Data center security

Data center security is the set of policies, precautions and practices adopted to avoid unauthorized access and manipulation of a data center's resources.[1] The data center houses the enterprise applications and data, hence why providing a proper security system is critical. Denial of service (DoS), theft of confidential information, data alteration, and data loss are some of the common security problems afflicting data center environments.[2]

Contents

Overview

According to the *Cost of a Data Breach Survey*,[3] in which 49 U.S. companies in 14 different industry sectors participated, they noticed that:

- 39% of companies say negligence was the primary cause of data breaches
- Malicious or criminal attacks account for 37 percent of total breaches.
- The average cost of a breach is $5.5 million.

The need for a secure data center

Physical security is needed to protect the value of the hardware therein.[4]

Data protection

The cost of a breach of security can have severe consequences on both the company managing the data center and on the customers whose data are copied. The 2012 breach at Global Payments, a processing vendor for Visa, where 1.5 million credit card numbers were stolen, highlights the risks of storing and managing valuable and confidential data.[5] As a result, Global Payments' partnership with Visa was terminated;[6] it was estimated that they lost over $100 million.

Insider attacks

Defenses against exploitable software vulnerabilities are often built on the assumption that "insiders" can be trusted.[7] Studies show that internal attacks tend to be more damaging because of the variety and amount of information available inside organizations.

Vulnerabilities and common attacks

The quantity of data stored in data centers has increased, partly due to the concentrations created by cloud-computing[3]

Threats

Some of the most common threats to Data Centers:

- DoS (Denial of Service)
- Data theft or alteration
- Unauthorized use of computing resources
- Identity theft

Vulnerabilities

Common vulnerabilities include:

- *Implementation*: Software design and protocol flaws, coding errors, and incomplete testing
- *Configuration*: Use of defaults, elements inappropriately configured

Exploitation of out-of-date software

Many "worm" attacks on data centers exploited well-known vulnerabilities:

- CodeRed[8]
- Nimda[9] and
- SQL Slammer[10]

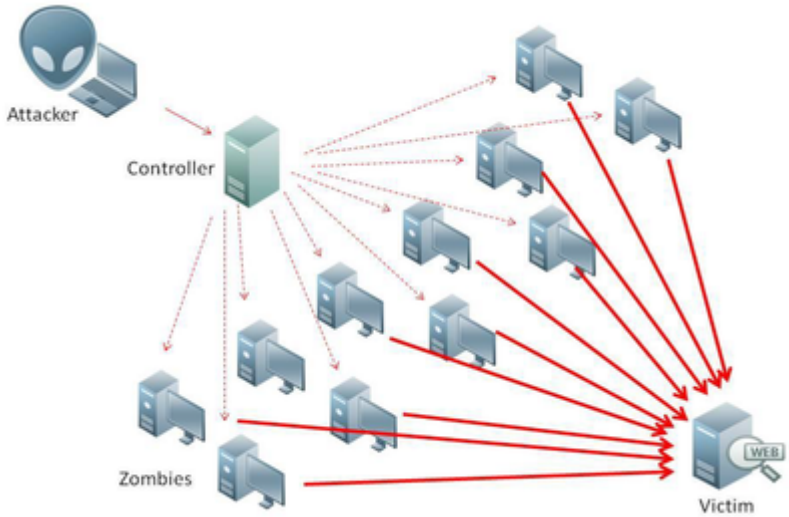
Exploitation of software defaults

Many systems are shipped with default accounts and passwords, which are exploited for unauthorized access and theft of information.

Common attacks

Common attacks include:

- *Scanning or Probing*: One example of a probe- or scan-based attack is a *port scan* - whereby "requests to a range of server port addresses on a host" are used, to find "an active port" and then cause harm via "a known vulnerability of that service.".[11][12] This reconnaissance activity often precedes an attack; its goal is to gain access by discovering information about a system or network.
- *DoS (Denial of service)*: A denial-of-service attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor.[13] This type of attack generates a large volume of data to deliberately consume limited resources such as bandwidth, CPU cycles, and memory blocks.
- *Distributed Denial of Service (DDoS)*: This kind of attack is a particular case of DoS where a large number of systems are compromised and used as source or traffic on a synchronized attack. In this kind of attack, the hacker does not use only one IP address but thousands of them.[14]



- *Unauthorized Access*: When someone other than an account owner uses privileges associated to a compromised account to access to restricted resources using a valid account or a backdoor.[15]
- *Eavesdropping*: Etymologically, *Eavesdropping* means Secretly listen to a conversation.[16] In the networking field, it is an unauthorized interception of information (usernames, passwords) that travels on the network. User logons are the most common signals sought.
- *Viruses and Worms*: These are malicious code that, when executed produce undesired results. Worms are self-replicating malware,[17] whereas viruses, which also can replicate, need some kind of human action to cause damage.[18]
- *Internet Infrastructure Attacks*: This kind of attack targets the critical components of the Internet infrastructure rather than individual systems or networks.
- *Trust Exploitation*: These attacks exploit the trust relationships that computer systems have to communicate.
- *Session Hijacking* also known as *cookie hijacking*: Consists of stealing a legitimate session established between a target and a trusted host. The attacker intercepts the session and

makes the target believe it is communicating with the trusted host.[19]

- *Buffer Overflow Attacks*: When a program allocates memory buffer space beyond what it had reserved, it results in memory corruption affecting the data stored in the memory areas that were overflowed.[20]
- *Layer 2 Attacks*: This type of attack exploit the vulnerabilities of data link layer protocols and their implementations on layer 2 switching platforms.
- *SQL injection*: Also known as code injection, this is where input to a data-entry form's, due to incomplete data validation, allows entering harmful input that causes harmful instructions to be executed.[21]

Network security infrastructure

The network security infrastructure includes the security tools used in data centers to enforce security policies. The tools include packet-filtering technologies such as ACLs, firewalls and intrusion detection systems (IDSs) both network-based and host-based.

ACLs (Access Control List)

ACLs are filtering mechanisms explicitly defined based on packet header information to permit or deny traffic on specific interfaces. ACLs are used in multiple locations within the Data Center such as the Internet Edge and the intranet server farm. The following describes standard and extended access lists:

Standard ACLs: the simplest type of ACL filtering traffic solely based on source IP addresses. Standard ACLs are typically deployed to control access to network devices for network management or remote access. For example, one can configure a standard ACL in a router to specify which systems are allowed to Telnet to it. Standard ACLs are not recommended option for traffic filtering due to their lack of granularity. Standard ACLSs are configured with a number between 1 and 99 in Cisco routers.

Extended ACLs: Extended ACL filtering decisions are based on the source and destination IP addresses, Layer 4 protocols, Layer 4 ports, ICMP message type and code, type of service, and precedence. In Cisco routers, one can define extended ACLs by name or by a number in the 100 to 199 range.[2]

Firewalls

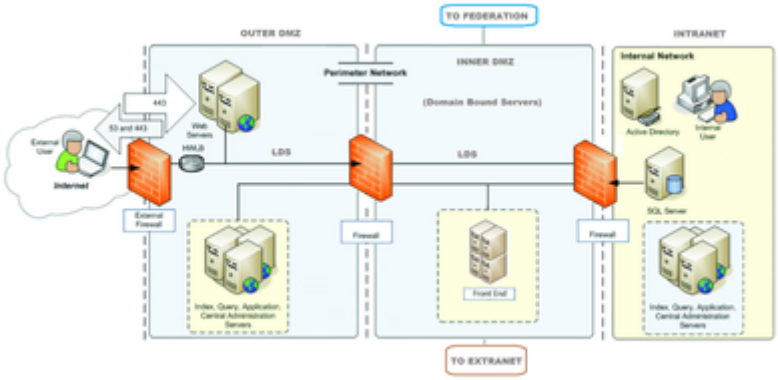
A firewall is a sophisticated filtering device that separates LAN segments, giving each segment a different security level and establishing a security perimeter that controls the traffic flow between segments. Firewalls are most commonly deployed at the Internet Edge where they act as boundary to the internal networks. They are expected to have the following characteristics:

Performance: the main goal of a firewall is to separate the secured and the unsecured areas of a network. Firewalls are then post in the primary traffic path potentially exposed to large volumes of data. Hence, performance becomes a natural design factor to ensure that the firewall meets the particular requirements.

Application support: Another important aspect is the ability of a firewall to control and protect a particular application or protocol, such as Telnet, FTP, and HTTP. The firewall is expected to understand application-level packet exchanges to determine whether packets do follow the application behavior and, if they do not, do deny the traffic.

