7 Elements of an Effective Defense in Depth (DiD) Security Strategy

How to Strengthen Your IT Environment With Layers of Protection

CASTLE LABS

Contents

What is Defense in Depth (DiD)?

The current threat landscape has advanced to a level where multiple, advanced attack vectors are waiting to exploit vulnerabilities within applications, interfaces, networks, devices, traffic and users to damage businesses. Relying on one basic security solution will therefore prove to be futile against sophisticated attack vectors. This is where an approach like **Defense in Depth (DiD)** finds its relevance.

The National Institute of Standards and Technology (NIST) defines DiD as "The application of multiple countermeasures in a layered or stepwise manner to achieve security objectives. The methodology involves layering heterogeneous security technologies in the common attack vectors to ensure that attacks missed by one technology are caught by another."

In simple terms, **DiD is a cybersecurity approach in which multiple defensive methods are layered to protect an organization**. Since no individual security measure is guaranteed to endure every attack, combining several layers of security is more effective. This layering approach was first conceived by the National Security Agency (NSA) and is inspired by a military tactic of the same name. But in IT, the approach is intended to prevent an incident and not delay it as in the military.

Remember not to confuse DiD with another cybersecurity concept called layered security. While layered security uses different security products to address a particular security aspect, such as email filtering, DiD is more comprehensive and includes multiple security measures to address distinct threats related to the entire IT infrastructure.

4 STATISTICS THAT DEMONSTRATE THE NEED FOR DiD

Close to **35%** of businesses are unprepared for a data breach.[1]

Cybercrime shot up by over 300% since the start of the pandemic.[2]

Experts estimate that the frequency of ransomware attacks will increase in the coming years.[3]

Close to **30%** of SMBs experience a cyberattack at least once a week.[4]

Keep an Eye on These Threats

Remember that all businesses, irrespective of their size and industry, can fall prey to malicious attacks. Insufficient cybersecurity measures can provide a freeway for cybercriminals to exploit vulnerabilities within your business.

Listed below are 23 cybersecurity threats you should be aware of:

⚠ MALWARE

Malware (abbreviated from malicious software) is a generic term for viruses, trojans and other dangerous computer programs used by cybercriminals to severely damage an IT environment or gain access to business-critical data.

⚠ RANSOMWARE

Ransomware is a type of malware that threatens to disclose sensitive data or blocks access to files/systems, most of the time by encrypting it, until the victim pays a ransom amount within a stipulated deadline. Failure to pay on time can lead to data leaks or permanent data loss.

⚠ CREDENTIAL THEFT

Credential theft involves the unlawful acquisition of information that an individual or business will use to access websites and sensitive data. Credential theft lets hackers reset passwords, lock the victim's account, download private data, gain access to other endpoints within the network or even erase sensitive data and backups.

⚠ PHISHING/BUSINESS EMAIL COMPROMISE (BEC)

Phishing is a cybercrime that involves a hacker masquerading as a genuine person/organization primarily through emails or sometimes other channels like SMS. Malicious actors use phishing to deliver links or attachments that can execute actions such as extraction of login credentials or installation of malware. Business email compromise (BEC) is a scam where cybercriminals use compromised or impersonated email accounts to manipulate victims into transferring money or sharing sensitive information.

⚠ CLOUD JACKING

Cloud jacking or cloud hijacking is a type of attack wherein cybercriminals exploit cloud vulnerabilities to steal the information of an account holder in order to gain server access. With an increasing number of companies adopting cloud solutions since the pandemic hit, IT leaders are worried about cloud jacking becoming a severe concern for years to come.

⚠ INSIDER THREATS

An insider threat originates from within a business. It may happen because of a current or former employee, vendors or other business partners who have/had access to sensitive business data and computer systems. Because it originates from the inside and may or may not be premeditated, an insider threat is hard to detect.

⚠ DENIAL-OF-SERVICE/DISTRIBUTED DENIAL-OF-SERVICE (DOS AND DDOS)

These attacks are common and easy to implement. When DoS or DDoS attacks happen, hackers flood the targeted system with multiple data requests, causing it to slow down, crash or shut down.

⚠ MAN-IN-THE-MIDDLE (MITM) ATTACKS

A MITM attack is a type of cyberattack that takes place when an unauthorized entity breaks into a company's network and behaves as part of the network.

⚠ DOMAIN NAME SYSTEM (DNS) ATTACKS

A Domain Name System (DNS) attack is a threat in which the hacker exploits vulnerabilities in the DNS protocol. This is a significant problem in cybersecurity because DNS is a vital component of the IT infrastructure.

⚠ BOTNETS

Botnets are networks of hijacked, inter-connected devices that are manipulated for scams and cyberattacks. The bots usually serve as a tool for attacks such as server crashes and data theft.

⚠ CRYPTOJACKING

In this type of cyberattack, hackers use a victim's computing power to secretly and illegally mine cryptocurrency. Cryptojacking can target individual users, big enterprises and even industrial control systems (ICS).

⚠ CYBERESPIONAGE

This cyberattack aims at stealing classified data from a corporate house or the government for financial, political or competitive reasons.

⚠ ARTIFICIAL INTELLIGENCE (AI) AND MACHINE LEARNING (ML) HACKS

Artificial intelligence (AI) and machine learning (ML) are two trending topics within the IT world for their path-breaking applications. But remember that AI and ML help hackers be more efficient in developing an in-depth understanding of how businesses guard against cyberattacks.

⚠ INTERNET OF THINGS (IOT) RISKS AND TARGETED ATTACKS

IoT adoption is skyrocketing and experts project that the total number of installed IoT-connected devices worldwide will amount to 30.9 billion units by 2025.[5] However, data sharing with no human intervention and inadequate legislation has made IoT a favorite target of cybercriminals.

⚠ WEB APPLICATION ATTACKS

Vulnerabilities within web applications permit hackers to gain direct access to databases to manipulate sensitive data. Business databases are regular targets because they contain sensitive data, including Personally Identifiable Information (PII) and banking details.

⚠ ADVANCED PERSISTENT THREATS (APTS)

An advanced persistent threat (APT) is a sustained and sophisticated cyberattack in which a malicious actor gains access to a network and continues undetected for a prolonged duration. Most of the time, it aims at stealing data rather than damaging the IT environment.

⚠ SQL INJECTION

SQL injection is a code injection technique in which hackers place malicious code in SQL statements. This technique is capable of destroying a database.

⚠ ZERO-DAY EXPLOITS

Zero-day exploits are cyberattacks aimed at vulnerabilities that a software vendor has not yet fixed or patched. By exploiting such an unpatched vulnerability, these attacks have a significant chance of success and are tough to protect against by using outdated security tools.

⚠ SPYWARE

Spyware is software that, if installed on your computer, stealthily monitors your online behavior without consent. It can gather information about an individual or business and transfer that data to other parties.

⚠ IDENTITY THEFT AND SYNTHETIC IDENTITIES

Identity theft is a type of fraud in which a cybercriminal creates a fake account/profile similar to a genuine one in order to carry out scams like money laundering. Synthetic identity theft is a form of identity theft in which scammers combine real and fake information to create a new false identity.

⚠ SOFTWARE VULNERABILITY EXPLOITS

A software vulnerability is a flaw present within a software or in an operating system (OS). Almost all software will have vulnerabilities in one form or another that must be fixed before cybercriminals rush to exploit them.

⚠ DEEPFAKES

A deepfake is a cyberthreat that uses artificial intelligence to manipulate or generate audio/video content that can deceive end users into believing something untrue.

⚠ 5G EXPLOITS

The initial overlaying of 5G technology will be over the existing 4G LTE network. Because of this, there will be vulnerabilities that the new technology will inherit from its predecessor.

3 RECENT CYBERATTACKS IN THE NEWS

1

Colonial Pipeline, one of the largest pipeline systems for refined oil in the U.S., was hit by a severe cyberattack that disrupted fuel distribution to the East Coast.[6]

2

The Health Service Executive (HSE) from Ireland had to temporarily shut down its IT systems because of a cyberattack that took place during the pandemic.[7]

3

The data of over 4.5 million people were exposed after an IT system hack on Indian national air carrier, Air India.[8]

Defend Against Threats by Implementing a DiD Strategy

DiD can be divided into three security control areas:

1. ADMINISTRATIVE CONTROLS

The policies and procedures of a business come under administrative controls. This ensures that there is appropriate guidance available and adhered to with regard to security. Examples include hiring practices or employee onboarding protocols, data processing and management procedures, information security policies, vendor risk management and third-party risk management frameworks, information risk management strategies, etc.

2. TECHNICAL CONTROLS

Hardware or software intended to protect systems and resources falls under technical controls. Examples of technical controls would be firewalls, configuration management, disk/data encryption, identity authentication (IAM), vulnerability scanners, patch management, virtual private networks (VPNs), intrusion detection systems (IDS), security awareness training, etc.

3. PHYSICAL CONTROLS

Anything aimed at physically limiting or preventing access to IT systems falls under physical controls. Examples are fences, keycards/badges, CCTV systems, locker rooms, trained guard dogs, etc.

7 Essential Elements of DiD

Mentioned below are the seven elements that must be a part of every good DiD strategy:

1. FIREWALLS

A firewall is a security system comprising hardware or software that can protect your network by filtering out unnecessary traffic and blocking unauthorized access to your data. Other than blocking unwanted traffic, firewalls can also prevent malicious software from infecting your network. Firewalls can provide various levels of protection, so you must select the level of protection your business needs.

2. INTRUSION PREVENTION AND DETECTION SYSTEMS

An Intrusion Prevention and Detection System monitors network traffic, evaluates it and provides resolution whenever malicious behavior is detected. It scans the network to see if anything is out of place. If a threatening activity is detected, it will alert the stakeholders and block attacks.

3. ENDPOINT DETECTION AND RESPONSE (EDR)

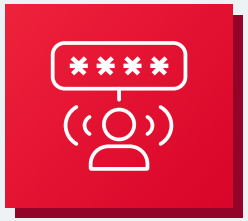
Endpoint Detection and Response (EDR) solutions operate by constantly monitoring endpoints to find suspicious or malicious behavior in real time. It is effective against internal and external attacks and is powered by innovative technologies such as machine learning.

4. NETWORK SEGMENTATION

Once you divide your business' network into smaller units, you can monitor data traffic between segments and safeguard segments from one another. Additionally, by automating the process, you can restrict unauthorized entities from accessing vital information.

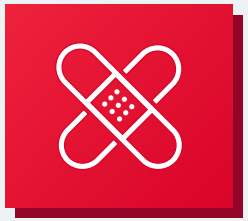
5. THE PRINCIPLE OF LEAST PRIVILEGE (POLP)

The principle of least privilege (PoLP) is a cybersecurity concept in which a user is only granted the minimum levels of access/permissions essential to perform their task. PoLP is considered an information security best practice to protect privileged access to business-sensitive data and assets.



6. STRONG PASSWORDS

Poor password hygiene, including the use of default passwords like "1234" or "admin" can put your business at risk. Equally risky is the habit of using the same passwords for multiple accounts. Therefore, it is essential to have strong passwords and an added layer of protection by using practices such as multifactor authentication (MFA).



7. PATCH MANAGEMENT

Security gaps left unattended due to poor patch management can make your business vulnerable to cyberattacks. As soon as a new patch gets delivered, you must deploy it without delay. Failing to do so could provide a freeway for hackers to exploit.

Address Vendor & Contractor Risks

Third-party and fourth-party vendors/contractors can put your business at risk. Case in point, in 2020, a breach at General Electric (GE) exposed about 200,000 records that included Personal Health Information (PHI). The hackers gained access to the records through a contractor.[9] Furthermore, multiple companies, such as SpaceX, Boeing, Tesla and Lockheed Martin, suffered a breach that originated through a parts vendor.[9]

These are just a few publicized cases; there could be hundreds of cases that go unreported. **Always remember that plugging third-party and fourth-party vendor/contractor risks is vital for the success of your DiD strategy.** Therefore, it is crucial to choose vendors that are committed to delivering best-in-class security. While no system is 100% secure, some vendors demonstrate a superior commitment to excellence in security matters compared to others.

Here are some security questions you must ask a potential vendor:

Does the vendor have necessary security measures in place?

This helps you check if the vendor can meet all of your security expectations and needs. Find out if they run regular vulnerability scans, do timely system updates, etc., as per your requirement.

Does the vendor have all the required security certifications?

The vendor must provide certifications to prove compliance with the industry's security standards.

How and where does the vendor store your data?

This is a crucial question because it helps you determine whether the vendor will handle your data carefully.

What happens to your data once the partnership ends?

You must know what happens once the contract ends and you choose not to continue with the vendor.

Will any other parties access your data?

Just like you're outsourcing a few tasks to a third-party vendor, they may in turn be outsourcing some tasks to a fourth-party vendor. It's vital that you know what they share.

Does the vendor have a business continuity and disaster recovery (BCDR) plan?

You have the right to know if your vendor has a BCDR strategy in place to withstand a disaster.

Does the vendor have cyber liability insurance?

This helps you know if your vendor can pay you for damages in a worst-case scenario.

Get Up and Running With DiD

If you have read this far, chances are you want to ramp up your security posture in a manner that makes it especially hard for multiple threats to break through. By now, you know that a Defense in Depth (DiD) strategy is what your business needs.

If you're wondering about where and how to begin, don't worry. By collaborating with a partner like us, and with our vast expertise in cybersecurity matters, you can build a secure fortress around your business' IT infrastructure.

Castle Labs: Security!

Get started today. Contact us for a consultation to learn the next steps to implementing or updating a DiD security strategy for your business.

www.castlelabs.com || (919) 598.6464 || info@castlelabs.com

CASTLE LABS

Sources:

1. Security Magazine
2. FBI Report
3. Cybersecurity Ventures
4. Info Security Magazine
5. Statista
6. NBC News
7. BBC News
8. SKY News
9. Dark Reading

Castle Labs
Box 133
Cary, NC 27512
(919) 598.6464
info@castlelabs.com
www.castlelabs.com

CASTLE LABS