

MẪU BÁO CÁO HOẠT ĐỘNG BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG NĂM 2017

tại các đơn vị trực thuộc trực tiếp Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ, Ủy ban nhân dân tỉnh, thành phố trực thuộc Trung ương

STT

Câu hỏi và trả lời

- 1 Tên đơn vị báo cáo:.....
 Cơ quan chủ quản:.....
- 2 Đề nghị thống kê số lượng các hệ thống thông tin do Quý đơn vị trực tiếp quản lý vào bảng sau:

Phân loại số lượng HTTT do đơn vị quản lý trực tiếp	Chưa phân loại	Cấp độ 1	Cấp độ 2	Cấp độ 3	Cấp độ 4	Cấp độ 5
Số HTTT nội bộ đơn vị (chỉ người trong đơn vị sử dụng)						
Số HTTT nội bộ dùng chung (cho nhiều đơn vị trực thuộc cơ quan chủ quản)						
Số HTTT công cộng (cung cấp dịch vụ cho cộng đồng vượt quá phạm vi nội bộ như trên)						

- 3 Có bao nhiêu đơn vị (trực thuộc trực tiếp cơ quan chủ quản) sử dụng các HTTT nội bộ dùng chung do Quý đơn vị trực tiếp quản lý?
- 4 Quý đơn vị cung cấp bao nhiêu dịch vụ độc lập (trọn gói) sử dụng cho các đối tượng ngoài cơ quan chủ quản trong cả nước hoặc phục vụ cộng đồng trên mạng Internet?
- 5 Đơn vị có ban hành quy chế, quy định riêng hoặc có áp dụng quy chế, quy định chung của cơ quan chủ quản về bảo đảm ATTTM không? Nếu có thì điền nội dung phù hợp vào bảng sau và trả lời thêm câu 6 và câu 7 dưới đây (nếu không có thì để trống)

Loại văn bản chính sách ATTTM được đơn vị áp dụng	Văn bản hiện hành		Văn bản cũ trước đây đã được thay thế bằng VB hiện hành (nếu có)	
	Năm	Số hiệu văn bản	Năm	Số hiệu văn bản
Quy định riêng				
Quy chế chung				

- 6 Trong các quy định, quy chế hiện hành về bảo đảm ATTTM của đơn vị có các nội dung sau đây không?

Quản lý thiết kế an toàn hệ thống thông tin	
Quản lý phát triển phần mềm thuê khoán	
Quản lý thử nghiệm và nghiệm thu hệ thống	
Quản lý vận hành an toàn mạng	
Quản lý vận hành an toàn máy chủ và ứng dụng	
Quản lý an toàn dữ liệu	

Cách ghi

Hướng dẫn

Các ô số phải trả lời nếu để trống thì được coi là có giá trị bằng 0. Các ô phải trả lời cho câu hỏi có/không thì được ghi 1 nếu là "có" và ghi 0 nếu là "không" (đấu tích v hoặc x được coi là 1, để trống coi là 0)

Đơn vị quản lý mạng LAN/WAN, có quyền quản trị hệ thống, thiết lập các chính sách quản lý, các tham số kỹ thuật và ban hành quy định với người dùng đầu cuối. Phân loại cấp độ HTTT 1-5 theo Nghị định 85/2016/NĐ-CP.

0,1,... Ghi số lượng hệ thống thông tin

0,1,... Ghi số lượng đơn vị đầu mối trực thuộc cơ quan. Bộ phận Lãnh đạo cơ quan tính như một đơn vị đầu mối. Để trống ô này nếu Quý cơ quan không có HTTT nội bộ dùng chung trong câu 2.

0,1,... Nếu không có ghi số 0, nếu có thì ghi số dịch vụ độc lập đang cung cấp (≥ 1), không tính số dịch vụ con trong một dịch vụ lớn.

1/0 Có thì ghi là 1, không có ghi 0

Văn bản nào không có thì các ô tương ứng để trống
 Nếu có nhiều văn bản hiện hành thì tăng số dòng tương ứng

1/0 Có nội dung nào thì ô tương ứng ghi là 1, không có thì ô tương ứng ghi 0

Quản lý vận hành an toàn thiết bị đầu cuối	
Quản lý phòng chống phần mềm độc hại	
Quản lý điểm yếu an toàn thông tin	
Quản lý giám sát an toàn hệ thống thông tin	
Quản lý sự cố an toàn thông tin	
Quản lý an toàn người sử dụng đầu cuối	
Quy trình đánh giá, quản lý và xử lý rủi ro về ATTT	
Quy trình thao tác chuẩn để phản ứng khẩn cấp với các sự cố mất ATTTM	

7 Đề nghị tự nhận xét về chất lượng văn bản hiện hành so với quy định của pháp luật Việt Nam và nhu cầu của đơn vị đến thời điểm hiện tại (chỉ chọn 1 đáp án)?

chọn 1 ô Ô nào chọn thì ghi là 1

+ Đầy đủ, chặt chẽ, có thể sử dụng ổn trong khoảng 2 năm trở lên	
+ Tương đối đầy đủ, có thể cần hoàn thiện nhưng sử dụng ổn trong ít nhất 1 năm tới	
+ Đã thấy có các điểm thiếu hoặc không phù hợp, cần sửa đổi hay bổ sung ngay	

8 Đề nghị tự đánh giá thực tế hiện nay tại đơn vị về mức độ áp dụng thực hiện tốt các quy chế, quy định bảo đảm ATTTM đạt khoảng độ bao nhiêu phần trăm theo thang điểm 100%

0 - 100 % Cơ quan tự đánh giá mức độ thực tế của mình, tỷ lệ chẵn đơn vị trong khoảng từ 0% đến 100%

9 Tổng số cán bộ, công chức, viên chức, người lao động làm việc trong đơn vị

0,1,... Ghi số lượng người làm việc trong cơ quan (bao gồm cả của các đơn vị trực thuộc được tổ chức đánh giá)

10 Tổng số cán bộ lãnh đạo quản lý (cấp đơn vị và cấp phòng/tương đương trực thuộc đơn vị) của đơn vị

0,1,... Ghi số lượng

11 Số người sử dụng máy tính hiện tại trong đơn vị

0,1,... Ghi số lượng

12 Đơn vị có phân công lãnh đạo (cấp đơn vị) phụ trách về ATTTM hay không?

1/0 Có thì ghi là 1, không có ghi 0

13 Đơn vị có tổ chức/bộ phận chuyên trách về ATTTM hay không? (Nếu có trả lời thêm câu 14 dưới đây)

1/0 Có thì ghi là 1, không có ghi 0

14 Vị trí và quan hệ công tác của bộ phận chuyên trách về ATTTM (có thể lựa chọn nhiều đáp án)

Có thể lựa chọn nhiều đáp án

Là bộ phận con thuộc tổ chức phụ trách CNTT của đơn vị ?	
Chịu sự chỉ đạo nghiệp vụ của bộ phận chuyên trách ATTTM của cơ quan chủ quản	
Là thành viên thuộc mạng lưới chuyên trách bảo đảm ATTT quốc gia?	
Có quy chế phối hợp ứng cứu sự cố ATTTM với doanh nghiệp cung cấp dịch vụ mạng?	
Có quy chế phối hợp ứng cứu sự cố ATTTM với các tổ chức ATTTM khác? Ví dụ:	

1/0 Đúng (có) thì ghi là 1, không đúng ghi 0

15 Tổng số cán bộ làm việc chuyên trách về ATTTM

16 Tổng số cán bộ làm việc bán chuyên trách về ATTTM

17 Quản lý nhân sự phù hợp yêu cầu ATTT như thế nào? - Có quy định từng khâu? Thực hiện đầy đủ không? (mỗi cột lựa chọn 1 đáp án)

1/0 Trong mỗi cột ghi một số 1 vào 1 ô phù hợp trong mỗi cột. Các ô còn lại trong cột để trống

Quản lý nhân sự về ATTT trong từng khâu	Tuyển dụng cán bộ ATTT	Quản lý quá trình làm việc	Chấm dứt, chuyển công việc
Chưa có quy định cụ thể			
Có quy định, thực hiện chưa tốt thường xuyên			

Có quy định, thực hiện tốt

- 18 Tổng số cán bộ nhân viên đã từng được qua lớp tập huấn về ATTTM
- 19 Tổng số cán bộ lãnh đạo quản lý (cấp đơn vị và cấp phòng/tương đương trực thuộc đơn vị) đã từng được đào tạo, tập huấn về quản lý ATTTM
- 20 Tổng số cán bộ kỹ thuật có trình độ tương đương đại học ngành ATTT trở lên
- 21 Tổng số cán bộ kỹ thuật có trình độ tương đương trung cấp về ATTT
- 22 Tổng số chuyên gia chuyên sâu về ATTTM
- 23 Đơn vị có kế hoạch đào tạo, tập huấn về ATTTM trong năm 2017 không?
- 24 Hãy cho biết kết quả đào tạo, tập huấn năm 2017 về ATTTM của đơn vị theo bảng sau:

- 0,1,... Ghi số lượng
- 0,1,... Ghi số lượng
- 0,1,... Có trình độ tương đương các điều kiện sau hoặc cao hơn:
1) ĐH ngành ATTT, hoặc: 2) ĐH CNTT và đã qua đào tạo các chứng chỉ chuyên nghiệp ATTT hay đã tham gia nghiên cứu/thực hành chuyên nghiệp về ATTTM hơn 3 năm, hoặc: 3) ĐH các ngành KHKT, đã qua đào tạo bồi dưỡng các chứng chỉ chuyên nghiệp ATTT và đã tham gia nghiên cứu/thực hành chuyên nghiệp về ATTTM hơn 5 năm.
- 0,1,... Có trình độ tương đương: 1) ĐH không chuyên ngành CNTT hoặc Trung cấp/cao đẳng CNTT, và được đào tạo bồi dưỡng các khóa kỹ thuật về ATTTM, hoặc 2) ĐH CNTT nhưng không làm việc về ATTTM.
- 0,1,... Cán bộ làm việc chuyên trách về ATTTM và có trình độ tương đương ĐH ngành ATTT hoặc cao hơn, có chứng chỉ đào tạo các khóa chuyên gia kỹ thuật quốc tế hoặc tương đương về ATTTM, có thâm niên công tác nghiên cứu, thực hành trong lĩnh vực ATTTM liên tục từ 5 năm trở lên.
- 1/0 Có thì ghi là 1, không có ghi 0

Số người	Theo kế hoạch chung của	Theo kế hoạch riêng của cơ
Số cán bộ lãnh đạo		
Số cán bộ, nhân viên chuyên trách ATTTM		
Số cán bộ, nhân viên khác sử dụng máy tính		

- 25 Đơn vị có được thụ hưởng kế hoạch tuyên truyền, phổ biến nâng cao nhận thức về ATTTM của cấp trên (cơ quan chủ quản, cơ quan quản lý nhà nước) trong năm 2017 hay không?
- 26 Đơn vị có kế hoạch định kỳ tuyên truyền, phổ biến nâng cao nhận thức của người sử dụng về ATTTM năm 2017 hay không?
- 27 Số đơn vị trực thuộc cùng cơ quan chủ quản được thụ hưởng kế hoạch tuyên truyền, phổ biến nâng cao nhận thức về ATTTM mà quý đơn vị triển khai trong năm 2017
- 28 Số đơn vị trực thuộc các cơ quan chủ quản khác được thụ hưởng kế hoạch tuyên truyền, phổ biến nâng cao nhận thức về ATTTM mà đơn vị triển khai trong năm 2017

- 0,1,... Ghi số lượng vào từng ô. Ô nào không có thì ghi 0 hoặc để trống
- 1/0 Có thì ghi là 1, không có ghi 0
- 1/0 Có thì ghi là 1, không có ghi 0
- 0,1,... Ghi số lượng
- 0,1,... Ghi số lượng

- 28 Đơn vị có chủ trương sử dụng dịch vụ thuê hosting hệ thống (thuê ngoài hệ thống máy chủ và lưu trữ cơ sở dữ liệu) do các công ty Việt Nam không có yếu tố nước ngoài cung cấp hay không?

+ Không có chủ trương hay quy định thuê ngoài	
+ Có chủ trương nhưng chưa có thuê ngoài	
+ Đã thuê ngoài dịch vụ bảo đảm ATTTM	

- 29 Đơn vị có chủ trương sử dụng dịch vụ thuê hosting hệ thống (thuê ngoài hệ thống máy chủ và lưu trữ cơ sở dữ liệu) do các công ty Việt Nam không có yếu tố nước ngoài cung cấp hay không?

+ Không có chủ trương này	
+ Có chủ trương nhưng chưa có thuê	
+ Đã thuê dịch vụ của các công ty Việt Nam không có yếu tố nước ngoài	

- chọn 1 ô Ô nào chọn thì ghi là 1. Các ô còn lại để trống
- chọn 1 ô Ô nào chọn thì ghi là 1. Các ô còn lại để trống

30 Đơn vị có chủ trương sử dụng dịch vụ thuê hosting hệ thống có yếu tố nước ngoài cung cấp hay sử dụng dịch vụ điện toán đám mây (cloud computing) trên Internet hay không?

+ Không có chủ trương này	
+ Có chủ trương nhưng chưa sử dụng dịch vụ này	
+ Đã sử dụng dịch vụ này	

chọn 1 ô Ô nào chọn thì ghi là 1. Các ô còn lại để trống.

31 Đơn vị bảo đảm ATTTM thường xuyên bằng cách nào:

+ Hoàn toàn sử dụng nội lực	
+ Sử dụng toàn bộ thuê và hỗ trợ từ bên ngoài	
+ Sử dụng một phần nội lực một phần lực lượng bên ngoài	

chọn 1 ô Ô nào chọn thì ghi là 1. Các ô còn lại để trống.

32 Đơn vị có tổng chi (bao gồm cả chi ngân sách thường xuyên và dự án đầu tư) cho CNTT trong 3 năm gần đây là bao nhiêu (xTriệu đồng)?

Chi cho CNTT	2015	2016	2017
Tổng chi (xTriệu đồng)			

Ghi số tiền. Lấy số liệu từ đơn vị phụ trách kế hoạch-tài chính để trả lời câu hỏi này

33 Ước tính tỷ lệ chi cho ATTTM chiếm bao nhiêu % trong tổng đầu tư dành cho CNTT tại đơn vị trong 3 năm gần đây?

Chi cho ATTTM so với	2015	2016	2017
Tỷ lệ chi ATTTM/chi			

% Ghi tỉ lệ %. Lấy số liệu từ đơn vị phụ trách kế hoạch-tài chính để trả lời câu hỏi này. Phải điền vào tất cả các ô.

34 Ước tính tỷ lệ chi cho ATTTM cho các hệ thống thông tin trọng yếu/quan trọng quốc gia do đơn vị quản lý chiếm bao nhiêu % trong tổng đầu tư CNTT của cơ quan trong 3 năm gần đây?

Chi ATTTM so với chi	2015	2016	2017
Tỷ lệ chi ATTTM/chi CNTT (%)			

% Ghi tỉ lệ %. Lấy số liệu từ đơn vị phụ trách kế hoạch-tài chính để trả lời câu hỏi này. Phải điền vào tất cả các ô.

35 Ước tính chi phí chung về ATTTM năm 2017 đáp ứng bao nhiêu % nhu cầu (dự toán) của đơn vị?

Mức đáp ứng nhu cầu	2015	2016	2017
Tỷ lệ chi ATTTM/nhu cầu (%)			

% Ghi tỉ lệ %. Lấy số liệu từ đơn vị phụ trách kế hoạch-tài chính để trả lời câu hỏi này. Phải điền vào tất cả các ô.

36 Đơn vị đã triển khai hệ thống quản lý ATTTM (hệ thống ISMS) theo tiêu chuẩn TCVN/ISO-IEC 27000 hoặc tiêu chuẩn TCVN 11930:2017 hay tiêu chuẩn khác chưa? (Ghi rõ TC khác là:)

--

1/0 Đã triển khai thì ghi là 1, chưa thì ghi 0

37 Đơn vị đã nhận chứng nhận hợp chuẩn quản lý ATTTM theo 1 trong những tiêu chuẩn trên chưa? Nếu có thì cho biết thời điểm chứng nhận đã cách thời điểm hiện tại bao nhiêu tháng:

--

1/0 Đã nhận thì ghi là 1, chưa thì ghi 0

Thời điểm hợp chuẩn	Lần đầu tiên	Lần gần đây nhất
Cách đây bao nhiêu tháng		

1,2,... Ghi số tháng kể cả tháng hiện tại, ghi 0 hay trống là không có thông tin

38 Đơn vị có bao nhiêu hệ thống thông tin quan trọng quốc gia (cấp độ 5) hoặc hệ thống thông tin cấp độ 4 thuộc trách nhiệm quản lý đã nhận chứng nhận hợp chuẩn quản lý ATTTM ?

HTTT đã được hợp chuẩn	Hệ thống cấp độ 5	Hệ thống cấp độ 4	Hệ thống quan trọng quốc gia khác
Số lượng HTTT đã hợp chuẩn			

0,1,2,... Ghi số lượng vào từng ô.

39 Đơn vị có thực hiện các biện pháp phân loại, xác định trách nhiệm về sở hữu tài sản thông tin hay không ?

