TÀI LIỆU ĐẶC TẢ CHỨC NĂNG HỆ THỐNG e-PTs

Version 1.1

Publication Details

Change Record

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Purpose |
| 1.0 | Thursday, June 27th, 2018 | Lam Thanh Tung | Created document. |
|  |  |  |  |

Document Properties

|  |  |
| --- | --- |
| File location: | \*\*\* |
| File name: | Guide Document |
| Last updated: |  |

Document authorisation

|  |  |
| --- | --- |
|  |  |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |
|  |  |
| ( ) |  |
| / / |  |
| **Review by:** | **Review By:** |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  |

1. **Yêu cầu chung hệ thống**

* Là chương trình cung cấp cổng thông tin điện tử và đăng ký thành viên.
* Là công cụ quản lý, điều phối, ứng cứu sự cố an toàn thông tin.

1. **Yêu cầu chức năng phần mềm:**

Hệ thống sẽ bao gồm một số chức năng chính có mục đích như sau:

* + - * Nhóm chức năng cổng thông tin điện tử
      * Nhóm chức năng điều phối ứng cứu sự cố
      * Báo cáo

Yêu cầu công nghệ sử dụng :

Để xây dựng và triển khai Công Thông Tin Điện Tử , cần rất nhiều công cụ từ hệ điều hành đến cơ sở dữ liệu, ngôn ngữ lập trình:

* Visual Studio, Sublime Text: Môi trường phát triển tích hợp (Integrated Development Environment; viết tắt: IDE), sử dụng để viết và chỉnh sửa mã nguồn.
* Mircosoft SQL Server: Hệ quản trị cơ sở dữ liệu.
* Ngôn ngữ lập trình C#, .NET Framwork, HTML, CSS, JQuery: là ngôn ngữ lập trình, xử lý trên máy chủ.
* Internet Information Service(IIS) Manager: một chương trình dành cho máy chủ đối thoại qua giao thức HTTP.

