PalArch's Journal of Archaeology of Egypt / Egyptology

ANALYTICAL RESEARCH OF DATA CENTER SECURITY IMPLEMENTATIONS AND CYBER ATTACKS

Hardiksinh Rayjada, Dr.Vaishali Parsania
(PhD. Scholar, Department of Computer Science, Atmiya University, Rajkot, (Gujarat), INDIA)
Assistant Professor, Department of Computer Science, Atmiya University, Rajkot, (Gujarat), INDIA)

Hardiksinh Rayjada, Dr.Vaishali Parsania, Analytical Research of Data Center Security Implementations and Cyber Attacks-Palarch's Journal Of Archaeology Of Egypt/Egyptology 17(7), ISSN 1567-214x

Abstract— As the Internet is not secure; data center security can be at a threat due to any anonymous attacks. The Physical Security setup on the data center is the set of protocols within the data center facilities. Virtual security is a very hard task to handle, as there exist many ways and confidentiality Datacenter. Standard attacks are daily threats for the data centers. WAN, LAN, and HOST security require server implementing security more than seven tins to protect server attack from a virus, Hacker, and human. Data centers maintain multiple levels of security on a 24*7*365Days, Network protection, inside and outside security Firewalls, and data protection is a major critical area for security break. Servers implementing security can have more safety data.

Index Terms— Physical Security, Virtual Security, Firewall Security, server security, Network Security, common attack, Inside and outside data center security, data privacy, security issues. WAN, LAN, HOST Protection

1 INTRODUCTION

Data center security is important features of the data center, mission-critical infrastructure, Data breaches, cyberattacks are a growing threat for any data center. Datacenter security is mentions to the physical and virtual security used to protect a data center from external risks and attacks. Data centers consider physical, technical, environmental hazards, natural disasters. Data centers maintain multiple levels of security on a 24*7*365 Days. In order to enter the premises, first, be given permission to pass through a gate entrance on a wall surrounding the property. Walking through the front entrance, which a guard protects, requires additional permission by an individual. Security levels heighten the closer you get to the core of the data, the servers, and networking areas. The entrance into the core done via a turnstile that opens with the badge and biometric permissions. Once actually in the core workspace, intrusion detection systems are in place to ensure that through all the levels of security, no unauthorized entry individuals are present. Multi-levels security to keep data safe.

Datacenter security is the established rules, or set of policy protections and practices for restrict unauthorized administration access of data center resources avoid. A data center security is system critical Theft of confidential information, data alteration, and data loss are common security problems.

2 WAN Security

WAN (Wide Area Network) a wide area network (WAN) is a wide geographically distributed private telecommunications network that interconnects multiple local area networks connect cities, states, or even countries. WAN connect to a company's headquarters, branch offices, colocation facilities, cloud services and other facilities. A router multifunction device is use to connect a LAN to a WAN. WANs are not restricted to the same geographical location as a LAN. A LAN can be setup in any number of geographical areas and connected to a WAN. WAN is not constrained to one specific location.

Man-in-the-middle attacks the attacker wants to intercept a communication between person A and person B. Person A sends their public key to person B, but the attacker intercepts it and sends a forged message to person B, representing themselves as A, but instead it has the attackers public key. B believes that the message comes from person A and encrypts the message with the attackers public key, sends it back to A, but attacker again intercepts this message, opens the message with private key, possibly alters it, and re-encrypts it using the public key that was firstly provided by person A. Again, when the message is transferrin back to person a, they believe it comes from person B, and this way, we have an attacker in the middle that eavesdrops the communication between two targets. Here are just some of the types of MITM attacks: DNS spoofing, HTTPS spoofing, IP spoofing, ARP spoofing, SSL hijacking, and Wi-Fi hacking

2.1 Virtual Security

Virtual security is measures placed in data centers to prevent remote unauthorized access that will affect the truthfulness, availability, or confidentiality of data stored on servers. Virtual security is a hard task to handle as there exist many ways it could be attacker. The wickedest part of it is attacker could decide to use a malware or similar make use of in order to bypass the multiple firewalls is access to the data. Old systems put security at risk, as they do not contain modern methods of data security.

