Bộ Thông tin và Truyền thông
Trung tâm VNCERT

VỀ TÌNH HÌNH TRIỂN KHAI ĐẢM BẢO AN TOÀN, AN NINH MẠNG TẠI VIỆT NAM

Trình bày: TS. Vũ Quốc Khánh

Security World - Hà Nội, 03/2012

Nội dung

I. MÔI TRƯỜNG CNTT

- *Hạ tầng mạng CNTT-TT*
- *Chính phủ điện tử*
- *Thương mại điện tử*
- *Phát triển và thách thức*

II. MÔI TRƯỜNG PHÁP LÝ

- *Một số nhận định*
- *Kế hoạch phát triển*

III. TÌNH HÌNH AN TOÀN THÔNG TIN SỐ

- *Quản lý ATTT*
- *Xử lý sự cố ATTT*
- *Đánh giá nguy cơ ATTT*
- *Giải pháp*

I. MÔI TRƯỜNG CNTT

HẠ TẦNG MẠNG CNTT-TT (2/2012)

Mạng truyền dẫn cáp quang	Hầu hết các xã
Mạng điện thoại cố định, di động	Hầu hết các xã
Mạng Internet	Hầu hết các xã
Vệ tinh viễn thông Vinasat	Cả nước

	Số thuê bao (x triệu)	Tăng/giảm so với cùng kỳ năm trước
Thuê bao điện thoại cố định	15,3	-1,4 %
Thuê bao điện thoại di động	119	+4,3 %
Số người sử dụng Internet	32,6	+18,4 %
Thuê bao Internet băng rộng	4,3	+18,2 %

Nguồn: Tổng cục Thống kê

PHÁT TRIỂN CHÍNH PHỦ ĐIỆN TỬ (12/2010)

	Bộ, Cơ quan ngang Bộ	Tỉnh, TP trực thuộc TƯ
Có mạng nội bộ và đơn vị chuyên trách CNTT	100%	100%
Có trang/cổng TTĐT	21/22	62/63
Tỷ lệ máy tính trên tổng số cán bộ, công chức	88,50%	63,19%
Tỷ lệ máy vi tính kết nối Internet	88,37%	85,53%
Dịch vụ công trực tuyến mức 1	4.841	88.387
Dịch vụ công trực tuyến từ mức 2-4	28	751
Ứng dụng CNTT trong quản lý điều hành (Tính đến đơn vị cấp trực thuộc)	95%	75%
Xây dựng và triển khai sử dụng hệ thống thư điện tử trong công việc	90%	93%
Tỷ lệ địa phương có ứng dụng CNTT tại bộ phận một cửa (tại trên 30% số quận, huyện)		87% (20%)

PHÁT TRIỂN THƯƠNG MẠI ĐIỆN TỬ (12/2010)

	Tỷ lệ
Sử dụng máy tính	100%
Kết nối Internet	98%
Kết nối Internet băng rộng	89%
Sử dụng thư điện tử trong SX-KD + Doanh nghiệp lớn + Doanh nghiệp vừa và nhỏ	 96% 80%
Đặt hàng qua email	53%
Nhận đặt hàng qua email	52%
Đặt hàng qua website	21%
Nhận đặt hàng qua website	15%
Có website riêng	38%
Tham gia sàn giao dịch điện tử	14%
Hộ gia đình sử dụng dịch vụ TMĐT ở TP lớn (Hà Nội...) + Dùng internet cho TMĐT + Có thanh toán trực tuyến	49% 18% 4%

PHÁT TRIỂN VÀ THÁCH THỨC

Dự báo (Đề án đưa VN thành nước mạnh về CNTT-TT)

+ 2015: *50% dân số, 20%-30% hộ GĐ sử dụng Internet băng rộng, 85% phủ sóng di động băng rộng, dịch vụ công mức 2,3*

+ 2020: *70% dân số, 50%-60% hộ GD sử dụng Internet băng rộng, 95% phủ sóng di động băng rộng, dịch vụ công mức 4.*

Thách thức:

+ Tài chính-Ngân hàng, TMĐT, CPĐT, Dịch vụ trên mạng
+ ĐT đám mây+3G+mạng xã hội = nền tảng mới CNTT
+ Sử dụng không an toàn, thiếu hiểu biết, thiếu quản lý
+ Kỹ thuật hacker > < Kỹ thuật ATTT
+ Tội phạm mạng, khủng bố mạng

➔ **ATTT ngày càng *quan trọng***

II. MÔI TRƯỜNG PHÁP LÝ VỀ ATTT

Giai đoạn 2005-2011

+ Luật liên quan: 5

+ Nghị định: 7

+ Thông tư: 9

+ Văn bản điều hành, Quyết định: 9

+ Tiêu chuẩn Việt Nam: 2

Một số nhận định chung

+ Các quy định khá phong phú

- ✓ *Tập trung giải quyết những vấn đề bức xúc*
- ✓ *Ưu tiên đưa ra các quy định định hướng*
- ✓ *Chú trọng các chế tài xử lý*

+ Vấn đề hệ thống:

- ➢ *Chưa có tính hệ thống cao,*
- ➢ *Nhiều văn bản gò bó, khái niệm chưa nhất quán*
- ➢ *Các văn bản QPPL nền tảng chưa đón đầu phát triển*

+ Vấn đề thực thi và tuân thủ:

- ➢ *Bước đầu quan tâm nhưng chưa nhiều*
- ➢ *Thiếu các hệ thống hướng dẫn, tài liệu đào tạo*
- ➢ *Thiếu các tiêu chuẩn, quy chuẩn*