1. Hệ điều hành: Windows
2. **Sơ đồ phân rã chức năng**
3. **Sơ đồ phân rã chức năng cổng thông tin điện tử**



1. **Sơ đồ phân rã chức năng điều phối ứng cứu sự cố**



1. **Các nhóm chức năng**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **HỆ THỐNG PHẦN MỀM** | | **Hệ thống** | **1** |
|  | **Các module chức năng bao gồm:** |  |  |  |
| **1** | **Module quản trị hệ thống** | |  |  |
|  | Quản lý cổng thông tin và trang thông tin | |  |  |
|  | Quản trị Banner Footer | |  |  |
|  | Quản trị các mẫu hiển thị nội dung | |  |  |
|  | Quản trị ngôn ngữ | |  |  |
|  | Thiết lập và quản trị danh sách danh mục nội dung thông tin | |  |  |
|  | Thiết lập và quản trị các loại menu | |  |  |
|  | Quản lý cấu hình | |  |  |
|  | Cài đặt, gỡ bỏ các khối chức năng trong khi hệ thống đang hoạt đông | |  |  |
|  | Quy trình đăng, kiểm duyệt và xuất bản thông tin | |  |  |
|  | Quản lý Backup & Restore: | - Xem danh sách Backup - Thêm mới Backup - Restore. |  |  |
|  | Thống kê báo cáo: | - Thông kê tin bài: Theo chuyên mục tin; Theo người biên tập. - Thống kê hỏi đáp: Theo trạng thái hỏi; Theo thời gian gửi câu hỏi; Theo chuyên mục; Theo thời gian trả lời; Theo người trả lời. |  |  |
| **2** | **Module quản trị người dùng** | |  |  |
|  | Quản trị Vai trò người dùng: | - Thêm vai trò.- Xóa vai trò.- Sửa vai trò.- Xem chi tiết vai trò. |  |  |
|  | Quản trị người dùng: | - Thêm người dùng. - Phân quyền người dùng. - Xem danh sách quyền - Chỉnh sủa người dùng. - Xem thông tin chi tiết |  |  |
|  | Quản trị nhóm người dùng: | - Xem danh sách nhóm. - Thêm người vào nhóm. - Tạo nhóm mới. - Chỉnh sửa thông tin nhóm. - Xóa nhóm người dùng. |  |  |
| **3** | **Module Quản trị nội dung, tin tức** | |  |  |
|  | Quản trị danh mục tin tức: | - Xem danh sách. - Thêm mới. - Chỉnh sửa. - Xóa phần tử. - Sắp xếp theo thứ tự. - Hiện / ẩn danh mục |  |  |
|  | Quản lý sự kiện tin: | - Xem danh sách. - Thêm mới. - Chỉnh sửa. - Xóa phần tử. - Tìm kiếm. - Xem phiên bản - Duyệt / Hủy duyệt. |  |  |
|  | Quản lý tin nổi bật: | - Xem danh sách. - Thêm mới. - Chỉnh sửa. - Xóa phần tử. - Sắp xếp - Tìm kiếm. - Xem phiên bản - Duyệt / Hủy duyệt. |  |  |
|  | Quản lý bài viết: | - Xem danh sách.- Thêm mới.- Chỉnh sửa.- Xóa phần tử.- Tìm kiếm.- Xem phiên bản- Duyệt / Hủy duyệt. |  |  |
|  | Quản lý bình luận, ý kiến bài viết: | - Xem danh sách bình luận của 1 tin bài. - Xem chi tiết 1 bình luận - Xóa phần tử. - Tìm kiếm. - Xem phiên bản - Duyệt / Hủy duyệt. |  |  |
|  | Quản lý thu thập tin tức: | - Quản lý tên miền - Quản lý dữ liệu xóa bỏ. - Quản lý cụm từ thay thế. - Quản lý dữ liệu thu thập |  |  |
| **4** | **Module Thủ tục hành chính** |  |  |  |
|  | Quản trị cơ quan ban hành: | - Xem danh sách - Thêm mới - Sửa - Xóa. - Ẩn / hiện - Sắp xếp theo thứ tự. |  |  |
|  | Quản trị danh mục thủ tục: | - Xem danh sách - Thêm mới - Sửa - Xóa - Ẩn / hiện - Sắp xếp theo thứ tự |  |  |
|  | Quản trị lĩnh vực: | - Xem danh sách - Thêm mới - Sửa - Xóa - Ẩn / Hiện - Duyệt - Tìm kiếm |  |  |
|  | Quản trị thủ tục hành chính: | - Xem danh sách- Thêm mới- Sửa- Xóa- Ẩn / Hiện- Kiểm duyệt- Thêm file đính kèm- Xóa file đính kèm |  |  |
|  | Thống kê báo cáo thủ tục: | - Theo thời gian - Theo cơ quan ban hành - Trạng thái - Xuất báo cáo dạng Excel. |  |  |
|  | Tìm kiếm tra cứu thủ tục hành chính: | - Theo thời gian - Theo cơ quan ban hành - Theo cấp ban hành - Theo tiêu đề - Theo nội dung - Hiển thị kế quả tìm kiếm - Sắp xếp kết quả theo thứ tự. |  |  |
| **5** | **Module Quản lý hỏi đáp, giao lưu & Thăm dò ý kiến** |  |  |  |
|  | Quản lý danh mục hỏi đáp: | - Thêm danh mục - Sửa danh mục - Xóa danh mục |  |  |
|  | Quản lý câu hỏi: | - Thêm mới câu hỏi - Sửa câu hỏi - Xóa câu hỏi - Tìm kiếm câu hỏi - Xem chi tiết câu hỏi - Trả lời câu hỏi - Xem phiên bản - Kiểm duyệt câu hỏi |  |  |
|  | Quản lý câu trả lời: | - Thêm mới câu trả lời - Sửa câu trả lời - Xóa câu trả lời - Tìm kiếm câu trả lời - Xem chi tiết câu trả lời - Xem phiên bản - Kiểm duyệt câu trả lời. |  |  |
|  | **Quản lý thăm dò ý kiến:** |  |  |  |
|  | Quản lý danh mục: | - Thêm danh mục- Sửa danh mục- Xóa danh mục- Tìm kiếm danh mục- Xem danh mục- Sắp xếp danh mục. |  |  |
|  | Quản lý danh sách câu hỏi: | - Thêm câu hỏi - Sửa câu hỏi - Xóa câu hỏi - Tìm kiếm câu hỏi - Xem chi tiết câu hỏi - Xem chi tiết phiên bản câu hỏi. - Xem ý kiến khác. |  |  |
| **6** | **Module Quản lý Hình ảnh – video** |  |  |  |
|  | **Quản lý hình ảnh.** |  |  |  |
|  | Quản lý danh mục hình ảnh: | - Thêm mới danh mục - Sửa danh mục - Xóa danh mục - Sắp xếp danh mục - Xem phiên bản - Xem danh mục - Duyệt / hủy duyệt danh muc - Tìm kiếm danh mục. |  |  |
|  | Quản lý Album ảnh: | - Thêm mới album - Sửa album - Xóa Album - Sắp xếp album - Xem phiên bản - Xem album - Duyệt / hủy duyệt album |  |  |
|  | Quản lý danh mục video: | - Thêm mới danh mục - Sửa danh mục - Xóa danh mục - Sắp xếp danh mục - Xem phiên bản - Xem danh mục - Duyệt / hủy duyệt danh muc - Tìm kiếm danh mục. |  |  |
|  | Quản lý Album video: | - Thêm mới album- Sửa album- Xóa album- Sắp xếp album- Xem phiên bản- Xem album- Duyệt / hủy duyệt album |  |  |
|  | Quản lý video: | - Thêm mới - Sửa video - Xóa video - Xem video - Tìm kiếm video |  |  |
| **7** | **Module Quản lý văn bản** |  |  |  |
|  | Quản trị cơ quan ban hành: | - Xem danh sách - Thêm mới - Sửa - Xóa. - Ẩn / hiện - Sắp xếp theo thứ tự. |  |  |
|  | Quản trị danh mục văn bản: | - Xem danh sách - Thêm mới - Sửa - Xóa - Ẩn / hiện - Sắp xếp theo thứ tự |  |  |
|  | Quản trị lĩnh vực: | - Xem danh sách - Thêm mới - Sửa - Xóa - Ẩn / Hiện - Duyệt - Tìm kiếm |  |  |
|  | Quản trị văn bản: | - Xem danh sách - Thêm mới - Sửa - Xóa - Ẩn / Hiện - Kiểm duyệt - Thêm file đính kèm - Xóa file đính kèm |  |  |
|  | Tìm kiếm tra cứu văn bản: | - Theo thời gian- Theo cơ quan ban hành- Theo cấp ban hành- Theo tiêu đề- Theo nội dung- Hiển thị kết quả tìm kiếm- Sắp xếp kết quả theo thứ tự. |  |  |
| **8** | **Module Quản lý RSS** |  |  |  |
|  | Chuyên mục RSS: | - Thêm chuyên mục - Sửa chuyên mục - Xóa chuyên mục - Tìm kiếm chuyên mục - Xem chuyên mục - Xem phiên bản - Kiểm duyệt |  |  |
|  | Quản lý danh sách kênh RSS: | - Thêm danh mục kênh - Sửa danh mục kênh - Tìm kiếm - Xem danh mục kênh - Sắp xếp theo thứ tự tăng dần. |  |  |
| **9** | **Module Quản lý Menu và sitemap** |  |  |  |
|  | Quản lý sitemap: | - Thêm mới nhánh - Sửa nhánh - Xóa nhanh - Sắp xếp theo thứ tự - Ẩn / Hiện sitemap |  |  |
| **10** | **Module Quản lý liên kết và quảng cáo** |  |  |  |
|  | Quản lý liên kết: | - Xem danh sách - Thêm mới liên kết - Sửa liên kết - Xóa liên kết. - Xem chi tiết từng liên kết. - Ẩn / hiện liên kết. |  |  |
|  | Quản lý danh mục quảng cáo: | - Thêm - Sửa - Xóa - Xem danh sách - Tìm kiếm - Sắp xếp theo thứ tự. |  |  |
|  | Thông tin quảng cáo: | - Xem danh sách- Thêm mới- Sửa- Xóa- Tìm kiếm- Sắp xếp theo thứ tự.- Ẩn / Hiện |  |  |
| **11** | **Module ứng dụng tra cứu thông tin** |  |  |  |
|  | Tìm kiếm thông tin | Tìm kiếm thông tin đã được báo cáo theo các tiêu chí:   * Loại sự cố. * Mức độ sự cố . * Các vấn đề nóng đang gặp phải. * Báo cáo thống kê được phép công bố |  |  |
| **12** | **Module báo cáo về sự cố ATTT** |  |  |  |
|  | Quản lý đơn vị thành viên | * Quản lý thông tin đơn vị thành viên   + Thêm bớt sửa xóa đơn vị thành viên   + Thêm bớt, sửa xóa người dùng thuộc đơn vị thành viên   + Phân quyền người dùng của đơn vị thành viên * Đăng ký thành viên mới   + Khai thông tin đăng ký,   + Phê duyệt đăng ký * Cập nhật thông tin đơn vị thành viên * Tìm kiếm thành viên * Dừng và khôi phục tư cách đơn vị thành viên |  |  |
|  | Chức năng của đơn vị thành viên | * Cập nhật thông tin đơn vị thành viên * Báo cáo sự cố ATTT * Truy cập các bản tin cảnh báo |  |  |
|  | Báo cáo, quản lý, giải quyết và thông báo sự cố | * Báo cáo sự sự cố đơn vị thành viên * Quản trị viên nhập sự cố trên hệ thống * Tiếp nhận, phân loại sự cố * Hướng dẫn, điều phối giải quyết sự cố. * Cảnh báo từ phía hệ thống |  |  |
|  | Báo cáo | * Báo cáo tổng hợp 6 tháng/1 năm hoạt động tiếp nhận xử lý sự cố. * Xuất các báo cáo từ ngày đến ngày và thống kê theo:   + Nhóm đơn vị thành viên   + Địa bàn khu vực thành viên   + Theo từng thành viên   + Theo loại sự cố đã được báo cáo   + Theo nhóm sự cố đã được báo cáo |  |  |

1. **Mô tả chức năng điều phối ứng cứu sự cố**
2. **Lưu đồ chức năng**



1. **Phân hệ Dashboard**
   1. ***Dashboard tổng thể***

Là chức năng hiển thị biểu đồ thống kê các sự cố theo thời gian

* + - Biểu đồ cột hiển thị số lượng sự cố xảy ra theo từng tháng: hiển thị số lượng sự cố đã xử lý, chưa xử lý.
    - Biểu đồ tròn top các ISP bị sự cố nhiều nhất trong khoảng thời gian được chọn.
  1. ***Dashboard theo loại sự cố***

Là chức năng hiển thị biểu đồ thống kê các tiêu chí theo từng loại sự cố theo thời gian.

* 1. Phishing
     + Biểu đồ tròn Top Target Phishing: hiển thị top 5 domain bị tấn công Phishing nhiều nhất trong khoảng thời gian được chọn.
     + Biểu đồ tròn TOP ISP: hiển thị top 5 đơn vị ISP bị tấn công Phishing nhiều nhất trong khoảng thời gian được chọn.
  2. Deface
     + Biểu đồ tròn TOP ISP: hiển thị top 10 đơn vị ISP bị tấn công Deface nhiều nhất trong khoảng thời gian được chọn.
  3. Malware
     + Biểu đồ tròn Top Virus name: hiển thị top 5 tên virus xuất hiện nhiều nhất trong khoảng thời gian được chọn.
     + Biểu đồ tròn TOP ISP: hiển thị top 5 đơn vị ISP bị Malware tấn công nhiều nhất trong khoảng thời gian được chọn.
  4. C&C Botnet
     + Biểu đồ tròn TOP ISP: hiển thị top 10 đơn vị ISP bị tấn công nhiều nhất trong khoảng thời gian được chọn.
  5. Attack
     + Biểu đồ tròn TOP ISP: hiển thị top 10 đơn vị ISP bị tấn công nhiều nhất trong khoảng thời gian được chọn.

1. **Phân hệ Quản lý sự cố**
   1. ***Quản lý Attack***
      * Mô tả: Cho phép người quản trị quản lý các Attack nói chung. Các attack bao gồm tất cả các sự cố an toàn thông tin không thuộc các phần sự cố còn lại
      * Thông tin attack được gửi cho các thành viên đưa vào mục Dịch vụ cảnh báo (mục 4.2).
      * Thông tin Attack:

|  |
| --- |
| timestamp |
| IP |
| asn |
| geo |
| url |
| type (downadup) |
| http\_agent(Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)) |
| src\_port(1938,1499 ...) |
| hostname (static.vnpt.vn, localhost ) |
| dst\_port (Địa chỉ cổng đích) |
| protocol (udp or tcp) |
| servername |
| server |
| header (HTTP/1.1 200 OK) |
| tag (netis\_vulnerability,cwmp,memcached,rdp ...) |
| handshake |

* 1. ***Quản lý sự cố C&C botnet***
     + Mô tả: Cho phép người quản trị quản lý các sự cố C&C botnet.
     + Thông tin botnet.

|  |
| --- |
| timestamp |
| ip |
| asn |
| geo |
| url |
| type (downadup) |
| http\_agent(Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)) |
| src\_port(1938,1499 ...) |
| hostname (static.vnpt.vn, localhost ) |
| dst\_port (Địa chỉ cổng đích) |
| protocol (udp or tcp) |
| servername |
| server |
| header (HTTP/1.1 200 OK) |
| tag (netis\_vulnerability,cwmp,memcached,rdp ...) |

* 1. ***Quản lý sự cố Phishing***

Mô tả: Cho phép người quản trị quản lý các sự cố Phishing và gửi emai thông báo đến các đơn vị gặp sự cố.

* + - Hiển thị danh sách các sự cố.
      * Với các sự cố đến từ cùng một domain và xảy ra ở nhiều đường dẫn khác nhau, hệ thống sẽ hiển thị các đường dẫn này trong cùng một sự cố. Khi click vào những sự cố này sẽ hiện ra các link chi tiết.

Ví dụ:

http[:]//year2000vn.com[.]vn/resource/.www.paypaI.co.uk/signin/country=login/locale=ln\_ln/

http[:]//year2000vn.com[.]vn/resource/.www.paypaI.co.uk/signin/country=login/locale=ln\_ln/rev.php

