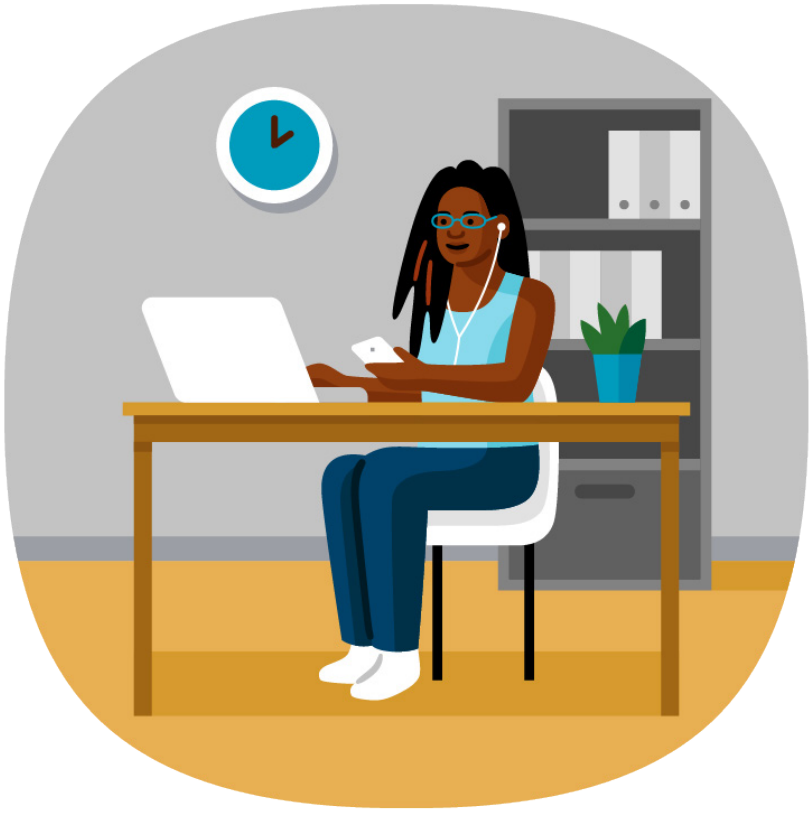
WHITE PAPER

Security Best Practices

medisked

Contents



Identity and Access Management Best Practices

With the annual costs of cybercrime expected to reach $10.5 trillion by 2025[1] businesses need to focus on improving network security measures and controlling user access. Identity and Access Management is a critical component of a successful protocol and requires the implementation of best practices to maintain the integrity of user and device identities.

What is the Average cost of a data breach?[2]

1. Identity Becomes the Security Perimeter

Cloud hosted services offer access to anyone, anywhere. More accessibility means more entry points, which means we must rethink how we approach security. Identity and verification at the user-level is where today's security perimeter resides. Commonly referred to as "Zero Trust Networking", users are authenticated to get into the network, but must be specifically authorized at every attempt to access data, systems, or connections to ensure the user is approved to access each resource. Identity and Access Management policies need to adapt to the fluid boundaries of today's technology. Strong authentication factors help build a circle of trusted identities, and the best enforcement is through verification.

1 - https://www.globenewswire.com/news-release/2020/11/18/2129432/0/en/Cybercrime-To-Cost-The-World-10-5-Trillion-Annually-By-2025.html
2 - https://www.ibm.com/security/data-breach

2. Enforce Strong Passwords

Strong passwords have always been one of the foundations of an effect Identity and Access Management strategy and will remain so moving forward. Excellent password creation practices come from the National Institute of Standards and Technology (NIST). Previous standards recommended restrictions on password length, complexity, and update frequency. However, new guidance recommends some significant changes based on how modern computing power makes it easier to 'crack' passwords.

NIST Password Guidelines[3]

- A minimum of 12 characters
- Recommendation to use 'pass phrases' which are longer but easier to remember
- Minimum of complexity (e.g., mix of numbers, lower & upper case characters)
- Only need to update passwords once per year
- Restrict the last three passwords used
- Restrict passwords obtained from previous breaches

How long will it take to crack your password?

Length of Password (Chars)	Only Numbers	Mixed Lower & Upper Case Letters	Mixed Numbers, Lower & Upper Case Letters	Mixed Numbers, Lower and Upper Case Letters, & Symbols
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	3 secs	10 secs
6	Instantly	8 secs	3 mins	13 mins
7	Instantly	5 mins	3 hours	17 hours
8	Instantly	3 hours	10 days	57 days
9	4 secs	4 days	153 days	12 years
10	40 secs	169 days	1 year	928 years
11	6 mins	16 years	106 years	71k years
12	1 hour	600 years	6k years	5m years
13	11 hours	21k years	108k years	423m years
14	4 days	778k years	25m years	5bn years
15	46 days	28m years	1bn years	2tn years
16	1 year	1bn years	97bn years	193tn years
17	12 years	36bn years	6tn years	14qd years

Table content from cloudnine.com

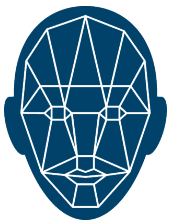
3. Use Multifactor Authentication (MFA)

Multifactor Authentication (MFA) is the first step in creating layers of trust. Sometimes referred to as Two-Factor Authentication (2FA), is a security enhancement that allows you to provide two pieces of evidence /credentials when logging in to an account.

Your credentials fall into any of these three categories:

Something you **know**
(like a password or PIN)

Something you **have**
(like a smart card)



Something you **are**
(such as fingerprint, retina scans, or voice recognition)

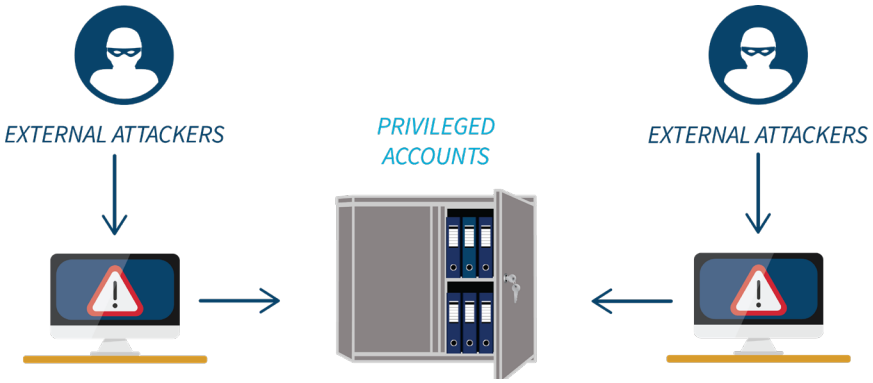
3 - https://pages.nist.gov/800-63-3/sp800-63b.html

Your credentials must come from two different categories to enhance security.
Multifactor authentication means that if one factor is compromised, an infiltrator still has at least one more barrier to breach before successfully breaking into your system.

4. Privileged Accounts Should Not Be Used for Day-to-Day Operations

Privileged accounts, or accounts that have more privileges that ordinary users, give those users the power to do anything in your cloud environment. They are necessary for some tasks but shouldn't be used for everyday use. Practicing a "policy of least privilege" means using the right account for the right job. While an IT manager might not get nefarious ideas while using a privileged account, using one opens the potential for accidentally causing a data breach.

To help enterprises better manage account access, Azure offers a Privileged Identity Management (PIM) feature. PIM allows you to allocate specific access to specific roles for a set time, and these accounts must be frequently reviewed to ensure only approved administrative accounts are used.



5. Use Physical and Logical Groups for Defining Permissions

Using network groups and security groups to define permissions is a logistical best practice for enterprises. Organizations with thousands of users need an easier way to manage cloud access. Access policies written at the group level turns thousands of individuals into a small handful of groups with the same access. Users can be grouped by department and given the access they need to do their specific jobs. For example, everyone in the Engineering team will be in one group and have access to specific things, while your Marketing team will be in another group with different access. Using groups rather than users to define permissions takes a substantial amount of hassle out of Identity and Access Management and creates the possibility for process automation.

6. Use Encrypted Connections

No matter how secure your password is, ensuring that all connections to the computer system are appropriately encrypted is crucial. This will protect the confidentiality of communications and help to ensure that unauthorized parties are prevented from viewing sensitive data. The best practice is to use Secure Sockets Layer (SSL), Transportation Layer Security (TLS), and Virtual Private Networks (VPN). This extends to third party web sites, and users should ensure that SSL/TLS connections are in place whenever they are entering their user ID and password – particularly for sites which contain sensitive user data (e.g., bank accounts or social security numbers).

7. Audit Access to Resources

Regularly reviewing access logs adds an extra layer of security to your process. You can see who accessed what and when. This can help you keep track of your users' activity and determine actions taken on the account and the resources. AWS, GCP, and Azure offer logging features that help make auditing access relatively straightforward.

Planned account access reviews (semi-annual or quarterly) also make sure users still have correct permissions and all inactive accounts are disabled. When individuals join or leave your organization, you know that their access is updated in an accurate and timely manner.

Security Information and Event Management

Protection of sensitive data and critical business assets has become a priority in the electronic age. Thousands of security vulnerabilities are identified each year. Compliance requirements, such as those of HIPAA, SOX, GLBA, and PCI require detailed reporting and analysis of security events. The sheer volume of activity occurring on a network requires sophisticated data analysis and data mining tools to effectively detect, analyze and research threats.

The common vulnerabilities and exploits (CVE) database lists more than 11,000 exploitable vulnerabilities in commonly used systems and software—and as of mid-2019, 34 percent had no patches available.[4]

4 - https://cve.mitre.org/cve/index.html

Security Information & Event Management (SIEM) technology provides real-time analysis of security alerts generated by network hardware and applications. The objective is to help companies respond to attacks faster and organize mountains of log data.

SIEM solutions are used to log security data and generate reports for real-time events, trend analysis and audit purposes. SIEM technology enables organizations to quickly and cost-effectively address reporting and analysis of security events, enhance organizational security posture, and reduce overall risk.

The MediSked SIEM solution includes:

- ✓ Analysis & correlation of security events from many different platforms
- ✓ Security operations centers staffed 24x7 with experienced security analysts
- ✓ Security portal for review of active events and analysis of trends
- ✓ Real-time advanced threat analysis, event correlation and escalation
- ✓ Custom reports to fulfill business and compliance requirements

Benefits

Regularly reviewing access logs adds an extra layer of security to your process. You can see who accessed what and when. This can help you keep track of your users' activity and determine actions taken on the account and the resources. AWS, GCP, and Azure offer logging features that help make auditing access relatively straightforward.

Planned account access reviews (semi-annual or quarterly) also make sure users still have correct permissions and all inactive accounts are disabled. When individuals join or leave your organization, you know that their access is accurate and timely.

Comprehensive Data Collection – Technology can monitor the critical devices in an environment, including firewalls, network, integrity, host and application Intrusion Prevention Systems (IPS)/Intrusion Detection Systems (IDS), web servers, databases, applications, operating systems, Virtual Private Network (VPNs), and network devices. This flexibility and breadth allow utilization of more sources and detect critical attacks missed by other monitoring solutions.

More than 93% of healthcare organizations have experienced a data breach over the past three years[5]

5 - https://securityboulevard.com/2020/01/u-s-healthcare-data-breach-cost-4-billion-in-2019-2020-wont-be-any-better/

Advanced Threat Detection and Prevention – Hackers can evade any single detection mechanism. This problem is solved by using different detection algorithms (signature-based, anomaly detection, statistical analysis, heuristic detection) to detect potential security events. These different analysis techniques are also used to detect anomalies in an environment, including zero-day-attacked (attacks that target publicly known but still unpatched vulnerabilities) and provide significant capabilities for reducing false positive alarms.

The detection mechanisms are implemented based on actual traffic patterns in the customers' unique environment. Unique self-checking mechanisms and analysis ensure that the integrity of the monitoring environment is in place at all times and generates alerts when there are any problems with any components.

Real-Time Response – Develop and continuously evolve custom response and countermeasure strategies to ensure responses correspond to the potential threat level of attacks. This may include an automated response to a set of scans or an intentional block after a certain number of alerts.

Data Mining and Trending – The security portal provides a user-friendly interface to respond to alerts and track remediation workflows through a web-based ticketing system. Additionally, it provides functionality for data mining and cross-correlation of historical events based on user-selected criteria, enabling security analysts to trace security event history with unmatched granularity and customization, from monthly event trending for the entire environment, to individual raw log lines for a single device.

