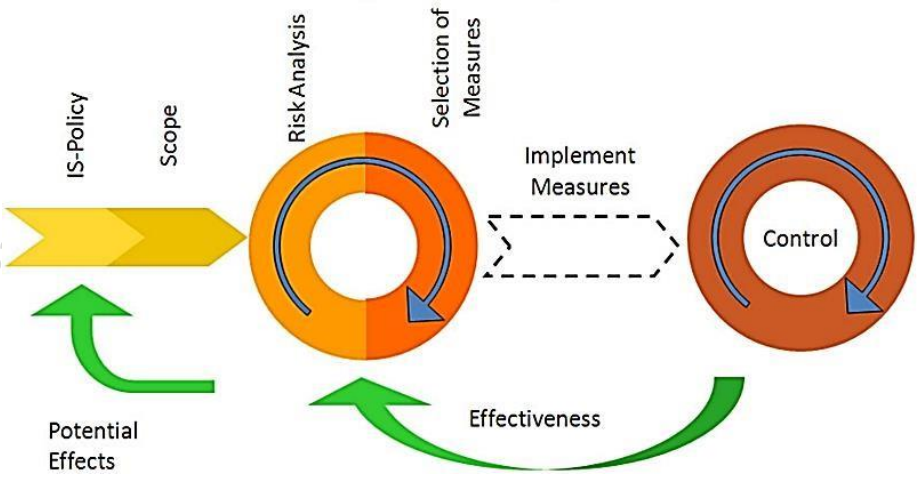
1. Khái quát về quản lý an toàn thông tin

Chúng ta bắt đầu mục này với khái niệm *Tài sản* (Asset) trong lĩnh vực an toàn thông tin, gọi tắt là *Tài sản an toàn thông tin*. Tài sản an toàn thông tin là thông tin, thiết bị, hoặc các thành phần khác hỗ trợ các hoạt động có liên quan đến thông tin. Tài sản an toàn thông tin có thể gồm:

- Phần cứng (máy chủ, các thiết bị mạng,…);
- Phần mềm (hệ điều hành, các phần mềm máy chủ dịch vụ,…); và
- Thông tin (thông tin khách hàng, nhà cung cấp, hoạt động kinh doanh,…).

Khái niệm tiếp theo là *Quản lý an toàn thông tin* (Information security management). Quản lý an toàn thông tin là một tiến trình (process) nhằm đảm bảo các tài sản an toàn thông tin quan trọng của cơ quan, tổ chức, doanh nghiệp được bảo vệ đầy đủ với chi phí phù hợp.



Hình 5.1. Quan hệ giữa các khâu trong quản lý an toàn thông tin

Quản lý an toàn thông tin là một thành phần rất quan trọng trong an toàn thông tin và nó phải trả lời được 3 câu hỏi:

1. Những tài sản nào cần được bảo vệ?
2. Những mối đe dọa nào có thể có đối với các tài sản này?
3. Những biện pháp có thể thực hiện để ứng phó với các mối đe dọa đó?

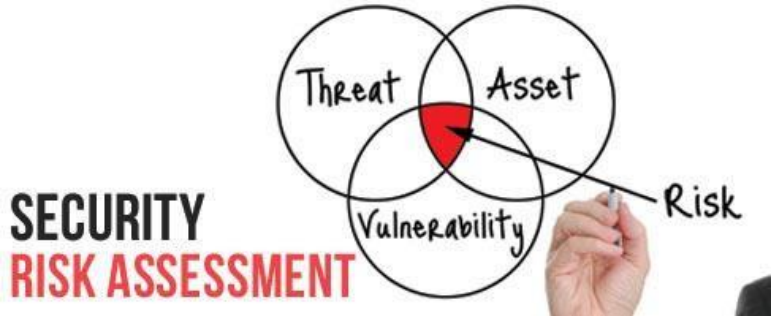
Quản lý an toàn thông tin có thể gồm các khâu: (1) xác định rõ mục đích đảm bảo an toàn thông tin và hồ sơ tổng hợp về các rủi ro; (2) đánh giá rủi ro với từng tài sản an toàn thông tin cần bảo vệ; và (3) xác định và triển khai các biện pháp quản lý, kỹ thuật kiểm soát, giảm rủi ro về mức chấp nhận được. Một điểm quan trọng cần lưu ý là, quá trình quản lý an toàn thông tin cần được thực hiện liên tục theo chu trình do sự thay đổi nhanh chóng của công nghệ và môi trường xuất hiện rủi ro.

