dụng sai phần mềm trong một tổ chức, nơi 80% các chính sách được xét không yêu cầu thực hiện bất kỳ loại đào tạo phần mềm nào.Tuy nhiên, điều này đã xuất hiện thường xuyên hơn trong chính sách ATTT mẫu hơn chính sách doanh nghiệp. Ví dụ, một trong những chính sách được thực hiện từ chính quyền địa phương yêu cầu để đảm bảo tính toàn vẹn của dữ liệu tổ chức, nhân viên nên “được đào tạo về bất kỳ ứng dụng nàohọ được yêu cầu truy cập và bất kỳ gói phần mềm nào họ được yêu cầu sử dụng ”. Tuy nhiên, không có chính sách nào ghi lại đánh giá về tính phù hợp hoặc tính hiệu quả của việc đào tạo như vậy khi được thực hiện.

## Chính sách không được tuân thủ

Khi xem xét "Chính sách không được tuân thủ", các chuyên gia đang tập trung vào việc liệu có bất kỳ quy định nào mà nhân viên phải được đào tạo về bảo mật thông tin hay không. Trường hợp phân tích của các chuyên gia đã làm nổi bật hai lý do chính dẫn đến việc không tuân thủ chính sách: chính sách không được đầy đủ hoặc xác định kém, hoặc nhân viên không biết chính sách ATTT. Nghiên cứu sâu hơn về tài liệu cho thấy các lý do tiềm ẩn khác về việc tại sao điều này có thể xảy ra; ví dụ, chính sách không được tuyên truyền tốt hoặc chính sách làm cho nhân viên khó thực hiện nhiệm vụ của họ.

## Email

Trong khi phần lớn các chính sách được khảo sát (60%) có một số cân nhắc để sử dụng đúng email, điều này thường tập trung vào cách sử dụng email (ví dụ: “sử dụng e-mail cá nhân được cho phép với điều kiện chỉ sử dụng trong thời gian rảnhvà khi khối lượng công việc không nhiều ”). Rất ít lời nhắc được đưa ra để bảo vệ chống lại việc sử dụng sai email bằng việc đính kèm nhầm tệp (20%) hoặc gửi đến không đúng người nhận (27%).

## Xử lý tài nguyên không đúng cách

Phần lớn các chính sách được xem xét (73%) có hướng dẫn về việc xử lý an toàn các nguồn tài nguyên, tuy nhiên, ở đó có ít chính sách chứa thông tin về việc loại bỏ an toàn phần cứng (67%) so với việc xử lý an toàn các tài nguyên làm từ giấy (74%). Điển hình là xử lý an toàn các tài nguyên làm từ giấy như đặt các tài liệu vào đúng vị trí, theo phân loại (ví dụ: “tài liệu bị hạn chế và bí mật có thể được đặt trong các thùng rác bí mật, trong khi vật liệu bí mật phải được cắt nhỏ ”). Ngược lại, khi xem xét két xử lý phần cứng, các chính sách thường ít mang tính quy định hơn. Ví dụ: một trong những chính sách ATTT học thuật được thu thập yêu cầu nhân viên phải đảm bảo rằng dữ liệu "được và được làm sạch một cách an toàn khỏi thiết bị đó khi tháo bỏ chúng ”. Quy định này đang nhấn mạnh vào việc người lao động phải đảm bảo rằng dữ liệu nhạy cảm được xóa một cách an toàn khỏi bất kỳ phần cứng nào,có thể được xem như một sự phân bổ không phù hợp của nhiệm vụ. Khả năng người lao động phổ thông sẽ được nhắc nhở đầy đủ về việc làm sạch kỹ lưỡng và an toàn là không cao.

