

Cloud Compromise



Introduction

Why is cybersecurity important?

In today's digital age, everything – from personal information and financial data to business operations and critical infrastructure – relies on computers and networks. This makes them prime targets for attackers with malicious intentions. A successful cyberattack can have devastating consequences.

The Cloud Compromise

SCENARIO: One of your organization's internal departments frequently uses outside cloud storage to store large amounts of data, some of which may be considered sensitive. You have recently learned that the cloud storage provider that is being used has been publicly compromised and large amounts of data have been exposed. All user passwords and data stored in the cloud provider's infrastructure may have been compromised.

Immediate Response:

1. Contain the Breach:

- a. **Isolate Affected System:** Disconnect the department's systems or accounts from the compromised cloud storage provider immediately. This prevents further data exfiltration and potential damage.
- b. **Prevent Access:** Disable all user accounts within your organization that accessed the compromised cloud storage. This eliminates unauthorized access attempts while you assess the situation further.
- c. **Reset Passwords:** Instruct all affected users to immediately change their passwords for any account potentially related to the compromised cloud storage, including organizational and personal accounts. Consider implementing mandatory password resets across the organization.

2. Assess the Impact:

- a. **Identify Exposed Data:** Determine what type of data was stored in the compromised cloud storage, its level of sensitivity, and potential implications of its exposure.
- b. **Alert Affected Individuals:** Notify any stakeholders whose data may have been exposed, including individuals, clients, or partners. Provide clear instructions on recommended actions like password changes and monitoring for suspicious activity.
- c. **Contact Cloud Storage Provider:** Reach out to the cloud storage provider for official information about the breach, including impacted data types, mitigation steps, and recommendations.

3. Remediate and Protect:

- a. **Investigate:** Conduct a thorough forensic investigation to understand the attack vector, identify any internal vulnerabilities, and prevent similar incidents in the future.
- b. **Legal advice:** Consult legal counsel to assess potential regulatory and compliance obligations related to the data breach, especially if sensitive data was exposed.

-
- c. **Review Cloud Storage Policy:** Reevaluate your organization's policy on cloud storage usage. Consider stricter regulations, including approved providers, data types allowed, and encryption requirements.
 - d. **Implement Additional Security Measures:** Consider implementing additional security measures like multi-factor authentication, data encryption, and intrusion detection systems to strengthen your overall security posture.

Vulnerabilities in the scenario: Risk

I. High-Severity Vulnerabilities

1. **Data Exposure:** The most critical vulnerability is the potential exposure of large amounts of data, especially sensitive information. This could include:
 - a. **Personally identifiable information (PII):** Names, addresses, social security numbers, financial data, medical records, etc.
 - b. **Trade secrets:** Proprietary information, algorithms, product plans, customer lists, etc.
 - c. **Internal documents:** Legal documents, contracts, employee records, etc
2. **Spam and Phishing Attacks:** Leaked email addresses can be used for spam and phishing attacks, which could lead to:
 - a. More data breaches.
3. **Malware Injection:** The compromised cloud storage provider might be used to distribute malware to your organization's systems. This could lead to:
 - a. **Data loss or corruption:** Hackers could gain access to your systems and steal or destroy data.
 - a. **System disruption:** Malware can disrupt your critical business operations.
 - b. **Financial losses:** You may need to pay for data recovery, repairs, and security upgrades.

II. Medium-Severity Vulnerabilities

1. **Account Takeover:** Hackers could use leaked passwords to gain access to user accounts in other systems within your organization. This could allow them to:
 - a. Steal additional data.

-
- b. Disrupt operations.
 - c. Launch further attacks.

2. **Financial Fraud:** If financial data was exposed, it could be used for:

- a. Identity theft.
- b. Credit card fraud.
- c. Bank account fraud.

3. **Reputational Damage:** Exposure of sensitive data can severely damage your organization's reputation and public trust. It can lead to:

- a. **Loss of customers and partners:** People may be hesitant to do business with an organization that has a history of data breaches.
- b. **Legal and financial implications:** Fines, lawsuits, and remediation costs can be significant.
- c. **Loss of employee morale and productivity:** Employees may be worried about their personal information being exposed.