2. Đánh giá rủi ro an toàn thông tin

2.1 Giới thiệu

Đánh giá rủi ro an toàn thông tin (Security risk assessment) là một bộ phận quan trọng của vấn đề quản lý rủi ro an toàn thông tin. Theo đó, mỗi tài sản của tổ chức cần được xem xét, nhận dạng các rủi ro có thể có và đánh giá mức rủi ro. Đánh giá rủi ro là một trong các cơ sở để xác định mức rủi ro chấp nhận được với từng loại tài sản. Trên cơ sở xác định mức rủi ro, có thể đề ra các biện pháp xử lý, kiểm soát rủi ro trong mức chấp nhận được, với mức chi phí phù hợp.

Có 4 phương pháp tiếp cận đánh giá rủi ro: phương pháp đường cơ sở (Baseline approach), phương pháp không chính thức (Informal approach), phương pháp phân tích chi tiết rủi ro (Detailed risk analysis) và phương pháp kết hợp (Combined approach). Tùy theo quy mô của hệ thống thông tin của đơn vị và tài sản an toàn thông tin cần được bảo vệ, đơn vị có thể xem xét lựa chọn phương pháp đánh giá rủi ro cho phù hợp.



Hình 5.2. Mô hình đánh giá rủi ro an toàn thông tin

2.2 Các phương pháp đánh giá rủi ro

2.2.1 Phương pháp đánh giá rủi ro đường cơ sở

Phương pháp đánh giá rủi ro đường cơ sở là phương pháp đơn giản nhất. Mục đích của phương pháp này là thực thi các kiểm soát an ninh ở mức cơ bản dựa trên các tài liệu cơ bản, các quy tắc thực hành và các thực tế tốt nhất của ngành đã được áp dụng. Phương pháp đường cơ sở có ưu điểm là không đòi hỏi các chi phí cho các tài nguyên bổ sung sử dụng trong đánh giá rủi ro chính thức và cùng nhóm các biện pháp có thể triển khai trên nhiều hệ thống. Tuy nhiên, nhược điểm của nó là không xem xét kỹ đến các điều kiện nảy sinh các rủi ro ở các hệ thống của các tổ chức khác nhau. Một vấn đề khác của phương pháp này là mức đường cơ sở được xác định chung nên có thể không phù hợp với từng tổ chức cụ thể. Nếu chọn mức quá cao có thể gây tốn kém, nhưng nếu chọn mức quá thấp có thể gây mất an toàn. Nhìn chung, phương pháp đường cơ sở phù hợp với các tổ chức với hệ thống công nghệ thông tin có quy mô nhỏ, có nguồn lực hạn chế.

2.2.2 Phương pháp không chính thức

Phương pháp không chính thức là phương pháp tiếp cận đánh giá rủi ro tiếp theo.

Phương pháp không chính thức liên quan đến việc thực hiện các nội dung sau:

- Thực hiện một số dạng phân tích rủi ro hệ thống công nghệ thông tin của tổ chức một cách không chính thức,
- Sử dụng kiến thức chuyên gia của các nhân viên bên trong tổ chức, hoặc các nhà tư vấn từ bên ngoài, và
- Không thực hiện đánh giá toàn diện các rủi ro đối với tất cả các tài sản công nghệ thông tin của tổ chức.

Phương pháp này có ưu điểm là không đòi hỏi các nhân viên phân tích rủi ro có các kỹ năng bổ sung, nên có thể thực hiện nhanh với chi phí thấp, và việc có phân tích hệ thống công nghệ thông tin của tổ chức giúp cho việc đánh giá rủi ro, lỗ hổng chính xác hơn và các biện pháp kiểm soát đưa ra cũng phù hợp hơn phương pháp đường cơ sở. Phương pháp không chính thức có các nhược điểm là:

- Do đánh giá rủi ro không được thực hiện toàn diện nên có thể một rủi ro không được xem xét kỹ, nên có thể để lại nguy cơ cao cho tổ chức, và
- Kết quả đánh giá dễ phục thuộc vào quan điểm của các cá nhân.

Trên thực tế phương pháp không chính thức phù hợp với các tổ chức với hệ thống công nghệ thông tin có quy mô nhỏ và vừa, có nguồn lực tương đối hạn chế.

