UBND THÀNH PHỐ HÀ NỘI
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

HIỆN TRẠNG HỆ THỐNG AN TOÀN THÔNG TIN TRONG CƠ QUAN NHÀ NƯỚC THÀNH PHỐ HÀ NỘI

Hà Nội, 5/2012

1

Hạ tầng thiết bị

Firewall và phần mềm diệt vius:

- Gần 70% số CQNN đã sử dụng firewall cứng hoặc mềm
- Hầu hết chưa trang bị thiết bị phát hiện và phòng chống thâm nhập IDS, IPS
- Hầu hết các CQNN và DNNN đều sử dụng phần mềm diệt virus, tuy nhiên các phần mềm diệt virus đa số là phần mềm không có bản quyền, tự do tải về từ Internet như BKAVHome, Symantec;

2

Bảng tổng hợp thiết bị an toàn bảo mật

Nội dung	Tổng đơn vị	Phần mềm diệt virus	Thiết bị phòng chống thâm nhập	Firewall			
				Chung	Cứng	Mềm	Cả cứng và mềm
Tổng hợp chung	**59**	**59 (100%)**	**0**	**41 (69.49%)**	6	17	18
Sở ban ngành	30	30 (100%)	0	21 (70%)	2	6	13
Quận huyện	29	29 (100%)	0	20 (68,96%)	4	11	5

3

Hạ tầng thiết bị

Máy chủ:

- Tổng số máy chủ trong các CQNN là 338 máy; Hầu hết các máy chủ được sử dụng cho dịch vụ mạng và ứng dụng chuyên ngành.
- Hệ điều hành cho máy chủ chủ yếu là Windows Server 99%%, Linux chỉ có 1% và phần lớn không có bản quyền;

4

Hạ tầng thiết bị

Hệ thống sao lưu dự phòng:

- Chỉ có 4 CQNN đầu tư hệ thống SAN để sao lưu dự phòng CSDL. Hầu hết các CQNN không được trang bị thiết bị sao lưu băng từ.
- Dịch vụ sao lưu dự phòng hiện tại mới ở mức người dùng tự tạo ra các bản sao nội dung của CSDL. Còn lại, gần như toàn bộ các CQNN hiện nay chưa sử dụng thiết bị và giải pháp sao lưu dự phòng và các giải pháp khôi phục dữ liệu khi có sự cố.....

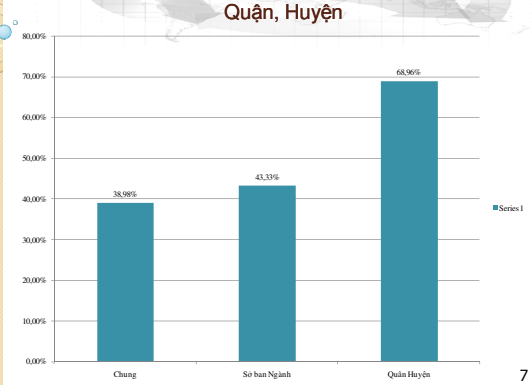
5

Áp dụng chính sách, qui trình bảo mật

- 38.98% số CQNN xây dựng văn bản quản lý hệ thống CNTT của đơn vị trong đó có quy định về an toàn thông tin. Các qui định này chưa đầy đủ.
- Hầu hết CQNN chưa áp dụng chính sách, qui trình đảm bảo an toàn, an ninh thông tin

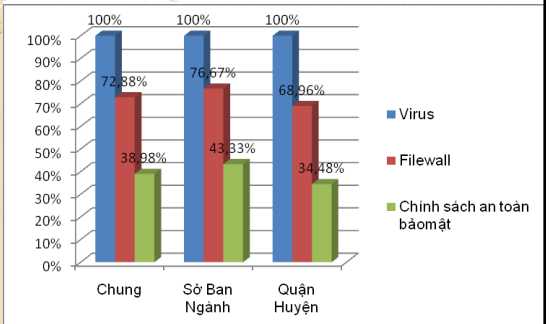
6

Biểu đồ so sánh mức độ áp dụng qui định an toàn bảo mật của khối Sở, Ban, Ngành và khối UBND Quận, Huyện



7

Biểu đồ so sánh mức độ áp dụng qui định an toàn bảo mật và thiết bị bảo mật của khối Sở, Ban, Ngành và khối UBND Quận, Huyện



8

Nguồn nhân lực

- Trên 90% số CQNN có cán bộ chuyên trách CNTT, trong đó 13,7% số CQNN có bộ phận chuyên trách CNTT. Hầu hết cán bộ CNTT có trình độ cao đẳng trở lên. Tuy vậy, các cán bộ CNTT vẫn còn thiếu kỹ năng quản lý, thiếu kiến thức và kỹ năng về quản trị, đảm bảo an toàn an ninh cho hệ thống CNTT
- Đại bộ phận cán bộ công chức, viên chức chưa được bồi dưỡng, đào tạo kỹ năng đảm bảo an toàn an ninh thông tin cũng như nhận thức chung về an toàn thông tin.

9

Kết luận

- Do hệ thống đảm bảo an toàn thông tin trong CQNN còn nhiều hạn chế, chưa được quan tâm đầu tư đúng mức dẫn đến nguy cơ mất ATTT trong CQNN và đang đặt ra những yêu cầu bức thiết, CQNN có thể bị tấn công từ bất kỳ nơi đâu bên trong, bên ngoài, gần, xa và do bất kỳ ai...
- Đặc biệt năm 2011, các hành vi gian lận, tội phạm trên môi trường mạng có chiều hướng gia tăng, một số website của CQNN đã bị tấn công
- Vì vậy các CQNN cần xây dựng hàng rào An toàn thông tin nhằm đảm bảo 3 yếu tố: Bảo mật, toàn vẹn và sẵn sàng, đảm bảo khả năng phòng chống các cuộc tấn công…

10

Kết luận

- Để cho hệ thống an toàn, bảo mật hoạt động thực sự hiệu quả, các đơn vị cần xây dựng một cơ chế quản lý tài nguyên hệ thống, quản lý và kiểm soát an toàn thông tin với quy trình quản trị và vận hành hệ thống, ngoài ra cần có chính sách quy định về việc sử dụng thông tin an toàn trong cơ quan; Tăng cường bồi dưỡng, đào tạo, thường xuyên kiểm tra, nhắc nhở cán bộ nhân viên về sự cần thiết của bảo mật cũng như việc thực hiện các biện pháp, quy định bảo mật của đơn vị. Các quy định, chính sách bảo mật cho người dùng cuối, các quy trình cho đội ngũ cán bộ chuyên trách CNTT cũng cần được rà soát/chỉnh sửa theo hướng chuẩn hóa, nâng cao tính bảo mật.

11

Trân trọng cảm ơn.

12