**PHỤ LỤC**

**Danh mục Đánh giá an toàn thông tin cho Trung tâm tích hợp dữ liệu tỉnh và diễn tập thực chiến ứng phó sự cố an toàn thông tin mạng**

1. **Đánh giá an toàn thông tin cho Trung tâm tích hợp dữ liệu tỉnh.**

Các nội dung đánh giá an toàn thông tin cụ thể như sau:

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Nội dung công việc** | **ĐVT** | **Số lượng** |
| **1** | **Kiểm tra rà quét, đánh giá lỗ hổng bảo mật cho máy chủ**1. Thu thập thông tin:- Thực hiện thu thập thông tin máy chủ bao gồm: IP, địa chỉ mac, các thông tin về hệ điều hành..2. Rà quét và phân tích lỗ hổng:- Sử dụng công cụ có bản quyền thực hiện rà quét các nguy cơ an ninh mạng trên máy chủ- Kiểm tra các bản vá cần cập nhật- Kiểm tra thông tin các nguy cơ theo chuẩn CVE, CPE và OVAL- Kiểm tra thông tin về các tiến trình đang thực thi- Kiểm tra các cổng kết nối, các dịch vụ, các chính sách thiết lập trên máy chủ3. Thử nghiệm xâm nhập:- Xác nhận, chứng minh sự tồn tại của các điểm yếu- Loại bỏ các kết quả thiếu chính xác- Phân tích chuyên sâu các lỗ hổng nếu có | **Máy chủ** | **100** |
| **2** | **Kiểm tra rà quét, đánh giá lỗ hổng bảo mật hệ thống các thiết bị mạng**1. Thu thập thông tin:- Thực hiện thu thập thông tin thiết bị bao gồm: IP, địa chỉ mac, tên hãng, model...2. Rà quét và phân tích lỗ hổng:- Sử dụng công cụ có bản quyền thực hiện rà quét các nguy cơ an ninh mạng trên thiết bị mạng- Kiểm tra các cổng kết nối, các dịch vụ, các chính sách thiết lập trên thiết bị3. Thử nghiệm xâm nhập:- Xác nhận, chứng minh sự tồn tại của các điểm yếu- Loại bỏ các kết quả thiếu chính xác- Phân tích chuyên sâu các lỗ hổng nếu có | **Thiết bị** | **12** |
| **3** | **Kiểm tra đánh giá an toàn thông tin hệ thống các thiết bị an ninh bảo mật**1. Thu thập thông tin:- Thực hiện thu thập thông tin thiết bị bao gồm: IP, địa chỉ mac, tên hãng, model...2. Rà quét và phân tích lỗ hổng:- Sử dụng công cụ có bản quyền thực hiện rà quét các nguy cơ an ninh mạng trên thiết bị mạng- Kiểm tra các cổng kết nối, các dịch vụ, các chính sách thiết lập trên thiết bị3. Thử nghiệm xâm nhập:- Xác nhận, chứng minh sự tồn tại của các điểm yếu- Loại bỏ các kết quả thiếu chính xác- Phân tích chuyên sâu các lỗ hổng nếu có | **Thiết bị** | **8** |
| **4** | **Kiểm tra, đánh giá hiệu quả, tính sẵn sàng của hệ thống theo phương án đảm bảo ATTT**- Kiểm tra tính đầy đủ và phù hợp của Quy chế bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin về quản lý được phê duyệt.- Đánh giá việc tuân thủ các quy định, quy trình trong Quy chế bảo đảm an toàn thông tin trong quá trình vận hành, khai thác, kết thúc hoặc hủy bỏ hệ thống thông tin.- Đánh giá việc thiết kế hệ thống theo phương án bảo đảm an toàn thông tin được phê duyệt.- Đánh giá việc thiết lập, cấu hình hệ thống theo phương án bảo đảm an toàn thông tin được phê duyệt.- Kiểm tra việc cấu hình, tăng cường bảo mật cho thiết bị hệ thống, hệ điều hàng, ứng dụng, cơ sở dữ liệu và các thành phần khác liên quan trong hệ thống theo hướng dẫn của Bộ Thông tin và Truyền thông. | **Hệ thống** | **5** |

- **Danh sách chi tiết các nội dung Đánh giá An toàn thông tin:**

1. **Kiểm tra rà quét, đánh giá lỗ hổng bảo mật cho máy chủ**

|  |  |  |
| --- | --- | --- |
| **STT** | **Máy chủ** | **Ghi chú** |
| **Một cửa** |
| 1 | DVC\_1 |   |
| 2 | DVC\_2 |   |
| 3 | MC\_ Notify |   |
| 4 | MC\_AD |   |
| 5 | MC\_Data 1 |   |
| 6 | MC\_Data 2 |   |
| 7 | MC\_HA\_APP\_01 |   |
| 8 | MC\_HA\_APP\_02 |   |
| 9 | MC\_HA\_CC\_1 |   |
| 10 | MC\_HA\_CC\_2 |   |
| 11 | MC\_HA\_CD\_1 |   |
| 12 | MC\_HA\_CD\_2 |   |
| 13 | MC\_Portal 1 |   |
| 14 | MC\_Portal 2 |   |
| 15 | MC\_Service\_01 |   |
| 16 | MC\_Service\_02 |   |
| **Số hóa** |
| 17 | Web\_Sohoa\_SNV\_(BK) |   |
| 18 | Web\_Sohoa\_SNV |   |
| 19 | DB\_Sohoa\_SNV |   |
| 20 | DB\_Sohoa\_SNV\_(BK) |   |
| 21 | DBFile\_Sohoa\_SNV |   |
| **Thanh toán TT** |
| 22 | DB\_Thanhtoantructuyen\_NEW |   |
| 23 | ThanhToanTrucTuyen |   |
| 24 | WebSV\_Thanhtoantructuyen |   |
| **Cổng tỉnh/tỉnh ủy** |
| 25 | SPDATA2013\_BK |   |
| 26 | SPFE2013\_02\_BK |   |
| 27 | SPFE2013\_240\_BK |   |
| 28 | SPSearch2013\_BK |   |
| 29 | SPDB\_01\_VPTU |   |
| 30 | SPDB\_02\_VPTU |   |
| 31 | SPDBAnalysis\_VPTU |   |
| 32 | SPFE\_02\_VPTU |   |
| 33 | SPWebApp\_VPTU |   |
| **Cổng SBN** |
| 34 | DB2\_Cong\_SBN |   |
| 35 | DB\_CongNew |   |
| 36 | HA\_Proxy\_CongSBN |   |
| 37 | WebCong\_SBN\_New\_4 |   |
| 38 | WebCong\_SBN\_New\_1 |   |
| **1022** |
| 39 | DB\_1022\_01 |   |
| 40 | DB\_1022\_02 |   |
| 41 | HAProxy\_1022\_01 |   |
| 42 | HAProxy\_1022\_02 |   |
| 43 | Web\_1022\_01 |   |
| 44 | Web\_1022\_02 |   |
| **eGov** |
| 45 | eGov-TDH-Ubuntu |   |
| 46 | eGOv\_Bmail\_New(2) |   |
| 47 | eGOv\_Bmail\_New |   |
| 48 | eGov\_Chat |   |
| 49 | eGov\_Data |   |
| 50 | eGov\_Data\_2\_BK |   |
| 51 | eGov\_Data\_VPUB |   |
| 52 | Egov\_New(thay173) |   |
| 53 | eGov\_VPUB\_NEW |   |
| 54 | eGov\_Web\_HuyenTP\_1 |   |
| 55 | eGov\_Web\_HuyenTP\_2 |   |
| 56 | eGov\_Web\_SBN\_1 |   |
| 57 | eGov\_Web\_SBN\_2 |   |
| 58 | eGovSBN3\_New |   |
| 59 | BMM\_KD |   |
| 60 | eGov\_DBVPTU |   |
| 61 | eGov\_KD\_01 |   |
| 62 | eGov\_KD\_02 |   |
| 63 | eGov\_KD\_DB01 |   |
| 64 | eGov\_KD\_DB02 |   |
| 65 | eGov\_KD\_SSO |   |
| 66 | eGov\_Mail\_KD  |   |
| 67 | eGov\_VPTU |   |
| 68 | eGovCHAT\_KD |   |
| **HKG** |
| 69 | DB\_HKG |   |
| 70 | Server\_HKG2012 |   |
| 71 | SQL\_HKG2012 |   |
| **Web SBN** |
| 72 | DATA-BAUCU |   |
| 73 | DATA\_SBN\_v2 |   |
| 74 | Hosting2012\_new |   |
| 75 | Hostweb2012\_v2 |   |
| **Smart Radio** |
| 76 | Web01\_SmartRadio |   |
| 77 | Web02\_SmartRadio |   |
| 78 | DB01\_SmartRadio |   |
| 79 | DB02\_SmartRadio |   |
| 80 | MGW01-SmartRadio |   |
| 81 | MGW02-SmartRadio |   |
| 82 | Proxy01\_SmartRadio |   |
| 83 | Proxy02\_SmartRadio |   |
| 84 | Streaming\_SmartRadio |   |
| **DNS** |
| 85 | DNS-EXT-SECOND |   |
| 86 | DNS-INT-Sec 2- (New) |   |
| 87 | DNS-INT-Sec2 |   |
| 88 | DNS\_NEW\_EXT\_2022 |   |
| 89 | DNS\_WIN2019\_INT |   |
| 90 | eKGIS\_SQL |   |
| **iLIS** |
| 91 | iLIS-3\_BK |   |
| 92 | iLIS-data\_BK |   |
| 93 | iLIS\_web\_BK |   |
| **QLCBCCVC** |
| 94 | QLCBCCVC\_APP1 |   |
| 95 | QLCBCCVC\_APP2 |   |
| 96 | QLCBCCVC\_APP3 |   |
| 97 | QLCBCCVC\_DB1 |   |
| 98 | QLCBCCVC\_DB2 |   |
| **TVĐT** |
| 99 | TVĐT\_DATA |   |
| 100 | TVĐT\_WEB |   |

