MOROĞLU ARSEVEN

The Presidency of the Republic of Turkey Issued a Notice on Information and Communication Security Measures

8 Aug 2019

The Presidential Circular numbered 2019/2 on Information and Communication Security Measures (the "**Circular**") was published in Official Gazette number 30823 on 6 July 2019. The Circular outlines the security measures to be taken in order to reduce and neutralize security risks as well as ensuring the security of critical data that could threaten national security or disrupt public order.

The Circular mainly regulates the following issues:

- In order to promote and expand the use of domestic cloud services and domestic and national cryptosystems,
    - The data relating to population, health, communication as well as the genetic, biometric, and critical information and data, should be stored domestically.
    - The critical data contained in the public institutions and organizations should be stored in an offline network and in a physically secured environment.
    - The data of the public institutions and organizations should be stored only in the institutions' own private systems or the local cloud storage services under the control of these institutions.
    - The confidential communication of the institutions should be carried out only through domestic and national cryptosystems.

- The use of domestic social media applications and communication applications are promoted. It is mentioned that there should be no classified data sharing and communication through social media. In addition, it is also stated that there should not be any data sharing or communication on the mobile applications except for the domestic applications developed by institutions authorized for coded or encrypted communication under legislations.
    - Measures should be taken to safely develop software. Necessary security tests should be performed before using the provided or developed software. Within this scope;
    - As much as possible, an undertaking should be obtained from the manufacturer and/or supplier to ensure that the software or hardware to be used by the public institutions and organizations does not contain any security vulnerabilities that are not suitable for their intended use and provide access to the systems without the users' knowledge/permission.
    - Necessary cybersecurity measures should be taken.
    - Extension security (TEMPEST) or other similar measures should be taken where classified information is processed by the public institutions and organizations.

- Mobile devices and devices capable of data transfer should not be kept in the workrooms, environments preserving critical data and documents and/or hosting critical interviews. Classified data and documents or data that contain corporate privacy should not be stored on laptops, mobile devices, external memories and similar devices that are not institutionally authorized or used personally.
- Industrial control systems should be kept offline, and where such systems are required to be online, necessary security measures such as firewall, end-to-end tunneling methods, authorization, and identification should be taken
- A security investigation or archive research should be conducted on senior managers and the critical personnel working at strategically important institutions and organizations with direct impact on the national security
- The settings of public e-mail systems should be configured to be secure, e-mail servers should be kept domestically and under the control of the relevant institution and encrypted communication between servers should be ensured. The corporate communication should not be carried out from non-corporate personal e-mail addresses. Corporate e-mails should not be used for private communication, personal social media accounts or any other similar personal purposes.
- The operators authorized to provide communication services are obliged to establish an internet exchange point in Turkey. Measures should be taken to prevent the cross-border transmission of the domestic communication traffic that needs to be exchanged domestically.
- An Information and Communication Security Guide including different security levels will be prepared under the coordination of the Turkish Presidency's Digital Transformation Office to be implemented in public institutions, organizations, and enterprises providing essential infrastructure services. All public institutions, organizations, and enterprises providing essential infrastructure services will be obliged to comply with procedures and principles stated under the guide in the information systems to be established.

Please see this link to read the full text of the Circular published in Official Gazette number 30823 on 6 July 2019 (Only available in Turkish).

Related Practices

- Information Technologies
- Privacy and Data Protection