PHÁT TRIỂN MÔI TRƯỜNG PHÁP LÝ

Đang trong kế hoạch xây dựng

+ Luật: 2

+ Nghị định: 4 và các thông tư

+ Tiêu chuẩn Việt Nam tương thích quốc tế: 31

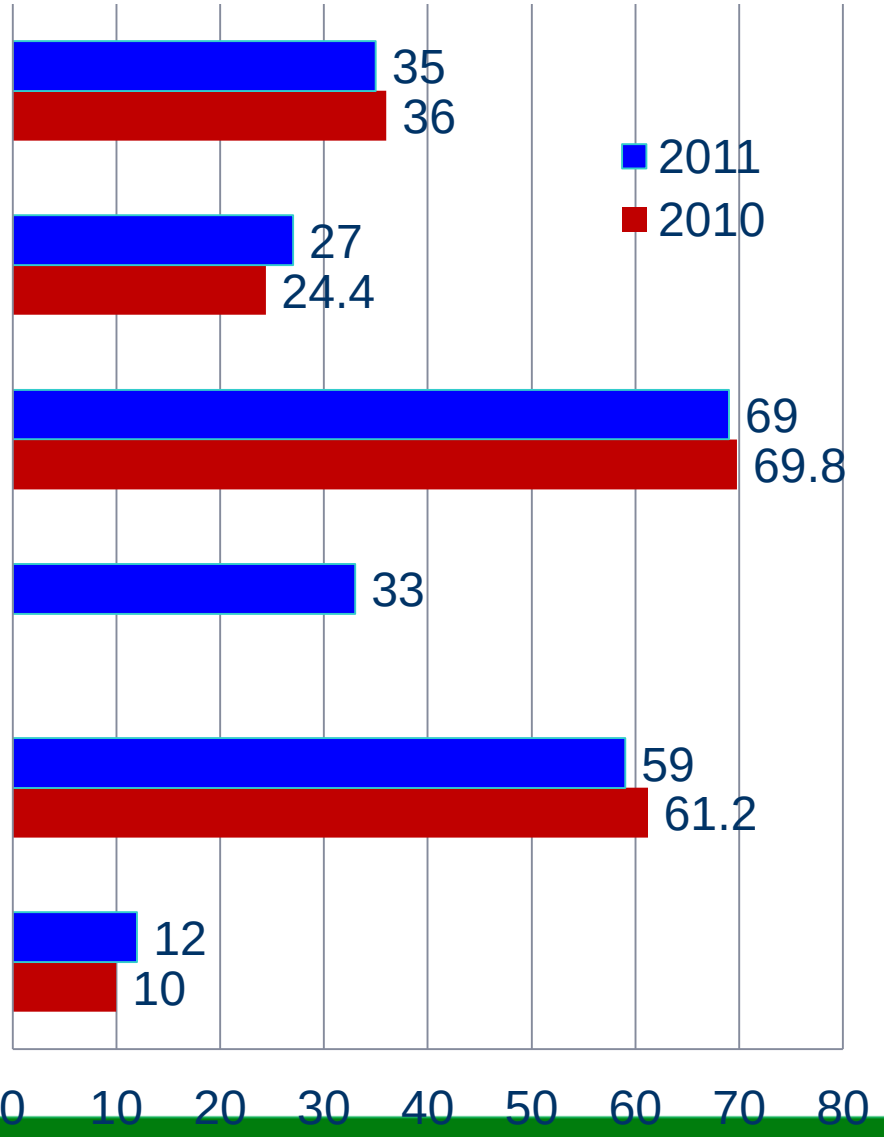
Nhóm tiêu chuẩn về quản lý an toàn thông tin: 6
Nhóm tiêu chuẩn về đánh giá ATTT: 8
Nhóm tiêu chuẩn về kỹ thuật AT mạng và ứng cứu sự cố: 9
Nhóm tiêu chuẩn về đào tạo ATTT: 3
Nhóm tiêu chuẩn về mật mã và chứng thực số: 5

II. TÌNH HÌNH AN TOÀN TT số

- ***Triển khai Quy hoạch phát triển ATTT số từ 2010***
- ***Triển khai Chỉ thị 897/CT-TTg ngày 10/6/2011 của Thủ tướng CP về tăng cường triển khai các hoạt động đảm bảo an toàn thông tin số***
- Theo báo cáo của các CQNN đến tháng 11/2011, phần lớn các bộ, ngành và địa phương đã xây dựng và phê duyệt kế hoạch đảm bảo an toàn thông tin số.
- Trên 30% các đơn vị chuyên trách về CNTT của các bộ, ngành và địa phương đã ban hành quy chế đảm bảo an toàn thông tin số.

VỀ QUẢN LÝ ATTT

69% đơn vị có cán bộ chuyên trách về ATTT và **59%** đơn vị có kế hoạch đào tạo về an toàn, an ninh thông tin.



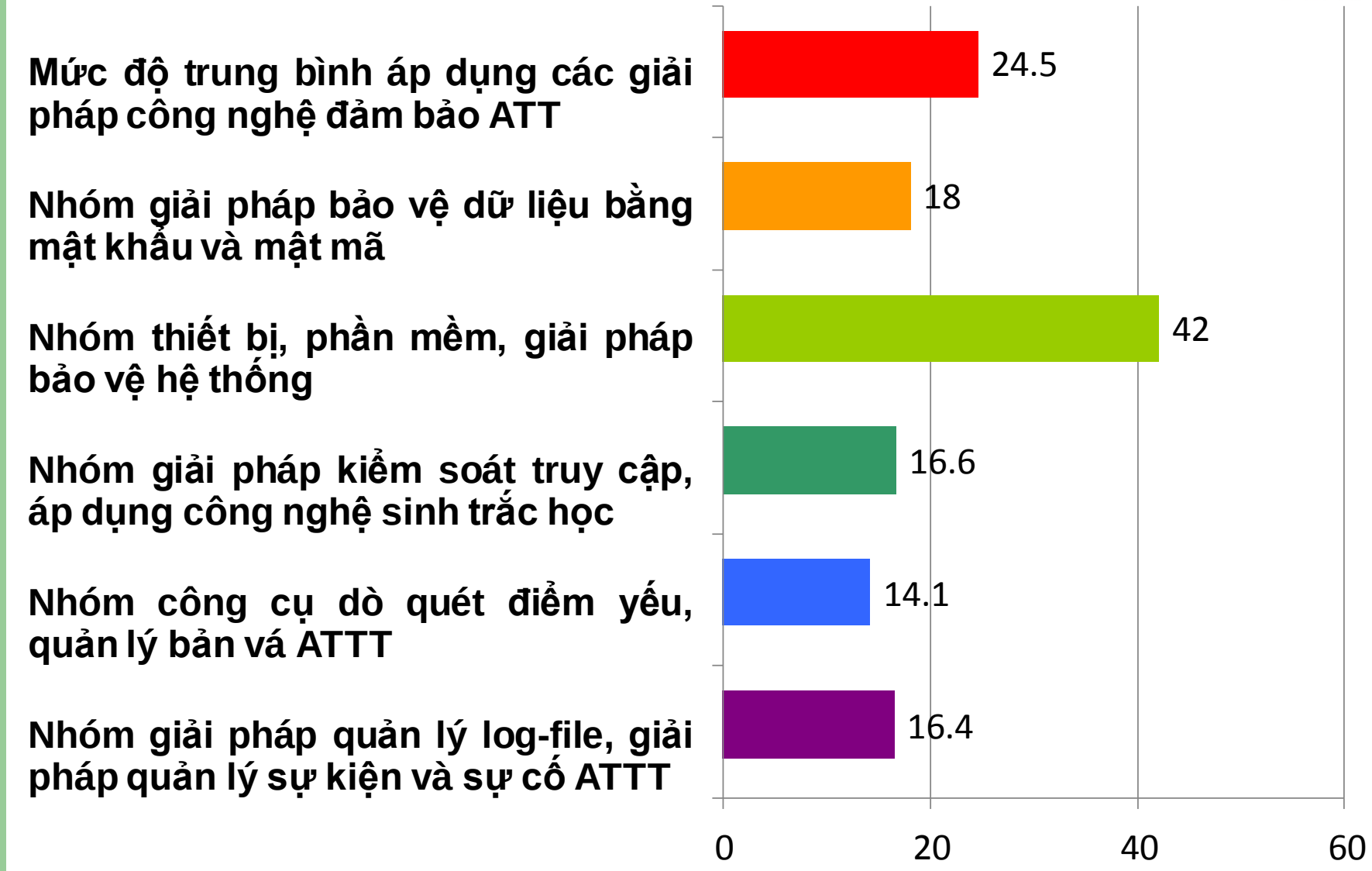
Nguồn: khảo sát của VNISA+VNCERT

Chỉ số mức độ quan tâm của các nhóm doanh nghiệp về công tác đảm bảo ATTT trong thương mại điện tử

TT	Nhóm doanh nghiệp được khảo sát	Số lượng	Mức độ quan tâm (từ 1-10) về công tác đảm bảo ATTT
1	Công nghiệp – Thương mại	15	5/10
2	Ngân hàng – Tài chính	10	10/10
3	Chứng khoán	08	10/10
4	Hàng không – vận tải	03	10/10
5	Viễn thông	04	8/10
6	Dịch vụ TMDT và CNTT	15	7/10

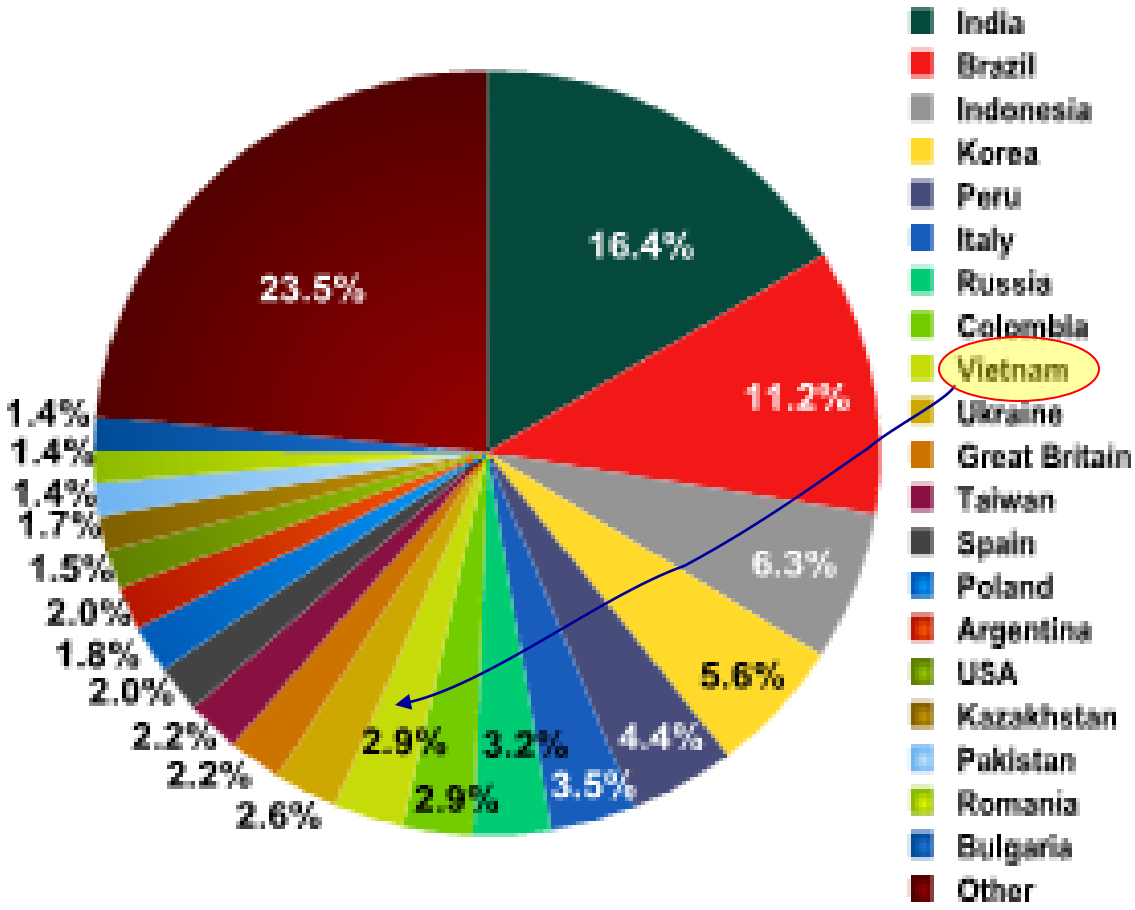
Nguồn: Cục TMĐT-CNTT, Bộ CT

CHỈ SỐ TỶ LỆ ÁP DỤNG GiẢI PHÁP ATTT (%)



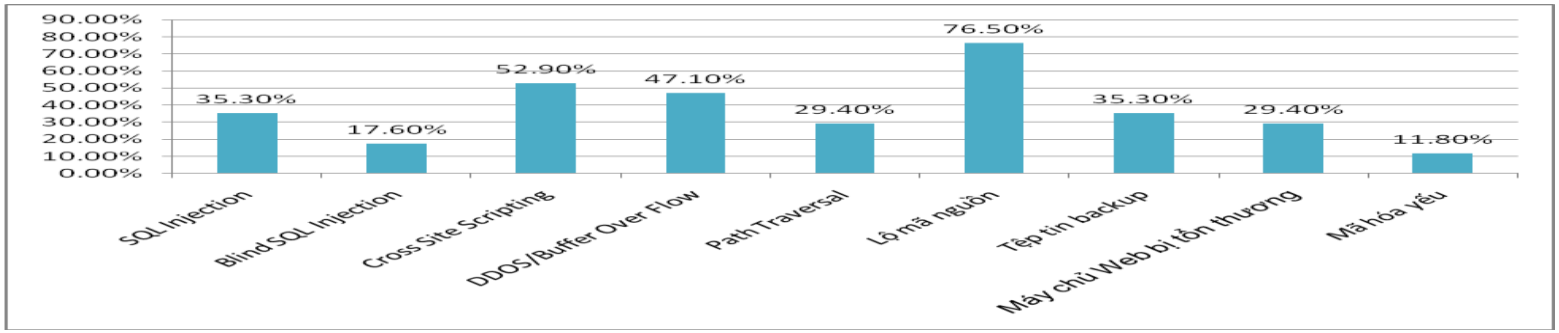
Thư điện tử rác (Spam) tại VN tháng 6/2011

