DIGIFENCE
TECHNOLOGY

27/4 Azatutyan Avenue
Yerevan 0014 Armenia
(374) 11 48 48 48
/digifence.tech
info@digifence.am
www.digifence.tech

Foundational Cybersecurity Level

▼ CONTROL 07

Email and Web Browser Protections

OBJECTIVE

Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and email systems.

IMPORTANCE

Web browsers and email clients are very common points of entry and attack because of their technical complexity, flexibility, and their direct interaction with users and with the other systems and websites. Content can be crafted to entice or spoof users into taking actions that greatly increase risk and allow introduction of malicious code, loss of valuable data, and other attacks. Since these applications are the main means that users interact with untrusted environments, these are potential targets for both code exploitation and social engineering.

▼ CONTROL 08

Malware Defenses

OBJECTIVE

Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

IMPORTANCE

Malicious software is an integral and dangerous aspect of internet threats, as it is designed to attack your systems, devices, and your data. It is fast-moving, fast-changing, and enter through any number of points like end-user devices, email attachments, web pages, cloud services, user actions, and removable media. Modern malware is designed to avoid defenses, and attack or disable them.

Malware defenses must be able to operate in this dynamic environment through large-scale automation, rapid updating, and integration with processes like incident response. They must also be deployed at multiple possible points of attack to detect, stop the movement of, or control the execution of malicious software. Enterprise endpoint security suites provide administrative features to verify that all defenses are active and current on every managed system.

▼ CONTROL 09

Limitation and Control of Network Ports, Protocols, and Services

OBJECTIVE

Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

IMPORTANCE

Attackers search for remotely accessible network services that are vulnerable to exploitation. Common examples include poorly configured web servers, mail servers, file and print services, and Domain Name System (DNS) servers installed by default on a variety of different device types, often without a business need for the given service. Many software packages automatically install services and turn them on as part of the installation of the main software package without informing a user or administrator that the services have been enabled. Attackers scan for such services and attempt to exploit these services, often attempting to exploit default user IDs and passwords or widely available exploitation code.

▼ CONTROL 10

Data Recovery Capabilities

OBJECTIVE

Manage the processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

IMPORTANCE

When attackers compromise machines, they often make significant changes to configurations and software. Sometimes attackers also make subtle alterations of data stored on compromised machines, potentially jeopardizing organizational effectiveness with polluted information. When the attackers are discovered, it can be extremely difficult for organizations without a trustworthy data recovery capability to remove all aspects of the attacker's presence on the machine.

▼ CONTROL 11

Secure Configuration of Network Devices and Ports

OBJECTIVE

Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

IMPORTANCE

As delivered from manufacturers and resellers, the default configurations for network infrastructure devices are geared for ease-of-deployment and ease-of-use – not security. Open services and ports, default accounts (including service accounts) or passwords, support for older (vulnerable) protocols, pre-installation of unneeded software; all can be exploitable in their default state. The management of the secure configurations for networking devices is not a one-time event, but a process that involves regularly reevaluating not only the configuration items but also the allowed traffic flows. Attackers take advantage of network devices becoming less securely configured over time as users demand exceptions for specific business needs. Sometimes the exceptions are deployed and then left undone when they are no longer applicable to the business needs. In some cases, the security risk of the exception is neither properly analyzed nor measured against the associated business need and can change over time. Attackers search for vulnerable default settings, gaps or inconsistencies in firewall rule sets, routers, and switches and use those holes to penetrate defenses. They exploit flaws in these devices to gain access to networks, redirect traffic on a network, and intercept information while in transmission. Through such actions, the attacker gains access to sensitive data, alters important information, or even uses a compromised machine to pose as another trusted system on the network.

▼ CONTROL 12
Boundary Defense

OBJECTIVE

Detect/prevent/correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

IMPORTANCE

Attackers focus on exploiting systems that they can reach across the internet, including not only DMZ systems but also workstations and laptop computers that pull content from the Internet through network boundaries. Threats such as organized crime groups and nation-states use configuration and architectural weaknesses found on perimeter systems, network devices, and Internet-accessing client machines to gain initial access into an organization. Then, with a base of operations on these machines, attackers often pivot to get deeper inside the boundary to steal or change information or to set up a persistent presence for later attacks against internal hosts. Additionally, many attacks occur between business partner networks, sometimes referred to as extranets, as attackers hop from one organization's network to another, exploiting vulnerable systems on extranet perimeters.

To control the flow of traffic through network borders and police content by looking for attacks and evidence of compromised machines, boundary defenses should be multilayered, relying on firewalls, proxies, DMZ perimeter networks, and network-based IPS and IDS. It is also critical to filter both inbound and outbound traffic.

It should be noted that boundary lines between internal and external networks are diminishing as a result of increased interconnectivity within and between organizations as well as the rapid rise in deployment of wireless technologies. These blurring lines sometimes allow attackers to gain access inside networks while bypassing boundary systems. However, even with this blurring of boundaries, effective security deployments still rely on carefully configured boundary defenses that separate networks with different threat levels, sets of users, data and levels of control. And despite the blurring of internal and external networks, effective multilayered defenses of perimeter networks help lower the number of successful attacks, allowing security personnel to focus on attackers who have devised methods to bypass boundary restrictions.

▼ CONTROL 13
Data Protection

OBJECTIVE

Manage the processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

IMPORTANCE

Data resides in many places. Protection of that data is best achieved through the application of a combination of encryption, integrity protection and data loss prevention techniques. As organizations continue their move towards cloud computing and mobile access, it is important that proper care be taken to limit and report on data exfiltration while also mitigating the effects of data compromise.

Some organizations do not carefully identify and separate their most sensitive and critical assets from less sensitive, publicly accessible information on their internal networks. In many environments, internal users have access to all or most of the critical assets. Sensitive assets may also include systems that provide management and control of physical systems (e.g., SCADA). Once attackers have penetrated such a network, they can easily find and exfiltrate important information, cause physical damage, or disrupt operations with little resistance. For example, in several high-profile breaches over the past two years, attackers were able to gain access to sensitive data stored on the same servers with the same level of access as far less important data. There are also examples of using access to the corporate network to gain access to, then control over, physical assets and cause damage.

▼ CONTROL 14

Controlled Access Based on the Need to Know

OBJECTIVE

Manage the processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

IMPORTANCE

Encrypting data provides a level of assurance that even if data is compromised, it is impractical to access the plaintext without significant resources; however, controls should also be put in place to mitigate the threat of data exfiltration in the first place. Many attacks occurred across the network, while others involved physical theft of laptops and other equipment holding sensitive information. Yet, in many cases, the victims were not aware that the sensitive data were leaving their systems because they were not monitoring data outflows. The movement of data across network boundaries both electronically and physically must be carefully scrutinized to minimize its exposure to attackers.

The loss of control over protected or sensitive data by organizations is a serious threat to business operations and a potential threat to national security. While some data are leaked or lost as a result of theft or espionage, the vast majority of these problems result from poorly understood data practices, a lack of effective policy architectures, and user error. Data loss can even occur as a result of legitimate activities such as e-Discovery during litigation, particularly when records retention practices are ineffective or nonexistent.

The adoption of data encryption, both in transit and at rest, provides mitigation against data compromise. This is true if proper care has been taken in the processes and technologies associated with the encryption operations. An example of this is the management of cryptographic keys used by the various algorithms that protect data. The process for generation, use and destruction of keys should be based on proven processes as defined in standards such as NIST SP 800-57.

Care should also be taken to ensure that products used within an enterprise implement well known and vetted cryptographic algorithms, as identified by NIST. Reevaluation of the algorithms and key sizes used within the enterprise on an annual basis is also recommended to ensure that organizations are not falling behind in the strength of protection applied to their data. For organizations that are moving data to the cloud, it is important to understand the security controls applied to data in the cloud multi-tenant environment, and determine the best course of action for application of encryption controls and security of keys. When possible, keys should be stored within secure containers such as Hardware Security Modules (HSMs).

Data loss prevention (DLP) refers to a comprehensive approach covering people, processes, and systems that identify, monitor, and protect data in use (e.g., endpoint actions), data in motion (e.g., network actions), and data at rest (e.g., data storage) through deep content inspection and with a centralized management framework. Over the last several years, there has been a noticeable shift in attention and investment from securing the network to securing systems within the network, and to securing the data itself. DLP controls are based on policy, and include classifying sensitive data, discovering that data across an enterprise, enforcing controls, and reporting and auditing to ensure policy compliance.

▼ CONTROL 15

Wireless Access Control

OBJECTIVE

Manage the processes and tools used to track/control/prevent/correct the security use of wireless local area networks (WLANs), access points, and wireless client systems.

IMPORTANCE

Major thefts of data have been initiated by attackers who have gained wireless access to organizations from outside the physical building, bypassing organizations' security perimeters by connecting wirelessly to access points inside the organization. Wireless clients accompanying travelers are infected on a regular basis through remote exploitation while on public wireless networks found in airports and cafes. Such exploited systems are then used as back doors when they are reconnected to the network of a target organization. Other organizations have reported the discovery of unauthorized wireless access points on their networks, planted and sometimes hidden for unrestricted access to an internal network. Because they do not require direct physical connections, wireless devices are a convenient vector for attackers to maintain long-term access into a target environment.

▼ CONTROL 16

Account Monitoring and Control

OBJECTIVE

Actively manage the life cycle of system and application accounts - their creation, use, dormancy, deletion - in order to minimize opportunities for attackers to leverage them.

IMPORTANCE

Attackers frequently discover and exploit legitimate but inactive user accounts to impersonate legitimate users, thereby making discovery of attacker behavior difficult for security personnel watchers. Accounts of contractors and employees who have been terminated and accounts formerly set up for Red Team testing (but not deleted afterwards) have often been misused in this way. Additionally, some malicious insiders or former employees have gained access to accounts left behind in a system long after contract expiration, maintaining their access to an organization's computing system and sensitive data for unauthorized and sometimes malicious purposes.