TCVN **T I Ê U C H U Ẩ N Q U Ố C G I A**

TCVN ISO/IEC 27043:2019

ISO/IEC 27043:2015

Xuất bản lần 1

CÔNG NGHỆ THÔNG TIN – CÁC KỸ THUẬT AN TOÀN – NGUYÊN TẮC VÀ QUY TRÌNH ĐIỀU TRA SỰ CỐ

Information technology - Security techniques - Incident investigation principles and processes

HÀ NỘI - 2019

Mục lục

Lời nói đầu

TCVN ISO/IEC 27043:2019 hoàn toàn tương đương với ISO/IEC 27043:2015.

TCVN ISO/IEC 27043:2019 do Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam biên soạn, Bộ Thông tin và Truyền thông đề nghị, Tổng cục Tiêu chuẩn Đo lường Chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố.

Lời giới thiệu

Về tiêu chuẩn này

Tiêu chuẩn này cung cấp hướng dẫn về nguyên tắc và quy trình điều tra sự cố an toàn thông tin dựa trên các mô hình lý tưởng cho các quy trình điều tra sự cố chung thông qua các kịch bản điều tra sự cố liên quan tới bằng chứng số. Việc này bao gồm các quy trình từ khâu chuẩn bị trước khi xảy ra sự cố đến các quy trình xác định, tập hợp, thu nhận, bảo quản, phân tích, diễn giải và trình bày bằng chứng số. Nguyên tắc cơ bản của các cuộc điều tra số là khả năng lặp lại, một điều tra viên có kinh nghiệm phù hợp phải có khả năng đạt được kết quả giống như một điều tra viên khác có kỹ năng tương tự làm việc trong những điều kiện tương tự. Nguyên tắc này vô cùng quan trọng đối với bất kỳ cuộc điều tra chung. Hướng dẫn cho các quy trình điều tra được cung cấp để đảm bảo rằng có sự rõ ràng và minh bạch trong việc đạt được kết quả cho từng quy trình cụ thể. Đây là sự thúc đẩy để cung cấp hướng dẫn cho các nguyên tắc và quy trình điều tra sự cố sau đó.

Các hướng dẫn trong tiêu chuẩn này được tạo lập bao gồm các nguyên tắc và quy trình điều tra sự cố giúp đẩy nhanh các cuộc điều tra sự cố do tiêu chuẩn này đã đưa ra trình tự chung các sự kiện mà một cuộc điều tra yêu cầu. Việc sử dụng các nguyên tắc này sẽ cho phép chuyển đổi từ sự kiện này sang sự kiện khác trong quá trình điều tra một cách dễ dàng, suôn sẻ. Những hướng dẫn này giúp đào tạo cho các chuyên gia điều tra sự cố còn ít kinh nghiệm. Hướng dẫn này nhằm mục đích đảm bảo tính linh hoạt trong quá trình điều tra vì trong thực tế có nhiều hình thức điều tra số khác nhau. Do đó cần có một nguyên tắc và quy trình điều tra sự cố chung, hài hòa có thể điều chỉnh theo các kịch bản điều tra khác nhau.

Một mô hình quy trình điều tra hài hoà là cần thiết trong các thiết lập tố tụng hình sự, tố tụng dân sự cũng như trong các môi trường khác, ví dụ các vi phạm an toàn thông tin của công ty và việc phục hồi thông tin số từ thiết bị lưu trữ bị lỗi. Nguyên tắc được cung cấp đưa ra hướng dẫn ngắn gọn về quy trình chính xác phải tuân theo trong bất kỳ kiểu điều tra số nào theo cách nếu không được thừa nhận thì không tồn tại nghi ngờ về sự đầy đủ của quá trình điều tra được thực hiện trong cuộc điều tra.

Mọi cuộc điều tra số đòi hỏi trình độ chuyên môn cao. Những người tham gia vào cuộc điều tra phải có năng lực, thành thạo các quy trình được sử dụng và phải sử dụng các quy trình đã được kiểm chứng (xem ISO/IEC 27041) tương thích với các chính sách và/hoặc luật pháp liên quan theo luật định.

