Security Incident Response Report Form

Please include as much information as possible.

INCIDENT IDENTIFICATION INFORMATION

Date and Time of Notification: 12 de maio de 2017

Incident Detector's Information:

Name: WANNACRY RANSOMWARE	Date and Time Detected: 2 de maio de 2017
Title: WANNACRY	Location: Mais de 150 países
Phone/Contact Info:	System or Application: Server Message Block (SMB)

INCIDENT SUMMARY

Type of Incident Detected:

□ Denial of Service
□ Unauthorized Access
□ Malicious Code
□ Unplanned Downtime
☑ Unauthorized Use
□ Other

Description of Incident:

1. Etapa 1 do Cyber Kill Chain: Reconhecimento
- Descrição: Os atacantes realizaram exploração ativa de sistemas vulneráveis que expunham a falha no protocolo SMBv1. A vulnerabilidade, conhecida como EternalBlue (CVE-2017-0144),

Names and Contact Information of Others Involved:

INCIDENT NOTIFICATION – OTHERS

☑ IS Leadership
☑ Security Incident Response Team
☑ Administration
□ Other:
☑ System or Application Owner
☑ Public Affairs
☑ Human Resources
☑ System or Application Vendor
□ Legal Counsel

ACTIONS

Identification Measures (Incident Verified, Assessed, Options Evaluated):

Containment Measures:

Evidence Collected (Systems Logs, etc.):

Eradication Measures:

Recovery Measures:

Other Mitigation Actions:

This form has been developed as a working tool for assessment and improvement activities; it is intended for internal use only.

Sample Security Incident Response Report

EVALUATION

How Well Did Work Force Members Respond?

Were the Documented Procedures Followed? Were They Adequate?

What Information Was Needed Sooner?

Were Any Steps or Actions Taken That Might Have Inhibited the Recovery?

What Could Work Force Members Do Differently the Next Time an Incident Occurs?

What Corrective Actions Can Prevent Similar Incidents in the Future?

What Additional Resources Are Needed to Detect, Analyze, and Mitigate Future Incidents?

Other Conclusions or Recommendations:

FOLLOW-UP

Reviewed By:

□ Security Officer

□ Privacy Officer

□ IS Department/Team

□ Other

Recommended Actions Carried Out:

Initial Report Completed By:

Follow-Up Completed By: