TR CYBERSECURITY ALLIANCE

10 Best Practices for Cyber Hygiene

INTRODUCTION

In today's rapidly advancing digital world, cyber threats pose significant risks not only to large organizations but also to individuals and small businesses. Cyber hygiene forms the foundation of preventive measures against these threats and plays a critical role in maintaining sustainable security.

This document was prepared as a result of the TR Cybersecurity Alliance workshop held on November 21, 2024, and outlines the top 10 methods for implementing cyber hygiene practices. Its aim is to guide everyone, from individuals to organizations, on how to manage and protect their digital assets more securely.

1. Identify and Manage Your Assets

The first step in cybersecurity is always asset management. Use methods that can automatically discover all devices in your system, including servers, clients, network devices, firewalls, databases, IoT devices, and unmanaged devices. Identify the business risks associated with your assets and monitor changes or incidents based on their risk levels.

2. Harden Your IT Systems

Apply security hardening to every asset in your IT system. Security hardening involves ensuring all assets are configured securely and monitoring their vulnerabilities to ensure timely patching. Use resources such as CIS Benchmarks for secure configurations.

3. Enforce Strong Password Policies and Use Password Vaults

Mandate strong and complex passwords for employees and system administrators. Passwords should be at least 12 characters long and include uppercase and lowercase letters, numbers, and symbols. Additionally, utilize password management and vault tools to maintain confidentiality and ensure periodic updates. Implement mechanisms to audit all access in compliance with these rules.

4. Implement Multi-Factor Authentication (MFA)

Wherever possible, enable multi-factor authentication (MFA) across all IT systems. MFA adds an additional layer of security to critical or publicly accessible systems beyond just passwords.

5. Encrypt Data

Unencrypted data is not secure. Encrypt critical and sensitive data, especially financial, personal, and healthcare information, both in storage and during transmission.

6. Backup Using the 3-2-1-0 Rule

Ensure reliable backups by adhering to the principle of at least 3 copies, stored on 2 different media, with 1 offline backup, and 0 faulty backups or restoration failures.

7. Use Basic Protection Tools

Implement security products such as firewalls, antivirus, EDR, Host IPS, Web Gateway, and Email Gateway to safeguard against cyberattacks. Regularly check their configurations and ensure they are up-to-date.

8. Conduct Training and Awareness Programs

Continuously educate company personnel on potential cyber threats and phishing attacks. Automate these processes using phishing simulators and training portals. Reward personnel with high awareness levels to encourage participation..

9. Perform Penetration Testing and Attack Simulations

Regularly conduct penetration testing and attack simulations to assess the quality of your cybersecurity system and identify potential vulnerabilities before actual attacks occur. These tests should be unexpected and conducted regularly without the knowledge of system administrators.

10. Develop a Cyber Incident Response Plan

It is impossible to eliminate cyber incidents entirely. To respond quickly and effectively to a cyberattack, create a cyber incident response plan that includes emergency procedures, communication methods, and clearly defined responsibilities. Conduct post-incident reviews to better prepare for future threats.

Cyber hygiene is a cornerstone of an effective cybersecurity strategy and begins with integrating security into daily habits. The 10 practices outlined in this document provide a strong defense mechanism against cyberattacks and guide the sustainable maintenance of organizational security.

As TR Cybersecurity Alliance, we will continue to share best practices to enhance security in the digital world and pursue our mission to raise awareness in this field. It should not be forgotten that cyber hygiene is not just an option but an indispensable necessity of the digital age.

Contributors to the Workshop

Ahmet Özkan
Ahmet Öztoprak
Ali Tursun
Alper Sulan
Asım Yıldız
Caner Dağlı
Deniz Şener
Ekrem Kolday
Gökhan Ilgıt
İlker Çağrı Güven
Kayıhan Altınöz
Murat Zaralı
Nusret Karakaya
Onur Mutlu İmamoğlu
Ömer Çuhadaroğlu
Özgür Orhan
Serkan Akcan
Tuncay Arslan