Khi có nhu cầu một chuyên gia thực hiện quy trình, chuyên gia đó sẽ chịu trách nhiệm về quy trình này. Do đó, mối liên hệ mật thiết giữa trách nhiệm về quy trình và đầu vào của chuyên gia sẽ xác định quy trình điều tra chính xác được yêu cầu theo các quy trình điều tra hài hoà được cung cấp theo hướng dẫn trong tiêu chuẩn này.

Tiêu chuẩn này được cấu trúc theo cách tiếp cận từ trên xuống. Điều này có nghĩa là các nguyên tắc và quy trình điều tra được trình bày đầu tiên ở mức độ cao (tổng quan) trước khi chúng được đi vào chi tiết. Ví dụ, đầu tiên tổng quan mức cao về các nguyên tắc và quy trình điều tra được cung cấp và trình bày dưới dạng "hộp đen", sau mỗi quy trình mức cao sẽ có phân chia thành các quy trình hạt nhân

(nguyên tác). Do đó, quan điểm ít tổng quan và nhiều chi tiết về tất cả các nguyên tắc và quy trình điều tra được trình bày ở gần cuối của tiêu chuẩn này như thể hiện trong Hình 8.

Tiêu chuẩn này nhằm bổ sung cho các tiêu chuẩn và tài liệu khác cung cấp hướng dẫn về việc điều tra và chuẩn bị điều tra sự cố an toàn thông tin. Đây không phải là hướng dẫn chi tiết nhưng là hướng dẫn cung cấp một cái nhìn tổng quan về toàn bộ quy trình điều tra sự cố. Hướng dẫn này cũng đưa ra một số nguyên tắc cơ bản nhằm đảm bảo rằng các công cụ, kỹ thuật và phương pháp có thể được lựa chọn phù hợp với mục đích khi cần.

Mối quan hệ với các tiêu chuẩn khác

Tiêu chuẩn này nhằm bổ sung cho các tiêu chuẩn và tài liệu khác hướng dẫn việc điều tra và chuẩn bị điều tra sự cố an toàn thông tin. Đây không phải là hướng dẫn toàn diện nhưng đưa ra một số nguyên tắc cơ bản nhằm đảm bảo rằng các công cụ, kỹ thuật và phương pháp có thể được lựa chọn và thể hiện phù hợp với mục đích khi cần thiết.

Tiêu chuẩn này cũng nhằm mục đích thông báo cho những người cần phải quyết định về độ tin cậy của bằng chứng số. Tiêu chuẩn được áp dụng cho các tổ chức cần bảo vệ, phân tích và diễn giải bằng chứng kỹ thuật số tiềm năng. Tiêu chuẩn này liên quan đến việc tạo ra và đánh giá các thủ tục liên quan đến bằng chứng số của các cơ quan hoạch định chính sách, thường là một phần của cơ quan lớn hơn về bằng chứng số.

Tiêu chuẩn này mô tả một phần của quá trình điều tra toàn diện, bao gồm, nhưng không giới hạn, các lĩnh vực sau đây:

- Quản lý sự cố, bao gồm việc chuẩn bị và lập kế hoạch điều tra;

- Xử lý bằng chứng số;

- Việc sử dụng, và các vấn đề gây ra bởi, biên tập số;

- Hệ thống phát hiện và ngăn chặn chặn xâm nhập, bao gồm thông tin có thể thu được từ các hệ thống này;

- An toàn lưu trữ, bao gồm cả việc vệ sinh hệ thống lưu trữ;

- Đảm bảo các phương pháp điều tra phù hợp với mục đích;

- Tiến hành phân tích và giải thích bằng chứng số;

- Hiểu được các nguyên tắc và quy trình về điều tra bằng chứng số;

- Quản lý sự kiện sự cố an toàn thông tin, bao gồm việc tập hợp bằng chứng từ các hệ thống liên quan đến quản lý sự kiện sự cố an toàn thông tin;

- Quan hệ giữa phát hiện điện tử và các phương pháp điều tra khác, cũng như việc sử dụng các kỹ thuật phát hiện điện tử trong các cuộc điều tra khác;

- Quản trị điều tra, bao gồm điều tra bằng chứng số.

Các lĩnh vực này được đề cập từng phần trong các tiêu chuẩn sau:

- TCVN ISO/IEC 27037:2019

Tiêu chuẩn này mô tả các phương thức mà những người tham gia vào giai đoạn đầu của cuộc điều tra, bao gồm phản ứng bước đầu, có thể đảm bảo bằng chứng số tiềm năng được tập hợp đầy đủ cho phép tiến hành điều tra thích hợp.

- ISO/IEC 27038

Một số tài liệu có thể chứa thông tin không được tiết lộ cho một số nhóm người. Các tài liệu đã sửa đổi có thể được phát hành cho các cộng đồng này sau khi xử lý thích hợp. Quá trình loại bỏ thông tin không được tiết lộ được gọi là "biên tập".

Việc biên tập các tài liệu kỹ thuật số là một lĩnh vực tương đối mới đối với việc quản lý tài liệu, đưa ra các vấn đề độc nhất và những rủi ro tiềm ẩn. Ở các tài liệu số được biên tập, thông tin đã bị gỡ bỏ phải không thể phục hồi. Do đó cần phải lưu ý sao cho thông tin đã được biên tập được xóa vĩnh viễn khỏi tài liệu số (ví dụ: thông tin này phải không được ẩn trong các phần không thể hiển thị của tài liệu).

ISO/IEC 27038 quy định các phương pháp biên tập đối với các tài liệu số. Tiêu chuẩn này cũng xác định các yêu cầu đối với phần mềm được sử dụng để biên tập.

- ISO/IEC 27040

Tiêu chuẩn này cung cấp hướng dẫn kỹ thuật chi tiết về cách thức các tổ chức có thể xác định mức độ giảm thiểu rủi ro phù hợp bằng cách sử dụng phương pháp tiếp cận nhất quán và đã được chứng minh phù hợp cho việc lập kế hoạch, thiết kế, lập hồ sơ và thực hiện an toàn lưu trữ dữ liệu. An toàn lưu trữ áp dụng cho việc bảo vệ (an toàn) thông tin ở nơi được lưu trữ và an toàn thông tin được chuyển qua các liên kết truyền thông liên quan đến lưu trữ. An toàn lưu trữ bao gồm việc đảm bảo an toàn thiết bị và phương tiện, an toàn cho các hoạt động quản lý liên quan đến thiết bị và phương tiện, an toàn cho các ứng dụng và dịch vụ, an toàn liên quan đến người dùng cuối trong suốt thời gian sử dụng thiết bị và phương tiện truyền thông và sau khi kết thúc sử dụng.

Các cơ chế đảm bảo an toàn như mã hóa và làm sạch dữ liệu có thể ảnh hưởng đến khả năng điều tra của điều tra viên. Chúng phải được xem xét trước và trong khi tiến hành điều tra. Chúng cũng quan trọng cho đảm bảo việc lưu trữ tài liệu bằng chứng trong và sau khi điều tra được chuẩn bị đầy đủ và an toàn.

- TCVN ISO/IEC 27041:2019

Điều quan trọng là các phương pháp và quy trình được triển khai trong cuộc điều tra có thể được đưa ra một cách phù hợp. Tài liệu này cung cấp hướng dẫn về cách thức đảm bảo các phương pháp và quy trình đáp ứng các yêu cầu của cuộc điều tra và đã được kiểm tra phù hợp.

- ISO/IEC 27042

Tiêu chuẩn này mô tả phương pháp và quy trình được sử dụng trong cuộc điều tra có thể được thiết lập và thực hiện để cho phép đánh giá đúng bằng chứng số tiềm năng, giải thích bằng chứng số và báo cáo kết quả.

Các tiêu chuẩn dưới đây đề cập đến một phần các lĩnh vực được xác định ở trên và có thể dẫn đến việc xuất bản các tiêu chuẩn có liên quan tại một thời điểm sau khi xuất bản tiêu chuẩn này.

- ISO/IEC 27035 (tất cả các phần)

Bộ tiêu chuẩn có ba thành phần cung cấp cho các tổ chức cách tiếp cận có cấu trúc và kế hoạch để quản lý việc quản lý sự cố an toàn. Tiêu chuẩn này bao gồm:

+ ISO/IEC 27035-1

+ ISO/IEC 27035-2

+ ISO/IEC 27035-3

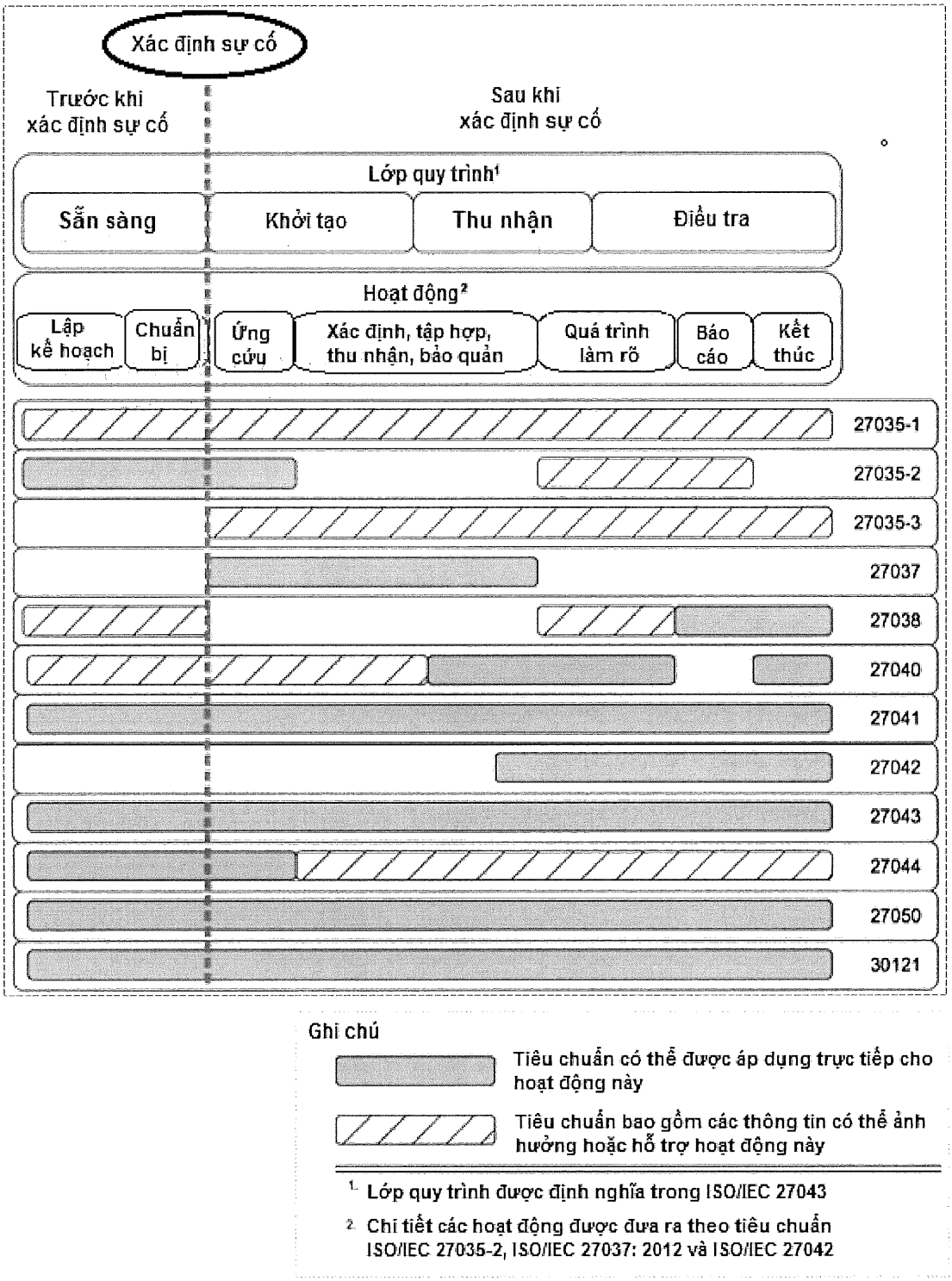
- ISO/IEC 27044

- ISO/IEC 27050 (tất cả các phần)