* + - Import các sự cố từ file excel.
      * Hệ thống đọc file excel và sử dụng API để lấy thông tin về IP, ISP của sự cố.
      * Link API: <https://whois.domaintools.com>.
    - Sửa, xóa các sự cố.
    - Gửi email đến đơn vị gặp sự cố.
      * Hệ thống cho phép quản trị viên tạo email theo mẫu có sẵn và gửi cho các đơn vị gặp sự cố.
      * Hệ thống tự động lấy email nhận từ thông tin của các thành viên của hệ thống, nếu đơn vị chưa là thành viên hoặc chưa có email, người quản trị sẽ điền thông tin này.
      * Cho phép sửa nội dung mẫu email.
      * Nội dung mẫu Email (xem mục 5.3).
    - Kiểm tra và đóng sự cố.
      * Người quản trị nhận email trả lời của đơn vị gặp sự cố trong mục Hỗ trợ xử lý, người quản trị có thể xem và trả lời email ở đây.
      * Người quản trị kiểm tra nếu sự cố đã được xử lý thì đóng sự cố. Khi đó, trạng thái của sự cố sẽ chuyển từ “Còn tồn tại” thành “Đóng”.
    - Thông tin Phishing

|  |
| --- |
| Link phishing |
| Đích giả mạo |
| Nguồn Thông tin |
| Thời gian |
| IP |
| Thông tin ISP |

* 1. ***Quản lý sự cố Deface*** 
     + Tương tự mục (2.3)
     + Thông tin Deface

|  |
| --- |
| Link Deface |
| Thời gian |
| Nguồn Thông tin |
| Nguười tấn công |
| IP |
| Thông tin ISP |

* 1. ***Quản lý sự cố Malware***
     + Tương tự mục (2.3)

|  |
| --- |
| Link nhiễm malware |
| Tên virus |
| IP |
| IPS |
| Thời gian |
| Nguồn Thông tin |

* + - Hệ thống tự động kiểm tra các sự cố malware xem còn tồn tại không và thực hiện việc đóng sự cố nếu như đã được giải quyết.
  1. ***Dịch vụ cảnh báo***
     + Hệ thống cho phép các đơn vị thành viên đăng ký nhận email cảnh báo mỗi khi có sự cố xảy ra với các domain do đơn vị quản lý.
       - Đơn vị thành viên đăng ký các dải IP(domain) nhận cảnh báo, hệ thông so sánh giải ip với các ip thuộc sự cố (trong mục attack, malware, phishing,deface) thông kê nếu có ip trùng thì báo cáo sự cố theo mẫu dưới và kèm theo file đính kèm thông báo chi tiết sự cố:

*Kính gửi đầu mối tiếp nhận sự cố XXX,*

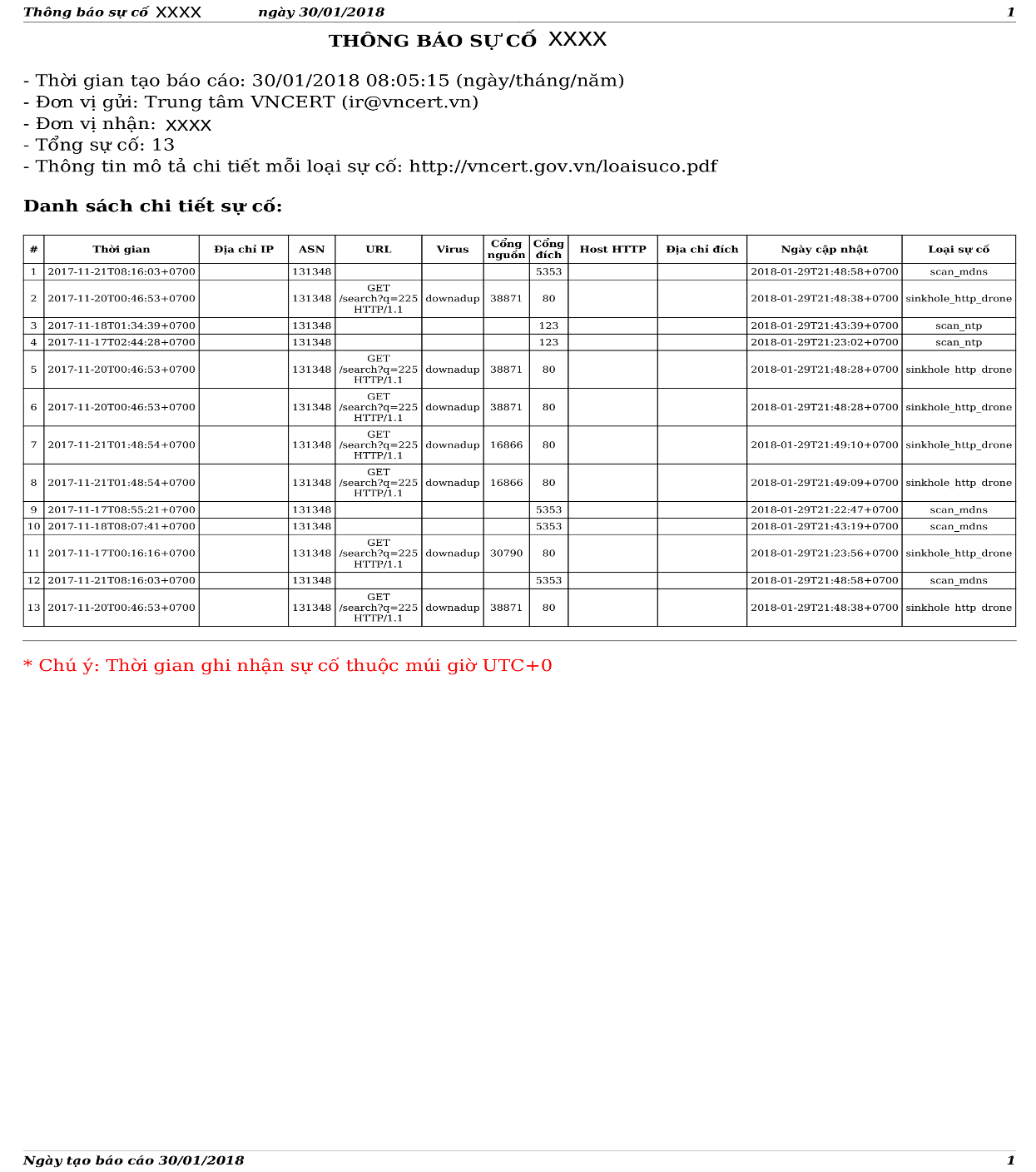
*Trong quá trình theo dõi sự cố tại Việt Nam, Trung tâm VNCERT phát hiện các sự cố liên quan đến XXXX.*

