February 28, 2024

Improvement Suggestions for National Cyber Security

What is TR Cybersecurity Alliance?

In the last quarter of 2023, Turkey's leading cyber security professionals joined forces and established a cyber security alliance called TR Cybersecurity Alliance.

TR Cybersecurity Alliance is a workshop group established with the initiative of well-known industry professionals who work in various sectors of Turkey and have an average of more than fifteen years of cyber security experience. Continuing its working group in the last two quarters, TR Cybersecurity Alliance aims to carry out studies that will support increasing Turkey's cyber resilience. Detailed information about the alliance is available on the website and LinkedIn page.

What is the Purpose of the Alliance?

Cyber security is an extremely technically difficult and complex field. For this reason, numerous laws, regulations, standards or guidelines have been published by relevant institutions to increase cyber resilience. Today, cyber security is not only important for the continuity of commercial and social life, but also for national security. In all this chaos, institutions and organizations have difficulty determining which areas to invest in, in what order, and how, and they have difficulty measuring the efficiency of the investments made.

TR Cybersecurity Alliance was established to combine the experiences of Turkey's leading and well-known cyber security experts and to offer the growing pool of experience free of charge to institutions and organizations that have difficulty in producing a cyber security strategy.

The main objectives of TR Cybersecurity Alliance are:

- Contributing to strengthening Turkey's cyber security infrastructure
- Keeping up with the latest developments in the industry by promoting innovation and research
- Increasing effective communication and collaboration between professionals in the industry
- To increase awareness about cyber security in the public and private sectors

What is the Working Order?

TR Cybersecurity Alliance increases interaction among its members by holding regular meetings and workshops every quarter. The purpose of these workshops is to combine the experiences of alliance members and produce solution suggestions that every institution or company can implement. Cyber security disciplines or regulations also fall within the alliance's areas of work. In this sense, the alliance will conduct special studies to produce recommendations for administrative or regulatory public institutions.

Contact TR Cybersecurity Alliance:

Website: www.tr-csa.org
LinkedIn: TR Cybersecurity Alliance

Improvement Suggestions for National Cyber Security

TR Cybersecurity Alliance members have produced the following suggestions for the security and continuity of public services and decided to submit them to all parties.

1. Although the tightening measures, which are article number five of the Information and Communication Security Guide published by the Digital Transformation Office of the Presidency of the Republic of Turkey, have brought important suggestions for having secure configurations, they are considered to be technically insufficient. The number of hardening measures, which are mainly considered for Linux and Windows operating systems, are incomplete and insufficient when compared to the Center for Internet Security (CIS) Benchmark documents. Moreover, although there are various suggestions under the heading of General Tightening Measures, it cannot be said that sufficient tightening has been achieved in many products and applications such as network devices, databases, web servers, virtualization systems, e-mail servers and internet browsers. The research conducted by the CIS institution (Source 1) reveals the importance of tightening measures in cyber security. We recommend that the security tightening measure be deepened and regulated to cover all information systems.

2. Endpoint Detection and Response (EDR) product group is of critical importance in the field of cyber security. For this reason, it became mandatory for American government institutions on October 8, 2021, with the memorandum numbered M-22-01 (Source 2) published by the United States Presidential Executive Office. With developing technology, EDR products have evolved into eXtended Detection and Response (XDR) products. We recommend making these technologies mandatory to prevent advanced threats.

3. Zero trust architecture is increasing its dominance in the field of cybersecurity. With the NIST SP 800-207 Zero Trust Architecture (Source 3) document published in 2020 and the Federal Zero Trust Strategy memorandum numbered M-22-09 (Source 4) published by the US Presidential Administration Office in 2022, zero trust in government institutions and related private companies was introduced. architecture has become mandatory. We recommend that the Information and Communication Security Guide published by the Presidential Digital Transformation Office evolve towards zero trust principles.

TR Cybersecurity Alliance Members Contributing to the Study:

Ahmet Özkan
Ahmet Öztoprak
Ali Tursun
Alper Şulan
Caner Dağlı
Cem Dursun
Cengiz Keskin
Cihan Yüceer
Çağrı Güven
Deniz Şener
Ekrem Kolday
Erhan Güleyüpoğlu
Ferhat Arpacı
Gökhan Ilgıt
Gürsel Arıcı
Kayıhan Altınöz
Mehmet Karadeniz
Metin Eser
Murat Zaralı
Nedim Kaya
Nusret Karakaya
Ömer Çuhadaroğlu
Özgür Orhan
Serkan Akcan
Serkan Kırmızıgül
Tonyukuk Özden
Tuncay Arslan
Yusuf Usta

Resource 1: https://www.cisecurity.org/insights/blog/cyber-attack-defense-cis-benchmarks-cdm-mitre-attck
Resource 2: https://www.whitehouse.gov/wp-content/uploads/2021/10/M-22-01.pdf
Resource 3: https://csrc.nist.gov/pubs/sp/800/207/final
Resource 4: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf