TR Cybersecurity Alliance Started Its Activities

In the last quarter of 2023, Turkey's leading cyber security professionals joined forces and established a cyber security alliance called TR Cybersecurity Alliance. The alliance, which held its first meeting at the Radisson Blu Ataşehir hotel, aims to carry out studies that will support increasing Turkey's cyber resilience.

What is TR Cybersecurity Alliance?

TR Cybersecurity Alliance is a workshop group established with the initiative of well-known industry professionals working in various sectors of Turkey and with an average of more than 15 years of cyber security experience. Detailed information about the alliance is available on the website and LinkedIn page.

Why Was It Established?

TR Cybersecurity Alliance was established to address Turkey's cybersecurity challenges, encourage information sharing, and adopt and source best practices in the industry. The Alliance aims to increase the sharing of knowledge and experience within the community, working together to effectively combat cyber threats.

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 encouraging innovation and research
- Increasing effective communication and collaboration between professionals in the industry
- Increasing awareness about cyber security in the public and private sectors

Who Does It Consist Of?

TR Cybersecurity Alliance brings together IT gurus of important finance, energy, insurance and e-commerce organizations in Turkey and experts from important manufacturers in the field of cyber security. The Alliance aims to have its members come from various areas of expertise and to interact with each other to create a strong knowledge pool.

What is the Working Order?

TR Cybersecurity Alliance increases interaction among its members by organizing regular meetings and workshops at least every quarter. The purpose of these events 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 - www.linkedin.com/company/tr-cybersecurity-alliance

Who Does It Consist Of?

TR Cybersecurity Alliance was established with the participation of cyber security experts from important institutions and organizations in Turkey such as finance, public, energy, telecom, logistics, insurance and e-commerce. It is also supported by important domestic and foreign cyber security companies such as Nebula, Binalyze, Picus, SecHard and Trellix.

TR CYBERSECURITY ALLIANCE

Members


Ahmet Özkan


Ahmet Öztoprak


Akın Börekçi


Ali Tursun


Alper Şulan


Alvaro Garcia


Ayed Al Qartah


Caner Dağlı


Cem Dursun


Cengiz Keskin


Cihan Yücer


Deniz Şener


Erhan Güleyüpoğlu


Ferhat Arpacı


Gürsel Arıcı


İlker Çağrı Güven


Kayıhan Altınoz


Metin Eser


Murat Zaralı


Nedim Kaya


Nusret Karakaya


Ömer Çuhadaroğlu


Özgür Orhan


Savaş Ergen


Serkan Akcan


Serkan Kırmızıgül


Tonyukuk Özden


Tuncay Arslan


Yusuf Usta

TR CYBERSECURITY ALLIANCE

10 Best Practices in Malware Protection

ENTRANCE

Founded by Turkey's leading cyber security experts, TR Cybersecurity Alliance aims to strengthen the cyber security of companies and public institutions by determining the best practices in the field of cyber security together with its members. This Best Practice document, which emerged as a result of the workshop, includes the basic principles of malware protection and is designed to guide organizations to increase their cyber resilience.

10 Best Practices in Malware Protection

1. Asset Management

The first step to be taken in every field of cyber security is the management of digital assets. With asset management tools that have discovery features, all assets that are in the information system or will be added to the system in the future should be detected, and the necessary security audits and applications should preferably be carried out automatically.

2. User Training and Simulation

The addressees of all IT assets are their users, and cyber security can only be as strong as the level of awareness of the users. Beyond all kinds of regulations and standards, users should be provided with extensive and frequent training, and their level of awareness should be tested with tools such as phishing simulators.

3. Using Endpoint Protection Platform (EPP) and Endpoint Detection and Response (EDR)

Faced with today's cyber security realities, all organizations should use Endpoint Protection Platform (EPP) and Endpoint Detection and Response (EDR) solutions. These technologies are effective methods of detecting and blocking malware. Depending on the technical specifications of the preferred products, the correct operation of the services should be constantly tested with a predetermined program or method.

4. Sandbox Solutions

Sandbox solutions that can work in different vectors such as e-mail, file and network are deployed against Advanced Persistent Threat (APT) attacks. This provides more effective protection against various attack methods. Content Disarm & Reconstruction (CDR) tools provide significant assistance in ensuring data hygiene and increase zero-day protection capability.

5. Security Tightenings

According to Center for Internet Security (CIS) Windows 10 Benchmark analyses, applying security hardening allows blocking malware by an average of 70% without the need for another security tool. Institutions and organizations must implement and constantly update security tightening in accordance with CIS Benchmark standards. For technologies that are not supported by authorities, customized hardening templates should be produced and applied.

6. Application Control Software

Application Control software increases the security of computer systems by allowing only designated applications to run. Therefore, institutions and organizations should use such software effectively.

7. Table Top Exercises

Institutions should conduct desktop exercises that simulate cyber attack scenarios at a frequency appropriate to the risk level and not less than twice a year.

8. Malware Attack Simulations

Whether the cyber security system is working properly or not should be tested at routine intervals by using Breach and Attack Simulation (BAS) tools. The intervals that should be determined according to the risk level should be between once a week or at least four times a year.

9. Incident Response and Computer Forensics Planning

Since it is not possible to completely prevent cyber attacks, institutions must create Incident Response Plans. Incident response teams must be able to quickly detect suspicious activity and initiate corrective and preventive actions. Research and analysis should be conducted after digital evidence has been collected quickly and precisely. After this entire process is completed and threats are evaluated, improvement actions should be taken in a timely manner in the light of the resulting report.

10. Cyber Security Trainings

Cybersecurity teams should attend regular training programs that cover emerging threats, the latest attack vectors, and advances in security technologies. Must undertake hands-on training sessions and workshops to increase practical expertise. It is also important to have industry-recognized certifications to increase and expand skill.

Resources and Regulations Used During the Workshop

- Center for Internet Security (CIS) Benchmarks
www.cisecurity.org/cis-benchmarks
- T.R. Presidential Digital Transformation Office – Information and Communication Security Guide
www.cbddo.gov.tr/bigrehber/
- MITRE Attack Framework
www.attack.mitre.org/
- CISA (Cybersecurity & Infrastructure Security Agency)
www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware

Glossary of Terms Used in the Document

Advanced Persistent Threat: It is a complex and long-lasting cyber attack in which attackers use targeted and covert techniques to gain unauthorized access to a network, maintain persistence, and exfiltrate sensitive information over a long period of time, often for espionage or data purposes.

Application Control / Whitelisting: It is a cybersecurity measure that regulates and monitors the execution of applications on endpoints, allowing only authorized programs to run and preventing unauthorized or malicious programs, thereby increasing overall security by minimizing the attack surface and potential risks.

Asset Management: It is the systematic identification and ongoing monitoring of an organization's hardware, software, and network assets to provide an accurate inventory, assess vulnerabilities, and implement effective security measures to protect against potential threats and breaches.

Breach and Attack Simulation: It is a proactive cybersecurity technique that involves simulating real-world cyber attacks on an organization's systems to evaluate and verify the effectiveness of security controls, identify vulnerabilities, improve incident response capabilities, and ultimately increase the overall resilience of the organization.

Center for Internet Security (CIS): It is a non-profit organization that promotes best security practices in the field of information technology, develops standards accordingly, and focuses on increasing cyber security.

CIS Benchmark: It is a set of security standards and recommendations created by the Center for Internet Security (CIS). These guidelines establish industry standards and best practices for improving the security of computer systems and networks.

Compromise Assessment: It is a cybersecurity application that systematically evaluates an organization's network, systems, and endpoints to detect and evaluate any signs of a security breach or breach, leveraging advanced detection techniques and tools to analyze potential threats and increase overall threat visibility for proactive incident response .

Content Disarm & Reconstruction: It is a cybersecurity technology that fragments and restructures files, removing potential malicious elements while preserving the underlying content, thus reducing the risk of malware infection via email attachments or other file transfers.

Endpoint Detection and Response: It is a cybersecurity technology that monitors and analyzes endpoint activity in real time, providing rapid detection, investigation and response capabilities to identify and mitigate advanced threats, suspicious behavior and security incidents on an organization's network.

Endpoint Protection Platform: It is a comprehensive security solution designed to protect servers or endpoints from a variety of cyber threats, including malware, ransomware and unauthorized access, using advanced detection and prevention mechanisms.

Forensic Planning: It involves developing a comprehensive strategy for the systematic collection, analysis and preservation of digital evidence to investigate and understand security incidents or cybercrimes, ensuring the integrity and admissibility of the information for legal and investigative purposes.

Incident Response Plan: It is a structured set of written procedures that outlines the steps an organization should take in the event of a cybersecurity incident, providing a systematic and coordinated approach to detecting, responding to, mitigating and recovering from security breaches or cyberattacks.

Malware: Malware refers to types of malicious software designed to damage computer systems or users' data, gain unauthorized access or steal information.

Phising: It is a cyberattack technique in which attackers use deceptive emails, messages or websites to trick individuals into revealing sensitive information such as usernames, passwords or financial details, often posing as trusted organizations and misusing or compromising their personal or corporate identities.

Sandbox: It is a secure and isolated environment in which untrusted or potentially malicious software can be safely executed and analyzed, allowing cybersecurity professionals to evaluate their behavior without the risk of damaging the actual system or network.

Security Hardening: It is the systematic application of security measures, configurations, and best practices to strengthen the defenses of a system or network device, minimize vulnerabilities, and reduce the potential for cyber attack or unauthorized access.

Tabletop Exercises: It is a Tabletop exercise in simulating a real event for the purpose of implementing and testing an organization's crisis management or cybersecurity plans.

CONCLUSION

By following the recommendations in this Best Practice document, organizations can increase their cyber resilience and provide a more effective defense against malware threats. It should not be forgotten that the cyber security process requires continuity. Complying with the stated principles will increase cyber security levels and contribute to organizations operating in a safer environment.

Contributors to the Study

Ahmet Özkan
Ahmet Öztoprak
Ali Tursun
Alvaro Garcia
Ayed Al Qartah
Caner Dağlı
Cihan Yüceer
Çağrı Güven
Ferhat Arpacı
Gürsel Arıcı
Kayıhan Altınöz
Metin Eser
Nedim Kaya
Ömer Çuhadaroğlu
Özgür Orhan
Serkan Akcan
Serkan Kırmızıgül
Tuncay Aslan
Yusuf Usta