Vulnerabilities	Firewalls	Databases	Application	Physical Security	Insecure Wireless	VPN	Total Score
Threats							
Password Attacks	9	3	9	9	9	3	42
Insider Attacks	3	3	3	9	3	1	22
DDoS	9	0	9	1	3	3	25
Theft of Hardware	1	1	1	9	3	1	16

Data encryption during heavy data transfer 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 with Secured usernames and passwords Encrypted via

256-bit SSL, for complex passwords scheduled expirations of the prevention password reused. Access based password on the level clearance AD and LDAP integration to control based IP addresses. Encryption based session ID creates cookies in order to identify each unique user and Two-factor authentication availability. Third party penetration testing performed annually, Malware prevention through firewalls and automated scanner. Today mostly attack endpoints, many hackers know that users implement firewalls and set many policies, so it is very hard and only one way to enter the network, but the endpoint target is easy to inserts into a network. Today many users use social site Emails and download multimedia, so the backside of all-think's vires placed and sent them after end node restart or specific time to trigger the virus to run and expand to all networks. Strongly secure end-user and then security get strong end network switch also use an only manageable switch and place some security policy.

2.2 FIREWALLS SECURITY

The web server's requirement to tolerate access website runs on public services can access this web services incognito on the internet. Private web services used when dealing with a database control panel and the number of selected user requires access to the webserver. Authorized to login into accounts with special privileges the servers.

Internal services are that it had better never be expos to the internet or outside world. They are reachable from the server and connections of internet and firewall policy is to allow or restrict access according to the service-authorized user for Configure the firewall to restrict all services except for your server. A firewall is a sophisticated internet data-filtering device that separates LAN and WAN segments, giving each segment a different security policy that applies to a different level and establishing a security parameter. The traffic flow controls between segments and Firewalls are most commonly deploy at the Internet Control, where they performed as a boundary to the internal networks.

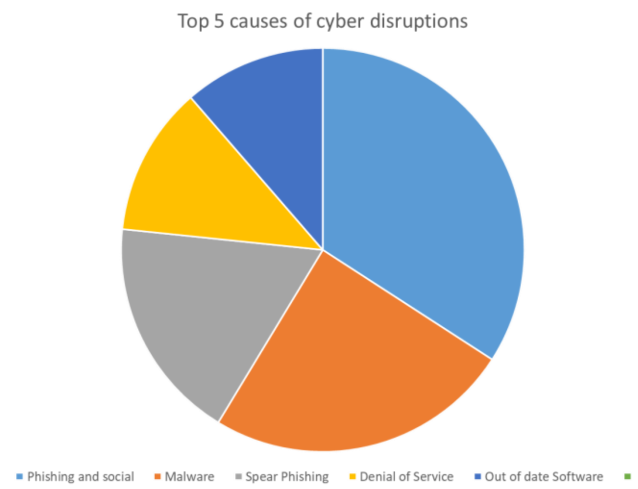
The firewall is to separate secured and unsecured areas of the network. Firewall Performance is becoming a natural design factor in ensuring that the firewall meets the particular requirements. Firewalls are work as a primary traffic path potentially exposed to large volumes of data. The firewall to control and protect a particular application or protocol application support is an important aspect. The connectivity is Telnet, SSH FTP, and HTTPS. The firewall is work to understand application-level packet exchanges and determine whether the packets move the application behavior and deny the traffic: the firewalls Filtering, Packet, Proxy, Stately, Hybrid information packet processing based on application-level capabilities.

2.3 COMMON ATTACKS

Scanning or Probing One of a probe or port scan-based attack is a port scanning requests a range of server port addresses to host are used to find an active port and then cause and effect harm via a known vulnerability of that service. This reconnaissance activity frequently precedes an attack. Its goal is to user access by discovering information about a system or network.

DoS (Denial of service): A denial of service attack when authorize users are unable to access systems, devices, and other network resources due to malicious cyber threat actors. This type of attack generates large data volume of intentionally consume limited internet resources as internet bandwidth and CPU utilization and blocks memory. Distributed Denial of Service: DDoS type of attack is a particular case use of DoS command a large number of systems are connected to a network and compromised used as source network or traffic on a synchronized dos attack. The hacker does not use this type of attack, only one IP address but thousands of them. Unauthorized access uses privileges associated with a compromised account to access restricted resources using a valid account or a backdoor. Etymologically, Eavesdropping Secretly listen to a conversation. Inside the networking is an unauthorized interception of information using usernames and passwords that progresses to network. Users can use logons to credential find.

Viruses and Worms when executed produce undesired results; there is malicious code that Worms are self-replicating malware, whereas viruses, which also can replicate, need some kind of human action to cause damage. Internet Infrastructure Attacks: This attack targets the critical components of the Internet infrastructure, preferably use separate network systems. Trust Exploitation: These type attacks exploit the trust relationships to computer systems ant connect to communicate that. Session Hijacking: cookie hijacking it is a Consists of stealing a legitimate session established between a target and a trusted host. Cookie hijacking the attacker intercepts the session and makes the target believe it is communicating with the trusted host. Buffer Overflow Attacks: the program allocates memory on buffer space. Behind the reserved results in a memory, corruption in the memory areas that were affecting the data stored overflowed. Layer 2 Attacks: This layer 2 type attack utilize the vulnerabilities of data link layer protocols on layer 2 switching platforms and implementations. SQL injection: code injection is inputs to a data entry form due to incomplete data validation and allows entering harmful input that causes harmful instructions to execute.



Cyber Disruptions, 50% of the organizations reportedly affected in 2017, this is top 5 causes of cyber disruptions

3 LAN SECURITY

LAN is a group of computers and network devices, which are all, connect to each other, a short geographical distance. A local area network is a small area Local LAN Network of computer network. LAN is limited to a single office and building or one LAN can be connect to other LANs. LANs connected in this way is a wide-area network. There are few different ways to provide security for local LAN networks. The common types of hardware and computer that used Local LAN Network setups. One common policy is to apply security is install a firewall it is also proper to use specific security protocols like WPA or WPA2 for password encryption on traffic coming in from the internet. The network administrators filter traffic using a detailed information of trusted network parts, authentication policies of network traffic inspected to network prevent different kinds of unauthorized user access. The TUNNEL technologies VPN, control packets through different layers of the OSI model. LANs normally need internal security strategies to routers, manage switches, antivirus, firewall that serve different parts of the network security. Anti-virus or anti-malware end user security is hacking functions are introduce to networks through user activity. Snooping viruses and malicious programs operate a user to opening an email, downloading a file from a banned site and source or otherwise opening the internal LAN to exterior threats are loopholes and prevent as many vulnerabilities as possible.

3.1 NETWORK INFRASTRUCTURE SECURITY

Access Control List is filtering machines clearly defined based on packet header information to permit or deny traffic on specific interfaces. Access Control List is use in multiple locations within the Data Center, the Edge of the Internet, and the intranet server farm. This standard and extended access lists.

Standard Access Control List the simplest type of ACL filtering traffic simply created on source IP addresses. Standard Access Control List is typically deploy to control access to network devices for network management or remote access. Configure a standard Access Control List in a router to specify which systems are allow to Telnet to it. Standard Access Control List is not the recommended option for traffic filtering due to their lack of granularity. Standard ACLs are configure with a number. Extended Access Control List filtering decisions are the source and destination IP addresses based on Layer 4 protocols ports ICMP message type and code, type of service, and precedence. Define extended Access Control List by name or by a number.

3.2 SERVER IMPLEMENTING SECURITY

Hackers are all times active and look out for server and network vulnerabilities. It is our responsibility to confirm our data is safe and secure. Curtail risks and be confident our data is safe and secure on server's implementing security. We deployed security features on our data center servers.

3.2.1 Password Requirements

The first step is to apply a password with complexity length, require policy rules, a password passphrase I love! ToEatPizzaAt1676MainSt is longer than a normal password, not allow empty or default passwords. Do not store passwords. Set Password Expiration Policy establishing requirements for users every week or month. It contains upper case and lower case letters, digits, numbers, and unique characters. Considerable easier to remember a passphrase than randomly letters. Use 49 characters. It is more difficult to crack. Remember password, do not write any paper, and hide any place in the office. Not to use personal information, mobile number, birthday date, hometown number, pet names these are easy to guess people know personally. The same password does not use multiple accounts.

3.2.2 Secure Server Connectivity

The SSH (Secure Shell) Remote server connection is important Protocol to provide a secure channel communication in establishes a protected connection. Telnet and SSH access encrypts protocols are all the data transmitted and exchange. Install SSH Client SSH protocol uses port 22 every one hackers change port numbers between 1024 and 32767.

3.2.3 SSH Keys Authentication

SSH authenticates in the server is using SSH keys pair, the SSH keys carry bits password and they are uncrack able RSA 2048-bit encryption is equal to a 617-digit password. The key pair change to a public key and private key. The public key shared with users and leftovers on the server. The private key can read this data. The data do not share by anyone and saved secure. The server requests the user have the private key before allowing privileged login access.

3.2.4 File Transfer Protocol

File Transfer Protocol Secure (FTPS) as a FileZilla server work without danger of hackers compromising or stealing encrypts data files and authentication information. File Transfer Protocol Secure uses a command channel and a data channel. The files protect encrypt during transfer. They reach the server and the data is no longer encrypt.

3.2.5 Secure Sockets Layer Certificates

Secure Socket Layer (SSL) that protect administration areas and forms information are pass between two systems connected to the internet. Secure Socket Layer can used individually in server to the client and in server-to-server communication.

3.2.6 Private Networks and VPNs

Private and virtual private networks (VPNs), Private networks use a private IP to establish isolated communication between servers and the user. Without exchange information and data exposure to a public network. Virtual Private Network (VPN) is just like a LAN. We provide VPN Connection to All users is more secure to the internet.

3.2.7 Login Attempts

Login attempts is to protect the server against to brute force attacks. These brute force attacks is automated attacks script use a trial-and-error method. Attempting to every thinkable combination of password with letters, digit and numbers to access to the server or nod. Software oversees all log files and detects suspicious login attempts. The user attempts numbers of time login then exceed the set norm, and software blocks the IP address.

3.2.8 Manage Users

Every user only roots the login server has a root user who can execute any root command; it falls into the wrong hands is hazardous to the server. Disable the root login in SSH. Hackers focus their attention to crack the root password. Create a limited user account and do not the same authority to perform administrative tasks using root commands

3.2.9 Update software regularly

Regularly updating and upgrade the software is the first line of defense. A server is a crucial step it safe from hackers. Automatic updating software in background and examine how the update and performs in a test environment. Update plugins, and security patches to check fix security issues.

3.2.10 Turn off All Unnecessary Services

This cybersecurity term mentions to install and maintain bare minimum requirements for running services. Server operating system installation necessary programs listed. Firewall allow only specific ports and deny all other port.

3.2.11 Hide Server Information

Provide less information about the underlying infrastructure as possible, hide the version numbers of any software installed on the server. We are deleting HTTP header.

3.2.12 Integrated Defense Security

Intrusion detection system detects any unauthorized activities, monitors processes running on a server. Check day-to-day operations. IDS Solutions are real-time systems that can detect intruders and suspicious activities and report them to a monitoring system. They are configure to block or reduce interruptions in progress and eventually immunize the systems from future attacks. They have two fundamental components.

3.2.13 File and Service Auditing

File and service auditing is an additional way to find out annoying users changes in system records of all the features of systems healthy. Service auditing discovers running protocols on the server, their protocols are which ports they use communicating from side to side.

3.2.14 Back-Up Server

Store encrypted back-ups of critical data offsite or use a cloud solution. Schedule an automated backup or manually, make a sure routine of this precautionary measure. Test complete back-up testing. This administrator user or even end-users can verify that data recovery process is correct.

3.2.15 Multi-server Environments

Multi server Environments can separate database servers and web application servers is a standard security practice. Isolation is one of the types of server protection separate database server's secure sensitive information and system files from hackers. That manage to advantage access to administrative accounts. Isolation system administrators to separately configure the web application security and minimize the attack web firewalls.

