



CYBERWELLNESS PROFILE TUNISIA



BACKGROUND

Total Population: 10 705 000

(data source: [United Nations Statistics Division](#), December 2012)

Internet users, percentage of population: 43.80%

(data source: [ITU Statistics](#), 2013)

1. CYBERSECURITY

1.1 LEGAL MEASURES

1.1.1 CRIMINAL LEGISLATION

Specific legislation on cybercrime has been enacted through the following instrument:

- [Art.199 bis and 199ter](#) of Tunisia Penal Law.

1.1.2 REGULATION AND COMPLIANCE

Tunisia has officially recognized regulations regarding cybersecurity and compliance requirements through the following instruments:

- [Law n° 2004-5](#), February 3, 2004, relative to computer security.

- [Decree n° 1248 - 2004](#), May 25, 2004, setting the administrative, financial and operating procedures of the ANSI.

- [Decree n° 1249 - 2004](#), May 25, 2004, on requirements and procedures for the certification of expert auditors in the field of computer security.

- [Decree n° 1250 - 2004](#), May 25, 2004, on the institutional computer systems and networks subjected to the compulsory periodic Risk Assessment of computer security, and on the criteria relating to the nature and periodicity of the Risk Assessment and to procedures for monitoring the implementation of the recommendations made in the Risk Assessment report.

1.2 TECHNICAL MEASURES

1.2.1 CIRT

Tunisia has an officially recognized National CIRT ([TunCERT](#)).

1.2.2 STANDARDS

There is no information available concerning any officially approved national (and sector specific) cybersecurity frameworks for implementing internationally recognized cybersecurity standards.

1.2.3 CERTIFICATION

The National Institute for Standardization and Industrial Property ([INNORPI](#)) is the leading certification body for Tunisia. Its objective is to undertake every action concerning standardization, the quality of products and services, metrology, industrial property protection and the maintaining of a central commercial register.

1.3 ORGANIZATION MEASURES

1.3.1 POLICY

Tunisia has an officially recognized national cybersecurity strategy.

1.3.2 ROADMAP FOR GOVERNANCE

The national governance roadmap for cybersecurity in Tunisia is elaborated in the National Agency for Computer Security ([ANSI](#)).

1.3.3 RESPONSIBLE AGENCY

The National Agency for Computer Security ([ANSI](#)) is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap in Tunisia.

1.3.4 NATIONAL BENCHMARKING

The National Agency for Computer Security ([ANSI](#)) is responsible for the benchmarking and measuring cybersecurity development in Tunisia.

1.4 CAPACITY BUILDING

1.4.1 STANDARDISATION DEVELOPMENT

There is no available information concerning any officially recognized national or sector-specific research and development (R&D) programs/projects for cybersecurity standards, best practices and guidelines to be applied in either the private or the public sector.

1.4.2 MANPOWER DEVELOPMENT

The National Agency for Computer Security ([ANSI](#)) is responsible for providing educational and professional training programs for raising awareness with the general public, promoting cybersecurity courses in higher education and promoting certification of professionals in either the public or the private sectors.

1.4.3 PROFESSIONAL CERTIFICATION

Tunisia has numerous public sector professionals certified under internationally recognized certification programs in cybersecurity such as ISO270001, CEH, CISA, CISM and CISSP.

1.4.4 AGENCY CERTIFICATION

There is no available information concerning any certified government and public sector agencies certified under internationally recognized standards in cybersecurity.

1.5 COOPERATION

1.5.1 INTRA-STATE COOPERATION

To facilitate sharing of cybersecurity assets across borders with other nation states Tunisia has officially recognized partnerships with the following organizations:

- [National Agency for Computer Security](#)
- [FIRST](#)
- [Honeypot Project](#)
- [OIC-CERT](#)
- [UNCTAD](#)

1.5.2 INTRA-AGENCY COOPERATION

The Tunisian honeypot project "[Saher-HoneyNet](#)" is an initiative launched by the Tunisian CERT, in order to mitigate threats related to malicious traffic and to improve the national cyberspace security by ensuring preventive and response measures to deal with malicious threats. It is the officially recognized program for sharing cybersecurity assets within the public sector.

1.5.3 PUBLIC SECTOR PARTNERSHIP

The Tunisian honeypot project "[Saher-HoneyNet](#)" is an initiative launched by the Tunisian CERT, in order to mitigate threats related to malicious traffic and to improve the national cyberspace security by ensuring preventive and response measures to deal with malicious threats. It is the officially recognized program for sharing cybersecurity assets within the private sector.

1.5.4 INTERNATIONAL COOPERATION

Tunisia is a member of the ITU-IMPACT initiatives and has access to relevant cybersecurity services. Tunisia participated in several cybersecurity activities with the following organizations/activities:

- [National Agency for Computer Security](#)
- [Honeypot Project](#)
- [Shadowserver](#)
- [ArborNetworks](#)

2. CHILD ONLINE PROTECTION

2.1 NATIONAL LEGISLATION

Specific legislation on child protection has been enacted through the following instrument:

- [Articles 226, 226bis and 233-235](#) of the Criminal Code.

2.2 UN CONVENTION AND PROTOCOL

Tunisia has acceded, with no declarations or reservations to articles 16, 17(e) and 34(c), to the [Convention on the Rights of the Child](#).

Tunisia has signed and ratified, with no declarations or reservations to articles 2 and 3, the [Optional Protocol to The Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography](#).

2.3 INSTITUTIONAL SUPPORT

Tunisia Computer Emergency Response Team ([TUN CERT \(*\)](#)) provides information on tools for parental control.

2.4 REPORTING MECHANISM

TUN CERT makes available the number (+216) 71 843 200 or (+216)71 846 020 - ext. 119 and the email address incident@ansi.tn to report a computer incident.

DISCLAIMER: Please refer to <http://www.itu.int/en/Pages/copyright.aspx>

More information is available on ITU website at <http://www.itu.int/en/ITU-D/Cybersecurity/Pages/default.aspx>

Last updated on 23th October 2014