Thống kê của VNCERT + VINASIS trong năm 2010: *Số thư điện tử rác ước tính năm sau gấp ba lần năm trước.*

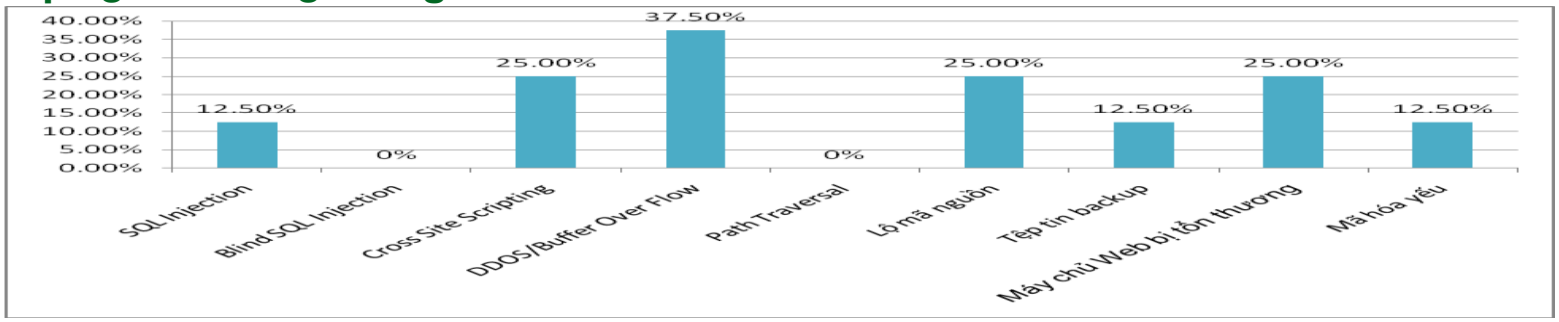


Lỗi bảo mật của cổng thông tin điện tử VN

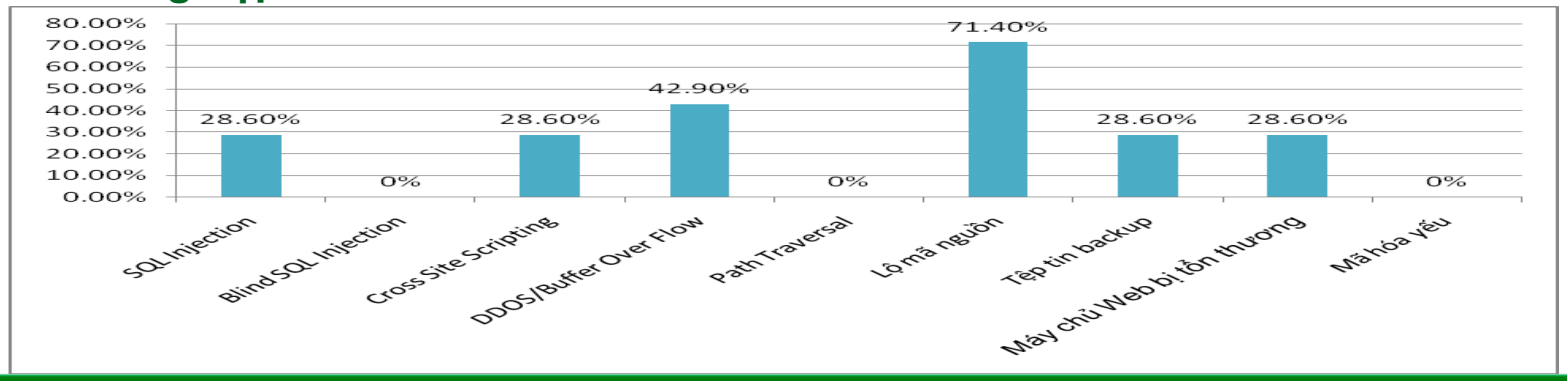
các địa phương



các bộ ngành trung ương

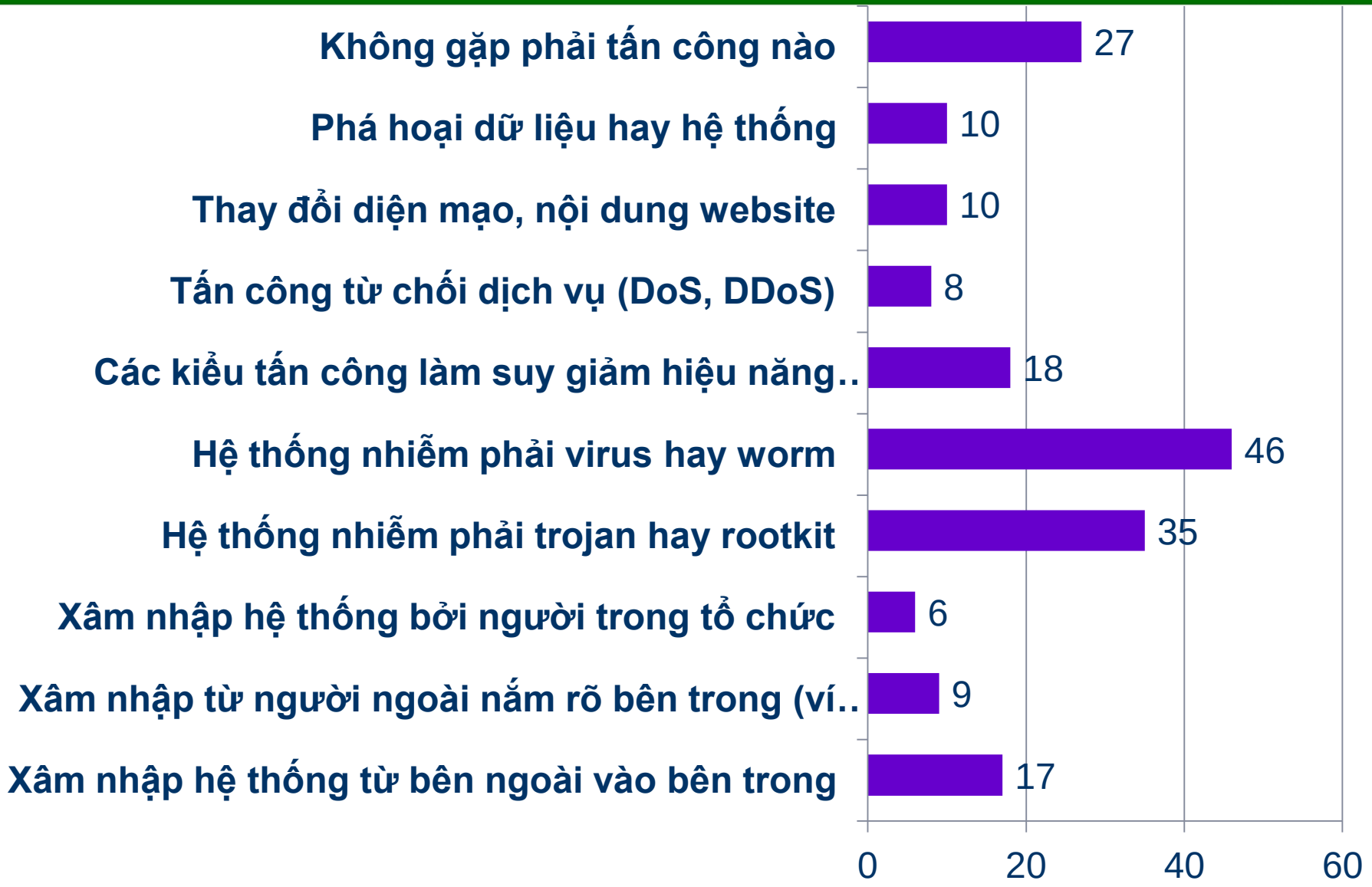


cácdoanh nghiệp nhà nước



Theo đánh giá của VNCERT 2010

NHẬN BIẾT DẠNGTẤN CÔNG MẠNG (%)



Nguồn: kết quả khảo sát của VNISA+VNCERT 2010

Tình hình xử lý sự cố tại VNCERT

Cơ cấu sự cố	2009		2010		2012	
Phishing	136	*66.0%*	233	*86.0%*	385	*50.9%*
Malware	10	*4.9%*	8	*3.0%*	13	*1.7%*
DoS/DDoS	6	*2.9%*	1	*0.4%*	3	*0.4%*
SMS Spams	19	*9.2%*	10	*3.7%*	14	*1.8%*
Deface	35	*17.0%*	19	*7.0%*	340	*44.9%*
Khác					2	*0.3%*
