**PHỤ LỤC I**

*(Kèm theo Công văn số /TTCNTT-KTHT ngày /06/2019 của Trung tâm Công nghệ thông tin)*

|  |  |
| --- | --- |
| ĐƠN VỊ CẤP TRÊN**TÊN ĐƠN VỊ-------** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAMĐộc lập - Tự do - Hạnh phúc ---------------** |
|   | *…………., ngày …. tháng …. năm …..* |

**BÁO CÁO**

**ĐỊNH KỲ CỦA CHỦ QUẢN HỆ THỐNG THÔNG TIN**

**(từ ngày ………đến ngày…………. )**

**Kính gửi: Trung tâm Công nghệ thông tin**

**I. Thông tin giám sát tổng hợp**

- Thời gian giám sát:... giờ... phút ngày ... đến ... giờ ... phút ngày ...

- Tổng số sự kiện an toàn thông tin thu thập được:

- Tổng số sự kiện an toàn thông tin nguy hiểm mức cao:

- Tình trạng an toàn thông tin: [Nghiêm trọng/Nguy Hiểm/Bình Thường/An toàn]

- Số lượng các sự cố xảy ra:

- Tóm tắt tình hình an toàn thông tin trong thời gian giám sát:

.................................................................................................................................

.................................................................................................................................

**II. Kết quả giám sát**

1. Danh sách kỹ thuật tấn công được phát hiện nhiều nhất (tối thiểu 05 kỹ thuật tấn công nhiều nhất)

|  |  |  |
| --- | --- | --- |
| **STT** | **Kỹ thuật tấn công** | **Số lượng cuộc tấn công** |
| 1 |   |   |
| 2 |   |   |
| 3 |   |   |
| 4 |   |   |
| 5 |   |   |

2. Danh sách dịch vụ bị tấn công nhiều nhất (tối thiểu 05 dịch vụ bị tấn công nhiều nhất)

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Số cổng dịch vụ/ địa chỉ IP** | **Dịch vụ** | **Số lượng cuộc tấn công** |
| 1 |   |   |   |
| 2 |   |   |   |
| 3 |   |   |   |
| 4 |   |   |   |
| 5 |   |   |   |

3. Danh sách địa chỉ IP bị tấn công nhiều nhất (tối thiểu 05 địa chỉ IP)

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Địa chỉ IP** | **Mô tả về thiết bị/phần mềm có địa chỉ IP bị tấn công** | **Số lượng cuộc tấn công** |
| 1 |   | - Các dịch vụ cung cấp:1. Tên dịch vụ:+ Mã số cổng cung cấp dịch vụ:+ Giao thức hoạt động:+ Phần mềm, phiên bản cung cấp dịch vụ:+ Thời gian2. Tên dịch vụ: …………………………. |   |
| 2 |   |   |   |
| 3 |   |   |   |
| 4 |   |   |   |
| 5 |   |   |   |

4. Danh sách địa chỉ IP nguồn tấn công nhiều nhất từ trong nước (tối thiểu 05 địa chỉ IP)

|  |  |  |
| --- | --- | --- |
| **STT** | **Địa chỉ IP** | **Số lượng cuộc tấn công** |
| 1 |   |   |
| 2 |   |   |
| 3 |   |   |
| 4 |   |   |
| 5 |   |   |

5. Danh sách địa chỉ IP nguồn tấn công nhiều nhất từ nước ngoài (tối thiểu 05 địa chỉ IP)

|  |  |  |
| --- | --- | --- |
| **STT** | **Địa chỉ IP** | **Số lượng cuộc tấn công** |
| 1 |   |   |
| 2 |   |   |
| 3 |   |   |
| 4 |   |   |
| 5 |   |   |

**III. Các loại tấn công điển hình**

1. Các loại tấn công nguy hiểm nhất (tối thiểu 05):

*1. 1. Kỹ thuật tấn công thứ 1:*

- Tên kỹ thuật tấn công: .........................................................................................

- Mã hiệu quốc tế (nếu có): ...................................................................................

- Các đối tượng bị tấn công: .................................................................................

- Dấu hiệu nhận biết: ............................................................................................

- Mô tả: .................................................................................................................

- Số lượng và thời gian xảy ra: .............................................................................

- Đánh giá mức độ nguy hiểm: ............................................................................

- Ảnh hưởng: .......................................................................................................

- Các biện pháp xử lý đã được triển khai: ...........................................................

- Tài liệu tham khảo: .........................................................................................

- Ghi chú khác: ..................................................................................................

*1.2. Kỹ thuật tấn công thứ 2: (Mô tả tương tự kỹ thuật tấn công thứ 1)*

*1.3. Kỹ thuật tấn công thứ 3: (Mô tả tương tự kỹ thuật tấn công thứ 1)*

*1.4. Kỹ thuật tấn công thứ 4: (Mô tả tương tự kỹ thuật tấn công thứ 1)*

*1.5. Kỹ thuật tấn công thứ 5: (Mô tả tương tự kỹ thuật tấn công thứ 1)*

............................................................................................................................

*1.n. Kỹ thuật tấn công n: ...................................................................................*

2. Các loại tấn công diễn ra nhiều nhất (tối thiểu 05)

*2.1. Kỹ thuật tấn công thứ 1:*

- Tên kỹ thuật tấn công: ....................................................................................

- Mã hiệu quốc tế (nếu có): ...............................................................................

- Các đối tượng bị tấn công: ..............................................................................

- Dấu hiệu nhận biết: .........................................................................................

- Mô tả: ..............................................................................................................

- Số lượng và thời gian xảy ra: .........................................................................

- Đánh giá mức độ nguy hiểm: .........................................................................

- Ảnh hưởng: ....................................................................................................

- Các biện pháp xử lý đã được triển khai: .......................................................

- Tài liệu tham khảo: .......................................................................................

- Ghi chú khác: ...............................................................................................

*2.2. Kỹ thuật tấn công thứ 2: (Mô tả tương tự kỹ thuật tấn công thứ 1)*

*2.3. Kỹ thuật tấn công thứ 3: (Mô tả tương tự kỹ thuật tấn công thứ 1)*

*2.4. Kỹ thuật tấn công thứ 4: (Mô tả tương tự kỹ thuật tấn công thứ 1)*

*2.5. Kỹ thuật tấn công thứ 5: (Mô tả tương tự kỹ thuật tấn công thứ 1)*

........................................................................................................................

*2.n. Kỹ thuật tấn công n:* ...............................................................................

3. Các loại tấn công mới xuất hiện (tối thiểu 05)

*3.1. Kỹ thuật tấn công thứ 1:*

- Tên kỹ thuật tấn công: ...................................................................................

- Mã hiệu quốc tế (nếu có): ..............................................................................

- Các đối tượng bị tấn công: .............................................................................

- Dấu hiệu nhận biết: ........................................................................................

- Mô tả: .............................................................................................................

- Số lượng và thời gian xảy ra: .........................................................................

- Đánh giá mức độ nguy hiểm: ........................................................................

- Ảnh hưởng: ...................................................................................................

- Các biện pháp xử lý đã được triển khai: ......................................................

- Tài liệu tham khảo: ......................................................................................

- Ghi chú khác: ...............................................................................................

*3.2. Kỹ thuật tấn công thứ 2: (Mô tả tương tự kỹ thuật tấn công thứ 1)*

*3.3. Kỹ thuật tấn công thứ 3: (Mô tả tương tự kỹ thuật tấn công thứ 1)*

*3.4. Kỹ thuật tấn công thứ 4: (Mô tả tương tự kỹ thuật tấn công thứ 1)*

*3.5. Kỹ thuật tấn công thứ 5: (Mô tả tương tự kỹ thuật tấn công thứ 1)*

..........................................................................................................................

*3.n. Kỹ thuật tấn công n:* .................................................................................

**IV. Các vấn đề khác về an toàn thông tin trong kỳ giám sát**

.........................................................................................................................

..........................................................................................................................

..........................................................................................................................

**V. Đề xuất và kiến nghị:**

...........................................................................................................................

............................................................................................................................

|  |  |
| --- | --- |
| ***Nơi nhận:****- Như trên;- Lưu ....* | **Thủ trưởng đơn vị***(ký, đóng dấu)* |

PHỤ LỤC II

*(Kèm theo Công văn số /TTCNTT-KTHT ngày /06/2019 của Trung tâm Công nghệ thông tin)*

1. Thông tin về Lãnh đạo phụ trách An toàn thông tin của đơn vị
* Họ và tên: ………………………………………………………………
* Chức vụ: ………………………………………………………………..
* Số điện thoại: …………………………………………………………..
* Email: ………………………………………………………………….
1. Thông tin về Cán bộ phụ trách An toàn thông tin của đơn vị
* Họ và tên: ………………………………………………………………
* Chức vụ: ………………………………………………………………..
* Số điện thoại: …………………………………………………………..
* Email: ………………………………………………………………….