BtCIRT Annual Report
(2019)

Table of Content

1. Highlights of 2019

1.1 Summary of major activities

In 2019, BtCIRT conducted security workshops, published articles and alerts on latest cyber trends, threats, vulnerabilities and best practices. BtCIRT also conducted vulnerability assessment, post-incident analysis, and awareness programs.

1.2 Achievements & milestones:

- Workshop on Secure Coding conducted.
- Child Online Protection: survey was conducted in 45 schools with 2400 students aged ranging from 12 to 17 to understand the overall situation of students on cyberspace. The survey also looked at how prepared students are to tackle issues they face online including intrusion of their privacy, cyberbullying

2. About BtCIRT

2.1 Introduction

Bhutan Computer Incident Response Team (BtCIRT) is a part of Department of Information Technology and Telecom, Ministry of Information and Communications. The overall mission of BtCIRT is to enhance cyber security in the country by coordinating cybersecurity information and establishing computer security incident handling capabilities in the country. It is also mandated to proactively monitor government systems for attacks and vulnerabilities.

2.2 Establishment

The BtCIRT's mandate was approved by the *Lhengye Zhungtshog*/Cabinet on 20 May 2016 formally identifying the team as the national focal point for cybersecurity activities and initiatives.

2.3 Resources

Currently, BtCIRT consist of 5 working team members.

2.4 Constituency

BtCIRT constituents are all government institutions which use government network infrastructure to host their IT resources and services. While BtCIRT services like awareness and reactive services are extended to all users within the country.

3. Activities & Operations

3.1 Scope and definitions:

- BtCIRT is a national contact in relation to cyber security issues.
- BtCIRT conducts end-user awareness at national level and disseminates information on threats and vulnerabilities, and conducts security workshops related to various cyber security domains.
- BtCIRT actively monitors systems hosted in the Government Data Centre (GDC) for

attacks and vulnerabilities, and provides timely reports to the GDC operating team along with system administrators. BtCIRT also conducts periodic security assessment of government systems while for non-government organisations it provides services on request basis.

- Represent the country in international forums.
- BtCIRT also develops strategies, policies, standards, guidelines and baseline documents.

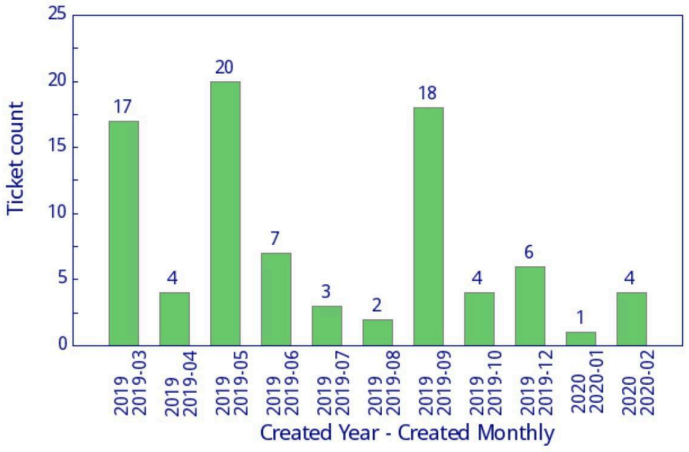
3.2 Incident Handling Report

This year saw a decrease in the number of incidents handled by the BtCIRT as compared to 2018 with 81 total incidents. This is attributed to frequent trainings and workshops on security related topics for the government and corporate ICT Officials.

131 government websites were assessed for security vulnerabilities and security flaws.

Periodic security assessment of government systems hosted at the Government Data Center

The following graphs provide a number of incidents resolved on a monthly basis in 2019. It also depicts the types of incidents resolved by the team during the year.



Created Year	Created Monthly	Ticket count
2019	2019-03	17
	2019-04	4
	2019-05	20
	2019-06	7
	2019-07	3
	2019-08	2
	2019-09	18
	2019-10	4
	2019-12	6
2020	2020-01	1
	2020-02	4
Total		86

3.3 Security Advisory and Alerts

BtCIRT publishes latest cyber security news and vulnerabilities to keep the constituents well informed about the latest development in the area of cybersecurity on its website (www.btcirt.gov.bt) and facebook page (BtCIRT).
In addition, the team also publishes advisories to assist constituents in resolving the most common threats and vulnerabilities observed. Besides, email advisory are also sent out to government and critical sector ICT officials to notify possible attacks as and when it is detected.

4. Events organized / hosted

4.1 Training/Workshops, Drills & exercises

4.1.1 The BtCIRT presented on the various cyber security initiatives of the government, challenges and technical recommendations to around 300+ ICT officials(Private, government and corporate sectors) at the annual BtNOG (Bhutan Network Operator's Group) Conference on 3rd June, 2019. The presentation was a good initiative in expanding the reach of the team and its mandates and to create awareness on cybersecurity in the country.

4.1.2 A workshop on Secure Coding was conducted from 19th to 23rd August 2019 for 50 participants involving ISPs, Banks, Colleges, Pvt Sectors, and Government Agencies.

4.1.3 BtCIRT participated in the annual APCERT drill on the theme "Catastrophic Silent Draining in Enterprise Network". This year's scenario was inspired by a latest security attack on an organization, which relates to the vulnerability that could allow attackers to completely take over vulnerable websites to deliver malware backdoor and cryptocurrency miners.

4.1.4 The BtCIRT presented on the theme "Managing Cyber Security Risk and Mitigation in Bhutan" at the Annual ICT Conference on 2nd December, 2019, further improving the reach of the team and its mandates.

5. International Collaboration

5.1 International partnerships and agreements

BtCIRT is a member of two international organisations, Asia Pacific Computer Emergency Response Team (**APCERT**) and Forum of Incident Response and Security Teams (**FIRST**) as of now.

5.2 Capacity building

5.2.1 Seminars & presentations

BtCIRT has attended following conference/seminars/workshops:

5.2.1.1 APAN48-CSIRT Capacity Building in Asia: TRANSITS I

6. Future Plans

6.1 BtCIRT also looks forward to collaborating with more organisations internally and internationally to strengthen its cooperation.

6.2 Conduct awareness programs in schools and colleges and through media outlets

6.3 Establish new cyber policies and standards and strengthen existing ones

7. Conclusion:

The BtCIRT will continue to focus on improving its visibility in the country and to create awareness on the importance of cybersecurity. Importance will be given to training and human resource development of ICT officials in the government and critical sectors to improve our cyber threat resilience.