*Danh sách các sự cố được gửi trong tập tin đính kèm (nếu có, nếu không có sẽ không có file đính kèm).*

*Trân trọng./.*

File đính kèm có dạng yyyymmdd\_XXX\_Report.pdf

* + - * Thành viên có thể cài đặt thời gian nhận cảnh báo vào một giờ nhất định trong ngày theo giờ GMT+7.
      * Nhận báo cáo theo ngày, tuần, tháng, quý, năm.
      * Mẫu báo cáo được tạo từ template có sẵn và có thể sửa lại các template.



* 1. **Thông báo sự cố an toàn thông tin**
     + Là chức năng cho phép các đơn vị thành viên, hoặc các đơn vị không phải là thành viên thông báo cho VNCert về các sự cố đang diễn ra tại đơn vị của mình.
     + Lưu đồ chức năng:



* + - Đơn vị thành viên thực hiện khai báo các vấn đề gồm các thông tin sau vào form thông báo:
    - Thông tin chung về đơn vị - lấy trong CSDL cho phép sửa thông tin đầu mối liên hệ:
    - Thông tin về hệ thống gặp vấn đề.
    - Lựa chọn các cấp độ phân loại vấn đề qua ma trận.
    - Mô tả về vấn đề
    - Ngày phát hiện vấn đề
    - Trạng thái của vấn đề: đã xử lý – chưa xử lý.
    - Cách thức phát hiện vấn đề.
    - Các đơn vị đã gửi thông báo
    - Các thông tin bổ sung về vấn đề
    - Kiến nghị đề xuất hỗ trợ.
    - Loại vấn đề (nếu loại vấn đề này được tồn tại trên hệ thống)
* Đơn vị thành viên thực cũng có thể gọi điện tới quản trị viên VNCert để thực hiện việc thông báo.
* Sau khi gửi báo cáo vấn đề phần mềm gửi thông báo tiếp nhận vấn đề qua email/tin nhắn đến đơn vị thành viên.
* Hệ thống cho phép quản trị viên kiểm tra thông cáo về sự cố xảy ra tại đơn vị, để đưa ra quyết định đóng sự cố hoặc điều phối nhân sự ứng cứu sự cố.

1. **Phân hệ quản lý CVE**
   1. ***Quản lý CVE***

Là chức năng cho phép người quản trị quản lý các bản cập nhật, bản vá lỗi mới nhất của các hệ thông thông tin của các đơn vị thành viên.

* + - Người quản trị import file chứa các CVE vào hệ thống.
    - Gửi email đến các đơn vị thành viên với các CVE phù hợp
      * Hệ thống tự động lọc các CEV theo các hệ thống thông tin của cá đơn vị thành viên đã đăng ký để gửi thông tin các bản vá lỗi, bản cập nhật phù hợp.
    - Thông tin CVE

|  |
| --- |
| CVE ID |
| Vulnerability Type(s) (Exec Code,DoS CSRF,+Info, XSS ...) |
| Product |
| Publish Date |
| Update Date |
| Score |
| Gained Access Level (None) |

1. **Phân hệ Quản lý thành viên**
   1. ***Quản lý thành viên***

Module quản lý hệ thống thành viên cho phép:

* Quản lý nhóm đơn vị thành viên
* Đăng ký thành viên mới
* Phê duyệt đăng ký thành viên mới
* Tìm kiếm thành viên: theo thông tin thành viên, tìm kiếm theo các đơn vị phối hợp, tìm kiếm theo các báo cáo phản hồi, các bản tin của thành viên.
  1. ***Chức năng đăng ký thành viên mới***