Cộng (= tỷ lệ so với năm trước)	**206**	***=261%***	**271**	***=132%***	**757**	***=279%***

Xu hướng thay đổi số sự cố được các CERT QG xử lý

	Phishing	Malware	Deface	Spam	Botnet
Ấn Độ		↑		↑	↓
Indonexia					
Hàn Quốc	↓	↑	↓	↓	↓
Nhật Bản		↑			
Malaysia		↑			
Philippin			↓	↑	
Singapore	↑				
Thái Lan		↑			
Trung Quốc		↑	↑		↓
Việt Nam	↑	↑	↑	↑	↑

ĐÁNH GIÁ NGUY CƠ ATTT

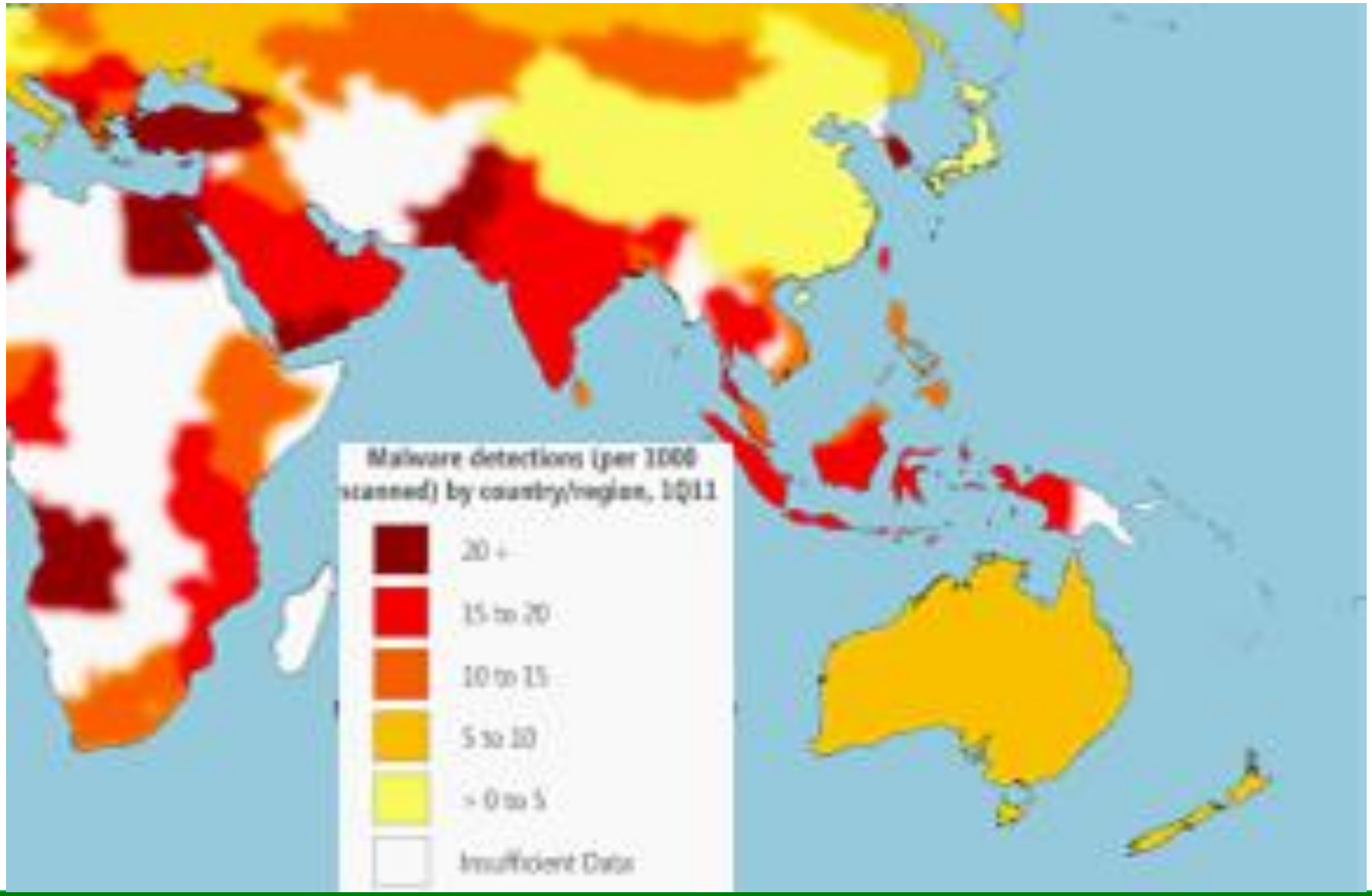
- Tấn công hệ thống tài chính, ngân hàng
- Đột nhập mạng chính phủ, hệ thống thông tin QG
- Nguy cơ tấn công mạng hiện nay
- Nguy cơ tội phạm mạng thế hệ mới
- Nguy cơ sử dụng công nghệ mới
- Nguy cơ an toàn thông tin trong viễn thông
- Nguy cơ chiến tranh mạng và sự chuẩn bị
- Nguy cơ phụ thuộc, không kiểm soát được ATTT

