Incident Reporting 2018

October 2018

Topics

What is an incident?

- Incidents versus events

What should I report?

Incidents versus events

Events

An event is any observable occurrence in a system or network. Events include a user connecting to a file share, a server receiving a request for a web page, a user sending email, and a firewall blocking a connection attempt.[1]

[1]Special Publication 800-61 Revision 2

Incidents versus events

Incidents

A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. Examples of incidents are:

- An attacker commands a botnet to send high volumes of connection requests to a web server, causing it to crash.
- Users are tricked into opening a “quarterly report” sent via email that is actually malware; running the tool has infected their computers and established connections with an external host.
- An attacker obtains sensitive data and threatens that the details will be released publicly if the organization does not pay a designated sum of money.
- A user provides or exposes sensitive information to others through peer-to-peer file sharing services. [1]

[1]Special Publication 800-61 Revision 2

What should I report?

E-Mail

- Account compromise
- Phishing (Social Engineering)
- E-mail Harassment
- Open Relay Complaints

What should I report?

Hacking

- Port scanning
- Unauthorized access
- SQL Injection
- Anonymous Proxies
- Web Defacements
- Denial of Service (DOS)
- Brute Force Attacks
- System Compromise

What should I report?

Malicious Software (aka. Malware)

- Malware Outbreaks
  - Multiple systems/users reporting infection
- AV Failures (Large Scale)
  - Fail to detect
  - Fail to clean
- Vectors of Infection
  - Hostile websites
  - Malicious email/text/social networking links

What should I report?

Inappropriate Use

- Copyright violations (Peer-to-Peer Networks –Torrents)
- Downloading and/or distribution of pornography
- Unauthorized access to remote system/account by state employee
- Use of state resources for personal gain or harassment

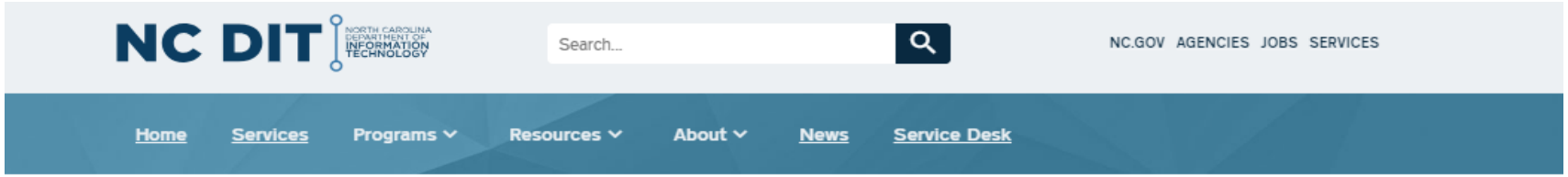
What should I report?

Other

- Law Enforcement Issues
  - Intelligence
  - Theft and Fraud
  - Stalking
  - Harassing Telephone Calls
- Data loss (Desktops, laptops, portable media, etc.)
  - *When reporting these incidents, you must note if the device and/or media contained sensitive data and if the device/data was protected with encryption.*
- Miscellaneous incidents not covered above!

How to report?

https://it.nc.gov/cybersecurity-situation-report



NC IT » Cybersecurity Situation Report

Cybersecurity Situation Report

Please complete this webform to report suspicious cyber activity. A member of the Enterprise Security and Risk Management team will contact you.

For questions about reporting an incident, or if you need Information Security staff to contact you immediately, please call the Customer Support Center at 1-800-722-3946.

Date of Incident *

Please indicate the date you noticed the suspicious activity. Click the calendar icon to open the pop-up calendar.

Month | Day | Year

Time of Incident *

Please indicate the time you noticed the suspicious activity.

Hour : 00 am pm

How to report?

DIT Service Desk
Phone: 919-754-6000
Toll Free: 800-722-3946
DIT.Incidents@its.nc.gov

Albert Moore
919-754-6245
albert.moore@nc.gov

David Webb
919-754-6149
david.webb@nc.gov

Dan Walser
919 754 6297
Dan.Walser@nc.gov

Learned Wilson
919-754-6608
learned.wilson@nc.gov

Mitch Haddadi
919-754-6714
mitchell.haddadi@nc.gov

Doug Mitchell
doug.mitchell@nc.gov

Meet the SOC

Alexandru Razvan Tufis-SOC Team Leader
alexandru.tufis@nc.gov

Alexandru Ciachir-SOC Sr. Analyst
alexandru.ciahir@nc.gov

Matache Marius-SOC Analyst
marius.matache@nc.gov

Raluca Serbanescu-SOC Analyst
raluca.serbanescu@nc.gov

Stefan-Mihai Anton-SOC Analyst
stefan.anton@nc.gov

Adrian Lupu-SOC Analyst
adrian.lupu@nc.gov

Diana Toader-SOC Analyst
diana.toader@nc.gov

24 x7

630-487-4667

soc@nc.gov

Questions?

Be on the lookout

Tabletop training exercises coming our way.

Let's Connect!

@NCDIT
@BroadbandIO
@ncicenter

NC Department of Information Technology

NCDIT

NC DIT

@NCDIT

it.nc.gov