2.2.3 Phương pháp phân tích chi tiết rủi ro

Phương pháp phân tích chi tiết rủi ro là phương pháp đánh giá toàn diện, được thực hiện một cách chính thức và được chia thành nhiều giai đoạn, bao gồm:

- Nhận dạng các tài sản,
- Nhận dạng các mối đe dọa và lỗ hổng đối với các tài sản này,
- Xác định xác suất xuất hiện các rủi ro và các hậu quả có thể có nếu rủi ro xảy ra với cơ quan, tổ chức, và
- Lựa chọn các biện pháp xử lý rủi ro dựa trên kết quả đánh giá rủi ro của các giai đoạn trên.

Ưu điểm của phương pháp này là cho phép xem xét chi tiết các rủi ro đối với hệ thống công nghệ thông tin của tổ chức, và lý giải rõ ràng các chi phí cho các biện pháp kiểm soát rủi do đề xuất. Đồng thời, nó cung cấp thông tin tốt nhất cho việc tiếp tục quản lý vấn đề an ninh của các hệ thống công nghệ thông tin khi chúng được nâng cấp, sửa đổi. Tuy nhiên, phương pháp này có 2 nhược điểm là:

- Chi phí lớn về thời gian, các nguồn lực và yêu cầu kiến thức chuyên gia có trình độ cao, và
- Có thể dẫn đến chậm trễ trong việc đưa ra các biện pháp xử lý, kiểm

soát rủi ro phù hợp.

Phương pháp phân tích chi tiết rủi ro phù hợp với các tổ chức chính phủ cung cấp các dịch vụ thiết yếu cho người dân và doanh nghiệp, hoặc các tổ chức có hệ thống công

nghệ thông tin quy mô lớn, hoặc các tổ chức cung cấp nền tảng hạ tầng truyền thông cho quốc gia.

2.2.4 Phương pháp kết hợp

Phương pháp kết hợp là phương pháp tiếp cận đánh giá rủi ro cuối cùng. Phương pháp này kết hợp các thành phần của 3 phương pháp đường cơ sở, không chính thức và phân tích chi tiết, với các mục tiêu là cung cấp mức bảo vệ hợp lý càng nhanh càng tốt và sau đó kiểm tra và điều chỉnh các biện pháp bảo vệ trên các hệ thống chính theo thời gian. Phương pháp kết hợp được thực hiện theo 3 bước:

- Thực hiện phương pháp đường cơ sở với tất cả các thành phần của hệ thống công nghệ thông tin của tổ chức;
- Tiếp theo, các thành phần có mức rủi ro cao, hoặc trọng yếu được xem xét đánh giá theo phương pháp không chính thức;
- Cuối cùng hệ thống được xem xét đánh giá toàn diện rủi ro ở mức chi tiết.

Các ưu điểm của phương pháp kết hợp là việc bắt đầu bằng việc đánh giá rủi ro ở mức cao dễ nhận được sự ủng hộ của cấp quản lý, thuận lợi cho việc lập kế hoạch quản lý an toàn thông tin, đồng thời có thể giúp sớm triển khai các biện pháp xử lý và kiểm soát rủi ro ngay từ giai đoạn đầu, cũng như có thể giúp giảm chi phí với đa số các tổ chức. Tuy nhiên, phương pháp kết hợp có nhược điểm là nếu đánh giá ở mức cao trong giai đoạn đầu không chính xác có thể dẫn đến áp dụng các biện pháp kiểm soát không phù hợp, hệ thống có thể gặp rủi ro trong thời gian chờ đánh giá chi tiết. Nói chung, phương pháp kết hợp phù hợp các tổ chức với hệ thống công nghệ thông tin quy mô vừa và lớn.

3. Phân tích chi tiết rủi ro an toàn thông tin

3.1 Giới thiệu

Phân tích chi tiết rủi ro an toàn thông tin là phương pháp xem xét, phân tích toàn diện các rủi ro của từng thành phần trong hệ thống công nghệ thông tin của cơ quan, tổ chức. Phân tích chi tiết rủi ro an toàn thông tin gồm nhiều hoạt động được chia thành 9 bước:

1. Mô tả đặc điểm hệ thống
2. Nhận dạng các mối đe dọa
3. Nhận dạng các lỗ hổng bảo mật
4. Phân tích các kiểm soát

5. Xác định xác suất rủi ro
6. Phân tích các ảnh hưởng
7. Xác định các rủi ro
8. Đề xuất các kiểm soát
9. Viết tài liệu kết quả phân tích.