ĐÁNH GIÁ NGUY CƠ ATTT

ĐÁNH GIÁ NGUY CƠ ATTT

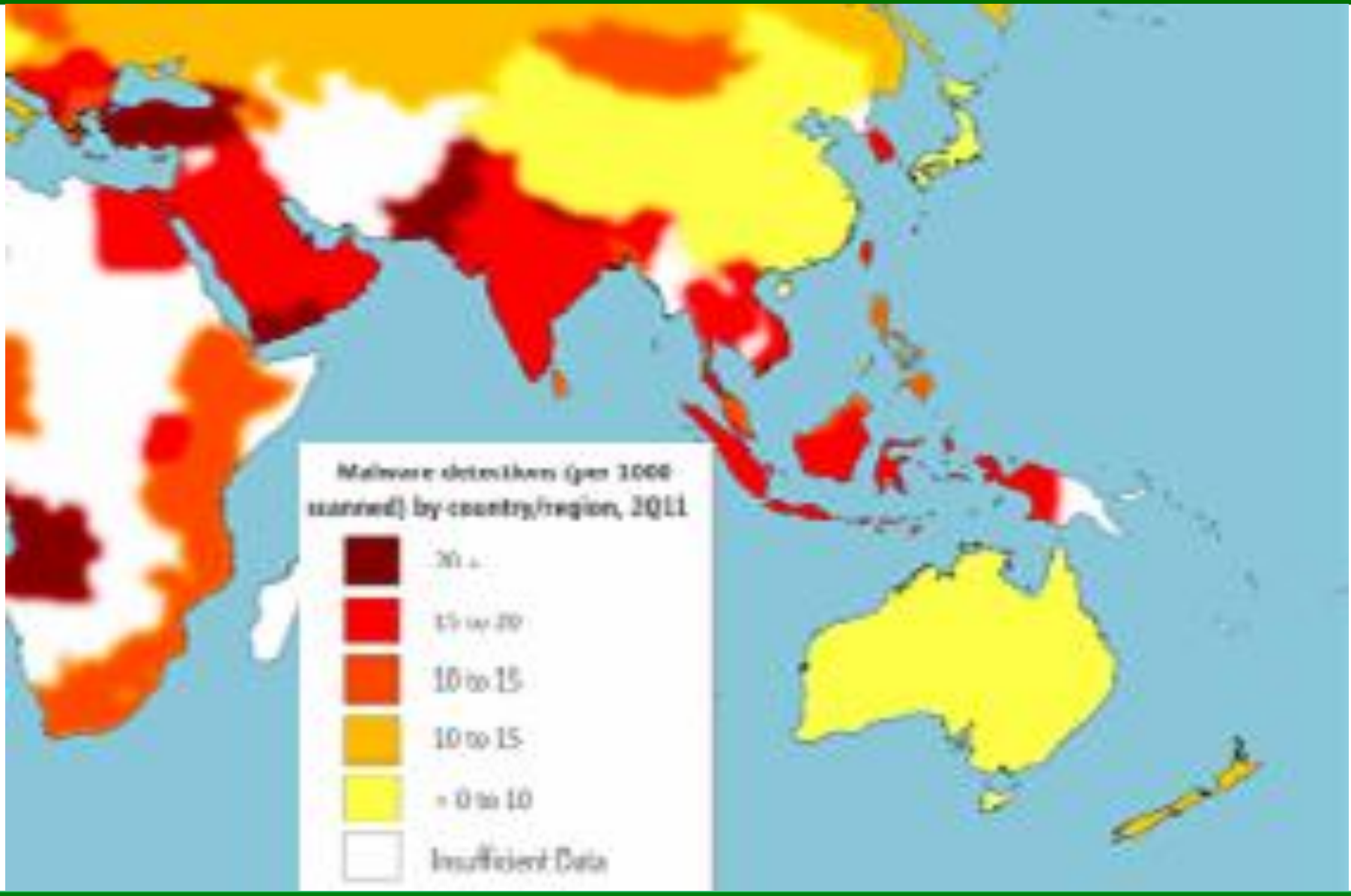
1	2	3
Khai thác lỗ hổng	**Sử dụng mã độc**	Tấn công xã hội

Bản đồ phát hiện mã độc Q1-2011



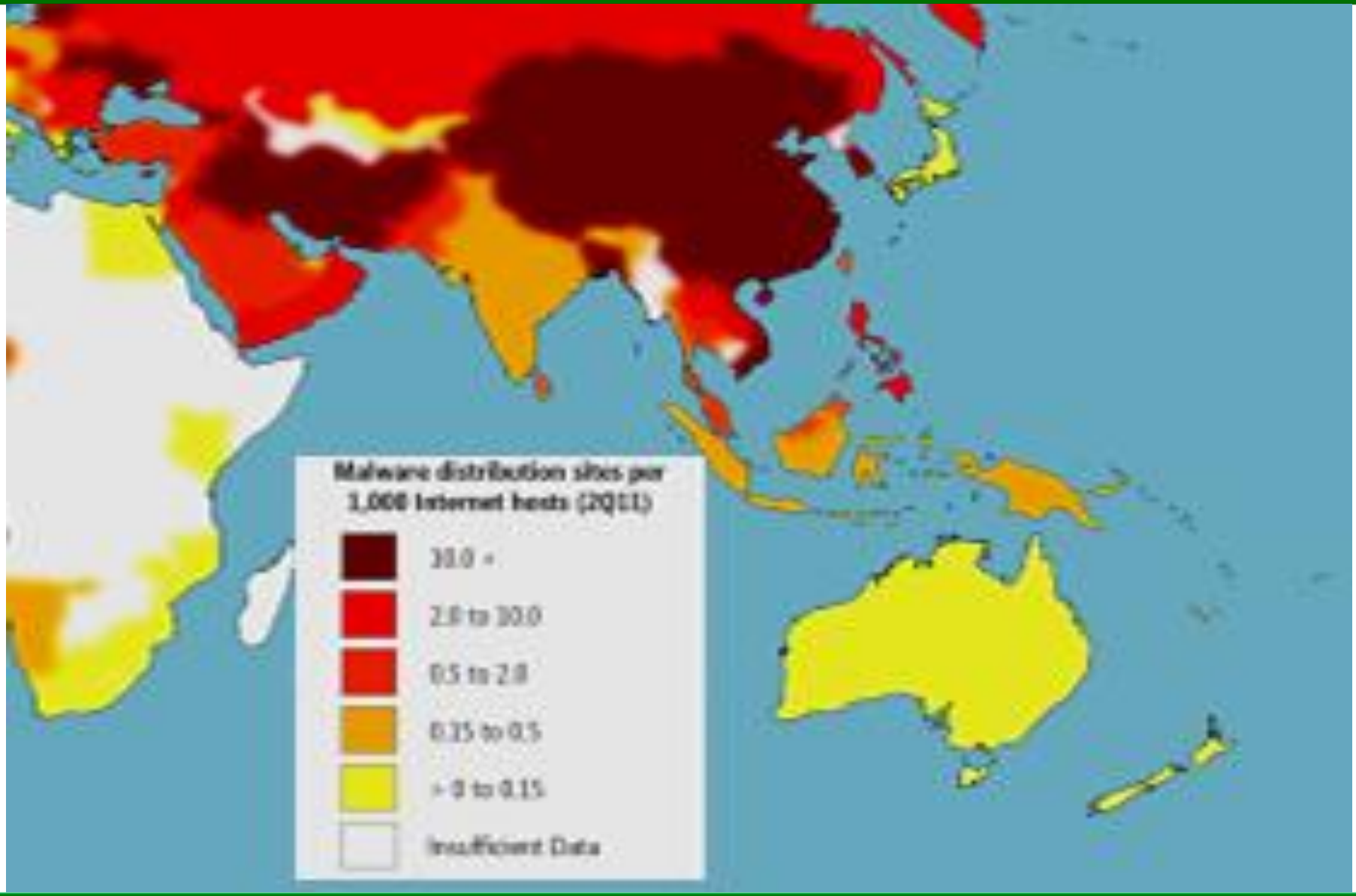
Theo thống kê của Microsoft

Bản đồ phát hiện mã độc Q2-2011



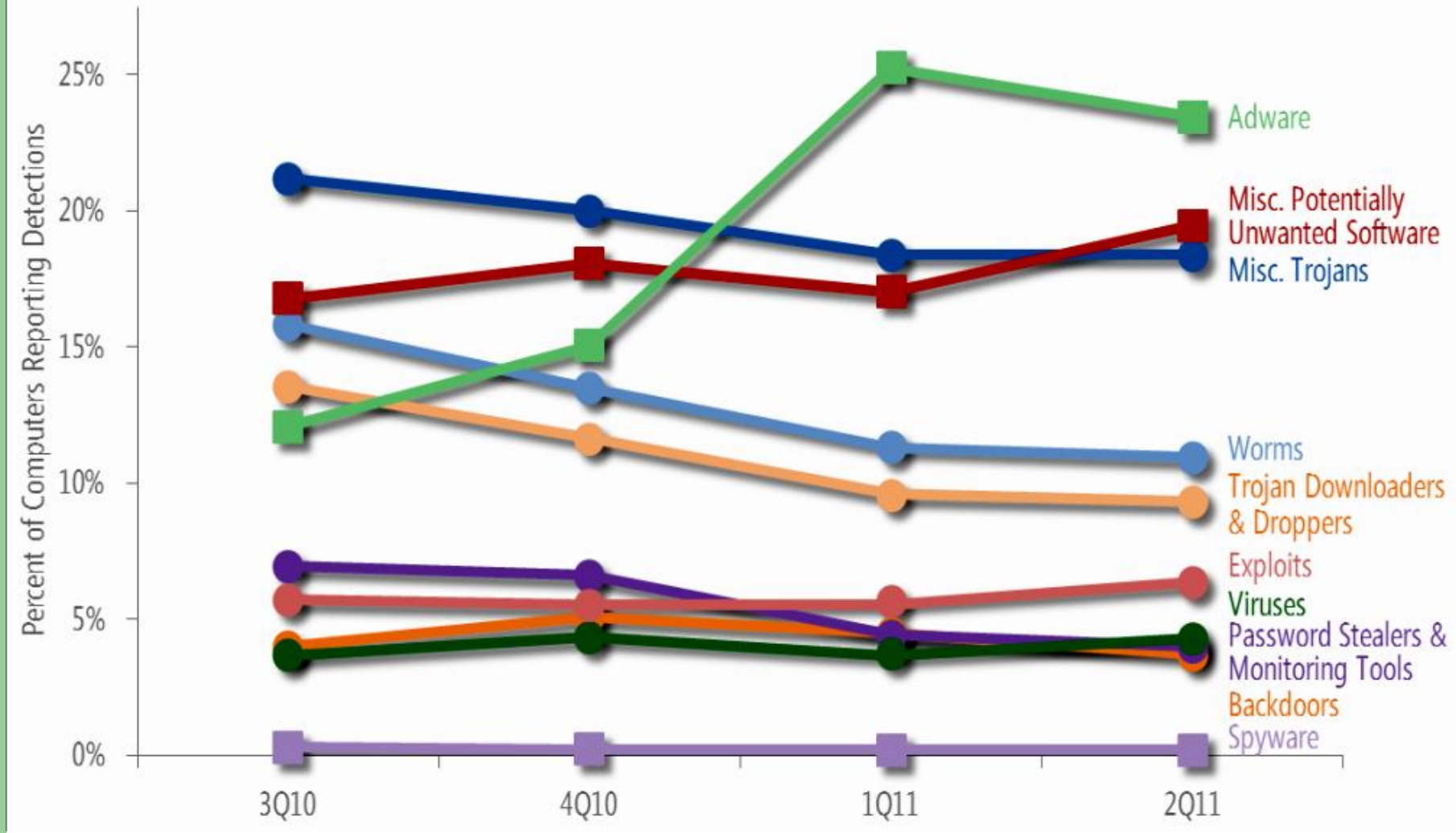
Theo thống kê của Microsoft

Máy chủ phát tán mã độc Q2 - 2011



Theo thống kê của Microsoft

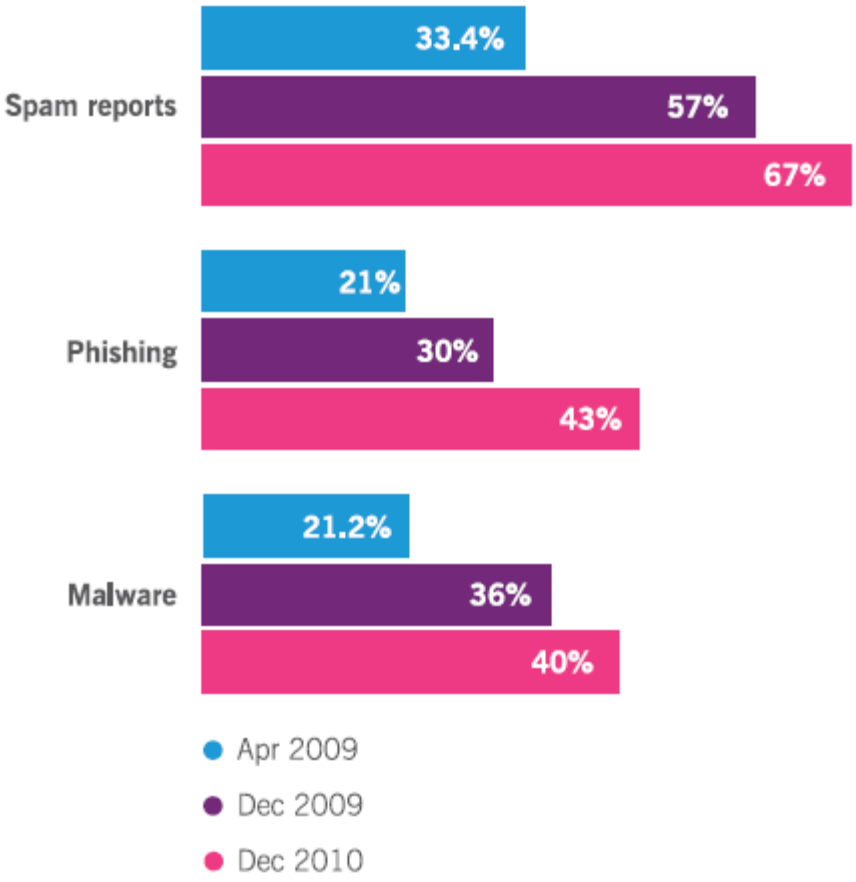
Thống kê các hiểm họa từ Q3-2010 đến Q2-2011



Sophos: During the first half of 2011, we saw a new malicious URL every 4 .5 seconds

Theo thống kê của Microsoft

Thống kê về social engineering



Theo thống kê của Microsoft

Tình hình lây lan mã độc hiện nay

- Botnet được sử dụng rộng rãi và tìm mọi cách để phát tán.
- Các mã độc có khả năng theo dõi, đánh cắp thông tin được sử dụng để tấn công vào nhiều cơ quan, tổ chức, doanh nghiệp.
- Các virus lây file vẫn là nguy cơ lớn, lây lan trên hàng triệu máy ở Việt Nam, đặc biệt là dòng virus lây file phức tạp Sality.
- Xuất hiện các mã độc trên các hệ điều hành di động như Android, và có xu hướng tăng mạnh.

Cách phát tán, lây lan của mã độc

- Lây lan qua các thiết bị USB
- Phát tán qua các chương trình chat như Yahoo và thậm chí cả Facebook.
- Lây lan thông qua lợi dụng điểm yếu của trình duyệt Web.
- Phát tán qua Email bằng cách gửi các file đính kèm độc hại, hay các đường link độc hại.
- Lây lan qua các tệp tin thực thi, ví dụ như nhúng mã độc vào các phần mềm crack.
- Giả mạo phần mềm để lây lan, ví dụ như giả mạo các trình diệt virus.
- Khai thác điểm yếu trong phần mềm, hệ điều hành để lây lan, đặc biệt là các phần mềm phổ biến như Microsoft Word.

IV. GIẢI PHÁP – HÀNH ĐỘNG

Khuyến cáo chống mã độc

- Bật tường lửa trên máy tính
- Để hệ điều hành ở chế độ cập nhật thường xuyên
- Sử dụng một trình diệt mã độc có khả năng cập nhật liên tục và để ở chế độ bảo vệ tự động.