## Vận chuyển dữ liệu

Thuật ngữ "vận chuyển dữ liệu" được sử dụng để mô tả tiến trình vật lý của vận chuyển dữ liệu (bao gồm băng, đĩa, thiết bị USB và dữ liệu trên giấy) đến các khu vực khác nhau của một tổ chức (ví dụ: đến một địa điểm khác) hoặc tới một tổ chức đối tác. Sự an toàn trong vận chuyển dữ liệu phần lớn không được đề cập trong các chính sách ATTT đã được xét. Chỉ 13% các chính sách có các điều khoản để kiểm soát hành động này.Ví dụ: một chính sách học thuật cung cấp biện pháp bảo vệ chống lại điều này bằng cách quy định rằng “phải sử dụng phương tiện giao thông vận tải hoặc người giao thông đáng tin cậy". Đã có một số sự cố được ghi lại nơi các mặt hàng được vận chuyển không được đóng gói đầy đủ vànhư vậy đã bị hư hỏng trong quá trình vận chuyển. Chỉ một trong các chính sách mà các chuyên gia xem xét đã cân nhắc khía cạnh này của việc vận chuyển dữ liệuvới yêu cầu rằng “việc đóng gói phải đủ để bảo vệ gói hàng chống lại bất kỳ thiệt hại vật chất nào có thể phát sinh trong quá trình vận chuyển ”.

## Kỹ nghệ xã hội

Khi so sánh loại sự cố này với tập các chính sách ATTT đã thu thập được mà các chuyên gia đã phân tích chính sách cho các điều khoản cung cấp hướng dẫn về mức độ đáng tin cậy của thông tin. Đối với hầu hết các phần, đây là một cái gì đó không được đề cập tốt trong các chính sách được khảo sát, chỉ với 33% chứa hướng dẫn về cách ngăn chặn các cuộc tấn công kỹ thuật xã hội, tuy nhiên, hai trong ba chính sách từ học viện có thông tin về vấn đề này. Thông tin phổ biến nhất được cung cấp về kỹ thuật xã hội tập trung vào mức độ đáng tin cậy của một thông tin nhận được qua email (ví dụ: "bạn không nhất thiết phải tin những gì bạn nhận được trong một email - cụ thể là bạn không bao giờ được trả lời yêu cầu email bắt cung cấp tên người dùng hoặc mật khẩu ').

## Bảo vệ chống lại vi-rút hoặc phần mềm độc hại

Bảo vệ chống lại phần mềm độc hại là một trong những lĩnh vực được đề cập trong tất cả các chính sách trong mẫu của các chuyên gia. Các kiểm soát để bảo vệ chống lại phần mềm độc hại đã được quy định tốt, tất cả các chính sách đã yêu cầu “phần mềm chống vi-rút phù hợp được cài đặt và bảo trì ”. Trong một số trường hợp, điều này sẽ được xử lý bởi CNTT của tổ chức, ở những nơi khác, có một danh sách các nhà cung cấp phần mềm chống vi-rút được chấp nhận và cuối cùng là một số chính sách tổ chức chỉ yêu cầu cài đặt và duy trì phần mềm mà không nhắc gì đến việc những thứ gì nên được cài trên máy tính. Trong những trường hợp này nhấn mạnh vào việc nhân viên duy trì việc kiểm soát bảo mật toàn vẹn, điều này có thể được coi là một kỳ vọng không hợp lí khi đặt nó vào một nhân viên, vì họ rất ít có cơ hội quen với cách tiếp cận tốt nhất để ngăn chặn vấn đề này. Quả thực việc một nhân viên tải xuống phần mềm độc hại giả dạng phần mềm chống vi-rút là điều hoàn toàn có thể xảy ra.

## Dữ liệu được bảo vệ không đúng cách

Khi xem xét liệu dữ liệu có được bảo vệ không đúng cách hay không, các chuyên gia đang đề cập đến việc liệu dữ liệu có bị sai sót hay để lộ ra hay không. Nhiều chính sách ATTT (73%) được phân tích chứa các điều khoản được coi là bảo vệ dữ liệu nhạy cảm. Điều đơn giản nhất trong số các điều khoản này thường được đề cập đến là đảm bảo rằng tổ chức và nhân viên của tổ chức tuân thủchẳng hạn như Đạo luật bảo vệ dữ liệu khi đề cập đến tính bảo mật của dữ liệu nhạy cảm mà nhân viên được giao nhiệm vụ "Đảm bảo tuân thủ Đạo luật bảo vệ dữ liệu".