--

1/0 Đã phân loại thì ghi là 1, chưa thì ghi 0

- | | | | | |
|----|--|--|-----------|--|
| 40 | Việc quản lý cán bộ vận hành, khai thác, sử dụng hệ thống của cơ quan có tuân thủ các chính sách về ATTTM hay không? | | 1/0 | Có thì ghi là 1, không có ghi 0 |
| 41 | Đơn vị có quy trình đánh giá, quản lý và xử lý rủi ro về ATTTM không? | | 1/0 | Có thì ghi là 1, không có ghi 0 |
| 42 | Đơn vị có quy trình thao tác chuẩn (Standard operating procedures) để phản ứng với các sự cố mất ATTT hay không? | | 1/0 | Có thì ghi là 1, không có ghi 0 |
| 43 | Trong quá trình triển khai dự án phát triển ứng dụng CNTT, đơn vị có thực hiện tư vấn, thẩm định, thẩm tra về ATTTM của hệ thống thông tin được xây dựng hay không? | | 1/0 | Có thì ghi là 1, không có ghi 0 |
| 44 | Tổng số lần đơn vị đã thực hiện kiểm tra đánh giá ATTTM định kỳ cho hệ thống thông tin của mình trong năm 2017 ? | | 0/1/... | Nếu không có ghi số 0, nếu có thì ghi tổng số lần đánh giá (≥ 1) |
| 45 | Tổng số lần đơn vị đã tổ chức hoặc trực tiếp tham gia diễn tập bảo đảm ATTTM cho hệ thống thông tin của mình trong năm 2017? | | 0/1/... | Nếu không có ghi số 0, nếu có thì ghi tổng số lần diễn tập (≥ 1) |
| 46 | Với các biện pháp kỹ thuật, công nghệ phù hợp đang được đơn vị đang áp dụng để bảo đảm ATTTM cho các HTTT nội bộ và HTTT công cộng, hãy cho biết lần trang bị, cập nhật, nâng cấp hay làm mới gần đây nhất là cách thời điểm hiện tại bao nhiêu tháng (tính cả tháng hiện tại)? | | 0,1,2,... | Biện pháp kỹ thuật, công nghệ nào có thì ghi số tháng ≥ 1 , không có ghi 0. |

Các biện pháp kỹ thuật, công nghệ bảo đảm an toàn mạng được trang bị, cập nhật, nâng cấp hay làm mới gần đây nhất cách hiện nay bao nhiêu tháng	HTTT nội bộ	HTTT công cộng
+ Hệ thống thiết bị sensor ghi log-file phát hiện sự cố và mối đe dọa ATTT đối với mạng		
+ Hệ thống giám sát và quản lý sự kiện an toàn thông tin (SOC-Security Operation Center/SIEM- Security Incident & Event Management)		
+ Giải pháp phân chia hệ thống mạng thành các vùng mạng chức năng với các chính sách quản lý và biện pháp kỹ thuật ATTTM phù hợp		
+ Hệ thống phát hiện xâm nhập (IDS/IPS) trong mạng		
+ Hệ thống phòng chống tấn công DoS/DDoS		
+ Tường lửa cho toàn mạng (Network Firewall)		
+ Phần mềm chống virus mức mạng (Anti-Virus)		
+ Bảo vệ kênh truyền bằng công nghệ mã hóa và xác thực		
+ Kiểm soát mọi kênh truy cập có bắt buộc định kỳ thay đổi mật khẩu người dùng		
+ Kiểm soát mọi kênh truy cập có giải pháp hạn chế đăng nhập tự động (tán công kiểu từ điển) và/hoặc có yêu cầu xác thực hai yếu tố người dùng		
+ Bảo mật truy cập qua mạng không dây và các thiết bị đầu cuối		

- 47 Với các biện pháp kỹ thuật, công nghệ phù hợp đang được đơn vị áp dụng để bảo vệ các hệ thống máy chủ trong các HTTT nội bộ và HTTT công cộng, hãy cho biết lần trang bị, cập nhật, nâng cấp hay làm mới gần đây nhất là cách thời điểm hiện tại bao nhiêu tháng (tính cả tháng hiện tại)?