1. **Kiểm tra rà quét, đánh giá lỗ hổng bảo mật hệ thống các thiết bị mạng**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Thiết bị** | **Số lượng** | **Ghi chú** |
| 1 | Router Cisco | 2 |  |
| 2 | Switch HA Aruba | 2 |  |
| 3 | Peplink Balance | 2 |  |
| 4 | Switch Aruba Core | 2 |  |
| 5 | Switch Aruba Lan-Wan | 2 |  |
| 6 | Switch Cisco | 1 |  |
| 7 | Linksys | 1 |  |

1. **Kiểm tra đánh giá an toàn thông tin hệ thống các thiết bị an ninh bảo mật**

|  |  |  |  |
| --- | --- | --- | --- |
| STT | **Tên thiết bị** | **Số lượng** | **Ghi chú** |
| 1 | Abor | 1 |  |
| 2 | Trend Micro tipping point | 1 |  |
| 3 | Barracuda Web | 1 |  |
| 4 | Barracuda Email | 1 |  |
| 5 | Forti Web | 1 |  |
| 6 | Sophos | 1 |  |
| 7 | Fortinet | 2 |  |

1. **Kiểm tra, đánh giá hiệu quả, tính sẵn sàng của hệ thống theo phương án đảm bảo ATTT**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Tên hệ thống** | **Số lượng** | **Ghi chú** |
| 1 | Hệ thống Cổng TTĐT | 1 |  |
| 2 | Hệ thống Một cửa | 1 |  |
| 3 | Hệ thống xử lý Văn bản và Điều hành (eGov) | 1 |  |
| 4 | Hệ thống phản ánh hiện trường (1022) | 1 |  |
| 5 | Hệ thống Dịch vụ công | 1 |  |

1. **Diễn tập thực chiến ứng phó sự cố an toàn thông tin mạng.**
2. **Kế hoạch diễn tập**

Thời gian diễn tập trong 10 ngày, cụ thể như sau:

|  |  |  |  |
| --- | --- | --- | --- |
| **Thời gian thực hiện** | **Nội dung thực hiện** | **Đầu mối chủ trì** | **Đầu mối hỗ trợ phối hợp** |
| **Ngày 01** | Quyết định thành lập BTC chương trình Thực chiến | Sở TT&TT | Đối tác phối hợp |
| **Ngày 01** | BTC gửi lại bảng danh sách các hệ thống nằm trong scope tổ chức chương trình. | BTC | Đối tác phối hợp |
| **Ngày 01** | Thống nhất quy chế thi lần cuối. | BTC | Đối tác phối hợp |
| **Ngày 02** | Các đội chuẩn bị nội dung và chiến thuật. | Hai đội tấn công và phòng thủ | Đối tác phối hợp |
| **Ngày 02** | Tổ trọng tài công bố danh sách hệ thống CNTT được sử dụng | Hai đội tấn công và phòng thủ | Đối tác phối hợp |
| **Ngày 03 - Ngày 09** | Diễn ra cuộc thi Thực chiến ATTT  | Hai đội tấn công và phòng thủ | Đối tác phối hợp |
| **Ngày 10** | * Hai đội tổ chức buổi trình bày Seminar.
* Tổ trọng tài đưa ra số điểm ban đầu dựa trên thực trạng các đội report trong quá trình.
* BTC ghi nhận những vướng mắc, khó khăn, phản hồi từ các đội.
 | Hai đội tấn công và phòng thủ | Đối tác phối hợp |
| **Ngày 10** | * Hội đồng họp thống nhất sau buổi trình bày.
* Hội đồng đưa ra điểm số cuối cùng
* Tổ chức trao giải.
 | BTC | Đối tác phối hợp |

1. **Nội dung diễn tập**

Diễn tập thực chiến ứng phó sự cố an toàn thông tin mạng gồm 5 nội dung, cụ thể như sau:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STT** | **Nội dung** | **Chi tiết** | **ĐVT** | **Số lượng** |
| **I** | **Diễn tập thực chiến** |  | **Gói dịch vụ** | **01** |
| **1** | Khảo sát, xây dựng kịch bản chi tiết | * Khảo sát Nghiên cứu, xây dựng đề cương, kế hoạch, kịch bản diễn tập;
* Xây dựng bài kiểm tra để đánh giá nhân sự tham gia diễn tập;
* Lập kế hoạch chi tiết xây dựng kịch bản, triển khai diễn tập phù hợp.
 |  |  |
| **2** | Đội tấn công Redteam (tấn công vào các hệ thống) | Thực hiện các biện pháp rà quét, tấn công, chiếm quyền hệ thống dựa trên các hình thức tấn công như:* Tấn công vào các ứng dụng web.
* Tấn công vào hệ thống email.
* Tấn công bằng mã độc.
* Tấn công DOS/DDOS.
* Tấn công bằng các biện pháp phi kỹ thuật.…

Sau khi tấn công thành công sẽ thử nghiệm lây lan và leo quyền tối đa trong hệ thống.Báo cáo lại kết quả, cách thức tấn công vào hệ thống khi tổng kết diễn tập. |
| **3** | Đội phòng thủ Blueteam | Phối hợp, hướng dẫn các đội thi nhận diện các cuộc tấn công, sự cố ATTT như:- Sự cố An toàn thông tin liên quan đến mã độc- Sự cố An toàn thông tin liên quan đến truy cập trái phép, leo quyền- Sự cố An toàn thông tin liên quan đến vi phạm chính sách An toàn thông tin- Sự cố An toàn thông tin liên quan đến tấn công từ chối dịch vụ DoS/DdoSHướng dẫn, phối hợp các đội thi ứng cứu sự cố ATTT như:- Phân tích và đưa ra khuyến nghị xử lý, khắc phục nhanh chóng- Điều tra truy vết, xác định nguyên nhân sự cố và khuyến nghị khắc phục |
| **4** | Dịch vụ đào tạo ATTT | * Tổ chức đào tạo giới thiệu về các cách thức tấn công, khai thác vào hệ thống công nghệ thông tin.
* Tổ chức đào tạo về quy trình ứng cứu sự cố.
* Tổ chức đào tạo về rà soát, thu thập mã độc cơ bản; phân tích cảnh báo; điều tra số.
 |
| **5** | Công tác tổ chức | * Chuẩn bị phòng họp, đào tạo online/ofline. Phòng họp có sức chứa 60 người trong đó trang bị đầy đủ thiết bị thiết bị cần thiết như máy chiếu, màn chiếu, thiết bị âm thanh, ánh sáng, ... và trang thiết bị hệ thống mô phỏng đào tạo nếu cần như máy tính, máy chủ, thiết bị mạng...
* Chuẩn bị các hệ thống phục vụ diễn tập.
* Tiến hành lắp đặt, cài đặt cấu hình hệ thống mô phỏng đào tạo để huấn luyện.
 |