3.2.16 Virtual Isolated Environments

Full isolation server does not afford to virtual isolate execution environments. Virtualization isolated server set up is another option for isolation and security measures.

Major Cyber Crime Registered in Gujarat

Name of Crime	Ration
Cheating	99
Identity Theft	46
Online Fraud	42
ATM Fraud	41
Explicit Material	36
Fake Profile	16
Cyber staffing	15
OTP Fraud	14

4 DATA CENTER OUTSIDES SECURITY

Physical Security Matters is typically protecting systems restricted to unauthorized persons for entering the data center. Protected with highly secure and fast working access control systems swipe cards, RFID, Biometric systems, server locked cages, and require additional CCTV Surveillance and Monitoring systems. Unauthorized use of computing resources Outsides of a data center. Application software and protocol errors, coding errors, and incomplete testing Configuration use, default configuration, and elements incorrectly use to outside attack.

5 DATA CENTER INSIDES SECURITY

Internal attacks are more damaging because of the variety and amount of information available inside organizations. Network Security, incoming and outgoing data center traffics, monitoring on the firewall, anti-virus endpoint security, application security for the data center is a control to insider users, and staff to use internal attacks. Many users use Portable IT Gadgets outside the infected network, with a virus and then use inside the data center and infected the same.

6 DATA PROTECTION

The importance of data protection is the process of safeguarding important information. The data amount created and stored continues to increases data variability. The tolerance for downtime that can make it impossible to access important information. Ministry of Electronics and Information Technology in Indian IT Act 2008, Section 43, corporate dealing or handling any sensitive individual data processing or information in a computer resource. It controls or works is negligent in implementing, maintaining, and reasonable security practices that can perform procedures. There causes wrongful loss or wrongful gain to any person that such body corporate shall be liable to pay the penalty or damages by way of compensation to the person so affected.

Computer virus are one of the most common threats to cybersecurity approximately 33% of household computers are affect with malware. Computer viruses are pieces of software that are design to spread from one computer to another. They frequently sent as email attachments or downloaded from specific websites with the intent to infect your computer. In addition, other computers on your contact list using systems on your network. Viruses are send to spam, disable your security settings and corrupt and steal data from your computer including personal information such as passwords, delete everything on your hard drive.

Rogue security software is malicious software that mislead users to trust a computer virus installed on their computer. Their security measures are not up to date and then offer to install or update users' security settings to ask you to download their program to remove the alleged viruses, or to pay for a tool. Both cases lead to actual malware installed on your computer. Trojan horse is a malicious bit of attacking code or software that tricks users into running it willingly tricking someone into inviting an attacker into a securely protected area. They spread frequently via email it may perform click on the email and its included attachment. Immediately downloaded malware to your computer. Trojans also spread when click on a false announcement. Once inside your computer a Trojan horse can record passwords by logging keystrokes, hijacking webcam, and stealing any sensitive data on computer.

Adware and spyware software that designed to track data of browsing and, pop-ups. Adware collects data with permission and is even a genuine source of income for companies that allow users to try their software free, But with advertisements showing while using the software. The adware clause is often hidden in related User Agreement docs, but it can be checked by carefully reading anything accept while installing software. The presence of adware on computer is noticeable only in those pop-ups, and sometimes it can slow down computer's processor and internet connection speed. Adware is download without agreement it is consider to malicious.

Spyware works similarly to adware but is install on computer without information. It can contain key loggers that record personal information including email addresses, passwords, credit card numbers, it dangerous of the high risk of identity theft. Computer worm Computer worms are pieces of malware programs that replicate quickly and spread from one computer to another. A worm computer sending data itself to all local network computers and then immediately contacts to the other computers. Activated firewall, WPA2 encryption, Guest Network, Physically secure network hardware, higher-quality routers, MAC address filtering, network up-to-date, VLANs to segregate traffic, 802.1X encryption authentication

7 PHYSICAL SECURITY

Data centers use to prevent physical attack techniques. The physical data center security is the set of protocols to build data centers secure physical damage to the machines storing the data. The protocols should be able to handle everything ranging from natural disasters to corporate espionage to terrorist attacks.

7.1 Staff Training

Each staff to given one weak Training for How to follows Rules and working style of a data center. Anti-pass-back turnstile gate Only One Person to enter his have Identity Card and go to Parking are or Reception Area. Reception area auditing for staff and user and then Entry for the related specific area. Every floor and room locked with RFID Security. Staff entry with Biometrics Finger Authentication and Face recognized.

7.2 RFID Tracking Systems

RFID Tracking systems central work and track CARD where to move and access Authentication use or unauthorized access. User Access Point, CCTV video recording, RFID Card Location Tracking are store back-up 90 Day storage available. Take actions and keeping their credentials safe by monitoring systems. Traffic control through dedicated data halls, suites, and cages staff — monitoring of Temperature and humidity of Datacenter entire Building and each equipment.

7.3 Fire Safety

Fire prevention with a zoned dry-pipe sprinkler for any emergency for fire protections 24×7×365 on-site security guards, NOC Services, and technical team monitoring each activity. Natural disaster risk-free locations and Sensor Security Alert Message for any changes in Environmental. Datacenter room entering must be two persons for security reasons for data and staff. Metal Detection is a scanned entry gate, each floor entry gate, and Datacenter rooms. Each server and rack sensor-based security to measure temperature, track a user who accesses physical, and identify RFID Authentication.

7.4 Biometric Security

Access Control Systems & Biometric identification has become an increasingly high-security method. It does not depend on password or access cards. Biometrics visitors have given a card, password another person for access, integrating an extra layer of security within the facility. Human involving two separate doors with small space airlock having two interlocking doors. Only one door open at a time at data center authentication required for both doors first doors must close before the second door opens. Usually, this type of security used in banks, financial institutions, detention facilities, pawnshops and jewelry stores, and secured offices.

7.5 CCTV Security

CCTV Security Camera video recording records every location movement and trace to object. Surveillance security system to watch whose walking into a data center and walking out with a disk or any hardware containing. Keep a record of persons enter the facility, and critical areas are restricted to ensure unauthorized user access to the data center itself. It is very important that the building is secure and protected at all times. Cameras installed throughout the building at every entrance, exit, and access point.

7.6 Dress Code

Dress Code is very important to the data center. Any person passes any tools or hardware hide in clothes. Jeans, Teaser, and shoes are requiring to dress code. No one-wearer jacket or two-layer wearer it is easy to hide and unauthorized hardware or tools.

7.7 Redundancy Security

Redundancy data center increases security, providing an extra layer of equipment, staff, or storage is primary sources of failure. the generators, batteries, heating, ventilation, and air conditioning (HVAC), water, power, and telephone lines, basic equipment's and tools are all utilities that may be redundantly reinforced.

Staffs redundancy the visitors are present in the data center, and staff or employees help them and same time contractors or repair crews present in the building.

CONCLUSIONS

Data Center Physical Security is Basic one of the requirements meant for the data center. It protects local peoples and anonymous who damage the data center physically. Virtually security provides technical strong and hard to crack security outside. Physical and Virtual are interconnected and hard to crack the combination of this security. Every day hackers or any systems generated attacks fire on the network to damage server and data mining. Server secure to passphrase technology to strong password creation and protect server if any anonymous insert our network and try to access server, so it is very difficult to crack the password. Network Security work on Layer 2 and three security protocols, ARP Inspections, Private VLANs to protect LAN WAN Security. Firewall Protect Unauthorized user access Local LAN and WAN Network. Data Protection is the main task to secure data to any hack or mining data and leak important or legal information. Network traffic analyzes and identifies suspicious activities.

Datacenter security and data protection are not possible to anyone protocols implementation it requires possible security points to protect data and day-to-day update and upgrade security.

ACKNOWLEDGMENT

I like to tell my sincere gratitude and appreciation to Dr. Vaishali Parshania, who helped me complete this research paper. Writing this paper was not possible without her constant guidance and support. I am also very thankful to Atmiya University and faculty members for providing knowledge. In addition, this platform to reflect what I have learned here in this paper.