3.2 Nội dung phân tích chi tiết rủi ro

Nội dung cụ thể từng bước của phân tích chi tiết rủi ro an toàn thông tin như sau.

Bước 1: Mô tả đặc điểm hệ thống

- Đầu vào: Các thành phần của hệ thống:

+ Phần cứng, phần mềm, giao diện
+ Dữ liệu và thông tin
+ Con người
+ Sứ mệnh của hệ thống.

- Đầu ra:

+ Ranh giới và chức năng hệ thống;
+ Tính trọng yếu của dữ liệu và hệ thống;
+ Tính nhạy cảm

Bước 2: Nhận dạng các mối đe dọa

- Đầu vào:

+ Lịch sử tấn công vào hệ thống
+ Dữ liệu từ các tổ chức chuyên về an toàn thông tin
+ Dữ liệu từ các phương tiện thông tin đại chúng.

- Đầu ra:

+ Báo cáo về các mối đe dọa đối với hệ thống

Bước 3: Nhận dạng các lỗ hổng bảo mật

- Đầu vào:

+ Các báo cáo đánh giá rủi ro đã có
+ Các nhận xét kiểm toán hệ thống
+ Các yêu cầu an ninh, an toàn
+ Các kết quả kiểm tra an ninh, an toàn

- Đầu ra:

+ Danh sách các lỗ hổng bảo mật tiềm tàng.

Bước 4: Phân tích các kiểm soát (control)

- Đầu vào:

+ Các kiểm soát hiện có
+ Các kiểm soát được lập kế hoạch
    - Đầu ra:
+ Danh sách các kiểm soát hiện có và được lập kế hoạch.

Bước 5: Xác định xác suất rủi ro

- Đầu vào:

+ Động cơ của các nguồn đe dọa
+ Khả năng của đe dọa
+ Bản chất của lỗ hổng bảo mật
+ Các kiểm soát hiện có
    - Đầu ra:
+ Đánh giá xác suất rủi ro.

Bước 6: Phân tích các ảnh hưởng (liên quan sự vi phạm tính toàn vẹn, sẵn dùng và bí mật của các tài sản hệ thống)

- Đầu vào:

+ Phân tích ảnh hưởng sứ mệnh
+ Đánh giá tầm quan trọng của tài sản
+ Tầm quan trọng của dữ liệu
+ Tính nhạy cảm của dữ liệu
    - Đầu ra:
+ Đánh giá các ảnh hưởng.

Bước 7: Xác định các rủi ro

- Đầu vào:

+ Khả năng bị mối đe dọa khai thác
+ Tầm quan trọng của ảnh hưởng
+ Sự phù hợp của các kiểm soát theo kế hoạch, hoặc hiện có
    - Đầu ra:
+ Các rủi ro và các mức rủi ro có liên quan.

Bước 8: Đề xuất các kiểm soát

- Đầu vào: Không
- Đầu ra: Đề xuất các biện pháp xử lý, kiểm soát rủi ro

Bước 9: Viết tài liệu kết quả phân tích

- Đầu vào: Không
- Đầu ra: Báo cáo đánh giá rủi ro.

4. Thực thi quản lý an toàn thông tin

4.1 Giới thiệu

Thực thi quản lý an toàn thông tin là bước tiếp theo của khâu đánh giá rủi ro, nhằm triển khai, thực thi các kiểm soát (control) nhằm đảm bảo an toàn thông tin cho hệ thống công nghệ thông tin của tổ chức. Các nội dung chính của thực thi quản lý an toàn thông tin gồm:

- Thực thi (Implementation): Thực thi các kiểm soát, và nâng cao ý thức và đào tạo an toàn thông tin.
- Thực thi tiếp tục (Implementation follow-up): Bảo trì, kiểm tra hợp chuẩn, quản lý thay đổi và xử lý sự cố.