III. Low-Severity Vulnerabilities

- a. **Loss of Productivity:** Employees may have to change their passwords and take other security measures, which can take time and disrupt their work.
- b. **Increased Security Costs:** The data breach may prompt you to invest in additional security measures, such as encryption and intrusion detection systems.
- c. **Negative Media Coverage:** Your organization may receive negative media coverage due to the data breach.

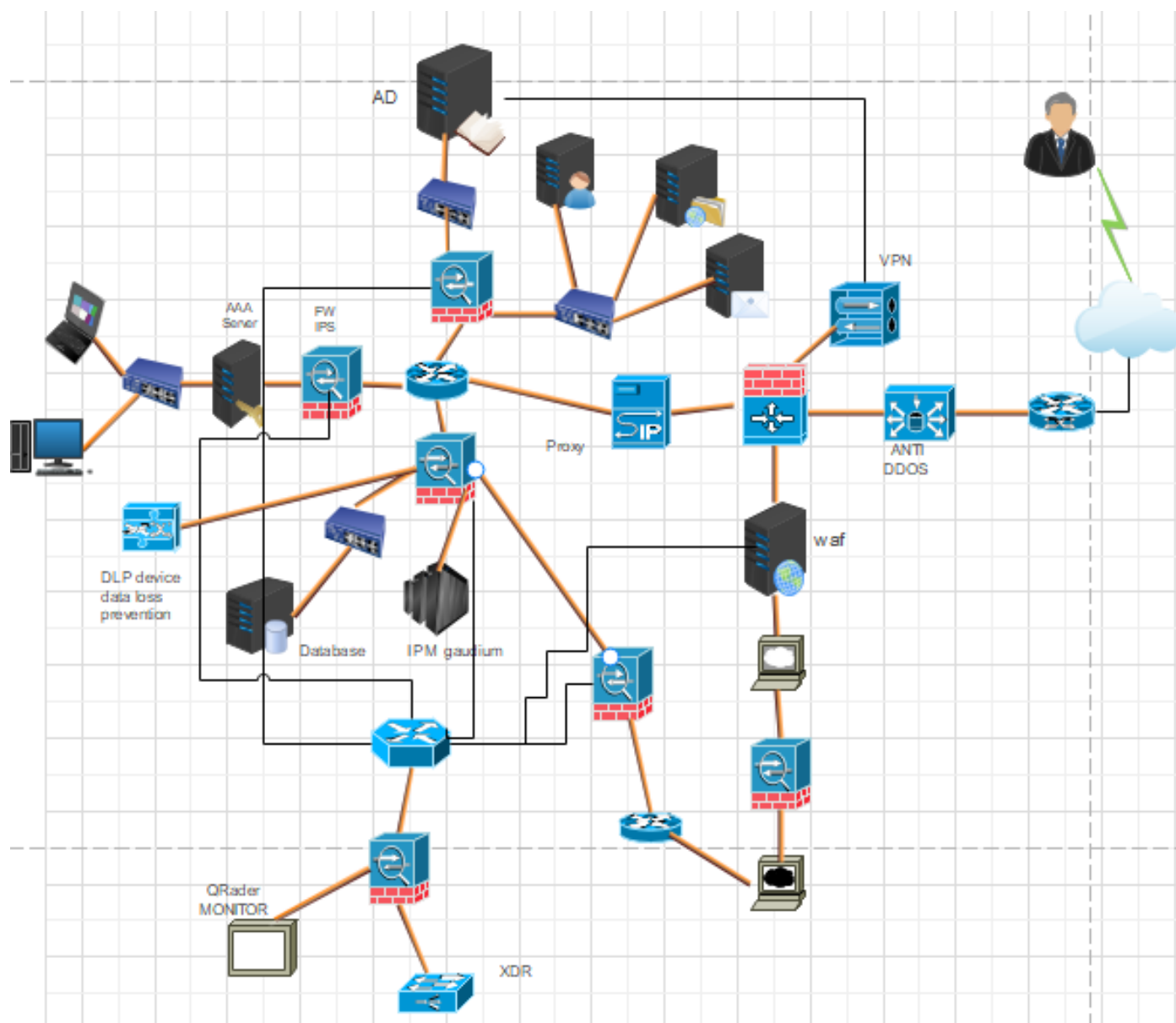
Recommendation for mitigation & Prevent

- a. We keep a copy of the data
- b. Block all unnecessary or unused ports
- c. The presence of an AAA device for verification and authorized access to the company's data
- d. We don't give people a lot of permission to access data
- e. Employees should know the security policies
- f. It must be present on the employee's personal device (endpoint detection software, antivirus software)
- g. The company must have devices such as (Proxy, firewall, IPS, IDS, WAF, DDOS Protection, SIME Monitoring, IPM gaurdium (database production), XDR)
- h. Check the (CLI: Confidentiality & Integrity & availability) on the company
- i. If remote access is needed, be sure to secure the connection, using tunneling and encryption protocols
- j. The data stored on the network must be encrypted, and it must be placed in a secure place that is difficult to access
- k. Must be used: MD5 Hash Function
- l. Used: HTTPS (SSL, TLS): Because it contains a certificate and through it the Website is protected by a certificate
- m. Slow down brute force and dictionary attacks with strong password policies and then audit be alert for logon failures

Key elements in a security policy

1. Some of the key elements of an organizational information security policy include the following.
2. Statement of the purpose.
3. Statement that defines who the policy applies;
4. Statement of objectives, which usually encompasses the CIA triad.
5. Authority and access control policy that delineates who has access to which resources.
6. Data classification statement that divides data into categories of sensitivity, the data covered can range from public information to information that could cause harm to the business or an individual if disclosed.
7. Data use statement that lays out how data at any level should be handled, this includes specifying the data protection regulations, data backup requirements and network security standards for how data should be communicated, with encryption, for example.
8. Statement of the responsibilities and duties of employees and who will be responsible for overseeing and enforcing policy.