- Sử dụng các phần mềm có nguồn gốc rõ ràng, tốt nhất là lấy nguồn từ trang chủ các phần mềm.
- Khi nhận được file đính kèm trên thư điện tử cần xem xét kĩ lưỡng trước khi mở ra kể cả đó là các file văn bản. Không mở các file đáng nghi ngờ.

5 GIẢI PHÁP theo QUY HOẠCH đến 2020

Đảm bảo cơ sở hạ tầng CNTT&TT

Đảm bảo an toàn cho ứng dụng CNTT

Phát triển nguồn nhân lực và nâng cao nhận thức

Hoàn thiện môi trường pháp lý

4 định hướng

QUY HOẠCH PT ATTT SỐ ĐẾN 2020

MỘT SỐ GỢI Ý ĐỐI VỚI TỔ CHỨC, DN

1. Quản lý ATTT

- *Mô hình PDCA theo tư tưởng của bộ TC ISO/IEC-27000.*
- *Quản lý toàn diện, quá trình liên tục, TUÂN THỦ.*

2. Sử dụng mạng đường truyền

- *Mạng TSLCD >>> mạng Internet trực tiếp.*
- *Không nối đồng thời 2 cổng mạng TSLCD và Internet.*
- *Mạng càng mở ➔ đặt chế độ bảo vệ càng chặt chẽ.*

3. Sử dụng phần mềm, dịch vụ

- *Phần mềm xây dựng theo nguyên tắc lập trình an toàn.*
- *Ưu tiên PM có ghi biên bản trạng thái, người truy cập.*
- *Thiết lập cấu hình quản trị hệ thống đúng.*
- *Dùng tên và mật khẩu truy cập có độ an toàn cao.*

MỘT SỐ GỢI Ý

4. Đầu tư công nghệ ATTT

- *Hệ thống sao lưu online, off-line.*
- *Chống virus, mã độc (giải pháp hệ thống)*
- *Giám sát ghi biên bản truy cập, chống DoS*
- *Phát hiện tấn công, truy cập trái phép*

5. Bảo mật dữ liệu

- *Ứng dụng PKI và CA*
- *Mã hóa dữ liệu lưu trữ và trao đổi*

6. Ứng cứu sự cố

- *CERT / CSIRT và Mạng lưới*

7. Kinh phí ATTT

- *Lồng ghép vào KH ƯD CNTT, chiếm từ 7-15%.*
- *Phải có KP đầu tư và chi phí vận hành*

Xin chân thành cảm ơn

Liên hệ: Vũ Quốc Khánh
Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam,
Bộ Thông tin và Truyền thông
18 Nguyễn Du, Hà Nội, Việt Nam

Tel: (84) 4 36404 420

Fax: (84) 4 36404 425

Email: vqkhanh@mic.gov.vn