Các công nghệ, biện pháp kỹ thuật bảo vệ các hệ thống máy chủ được trang bị, cập nhật, nâng cấp hay làm mới gần đây nhất cách hiện nay bao nhiêu tháng	HTTT nội bộ	HTTT công cộng
+ Hệ thống quản lý thu thập và phân tích log-file phát hiện sự cố và mối đe dọa ATTT		
+ Hệ thống phát hiện và chống tấn công xâm nhập máy chủ (IDS/IPS)		
+ Tường lửa (Firewall) cho máy chủ		
+ Phần mềm chống virus mã độc (Anti-Virus)		

+ Quản lý phân chia người dùng theo đặc quyền và có theo dõi phát hiện tài khoản người dùng lạ trong hệ thống		
+ Quản lý truy cập và chống tấn công leo thang đặc quyền		
+ Bảo mật thiết bị di động và thiết bị đầu cuối truy cập từ xa		
+ Sử dụng hệ thống máy chủ dự phòng nóng (chạy song song, on-line)		
+ Sử dụng hệ thống máy chủ dự trữ (dự phòng off-line)		

48 Với các biện pháp kỹ thuật, công nghệ phù hợp đang được đơn vị đang áp dụng để bảo vệ các ứng dụng trong các HTTT nội bộ và HTTT công cộng, hãy cho biết lần trang bị, cập nhật, nâng cấp hay làm mới gần đây nhất là cách thời điểm hiện tại bao nhiêu tháng (tính cả tháng hiện tại)?

0,1,2... Biện pháp kỹ thuật, công nghệ nào có thì ghi số tháng >= 1, không có ghi 0.

Các công nghệ, biện pháp kỹ thuật phù hợp bảo vệ các ứng dụng được trang bị, cập nhật, nâng cấp hay làm mới gần đây nhất cách hiện nay bao nhiêu tháng	HTTT nội bộ	HTTT công cộng
+ Hệ thống ghi nhật ký (log-file) các ứng dụng		
+ Hệ thống quản lý và phân tích log-file		
+ Quản lý truy cập có xác thực nhiều bước		
+ Phần mềm chống virus mã độc (Anti-Virus)		
+ Tường lửa mức ứng dụng (ví dụ web-firewall,...)		
+ Lọc nội dung Web		
+ Bộ lọc chống thư rác (Anti-Spam)		
+ Sử dụng hệ thống máy chủ dự phòng nóng (chạy song song, on-line)		
+ Sử dụng hệ thống máy chủ dự trữ (dự phòng off-line)		

49 Với các biện pháp kỹ thuật, công nghệ phù hợp đang được đơn vị áp dụng để bảo vệ dữ liệu cho các HTTT nội bộ và HTTT công cộng, hãy cho biết lần trang bị, cập nhật, nâng cấp hay làm mới gần đây nhất là cách thời điểm hiện tại bao nhiêu tháng (tính cả tháng hiện tại)?

0,1,2... Biện pháp kỹ thuật, công nghệ nào có thì ghi số tháng >= 1, không có ghi 0.

Các biện pháp kỹ thuật, công nghệ phù hợp bảo vệ dữ liệu được trang bị, cập nhật, nâng cấp hay làm mới gần đây nhất cách hiện nay bao nhiêu tháng	HTTT nội bộ	HTTT công cộng
+ Hệ thống giám sát tính toán vẹn CSDL		
+ Hệ thống phát hiện xâm nhập CSDL		
+ Bảo vệ dữ liệu quan trọng trong hệ thống bằng công nghệ mã hóa		
+ Bảo vệ dữ liệu quan trọng trong hệ thống bằng công nghệ chữ ký số		
+ Hệ thống quản lý chống thất thoát dữ liệu (Data Loss protection)		
+ Sử dụng hệ thống sao lưu dữ liệu dự phòng nóng (on-line back-up)		
+ Sử dụng hệ thống sao lưu dữ liệu dự phòng định kỳ (off-line back-up)		

50 Với các biện pháp kỹ thuật, công nghệ phù hợp đang được đơn vị đang áp dụng để bảo đảm an toàn về mặt vật lý cho các HTTT nội bộ và HTTT công cộng, hãy cho biết lần trang bị, cập nhật, nâng cấp hay làm mới gần đây nhất là cách thời điểm hiện tại bao nhiêu tháng (tính cả tháng hiện tại)?

0,1,2... Biện pháp kỹ thuật, công nghệ nào có thì ghi số tháng >= 1, không có ghi 0.

