BGD e-GOV CIRT

BANGLADESH COMPUTER COUNCIL

09-Sep-2023

Enhancing Situational Awareness on Emerging Cyber Threats

The Bangladesh Government's Computer Incident Response Team (BGD e-GOV CIRT) carries out its primary mission of safeguarding the nation's cyberspace through proactive management of computer security incidents and related activities. This mission involves close collaboration with international organizations and entities to effectively mitigate risks. Our goal is to maintain a continuous state of vigilance and preparedness, both in anticipation of potential incidents and in response to them, thus ensuring the security of institutions throughout the country.

We've noticed that various global critical information infrastructures such as healthcare, banking, government institutions, etc. have been targeted by various hacktivist groups. These groups remain active and persist in carrying out hacking activities. As a result, it's crucial for us to remain highly vigilant about the state of our own infrastructure and rigorously follow best practices.

In light of this ongoing threat landscape, we earnestly request all entities in Bangladesh to implement the following measures to fortify the security of their infrastructure:

1. Maintain continuous network and user activity monitoring around the clock (24x7), especially outside regular office hours, to detect any signs of data exfiltration.
2. Provide comprehensive training on Information and Cyber Security awareness for all employees, customers, and consumers, covering topics such as phishing emails, password policies, best practices etc. Encourage them to report any anomalies or suspicious activities they may encounter.
3. Implement load balancing solutions to ensure that no individual server becomes overwhelmed in the event of an attack.
4. Deploy a Web Application Firewall to examine incoming HTTP/HTTPS traffic and filter out malicious requests and traffic patterns commonly associated with DDoS attacks.
5. Securely configure essential services like DNS, NTP, and network middleboxes, ensuring they are not exposed to the internet.
6. Thoroughly validate and sanitize all user input to prevent the injection of malicious code (e.g., SQL injection or Cross-Site Scripting) that could result in website defacement.
7. Regularly back up your website's content and database. In the event of defacement, having up-to-date backups enables rapid restoration of your website.
8. Enforce the use of HTTPS on your website, incorporating SSL/TLS encryption. This safeguards data during transmission and prevents attackers from tampering with website content during transit.
9. Keep all web server software, content management systems (CMS), plugins, and other software components up-to-date by applying the latest security patches.
10. Configure and harden web application as per OWASP guideline, https://owasp.org/www-project-web-security-testing-guide/v41/
11. Report or inform BGD e-GOV CIRT regarding the detection of IOCs and/ or any suspicious activities you observe within your environment, to work in collaboration through https://www.cirt.gov.bd/incident-reporting/ or notify@dsa.gov.bd