- ISO/IEC 30121

Tiêu chuẩn này cung cấp khung mẫu cho người quản trị của các tổ chức (bao gồm chủ sở hữu, thành viên hội đồng quản trị, giám đốc, đối tác, giám đốc điều hành hoặc tương tự) về cách tốt nhất để chuẩn bị cho việc điều tra số trước khi sự cố xảy ra. Tiêu chuẩn này áp dụng cho việc phát triển các quy trình chiến lược (và các quyết định) liên quan đến việc duy trì, tính sẵn sàng, sự truy cập, hiệu quả chi phí cho việc phát hiện bằng chứng số. Tiêu chuẩn này áp dụng cho tất cả các loại hình và quy mô tổ chức. Tiêu chuẩn này nói về việc chuẩn bị chiến lược cho quá trình điều tra số của một tổ chức. Việc chuẩn bị sẵn sàng cho cuộc điều tra số đảm bảo rằng tổ chức đã chuẩn bị chiến lược riêng biệt và phù hợp cho việc chấp nhận sự kiện tiềm năng của bằng chứng số. Các tác động có thể xảy ra do các hành vi vi phạm an toàn, gian lận và việc khẳng định uy tín. Trong mọi tình huống công nghệ thông tin phải được triển khai theo chiến lược để tối đa hóa hiệu quả của tính sẵn sàng, khả năng tiếp cận và hiệu quả chi phí.

Hình 1 mô tả các hoạt động điển hình quanh một sự cố và việc điều tra sự cố. Những con số được hiển thị trong biểu đồ này (ví dụ: 27037) cho biết tiêu chuẩn được liệt kê ở trên và các thanh được tô bóng hiển thị nơi có nhiều khả năng áp dụng trực tiếp hoặc có một số ảnh hưởng đối với quá trình điều tra (ví dụ bằng cách thiết lập chính sách hoặc tạo ra các ràng buộc). Tuy nhiên, khuyến nghị tham khảo tất cả các tiêu chuẩn này trước và trong quá trình lập kế hoạch và chuẩn bị. Các lớp quy trình được trình bày đã được xác định đầy đủ trong tiêu chuẩn này và các hoạt động được xác định phù hợp với những nội dung được đề cập chi tiết hơn trong ISO/IEC 27035-2, TCVN ISO/IEC 27037:2019 và ISO/IEC 27042.



Hình 1 - Khả năng áp dụng các tiêu chuẩn đối với các lớp và hoạt động của quy trình điều tra sự cố

Công nghệ thông tin - Các kỹ thuật an toàn - Nguyên tắc và quy trình điều tra sự cố

Information technology - Security techniques - Incident investigation principles and processes

1 Phạm vi áp dụng

Tiêu chuẩn này cung cấp hướng dẫn dựa trên các mô hình lý tưởng cho các quy trình điều tra sự cố phổ biến thông qua nhiều kịch bản điều tra sự cố liên quan đến bằng chứng số. Hướng dẫn này bao gồm các quy trình từ chuẩn bị trước khi xảy ra sự cố đến việc kết thúc điều tra, cũng như bất cứ lời khuyên và cảnh báo nào về quy trình. Hướng dẫn này mô tả các quy trình và các nguyên tắc áp dụng cho các loại điều tra khác nhau bao gồm, nhưng không giới hạn: truy cập trái phép, sửa đổi dữ liệu, sự cố hệ thống, hoặc vi phạm về an toàn thông tin của tổ chức, hay bất kỳ cuộc điều tra số nào khác.

Tiêu chuẩn này cung cấp tổng quan chung về tất cả các nguyên tắc và quy trình điều tra sự cố mà không quy định các chi tiết cụ thể trong các nguyên tắc và quy trình điều tra. Các tiêu chuẩn liên quan khác được đề cập trong tiêu chuẩn này cung cấp nội dung chi tiết hơn về các nguyên tắc và quy trình điều tra cụ thể.

2 Tài liệu viện dẫn

Các tài liệu viện dẫn sau rất cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả các sửa đổi, bổ sung (nếu có).

TCVN 11238:2015 (ISO/IEC 27000:2014), Công nghệ thông tin - Các kỹ thuật an toàn - Hệ thống quản lý an toàn thông tin - Tổng quan và từ vựng.

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa trong TCVN 11238:2015 và các thuật ngữ, định nghĩa sau:

3.1

Thu nhận (acquisition)

Quy trình tạo ra một bản sao dữ liệu bên trong một tập dữ liệu đã được xác định.

CHÚ THÍCH: Sản phẩm của việc thu nhận là một bản sao bằng chứng số tiềm năng.

[Nguồn: ISO/IEC 27037:2012, 3.1]

3.2

Hoạt động (activity)

Tập các nhiệm vụ gắn kết với một quy trình.