Các biện pháp kỹ thuật, công nghệ phù hợp bảo đảm an toàn vật lý được trang bị, cập nhật, nâng cấp hay làm mới gần đây nhất cách thời điểm hiện tại bao nhiêu tháng	HTTT nội bộ	HTTT công cộng
+ Giải pháp lựa chọn vị trí vật lý		
+ Giải pháp kiểm soát truy cập vật lý		
+ Giải pháp chống trộm, chống phá hoại		
+ Giải pháp chống sét		
+ Hệ thống chống cháy nổ		
+ Giải pháp chống âm và chống thấm		
+ Giải pháp chống bụi và tĩnh điện		
+ Giải pháp kiểm soát nhiệt độ và độ ẩm		

+ Hệ thống nguồn cung cấp điện dự phòng		
+ Giải pháp bảo vệ điện từ trường		

- 51 Đơn vị có khả năng ghi nhận các hành vi tấn công (kể cả chưa thành công) vào hệ thống của mình hay không?
- 52 Khi hệ thống của đơn vị gặp sự cố mất ATTTM, quý vị sẽ báo cáo/thông báo tin này đi đâu? Đánh dấu tương ứng vào các ô phù hợp trong bảng sau:

- 1/0 Có thì ghi là 1, không có ghi 0
- 1/0
- 1/0 Ghi 1 vào ô chọn

Phản ứng Loại sự cố nguy cơ ATTTM	Tự xử lý, không báo cáo	Mời DN, sử dụng dịch vụ ngoài	Báo cáo cấp trên, ngành đọc	Báo và hợp tác với nhà mạng	Báo và hợp tác với đơn vị Bộ Quốc phòng	Báo và hợp tác với đơn vị Bộ Công an	Báo và hợp tác với đơn vị Bộ TTTT
Đơn vị đủ khả năng phát hiện và xử lý							
Đơn vị phát hiện được, chưa gây tác hại, nhưng khó xử lý							
Loại mới hoặc tấn công gây tác hại lớn, chưa tự xử lý được							

- 53 Từ 1/1/2017 đến hết 31/12/2017, đơn vị đã phát hiện được bao nhiêu sự cố ATTTM vào hệ thống của mình chưa gây ra thiệt hại hoặc gây ra thiệt hại nhỏ? Thống kê số vụ tấn công mạng đã xảy ra với các hệ thống thông tin do đơn vị quản lý (phân loại theo kiểu tấn công và hậu quả).

- 0,1,2,... Ghi số lượng sự cố tương ứng vào các ô

Số vụ tấn công mạng ít nghiêm trọng từ 1/1/2017 đến 31/12/2017	Số vụ tấn công web deface hay cài Phishing	Số lần tấn công từ chối dịch vụ (DDoS)	Số vụ tấn công bằng thư điện tử (spam-mail)	Số máy tính trạm đã bị lây nhiễm mã độc	Số lần máy chủ bị tấn công bằng mã độc	Số vụ tấn công vào lỗ hổng ATTT của HTTT	Số sự cố khác (lỗi hạ tầng, vật lý, phần mềm)	Số vụ xâm nhập mạng do ATP, lộ mật khẩu
Số vụ đã phát hiện và ngăn chặn sớm, chưa gây ra thiệt hại								
Số vụ tấn công đã bị xâm nhập, lây nhiễm mã độc, nhưng chỉ gây ra thiệt hại nhỏ								

- 54 Số vụ tấn công, mất ATTTM nghiêm trọng (gây ra hậu quả nghiêm trọng về kinh tế, gián đoạn dịch vụ mạng, lộ lọt thông tin quan trọng...) xảy ra từ 1/2017 đến hết 31/12/2017

- 0,1,2,... Ghi số lượng sự cố tương ứng vào các ô

Số vụ việc mất ATTTM nghiêm trọng xảy ra từ 1/1/2017 đến hết 31/12/2017	Số lần tấn công từ chối dịch vụ (DDoS)	Số lần máy chủ bị tấn công bằng mã độc	Số máy tính trạm đã bị lây nhiễm mã độc	Số vụ xâm nhập mạng do ATP, lộ mật khẩu	Số vụ tấn công vào lỗ hổng do ATTT của HTTT	Số vụ tấn công web deface hay cài Phishing	Số vụ tấn công bằng thư điện tử (spam-mail)	Số sự cố khác (lỗi hạ tầng, vật lý, phần mềm)
Tổng số vụ việc đã phát hiện, xử lý								
Đơn vị tự xử lý, khắc phục hậu quả thành công trong vòng 24h								
Được đơn vị khác hỗ trợ xử lý, khắc phục hậu quả thành công trong vòng 24h								

55 Theo quý vị những động cơ nào được nghi ngờ là nguyên nhân gây ra những hành động tấn công ở trên? (có thể chọn nhiều đáp án là các mục sau)