Các chính sách khác chi tiết hơn về các biện pháp kiểm soát và các biện pháp cần được sử dụng để đảm bảo dữ liệu đó (cả phần cứng và điện tử) đã được bảo vệ đầy đủ. Các chính sách đưa ra hướng dẫn để bảo vệ dữ liệu theo một số cách. Các trường hợp đe dọa nội bộ được phân tích đã làm nổi bật rằng cấu hình sai máy chủ web thường là nguyên nhân gây ra dữ liệu online bị hiển thị sai. Hơn một nửa(53%) các chính sách được phân tích đã giảm nhẹ đối với các loại mất mát dữ liệu, ví dụ, một chính sách ATTT học thuật yêu cầu rằng cần xem xét các vấn đề liên quan đến “ý nghĩa bảo mật và bảo vệ dữ liệu của việc công bố các đầu mục thư mục ”

## Dữ liệu được sao chép vào thiết bị không an toàn

Việc bảo vệ chống mất dữ liệu, bằng cách sao chép dữ liệu vào một thiết bị không an toàn, là một trong những vấn đề được đề cập trong tất cả các chính sách ATTT đã được xem xét. Có baphương pháp tiếp cận mà các chính sách đã thực hiện khi xem xét việc sử dụng các thiết bị di động. Cái đầu tiên là đơn giản nhất,nghiêm cấm sao chép dữ liệu vào ổ nhớ rời và mang nó ra khỏi tổ chức. Phương pháp tiếp cận thứ hai là yêu cầu tất cả các thiết bị có thể tháo rời, chứa dữ liệu nhạy cảm, cần được mã hóa trước khi chúng được mang ra khỏi tổ chức. Cuối cùng, cách tiếp cận thứ ba là bắt buộc bất kỳ thiết bị di động, máy tính xách tay hoặc phần cứng nào được bảo mật hoặc ẩn khỏi tầm nhìn khi bị xóa khỏi tổ chức và hoặc khi không được sử dụng.

## Tổng hợp

Phân tích được trình bày ở trên cho thấy rằng có rất nhiều sự khác biệt trên tất cả các chính sách trong mẫu của các chuyên gia. Tuy nhiên, có một mức độ tương đồng đối với các lĩnh vực nhất định trong các chính sách được phân tích. Ví dụ, tất cả trong số các chính sách được khảo sát có hướng dẫn về việc ngăn ngừa lây nhiễm phần mềm độc hại và cả về các phương pháp sao chép an toàn dữ liệu vào một thiết bị di động. Ngược lại, trong khi không có các lĩnh vực hoàn toàn bị bỏ qua bởi tất cả các chính sách thì chắc chắn lại có một số lĩnh vực được đề cập rất thưa thớt. Ví dụ, rất ít chính sách cân nhắc về việc giảm nhẹ chống lại việc dữ liệu bị mất hoặc bị hư hỏng trong quá trình vận chuyển. Điều này cũng đúng khi xem xét việc sử dụng email đúng cách; khi xem xét vấn đề gửi nhầm email người nhận hoặc đính kèm nhầm tệp vào email. Kết quả trong Bảng 1 minh họa điều đó, phần lớn, các chính sách bao gồm trong phân tích của các chuyên gia cung cấp mức độ bao phủ rộng hơn về "Hành động" hơn là "Lý do" liên quan đến một sự cố trong nội bộ. Hai trong số các chính sách ATTT được khảo sát không

A screenshot of a computer

Description automatically generated with medium confidence

*Hình 3. Các câu hỏi có thể được sử dụng để đánh giá mức độ phù hợp của chính sách ATTT chống lại mối đe dọa trong nội bộ*

cung cấp bất kỳ điều khoản nào để chống lại các nguyên do với các trường hợp sơ suất làm tổn hại nội bộ mà các chuyên gia đã xác định. Những lý do mà các chuyên gia phát hiện ra phần lớn có liên quan đến đào tạo nhân viên, chẳng hạn, việc cung cấp đào tạo bao gồm chính sách ATTT thông tin của tổ chức hoặc cách để sử dụng chính xác các gói phần mềm khác nhau. Các hành động, nói chung, liên quan đến việc kiểm soát công nghệ hoặc các tiến trình vật lý và như vậy được cho là dễ dàng hơn để ủy thác trong một chính sách ATTT.