9. Security awareness training that instructs employees on security best practices, this includes education on potential security threats, such as phishing, and computer security best practices for using company devices.
10. Effectiveness measurements that will be used to assess how well security policies are working and how improvements will be made.

Topology



Components

Switches are essential networking devices that connect multiple devices on a network, Through it is carried out:

- a. Allow for traffic prioritization, VLAN creation, security settings, monitoring, destination MAC address, Layer 2, and more.
- b. Ideal for larger networks or those with specific needs

Routers are intelligent networking devices that connect different networks and direct traffic between them. They operate at Layer 3 of the OSI model, using IP addresses to make routing decisions, Key functions of routers:

- a. Packet forwarding
- b. Path selection
- c. Network segmentation
- d. WAN connectivity
- e. NAT (Network Address Translation): Translate private IP addresses within a local network into public IP addresses for internet access, conserving IP address space.
- f. Firewall features: Many routers offer built-in firewall capabilities to filter traffic and protect networks from unauthorized access.

AAA Server (Authentication, Authorization, and Accounting) is a central server that manages user access to network resources and services. It acts as a digital security guard, ensuring only authorized users can access specific resources and keeping track of their activities.

- Check policy on device user

Authentication: Verifies the identity of users attempting to access the network, Commonly uses usernames and passwords.

Authorization: Grants or denies access to specific resources or services based on user privileges.

Accounting: Tracks and records user activity on the network.

Firewall: a network firewall monitors and controls incoming and outgoing network traffic, filtering out malicious or unauthorized activity. It sits at the gateway between a trusted network (like your internal office network) and an untrusted network (like the internet), analyzing data packets and allowing or blocking them based on predefined security rules.

Types of firewalls:

Packet-filtering firewalls:

- a. Understanding source and destination IP addresses
- b. Which permit or denies traffic based on (Layer 3, Layer 4)

Stateful firewalls:

- a. Which permit or denies traffic based on (Layer 3, Layer 4)
- b. Understanding source and destination IP addresses
- c. monitoring data packets and conversation between devices (Loges)
- d. Zoning
- e. can detect and block attacks like port scans and denial-of-service attacks.


Application-level firewalls:

- a. Like the previous Plus
- b. Understanding (Web Application) based on Layer 7

Next-generation firewalls (NGFWs):

- a. Like the previous Plus
- b. They often include additional features like intrusion detection and prevention systems (IDS/IPS), deep packet inspection (DPI), and virtual private networks (VPNs).
- c. URL Filtering & Web Filtering

Application gateway Proxy:

- a. Understanding (Web Application) based on Layer 7
- b. web security appliance (WSA)
- c. Anonymity and Privacy
- d. Used by organizations to manage internet access for multiple users, preventing employees from accessing certain websites
- e. **Advanced Proxy:** Sand box  Zero day attacks

Web Application Firewall (WAF) is a protecting your web applications from malicious attacks and unauthorized access.

- a. They scrutinize data packets for suspicious patterns or malicious content indicative of attacks, web application attacks like SQL injection, cross-site scripting (XSS), and session hijacking.
- b. They can also detect zero-day attacks and evolving threats.
- c. F5 Company

XDR (Extended Detection and Response):

- a. Acts as a unifying platform, ingesting data from both **EDR** (Endpoint Detection and Response) and **NDR** (Network Detection and Response) tools, along with other security sources.
- b. Correlates data from across your entire environment to identify threats that span multiple points (e.g., an attack initiated on the network targeting endpoints).

Data Loss Prevention (DLP) is a set of tools and processes designed to prevent unauthorized access, exfiltration, or sharing of sensitive data.

- a. Data loss prevention.
- b. Preventing the data from being transferred or shared.
- c. Alerting: Notifying administrators or users about the potential data leak.
- d. Encrypting the data to render it unusable if accessed by unauthorized parties.

DLP works:

- a. Data classification
- b. Data monitoring
- c. Policy enforcement

QRadar: for monitoring and analyzing security data within an IT environment, monitoring your network and systems, reporting suspicious activity and potential threats.

SIME QRadar monitoring works:

- a. Data collection
- b. Correlation and analysis
- c. Alerting and reporting
- d. Threat Hunting and Investigation

"Anti-DDoS" (DoS) attacks: Protection from DDoS attack these attacks try to overcome a system with excessive traffic, making it inaccessible to legitimate users.

Other DDoS mitigation methods:

- a. Redundancy and scaling: Distribute traffic across multiple servers to handle increased load.
- b. Backup and recovery plans: Minimize downtime and enable quick restoration after an attack.
- c. DDoS response training: Improve incident response protocols to effectively react to attacks.

AD Active directory: Save (username, password, other data)

Intrusion Detection System (IDS): It monitors the system or network without taking a reaction, or blocking the virus

Intrusion Prevention System (IPS): It monitors the system or the network and takes a reaction if any virus or infiltration is found on the network, blocking the virus

IBM Guardium:

- a. protection sensitive data across various environments.
- b. Detects and prevents threats
- c. Provides audit trails and reporting
- d. Data discovery and classification
- e. Activity monitoring in database
- f. Vulnerability assessment
- g. Threat intelligence

Budget of appliance:

Appliance	Cost
ASA-IPS-60-INC-K9	\$165,000.00
Switch: Catalyst 9200L 24-port PoE+ 4x10G uplink Switch, Network Advantage	US\$2,447.00
Router cisco: <u>CISCO891-K9</u>	US\$547.00
Juniper Routers: MX480 Base Chassis with Midplane, 1 nos. SCB-E, AC Power, Discounted RE incl. Junos	US\$16,356.55
CISCO ISE-3395-K9 Cisco Identity Services Engine 3395 Hardware Appliance	US \$663.80
IBM Security Guardium:	\$1650
Qrader IBM	\$50,000 per month
AINT DDOS	\$2 000 monthly
Allen & Heath xDR-16 16-Input/8-Output Expander (church owned) CG000BR	\$499.99
NEW IN BOX HPE ProLiant ML110 GEN 10 8SFF Server (872309-B21) *FIRESALE PRICE*	\$899.00
Data Loss Prevention (DLP) Blade for 1 year - for ultra high-end appliances	\$13,480.00
BIG-IP Add-On Advanced Web Application Firewall (WAF) - License	\$22,336.00
Total Cost	\$ 914,973.34 & 2,050 monthly