Kiểm soát (control), đảm bảo an toàn (safeguard), hoặc biện pháp đối phó (countermeasure) là các thuật ngữ có thể được sử dụng tương đương, hoặc tráo đổi cho nhau trong quản lý an toàn thông tin. Kiểm soát là phương tiện để quản lý rủi ro, bao

gồm các chính sách, thủ tục, các hướng dẫn, các thực tế, hoặc cấu trúc tổ chức. Kiểm soát có thể là vấn đề quản lý hành chính hoặc kỹ thuật, hoặc có bản chất luật pháp.

Các kiểm soát được thực thi trong quản lý an toàn thông tin có thể gồm 6 loại:

- Kiểm soát quản lý (Management controls)
- Kiểm soát vận hành (Operational controls)
- Kiểm soát kỹ thuật (Technical controls)
- Kiểm soát hỗ trợ (Supportive controls)
- Kiểm soát ngăn ngừa (Preventive controls)
- Kiểm soát phát hiện và phục hồi (Detection and recovery controls).

4.2 Các loại kiểm soát

Kiểm soát quản lý bao gồm các nội dung:

- Tập trung vào các chính sách, lập kế hoạch, hướng dẫn và chuẩn an toàn thông tin;
- Các kiểm soát có ảnh hưởng đến việc lựa chọn các kiểm soát vận hành và kiểm soát kỹ thuật nhằm giảm tổn thất do rủi ro và bảo vệ sứ mệnh của tổ chức;
- Các kiểm soát tham chiếu đến các vấn đề được giải quyết thông qua lĩnh vực quản lý.

Kiểm soát vận hành bao gồm các nội dung:

- Giải quyết vấn đề thực thi chính xác và sử dụng các chính sách và

chuẩn an toàn thông tin, đảm bảo tính nhất quán trong vận hành an toàn thông tin và khắc phục các khiếm khuyết vận hành đã được nhận dạng;

- Các kiểm soát này liên quan đến các cơ chế và thủ tục được thực thi chủ yếu bởi con người, hơn là bởi hệ thống;
- Được sử dụng để tăng cường an ninh cho một hệ thống hoặc một nhóm các hệ thống.

Kiểm soát kỹ thuật bao gồm các nội dung:

- Liên quan đến việc sử dụng đúng đắn các biện pháp đảm bảo an ninh bằng phần cứng và phần mềm trong hệ thống;
- Bao gồm các biện pháp từ đơn giản đến phức tạp để đảm bảo an toàn cho các thông tin nhạy cảm và các chức năng trọng yếu của các hệ thống;
- Một số kiểm soát kỹ thuật: xác thực, trao quyền và thực thi kiểm soát truy nhập,...

Kiểm soát hỗ trợ là các kiểm soát chung ở lớp dưới, có quan hệ với và được sử dụng bởi nhiều kiểm soát khác.

Kiểm soát ngăn ngừa là kiểm soát tập trung vào việc ngăn ngừa việc xảy ra các vi phạm an ninh, bằng cách khắc chế các nỗ lực vi phạm chính sách an ninh hoặc khai thác các lỗ hổng bảo mật.

Kiểm soát phát hiện và phục hồi là kiểm soát tập trung vào việc đáp trả vi phạm an ninh bằng cách đưa ra cảnh báo vi phạm, hoặc các nỗ lực vi phạm chính sách an ninh,

hoặc khai thác các lỗ hổng bảo mật, đồng thời cung cấp các biện pháp phục hồi các tài nguyên tính toán bị ảnh hưởng do vi phạm an ninh.

4.3 Xây dựng kế hoạch đảm bảo an toàn

Kế hoạch đảm bảo an toàn (Security plan) là một tài liệu chỉ rõ các phần việc sẽ được thực hiện, các tài nguyên cần sử dụng và những người, hoặc nhân viên chịu trách nhiệm thực hiện. Mục đích của Kế hoạch đảm bảo an toàn là cung cấp chi tiết về các hành động cần thiết để cải thiện các vấn đề đã được nhận dạng trong hồ sơ đánh giá rủi ro một cách nhanh chóng. Kế hoạch đảm bảo an toàn nên gồm các thông tin chi tiết sau (theo chuẩn hướng dẫn quản lý rủi ro năm 2002 của NIST):

- Các rủi ro (sự kế hợp của tài sản/mối đe dọa/lỗ hổng)
- Các kiểm soát được khuyến nghị (từ đánh giá rủi ro)
- Các hành động ưu tiên cho mỗi rủi ro
- Các kiểm soát được chọn (dựa trên phân tích lợi ích – chi phí)

- Các tài nguyên cần có cho thực thi các kiểm soát đã chọn
- Nhân sự chịu trách nhiệm
- Ngày bắt đầu và kết thúc việc thực thi
- Các yêu cầu bảo trì và các nhận xét khác.