Có lẽ cần lưu ý rằng trong bộ chính sách ATTT mẫu của các chuyên gia, không có chính sách nào cung cấp đầy đủ độ bao quát để chống lại tất cả các mối đe dọa nội bộ tiềm ẩn. Ngay cả chính sách với độ bao quát tốt nhất (chính sách 3 trong Bảng 1), chỉ cung cấp các hướng dẫn giúp ngăn ngừa 80% nguyên căn và 86,7% các hành động liên quan đến mối đe dọa trong nội bộ.

Dưới đây, các chuyên gia cung cấp phân tích về mức độ phù hợp của các chính sách khi so sánh với các trường hợp nội bộ được thu thập, dựa trên về lĩnh vực ngành của chính sách. Phân tích này giả định rằng các chính sách được thực hiện một cách hoàn hảo, điều này tất nhiên không có trong thực tế. Các chính sách 1–3 đều là từ khu vực học thuật và ngay cả khi kết hợp vẫn tồn tại một khoảng cách trong các chính sách liên quan đến các trường hợp do lỗi của con người, trong đó dữ liệu đã bị lộ chiếm 20% các trường hợp được nghiên cứu. Các chính sách thu thập từ chính quyền địa phương (chính sách 4–6) có lỗ hổng trong các lý do cho các sự cố trong biểu mẫu cấu hình không chính xác do lỗi của con người, chiếm 21,7% các trường hợp. Các hành động không cung cấp bất kỳ giảm nhẹ nào đối với một tệp được đính kèm nhầm vào email (10%) hoặc dữ liệu bị mất hoặc bị hỏng trong quá trình vận chuyển (3,3%). Các chính sách thu thập từ ngành y tế chỉ đưa ra hướng dẫn cho các trường hợp mà nguyên nhân là do thiếu nhận thức về chính sách, điều này có nghĩa là 55% các trường hợp được khảo sát đều có nguy cơ bị tấn công. Cũng chỉ xét cho một số lượng hạn chế các hành động (bảo vệ khỏi phần mềm độc hại và sao chép dữ liệu vào một thiết bị không an toàn), có nghĩa là chính sách này dễ bị tấn công bởi 83,3% các trường hợp. Chính sách 8 (lĩnh vực tài chính) thiếu thông tin để bảo vệ chống lại 58,8% nguyên do của các sự cố trong nội bộ,cũng như để hổng tới 51,5% các trường hợp được khảo sát. Cácchính sách của ngành khoa học và công nghệ thiếu các điều khoản chiếm 65% nguyên do cho sự cố nội bộ, nhưng cung cấp độ bao phủ tốt hơn chống lạicác hành động liên quan đến các trường hợp chỉ có 32,6% không được bao quát. Cuối cùng,chính sách 10 (thực thi pháp luật) đã cung cấp thông tin có thể có khả năng được bảo vệ khỏi 20% nguyên do trong các trường hợp được nghiên cứu, nhưng có khả năng dễ bị tấn công chỉ 24,3% trong số các trường hợp được khảo sát.

# KẾT LUẬN

Chính sách ATTT của một tổ chức là một tuyên bố quan trọng về những kỳ vọng của nhân viên, về hành vi và văn hóa của doanh nghiệp đó. Các mối đe dọa trong nội bộ là một mối quan tâm thực sự đối với tất cả các tổ chức và đe dọa đáng kể tới hệ thống, dữ liệu và danh tiếng của tổ chức, có lẽ còn hơn thế nữa khi nó gây ra bởi những nhân viên nội bộ có chủ đích xấu.