Để đăng ký là thành viên hệ thống cần thực hiện các bước sau:

*Bước 1: Người dùng muốn đăng ký đơn vị thành viên cần điền các thông tin đăng ký trên form đăng ký.*

Thông tin đăng ký thành viên mới bao gồm:

* Thông tin chung về thành viên
* Thông tin về đầu mối tiếp nhận thông báo
* Thông tin về đầu mối liên lạc của hệ thống
* Giới thiệu về hạt động của đơn vị
* Thông tin về các hệ thống thuộc phạm vi phụ trách của đơn vị
* Thông tin về nhân lực của đơn vị thành viên
* Đầu mối liên lạc của đơn vị: trong giờ làm việc, ngoài giờ làm việc, người có thẩm quyền, và các phương tiện liên lạc khác

Sau khi thực hiện đăng ký đơn vị thành viên, hệ thống sẽ trả lại thông báo tiếp nhận hồ sơ đăng ký qua email.

*Bước 2: Tải hồ sơ đăng ký và phê duyệt đăng ký.*

Người dùng quản trị có thể xem danh sách các đơn vị thành viên đang đăng ký, lọc sắp xếp theo thời gian.

Khi được phê duyệt làm thành viên: người quản trị cần upload các file scan hồ sơ bản cứng của đơn vị thành viên lên hệ thống. Bấm nút phê duyệt đăng ký để hoàn thành.

*Bước 3: Hệ thống gửi thông báo xác nhận hồ sơ đăng ký đơn vị thành viên đã được phê duyệt*

* 1. ***Chức năng tìm kiếm thành viên***

Phần mềm cho phép tìm kiếm thành viên của hệ thống theo các tiêu chí:

* + - Tên đơn vị
    - Loại đơn vị
    - Địa bàn hoạt động của đơn vị
    - Thời gian đăng ký thành viên
    - Trạng thái đơn vị thành viên

Khi tìm kiếm được thành viên hệ thống cho phép xem các thông tin liên quan tổng quan về thành viên đó:

* + - Thông tin cơ bản
    - Thông tin về đầu mối liên lạc.
    - Tổng hợp các vấn đề mà đơn vị thành viên đã báo cáo gồm: tổng số lượng vấn đề, số lượng vấn đề theo từng cấp độ, danh sách các vấn đề đã báo cáo theo thời gian.

Trên thông tin đơn vị thành viên có chức năng dừng tư cách đơn vị thành viên.

* 1. ***Chức năng dừng và khôi phục tư cách đơn vị thành viên***
     + Để thực hiện dừng đơn vị thành viên người quản trị cần upload bản scan các tài liệu liên quan đến việc dừng tư cách đơn vị thành viên.
     + Hệ thống sẽ thông báo đến đơn vị thành viên bằng email/tin nhắn về kết quả của việc dừng tư cách đơn vị thành viên
     + Để thực hiện khôi phục tư cách đơn vị thành viên, người quản trị cần tìm theo trạng thái “Đã dừng tư cách đơn vị thành viên” và upload bản scan các tài liệu liên quan đến việc khôi phục tư cách đơn vị thành viên.
     + Hệ thống sẽ thông báo đến đơn vị thành viên bằng email/tin nhắn về kết quả của việc dừng tư cách đơn vị thành viên.

1. **Phân hệ quản lý hệ thống**
   1. ***Quản lý người dùng***
      * Là chức năng cho phép người quản trị tạo người dùng.
      * Thêm sửa xóa người dùng.
   2. ***Quản lý phân quyền***

* Là chức năng cho phép người quản trị tạo ra các nhóm quyền và quản lý các quyền của hệ thống.
* Thêm, sửa, xóa các nhóm quyền.
  1. ***Quản lý mẫu email***
* Là chức năng cho phép quản trị viên chỉnh sửa nội dung mẫu email thông báo sự cố đến các thành viên.
* Nội dung mẫu email:

**Email tiếp nhận:** Lấy từ danh sách mục ISP (có thể sửa được)

**Email CC:** là email để báo cáo (mặc định: [tnchung@vncert.vn](mailto:tnchung@vncert.vn)) hoặc thêm sửa.

**Tiêu đề:** *Đề nghị xử lý sự cố trên dịch vụ của (Tên đơn vị ISP,)*

**Nội dung:**

*Kính gửi (Tên đơn vị ISP)*

*Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam, Bộ Thông tin và Truyền thông (VNCERT) ghi nhận, hiện có những domain*

*(Các hoặc một domain bị sự cố vidu nếu click vào email ở đầu đường link*

*http[:]//year2000vn.com[.]vn*

*trong nội hiển thị:*

*http[:]//year2000vn.com[.]vn/resource/.www.paypaI.co.uk/signin/country=login/locale=ln\_ln/*