0/1 Ghi 1 vào ô chọn

Nhằm thể hiện kỹ năng tấn công	
Phá hoại hệ thống có chủ đích	
Nhằm chiếm dụng tài nguyên hệ thống để dẫn tới những cuộc tấn công nặc danh	
Thù hằn cá nhân (ví dụ: cán bộ hoặc người ngoài có thù hằn cá nhân)	
Nhằm tạo lợi thế cạnh tranh thương mại (ví dụ: tình báo công nghiệp)	
Chiếm đoạt tài nguyên hệ thống của cơ quan để sử dụng cho mục đích cá nhân	
Bị tấn công từ nước ngoài do các nguyên nhân liên quan đến chủ quyền	
Tạo nguồn thu tài chính bất hợp pháp	
Nhằm chiếm dụng tài nguyên hệ thống để dẫn tới những cuộc tấn công nặc danh	
Thù hằn cá nhân (ví dụ: cán bộ hoặc người ngoài có thù hằn cá nhân)	

56 Với tình hình hiện tại thì trong thời gian tới, đối tượng đe dọa tới ATTTM của hệ thống mà quý vị lo ngại nhất là gì ? (Ghi các số 1/2/3 tương ứng với các hạng mục lo ngại nhất, nhì và ba)

0/1/2/3 Chọn 3 hạng mục theo thứ tự giảm dần xét theo mức độ lo ngại trong số những hạng mục được liệt kê và ghi các số 1/2/3 vào ô được chọn tương ứng

- Cán bộ đang làm việc tại đơn vị	
- Cán bộ đã nghỉ việc tại đơn vị	
- Tội phạm máy tính như hacker bất hợp pháp	
- Đối thủ cạnh tranh (gián điệp công nghiệp)	
- Băng nhóm tội phạm máy tính có tổ chức (khung bố mạng v.v...)	
- Doanh nghiệp gia công bên ngoài (nhân viên) Outsourcing company (employees)	
- Các thể lực đến từ nước ngoài	
- Những mối đe dọa khác (vui lòng ghi rõ):	

57 Những vấn đề khó khăn nhất mà đơn vị gặp phải trong việc bảo đảm ATTTM cho hệ thống thông tin là gì? (Ghi các số 1/2/3/4/5 tương ứng với các hạng mục khó khăn nhất, nhì, ba, tư và năm)

Lãnh đạo chưa hỗ trợ đúng mức cần thiết cho ATTTM	
Sự thiếu hiểu biết về ATTTM trong đơn vị, thiếu cán bộ am hiểu kỹ thuật và quản lý ATTTM	
Việc nâng cao nhận thức và mặt bằng kiến thức cho người sử dụng máy tính về ATTTM	
Việc xác định chính xác mức độ ưu tiên của ATTTM trong tương quan chung với các vấn đề khác của đơn vị	
Việc áp dụng các nguyên tắc quản lý rủi ro (Risk Management principles) cho hệ thống thông tin	
Việc cập nhật kịp thời những cách thức tấn công hay những những điểm yếu mới xuất hiện	
Việc giám sát phát hiện, cảnh báo sớm các cuộc tấn công mạng	
Không đủ khả năng phản ứng nhanh và xử lý chính xác khi xảy ra những vụ tấn công qua mạng	
Việc quản lý chặt chẽ cấu hình hệ thống mạng (Configuration Management)	
Những hệ thống máy tính không được quản lý tốt	
Kinh phí/ngân sách dành cho ATTTM quá thiếu so với mặt bằng chung	
Các vấn đề khác (Nếu có thì vui lòng ghi rõ):	

0/1.../5 Chọn 5 hạng mục theo thứ tự giảm dần xét theo mức độ khó khăn trong số những hạng mục được liệt kê và ghi các số 1/2/3/4/5 vào ô được chọn tương ứng

58 Số lần đơn vị đã rút kinh nghiệm bài học khác phục sự cố dẫn đến việc thay đổi, bổ sung, hoàn thiện quy định, quy chế ứng cứu sự cố và bảo đảm ATTTM trong năm 2017

0,1,... Ghi số lần

59 Đơn vị có sử dụng chữ ký số để bảo đảm an toàn cho các giao dịch điện tử hay không?

--

1/0 Có thì ghi là 1, không có ghi 0

Lãnh đạo đơn vị
(Ký, ghi rõ họ tên và đóng dấu)

Người lập bản báo cáo
Họ tên:.....
Điện thoại:.....
Email:.....

Báo cáo đã điền đầy đủ nội dung xin gửi đơn vị đầu mối của cơ quan để tổng hợp, sau đó gửi về Cục An toàn thông tin, Bộ Thông tin và Truyền thông, địa chỉ: tầng 8, số 115 Trần Duy Hưng, Hà Nội.