Bài viết này đã nêu bật lên các lĩnh vực chung, trong các chính sách ATTT thông tin của tổ chức, đã thiếu sót khi xét đến khả năng của chính sách trong việc tạo điều kiện ngăn chặn sự cố trong nội bộ. Các chuyên gia đã khảo sát 15 trường hợp của chính sách an toàn thông tin để xác định các lĩnh vực bao quát chính đối với mối đe dọa trong nội bộ. Rõ ràng là một số loại sự cố thường được xử lý hơn là những loại sự cố khác bởi bộ chính sách ATTT mẫu của các chuyên gia. Ví dụ, điều khoản được thấy trong tất cả các chính sách được khảo sát là bảo vệ chống lại sự lây nhiễm của phần mềm độc hại và cũng để ngăn chặn việc sao chép dữ liệu vào một thiết bị không an toàn. Có thể lập luận rằng đây là hai sự kiểm soát về mặt kỹ thuật đơn giản để triển khai và giám sát, trong khi một số lượng lớn các mối đe dọa tiềm ẩn khác rất khó để quản lý chỉ với các biện pháp kiểm soát công nghệ. Lấy ví dụ, sẽ rất khó để đảm bảo rằng các email chỉ chứa các tệp đính kèm hoặc người nhận chính xác.

Công việc được trình bày trong bài viết này được sử dụng để thiết lập rủi ro do nhân viên nội bộ sơ suất gây ra trong tổ chức, và mức độ mà các chính sách ATTT doanh nghiệp giúp giảm thiểu rủi ro này. Các chuyên gia đề xuất sự chuyên môn hóa của mô hình đang tồn tại để nắm bắt các điểm dữ liệu thích hợp mà sau đó có thể cô đọng lại thành một tập hợp các nguyên nhân, vector tấn công và tác động của một tổ chức. Hiện tại các chuyên gia đã sử dụng mô hình và thông tin này để đưa ra đánh giá về chính sách ATTT có thể truy cập công khai, để làm nổi bật điểm mạnh và điểm yếu của chúng khi xử lý các mối đe dọa này. Trong tương lai công việc của các chuyên gia sẽ xét một mẫu lớn hơn các trường hợp mối đe dọa nội bộ và một mẫu chính sách ATTT thông tin rộng hơn để xác định xem liệu mô hình của các chuyên gia có thể được sử dụng để xác định chính sách sàng lọc và các tùy chọn kiểm soát rủi ro cần được giải quyết hay không.

Nghiên cứu đã chỉ ra rằng các vấn đề trong nội bộ là vấn đề quan trọng và việc nghiên cứu của các chuyên gia nhấn mạnh sự bức thiết để có một chính sách mạnh mẽ khi xem xét việc giảm thiểu những sự cố. Trong tương lai, các chuyên gia sẽ xem xét các phương pháp mà một chính sách ATTT có thể được thiết kế để giải quyết trực tiếp mối đe dọa nội bộ.

Nhờ phân tích chính sách của các chuyên gia, họ đã có thể tạo ra một tập các câu hỏi có thể được hỏi về chính sách ATTT để giúp thực hiện việc tự đánh giá về mức độ bao quát của chính sách, đối với các sự cố trong nội bộ. Bộ câu hỏi có thể được nhìn thấy trong Hình 3. Trong công việc tương lai, các chuyên gia sẽ xem xét phát triển thêm bộ câu hỏi này để cung cấp hướng dẫn về một luồng riêng biệt có thể được sử dụng để tạo hoặc phân tích chính sách ATTT hiện có. Tất nhiên một chính sách ATTT tốt chỉ là một phần nhỏ của bức tranh lớn và còn rất nhiều các yếu tố khác góp phần vào việc tác động lên hiệu quả của chính sách.

Các chuyên gia nhận ra những hạn chế trong cách tiếp cận của họ trong việc chỉ sử dụng các chính sách ATTT công khai. Trong công việc tương lai, các chuyên gia sẽ xem xét mở rộng nghiên cứu ban đầu của họ để đưa ra thông tin chi tiết hơn , phân tích các chính sách ATTT của công ty không được công khai, và liên quan đến các trường hợp sơ suất trong nội bộ. Ngoài ra, các chuyên gia muốn mở rộng công việc của họ để bao gồm chi tiết các tác động và mức độ nghiêm trọng của các trường hợp đe dọa nội bộ.