*http[:]//year2000vn.com[.]vn/resource/.www.paypaI.co.uk/signin/country=login/locale=ln\_ln/rev.php*

*)*

*(IP bị sự cố)*

*IP này  thuộc (Tên đơn vị ISP,)  
  
Thực hiện Quyết định số 05/2017/QĐ-TTg của Thủ tướng Chính phủ và Thông tư số 20/2017/TT-BTTTT ngày 12/9/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc, Trung tâm VNCERT đề nghị Quý Công ty xử lý sự cố (giả mạo (phishing), nhiễm mã độc (malware), (thay đổi giao diện) Deface ), và các cố (giả mạo (phishing), nhiễm mã độc (malware), (thay đổi giao diện) Deface ) trong vòng 24 giờ kể từ khi nhận được Email này nhằm ngăn chặn website cố (giả mạo (phishing), nhiễm mã độc (malware), (thay đổi giao diện) Deface ).  
  
Sau khi hoàn thành việc xóa các website cố (giả mạo (phishing), nhiễm mã độc (malware), (thay đổi giao diện) Deface ), đề nghị Công ty gửi báo cáo kết thúc sự cố (ban hành kèm theo Thông tư số 20/2017/TT-BTTTT, có thể tải tại địa chỉ:*[*http://vncert.vn*](http://vncert.vn/)*) về Đầu mối tiếp nhận sự cố của Trung tâm VNCERT qua địa chỉ*[*ir@vncert.vn*](mailto:ir@vncert.vn) *Cảm ơn sự hợp tác của Quý Công ty.*

*--------------------------------------------  
Nguyen Thanh Chuong (Mr)  
VNCERT, MIC  
Mobile:*[*+84 91 8228 754*](callto:+84%2091%208228%20754)*Website:*[*www.vncert.gov.vn*](http://www.vncert.gov.vn/)

* 1. ***Quản lý tin tức***
* Là chức năng cho phép quản trị viên tạo các tin tức và phân quyền cho các thành viên trong hệ thống vào xem.
* Tin tức bao gồm: các tin tức mới nhất về an toàn thông tin trong tuần và thống kê các sự cố, tổng hợp các lỗ hổng, bản vá bảo mật trên các sản phẩm/dịch vụ phổ biến tại Việt Nam.
* Tài khoản quản trị viên duyệt tin tức do người dùng tạo.
* Phân quyền cho các thành viên được xem những mục tin tức nào. Người quản trị có thể tùy biến các quyền xem cho từng thành viên.
* Danh sách các mục thông tin trong tin tức

Tình hình tấn công gây nguy hại trên các trang web tại Việt Nam.

Theo dõi, phân tích, phát hiện các dấu hiệu, nguy cơ ảnh hưởng đến tính sẵn sàng của Cổng/Trang thông tin điện tử cấp Bộ, tỉnh hoặc tương đương.

Lỗ hổng/điểm yếu an toàn thông tin trong tuần(CVE).

Hoạt động một số mạng botnet, APT, mã độc tại Việt Nam.

Theo dõi, thu thập, thống kê thông tin nổi bật về an toàn thông tin trong kỳ báo cáo: phishing, malware, deface.

1. **Phân hệ Báo cáo thống kê**
   1. ***Quản lý báo cáo***

* Là chức năng cho phép xem các báo cáo về sự cố dựa theo thời gian(từ ngày đến ngày).
* Báo cáo theo từng thành viên.
* Check sự cố trùng: nếu có các sự cố trùng lặp từ 2 hoặc nhiều hơn trong khoảng thời gian trích xuất báo cáo thì chỉ thống kê là một sự cố.
* Các loại báo cáo:
  + - * 1. Phishing
    - Báo cáo Top Target Phishing: top các domain bị tấn công Phishing nhiều nhất trong khoảng thời gian được chọn.
    - Báo cáo TOP ISP: top các đơn vị ISP bị tấn công Phishing nhiều nhất trong khoảng thời gian được chọn.
      * 1. Deface
    - Báo cáo TOP ISP: top các đơn vị ISP bị tấn công Deface nhiều nhất trong khoảng thời gian được chọn.
      * 1. Malware
    - Báo cáo Top Virus name: top các tên virus xuất hiện nhiều nhất trong khoảng thời gian được chọn.
    - Báo cáo TOP ISP: top các đơn vị ISP bị Malware tấn công nhiều nhất trong khoảng thời gian được chọn.
      * 1. Botnet
    - Báo cáo TOP ISP: top các đơn vị ISP bị tấn công nhiều nhất trong khoảng thời gian được chọn.
  1. ***Export báo cáo***
     + Hệ thống cho phép xuất báo cáo theo ngày tháng dưới dạng excel và pdf.