INTRODUCTION

The Essential Guide to Election Security

MATURITY

Maturities

Determining Your Maturity Level

Prioritizing Best Practices for the Level 1 maturity

Prioritizing Best Practices for the Level 2 and Level 3 maturities

BEST PRACTICES

Index of Best Practices

Addressing Physical Threats

Join the EI-ISAC

Asset Management

Encrypt Data at Rest

Encrypt Data in Transit

Managing Infrastructure with Secure Configurations

User Management

Backups

Incident Response Planning

Building and Managing Staff

Patching and Vulnerability Management

Remediate Penetration Test Findings

Perform Internal Penetration Test

v: latest

Glossary

NIST’s Computer Security Resource Center Glossary is a useful reference for information security terms, acronyms, and organizations.

authentication

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system

CIS Controls

A prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks

common vulnerabilities and exploits

The generic name for known cybersecurity vulnerabilities that have been catalogued by the CVE program. There is one CVE Record for each vulnerability in the catalog.

Community Defense Model

A set or real-world analyses used to design, prioritize, implement, and improve an enterprise’s cybersecurity program. See the CDM 2.0 release.

disinformation

Information deliberately created to mislead, harm, or manipulate a person, social group, organization, or country

domain name system

The system by which Internet domain names and addresses are tracked and regulated as defined by IETF RFC 1034 and other related RFCs.

encryption

Any procedure used in cryptography to convert plain text into cipher text to prevent anyone but the intended recipient from reading that data

endpoint detection and response

Security software that is deployed on workstations and servers, to collect technical data and analyze it for suspicious patterns and threats.

endpoint protection

Safeguards implemented through software to protect end-user machines such as workstations and laptops against attack (e.g., antivirus, antispyware, anti-adware, personal firewalls, host-based intrusion detection and prevention systems, etc.)

generative artificial intelligence

a technology that can create images, text, and videos with very little instruction from a user by learning patterns from very large datasets to predict the most likely response to a given prompt

hashing

The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data

Implementation Group

The recommended guidance to prioritize implementation of the CIS Critical Security Controls (CIS Controls). They are based on the risk profile and resources an enterprise has available to them to implement the CIS Controls.

malinformation

Information based on fact, but used out of context to mislead, harm, or manipulate

malicious domain blocking and reporting

Technology that prevents IT systems from connecting to harmful web domains, helping limit infections related to known malware, ransomware, phishing, and other cyber threats

malware

Malware is malicious software or software designed to perform malicious actions on a device. It can be introduced to a system in various forms, such as emails or malicious websites.

misinformation

Information that is false but not created or shared with the intention of causing harm

multi-factor authentication

An authentication system that requires more than one distinct authentication factor for successful authentication. Multi-factor authentication can be performed using a multi-factor authenticator or by a combination of authenticators that provide different factors. The three authentication factors are something you know, something you have, and something you are.

patching

The act of applying a change to installed software – such as firmware, operating systems, or applications – that corrects security or functionality problems or adds new capabilities

ransomware

A type of malware that blocks access to a system, device, or file until a ransom is paid

salting

A non-secret value used in a cryptographic process, usually to ensure that the results of computations for one instance cannot be reused by an attacker

virtual private network

Protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line

Previous
Election Results Reporting and Publishing

Next
Acronyms

Made with Sphinx and @pradyunsg's Furo
Last updated on Mar 13, 2024