There are different types of firewalls based on their packet-processing capabilities and their awareness of application-level information:

1. Packet-filtering firewalls
2. Proxy firewalls
3. Stateful firewalls
4. Hybrid firewalls[2]



IDSs

IDSs are real-time systems that can detect intruders and suspicious activities and report them to a monitoring system. They are configured to block or mitigate intrusions in progress and eventually immunize the systems from future attacks. They have two fundamental components:

- Sensors: Appliances and software agents that analyze the traffic on the network or the resource usage on end systems to identify intrusions and suspicious activities.
- IDS management: Single- or multi-device system used to configure and administer sensors and to additionally collect all the alarm information generated by the sensors. The sensors are equivalent to surveillance tools, and IDS management is the control center watching the information produced by the surveillance tools.[2]

Layer 2 security

Cisco Layer 2 switches provide tools to prevent the common Layer 2 attacks (Scanning or Probing, DoS, DDoS, etc.). The following are some security features covered by the **Layer 2 Security**:

- Port Security
- ARP Inspection
- Private VLANs
- Private VLANs and Firewalls

Data center security measures

The process of securing a Data Center requires both a comprehensive system-analysis approach and an ongoing process that improves the security levels as the Data Center evolves. The Data Center is constantly evolving as new applications or services become available. Attacks are becoming more sophisticated and more frequent. These trends require a steady evaluation of security readiness.

A key component of the security-readiness evaluation is the policies that govern the application of security in the network including the Data Center. The application includes both the design best practices and the implementation details.[2] As a result, security is often considered as a key component of the main infrastructure requirement. Since a key responsibility of the data centers is to make sure of the availability of the services, data center management systems often consider how its security affects traffic flows, failures, and scalability. Due to the fact that security measures may vary depending on the data center design, the use of unique features, compliance requirements or the company's business goals, there is no set of specific measures that cover all possible scenarios.[22]

There exist in general two types of data center security: the Physical Security and the Virtual Security.[23]

Physical Security

The physical security of a data center is the set of protocol built-in within the data center facilities in order to prevent any physical damage to the machines storing the data. Those protocols should be able to handle everything ranging from natural disasters to corporate espionage to terrorist attacks.[24]

To prevent physical attacks, data centers use techniques such as:

- CCTV security network: locations and access points with 90-day video retention.[25]
- 24×7
  - on-site security guards,
  - Network operations center (NOC) Services and technical team
- Anti-tailgating/Anti-pass-back turnstile gate. Only permits one person to pass through after authentication.
- Single entry point into co-location facility.
- Minimization of traffic through dedicated data halls, suites, and cages.
- Further access restriction to private cages
- Three-factor authentication
- SSAE 16 compliant facilities.
- Checking the provenance and design of hardware in use
- Reducing insider risk by monitoring activities and keeping their credentials safe[26]
- Monitoring of temperature and humidity
- Fire prevention with zoned dry-pipe sprinkler
- Natural disaster risk-free locations[27]

Virtual Security

Virtual security is security measures put in place by the data centers to prevent remote unauthorized access that will affect the integrity, availability or confidentiality of data stored on servers.[28]

Virtual or network security is a hard task to handle as there exist many ways it could be attacked. The worst part of it is that it is evolving years after years. For instance, an attacker could decide to use a malware (or similar exploits) in order to bypass the various firewalls to access the data. Old systems may as well put security at risk as they do not contain modern methods of data security.[23]

Virtual attacks can be prevented with techniques such as

- Heavy data encryption during transfer or not: 256-bit SSL encryption for web applications.1024-bit RSA public keys for data transfers. AES 256-bit encryption for files and databases.
- Logs auditing activities of all users.
- Secured usernames and passwords: Encrypted via 256-bit SSL, requirements for complex passwords, set up of scheduled expirations, prevention of password reuse.
- Access based on the level of clearance.
- AD/LDAP integration.
- Control based on IP addresses.
- Encryption of session ID cookies in order to identify each unique user.
- Two-factor authentication availability.

- Third party penetration testing performed annually[25]
- Malware prevention through firewalls and automated scanner[29]