Compliance Reporting – The reporting engine in the security portal allows creation of template-based reports, based on role-based permissions. These reports include monthly, quarterly and yearly attack data analysis with trends for better environment awareness and proactive improvements.

Best Security Practices for Remote Access

Secure access to your organization network and services from any location is a critical component of a successful Information Security Program and requires the implementation of best practices to maintain data integrity.

What is Remote Access?

According to the National Institute of Standards and Technology (NIST), remote access is "the ability of an organization's users to access its nonpublic computing resources from locations other than the organization's facilities" (NIST SP 800-114). The main requirement is the ability to access any pertinent resources on the organization's network that are part of their daily work responsibilities.

Training and Awareness of Security

Remote work demands a higher level of vigilance when it comes to protecting the company's IT resources. Employees should receive education and documentation on best practices for remote access security. Sometimes, face-to-face or in-classroom training may not be possible. But that does not preclude the use of video chats, emails, online documents, or training videos to communicate the necessary information. Every remote employee must earnestly accept the responsibility of maintaining proper IT security at all times.

VPN Connection

Road warriors learned long ago the need to secure their connections with a Virtual Private Network (VPN). Especially important in public Wi-Fi environments such as cafes or libraries, a VPN will encase all your data in an encrypted tunnel as it travels through the public internet. That means that the information is scrambled in such a way that no one can read it without the proper encryption key.

Password Management and Software Implementation

Many breaches occur due to weak password policies and process management. Password management software is critical to cybersecurity. Here are a few steps to ensure proper password management:

- ***One-time Credentials*** – The first thing you can do is create one-time-use passwords only. You can create a log of all your passwords and use them to access essential data. Once done, discard it and use the next.
- ***Password Rotation*** – Password management software entails an automated password rotation. Here, passwords are constantly reset, and you have a limited time to use it. As the lifespan of a password decreases, sensitive data becomes less vulnerable.

Data Encryption

From a security standpoint, data encryption is always a great practice. But it is especially critical because when employees start working remotely, their devices could get lost when they are out of the corporate setting, and that data becomes vulnerable to cyberthreats. Organizations should ensure that all data exchanged between company systems is encrypted by using built-in encryption and test for verification. Futhermore, end-point devices (e.g. laptops) should have full-disk encryption to ensure sensitive data is also secure when at rest.

Physical and Technological Security

A lost or stolen laptop with sensitive information can be a disaster for an organization — and a possible career ender for the employee. The user should not leave a company device unattended while in a public cafe or other venue. At home, the user should be careful not to let children or guests use or play with company laptops. Ask your employees to use a safe internet connection; ask them to set a strong password for their internet router. Secondly, teach employees to identify malicious content online. Most of the time, employees may download malicious software, click open an email sent for phishing purposes, and so on.

Two-Factor Authentication

Before your employees can access the company resources remotely, they should be subject to strict access control. The best way to do this is two-factor authentication. One of the best practices here is to adopt the golden principle of least privilege. This means that access to all employees is blocked by default settings and will only be enabled for users who require it. Although it requires extensive configuration, the added security is worth it.

Conclusion

We have witnessed some major cybersecurity lapses time and again which have cost companies big time. Even tech giants are not safe from it as hackers are able to penetrate through their defenses to access their databases. Therefore, you must provide secure remote access to your team to protect your company's sensitive information. We have shared some of the best practices above, by implementing them, your organization can achieve a great productivity level without compromising on the security.

MediSked is the leading brand in holistic solutions that improves lives, drives efficiencies, and generates innovations for health and human service organizations that support our community. MediSked supports three lines of business: provider agencies, care coordination / payer organizations, and government oversight. MediSked Connect, MediSked Coordinate, MediSked Connect Exchange, and MediSked Portal combine to provide innovative, person-centered technology that improves outcomes and quality while reducing costs for individuals receiving home and based community services and long-term services and supports. Founded in 2003, MediSked currently supports clients and users across the United States. MediSked is number 1068 on the 2020 list of Inc. 5000 Fastest Growing Companies.

Want to learn more? Check out medisked.com!