REFERENCES

[1] Ben Joan, differencebetween.net, [Online Available]: http://www.differencebetween.net/technology/difference-between-vpn-and-internet/#ixzz64kykAH2l

[2] R. Soni, S. Ambalkar and P. Bansal, "Security and privacy in cloud computing," 2016 Symposium on Colossal Data Analysis and Networking (CDAN), Indore, 2016, pp. 1-6., doi: 10.1109/CDAN.2016.7570962

[3] colohouse.com, APRIL 30 2019 [Online Available]: https://colohouse.com/why-is-data-center-security-important/, [Accessed may. 01, 2020]

[4] M. S. Al-Qahtani and H. M. Farooq, "Securing a Large-Scale Data Center Using a Multi-core

Enclave Model," 2017 European Modelling Symposium (EMS), Manchester, 2017, pp. 221-226., doi: 10.1109/EMS.2017.45

[5] iclg.com, [Online Available]: https://iclg.com/practice-areas/data-protection-laws-and-regulations/india, [Accessed may. 02, 2020]

[6] State IT Secretaries Conf, 12,13 February ,,18, [Online Available]: https://digitalindia.gov.in/writereaddata/files/6.Data%20Protection%20in%20India.pdf, [Accessed may. 03, 2020]

[7] Sofija Simic, phoenixnap.com, posted April 20, 2019, [Online Available]: https://phoenixnap.com/kb/server-security-tips, [Accessed may. 04, 2020]

[8] niti.gov.in, [Online Available]: https://niti.gov.in/sites/default/files/2019-07/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf, [Accessed may. 03, 2020]

[9] Parth Shastri, 26, 10, 2019, [Online Available]: https://timesofindia.indiatimes.com/city/ahmedabad/cyber-crimes-jump-90-in-2-years-in gujarat/articleshow/ 71768981.cms, [Accessed may. 04, 2020]

[10] R. Ward and P. Skeffington, "Network management security," [1990] Proceedings of the Sixth Annual Computer Security Applications Conference, Tucson, AZ, USA, 1990, pp. 173-180. doi: 10.1109/CSAC.1990.143766,

[11] Katherine Wenger, [Online Available]: https://study.com/academy/lesson/ data-center-security-levels.html, [Accessed may. 02, 2020]

[12] INC. EDITORIAL, INC. STAFF, February 2006. [Online Available]: https://www.inc.com/encyclopedia/wide-area-networks-wans.html, [Accessed may. 01, 2020]

[13] SECURITYTRAILS TEAM, securitytrails.com, OCT 16 2018, [Online Available]: https://securitytrails.com/blog/top-10-common-network-security-threats-explained, [Accessed may. 03, 2020]·

[14] Vangie Beal, techopedia.com, [Online Available]: https://www.techopedia.com/7/30065/networking/how-can-a-local-area-network-lan-be-secured, [Accessed may. 01, 2020]

Source details

PalArch's Journal of Archaeology of Egypt/ Egyptology

Scopus coverage years: from 2012 to 2013, 2015, 2017, from 2019 to 2020

Publisher: PalArch Foundation

E-ISSN: 1567-214X

Subject area: Arts and Humanities: History | Arts and Humanities: Archeology (arts and humanities) | Social Sciences: Archeology

View all documents >   Save to source list

CiteScore 2019
0.2

SJR 2019
0.108

SNIP 2019
0.000

CiteScore   CiteScore rank & trend   Scopus content coverage

i Improved CiteScore methodology

CiteScore 2019 counts the citations received in 2016-2019 to articles, reviews, conference papers, book chapters and data papers published in 2016-2019, and divides this by the number of publications published in 2016-2019. Learn more >

CiteScore 2019

$$0.2 = \frac{\text{1 Citations 2016 - 2019}}{\text{5 Documents 2016 - 2019}}$$

Calculated on 06 May, 2020

CiteScoreTracker 2020

$$0.3 = \frac{\text{4 Citations to date}}{\text{15 Documents to date}}$$

Last updated on 07 December, 2020 • Updated monthly

CiteScore rank 2019

Category	Rank	Percentile
Arts and Humanities History	#741/1259	40th
Arts and Humanities Archeology (arts and humanities)	#198/278	28th

View CiteScore methodology >   CiteScore FAQ >   Add CiteScore to your site