References

1. Craig Wolff (December 13, 1989). "Report Finds Fault With E.M.S. Computers" (https://www.nytimes.com/1989/12/13/nyregion/report-finds-fault-with-ems-computers.html). *The New York Times*. "too many E.M.S. employees have access to ..."
2. Maurizio Portolani, Mauricio Arregoces(2004). *Data Center Fundamentals* (https://books.google.it/books/about/Data_Center_Fundamentals.html?id=DRIryrLoxKkC&redir_esc=y). Publishers, Cisco Press, 800 East 96th Street Indianapolis, IN 46240 USA, Chap.5
3. The Four Layers of Data Center Physical Security for a comprehensive and integrated Approach [1] (https://www.anixter.com/content/dam/Anixter/White%20Papers/12F0010X00-Four-Layers-Data-Center-Security-WP-EN-US.pdf)
4. "Data center robbery leads to new thinking on security" (https://www.computerworld.com/article/2538534/data-center-robbery-leads-to-new-thinking-on-security.html).
5. Jessica Silver-Greenberg (April 2, 2012). "After a Data Breach, Visa Removes a Service Provider" (https://www.nytimes.com/2012/04/02/business/after-data-breach-visa-removes-a-service-provider.html). *The New York Times*.
6. Robin Sidel (April 2, 2012). "Card Processor: Hackers Stole Account Numbers" (https://www.wsj.com/articles/SB10001424052702304750404577318083097652936). *The Wall Street Journal (WSJ)*. "Visa yanked its seal of approval"
7. 2003 CSI/FBI report "Computer Crime and Security Survey." (http://www.firenetltd.it/material e/FBI2003.pdf)
8. David Moore; Colleen Shannon (2001). "The Spread of the Code-Red Worm (CRv2)" (http://www.caida.org/research/security/code-red/coderedv2_analysis.xml). Retrieved 2006-10-03.
9. "Net-Worm: W32/Nimda Description" (https://www.f-secure.com/v-descs/nimda.shtml). *F-secure.com (F-Secure Labs)*.
10. John Leyden (February 6, 2003). "Slammer: Why security benefits from proof of concept code" (https://www.theregister.co.uk/2003/02/06/slammer_why_security_benefits).
11. "Port Scan attacks and its detection methodologies" (http://vlab.amrita.edu/?sub=7&brch=199&sim=362&cnt=1).
12. Vitaly Shmatikov; Ming-Hsiu Wang. "Security Against Probe-Response Attacks in Collaborative Intrusion Detection" (https://www.cs.cornell.edu/~shmat/shmat_lsad07.pdf) (PDF). The University of Texas at Austin.
13. "Understanding Denial-of-Service Attacks" (https://www.us-cert.gov/ncas/tips/ST04-015). US-CERT. February 6, 2013. Retrieved May 26, 2016.
14. Khalifeh,, Soltanian, Mohammad Reza. Theoretical and experimental methods for defending against DDoS attacks (https://www.worldcat.org/title/theoretical-and-experimental-methods-for-defending-against-ddos-attacks/oclc/930795667). Amiri, Iraj Sadegh, 1977-. Waltham, MA. ISBN 0128053992. OCLC 930795667.
15. GIAC Certifications. *Global Information Assurance Certification Paper* (https://www.giac.org/paper/gsec/3161/unauthorized-access-threats-risk-control/105264).
16. "eavesdrop - Definition of eavesdrop in English by Oxford Dictionaries" (https://en.oxforddictionaries.com/definition/eavesdrop). Oxford Dictionaries - English.
17. Barwise, Mike. "What is an internet worm?" (http://www.bbc.co.uk/webwise/guides/internet-worms). BBC.
18. Stallings, William (2012). *Computer security : principles and practice*. Boston: Pearson. p. 182. ISBN 978-0-13-277506-9.

19. "Warning of webmail wi-fi hijack" (http://news.bbc.co.uk/2/hi/technology/6929258.stm). BBC News. August 3, 2007.
20. "Modern Overflow Targets" (https://dl.packetstormsecurity.net/papers/general/ModernOverflowTargets.pdf) (PDF).
21. Li, Q. (May 2019). "LSTM-Based SQL Injection Detection Method for Intelligent Transportation System". *IEEE Transactions on Vehicular Technology*. **68** (5): 4182–4191.
22. Cisco SAFE Reference Guide [2] (https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/SAFE_RG/SAFE_rg/chap4.pdf) chap.4
23. Rich Banta *Types of Data Center Security* (https://lifelinedatacenters.com/colocation/types-of-data-center-security/)
24. Sara D. Scalet 19 ways to build physical security into your data center (https://www.csoonline.com/article/2112402/physical-security/physical-security-19-ways-to-build-physical-security-into-a-data-center.html)
25. Security and Data Center Overview (https://www.accesscorp.com/wp-content/uploads/2016/03/AccessFileBRIDGE_SecurityDataCenterOverview.pdf)
26. Google Infrastructure Security Design Overview (https://cloud.google.com/security/infrastructure/design/#introduction)
27. Iliad Data Center, 'Data Center Security' (http://www.iliad-datacenter.com/pdf/iliad-dc-security.pdf) chap.4
28. Securing Microsoft's Cloud Infrastructure (https://cloud.google.com/security/infrastructure/design/#introduction) 2009.
29. Data Centre Management (https://ito.hkbu.edu.hk/pub/is_newsletter/professional/Issue_08_DCM/JUCC%20Newsletter-IT-8%20DCM.pdf)