4.4 Nội dung thực thi quản lý an toàn thông tin

Như đã đề cập trong mục 5.1.4.1, việc thực thi quản lý an toàn thông tin gồm 2 khâu là (1) *thực thi* (Implementation) và (2) *thực thi tiếp tục* (Implementation follow-up). Khâu *thực thi* gồm 2 phần việc là thực thi các kiểm soát, và nâng cao ý thức và đào tạo an toàn thông tin. Thực thi các kiểm soát là phần việc tiếp theo cần thực hiện trong kế hoạch đảm bảo an toàn của tiến trình quản lý an toàn thông tin. Thực thi các kiểm soát có liên hệ mật thiết với việc đào tạo nâng cao ý thức an toàn thông tin cho nhân viên nói chung và đào tạo chuyên sâu về an toàn thông tin cho nhân viên an toàn thông tin trong tổ chức.

Khâu *thực thi tiếp tục* là việc cần lặp lại trong chu trình quản lý an toàn thông tin để đáp ứng sự thay đổi trong môi trường công nghệ thông tin và môi trường rủi ro. Trong đó, các kiểm soát đã được thực thi cần được giám sát để đảm bảo tính hiệu quả, và bất kỳ một sự thay đổi trên hệ thống cần được xem xét vấn đề an ninh và hồ sơ rủi ro của hệ thống bị ảnh hưởng cần được xem xét nếu cần thiết. Giai đoạn thực thi tiếp tục bao gồm các khía cạnh: bảo trì các kiểm soát an ninh, kiểm tra hợp chuẩn an ninh, quản lý thay đổi và cấu hình và xử lý các sự cố.

Bảo trì các kiểm soát an ninh gồm các phần việc phải đảm bảo các yêu cầu sau:

- Các kiểm soát được xem xét định kỳ để đảm bảo chúng hoạt động như mong muốn;
- Các kiểm soát cần được nâng cấp khi các yêu cầu mới được pháp hiện;
- Các thay đổi với hệ thống không được có các ảnh hưởng tiêu cực đến các kiểm soát;
- Các mối đe dọa mới hoặc các lỗ hổng đã không trở thành được biết đến.

Kiểm tra hợp chuẩn an ninh là quá trình kiểm toán việc quản lý an toàn thông tin của tổ chức nhằm đảm bảo tính phù hợp với kế hoạch đảm bảo an ninh. Việc kiểm toán có thể được thực hiện bởi nhân sự bên trong hoặc bên ngoài tổ chức. Cần sử dụng danh sách kiểm tra (checklist) các vấn đề: các chính sách và kế hoạch an ninh được tạo ra, các kiểm soát phù hợp được lựa chọn và các kiểm soát được sử dụng và bảo trì phù hợp.

Quản lý thay đổi và cấu hình là tiến trình được sử dụng để xem xét các thay đổi được đề xuất cho hệ thống trong quá trình sử dụng. Các thay đổi với các hệ thống hiện có là cần thiết do nhiều lý do, như hệ thống có trục trặc, hoặc sự xuất hiện của các mối đe dọa hoặc lỗ hổng mới, sự xuất hiện của yêu cầu mới, nhiệm vụ

mới,… Các thay đổi cần được xem xét kỹ lưỡng cả vấn đề vận hành, tính năng và vấn đề an toàn,… Quản lý cấu hình liên quan đến việc lưu vết các cấu hình của mỗi hệ thống khi chúng được nâng cấp, thay đổi. Việc này bao gồm danh sách các phiên bản của phần cứng, phần mềm cài đặt trong mỗi hệ thống, và thông tin quản lý cấu hình hữu ích để khôi phục hệ thống khi việc thay đổi hoặc nâng cấp thất bại.

Xử lý các sự cố bao gồm các thủ tục được sử dụng để phản ứng lại các sự cố an ninh. Xử lý sự cố có liên quan đến vấn đề đào tạo nâng cao ý thức an toàn thông tin cho người dùng và đào tạo chuyên sâu cho chuyên viên an toàn thông tin.