Social media applications: Protect enterprise’s crown jewels from access control vulnerabilities

Table of content

1 Overview

2 Key Challenges in social media applications’ security management

3 Who are the malefactors?

4 What can be done to protect social media applications?

5 How ARCON fulfils significant functional requirements in securing corporate social media applications

6 Conclusion
Social media applications are prized-assets for today’s organizations. As rightly said, these crown jewels, thanks to their ability to influence the decision-making process and people in general, are one of the most critical components to build brands. However, misuse or abuse of social media applications can be equally devastating for an organization. For instance, uncontrolled access to corporate social media applications or their credentials/password theft can inflict heavy damage.

It’s time to reflect on the way enterprises manage social media applications. The reputational damage caused by social media application misuse can be irreversible. The security and risk management staff should implement a continuous approach to control and govern social media applications. In this whitepaper we will explain how ARCON’s enhancements in endpoint security and password management can help protect social media applications from unauthorized access.
Key challenges in social media applications’ security management

a) Lack of centralized governance framework

Ad hoc controls and decisions as to using social media applications increase security vulnerabilities. If there is no framework to govern and authorize social media application users, unauthorized access can cost organizations dearly. Enforcement of relevant social media application access policies reduces risks.

b) Lackadaisical attitude towards end-user visibility over social media applications compared to other mission-critical data assets

IT visibility encompasses authentication, passwords rotation, and elevation of end-users with time-bound restrictive access to applications. Unfortunately, much of the attention is geared toward other business-critical applications like HR applications, CRMs, ERP application among other IT resources for daily business and IT operations use-cases. Therefore, business SaaS applications, human Privileged accounts, non-human privileged accounts (DevOps, APIs, Bots) et al. receive more security attention. As these data assets are awash with sensitive information, IT security staff tend to regulate end-users’ access by formulating stringent validation and identity management, access and control policies. However, resetting passwords and elevating admin access just-in-time to corporate social media applications is equally important.

c) Outsourced social media services

There is a growing trend, especially among small and medium-scale enterprises, to hire external marketing agencies. This model serves their purpose as they tend to benefit from digital marketing agencies’ expertise on effective use of social media applications. However, lack of security controls and policy enforcements in a third-party environment can expose social media applications to malefactors.
Who are the malefactors?

Corporate Insider

The corporate insider may have malicious intentions to harm an organization. The malicious insider may snoop around social media users (admins), their credentials, and their marketing materials. When this insider is in complete control of all the information, social media applications can be misused to tarnish the reputation of an organization.

Third-Party Users

Just like corporate insiders, any person privy to access credentials with uncontrolled elevation to endpoints can misuse social media accounts in a third-party environment. Greed, social engineering and/or espionage can be the factors.
What can be done to protect social media applications?

While managing corporate social media applications, an organization's IT security team must keep in mind the following key questions:

- Is there an access control management to secure corporate social media applications?
- Are passwords frequently changed?
- Are there proper controls and policy enforcements in an outsourced digital marketing agency?
- Are shared credentials being used by admins and mutual access permitted for corporate social media accounts?
**Centralized policy enforcement for social media administrators**

In the backdrop of ever-increasing number of SaaS applications, IT security teams often find themselves in difficult situations. The key challenge is establishing governance and control over endpoints and applications. ARCON | Endpoint Privilege Management (EPM), a solution that can also be integrated with ARCON | Privileged Access Management, fosters centralized policy enforcement.

Centralized policy enforcement ensures priority-wise profiling of all on-boarded end-users. This unified control framework establishes rule and roles based on end-users’ access to applications, including social media administrators.

**Endpoint privilege elevation on-demand**

Furthermore, EPM enforces time-bound access to applications. So, if there is one or more than one social media administrator, then an IT administrator or IT risk management team can grant the on-demand endpoint privileges to a particular social media application on just-in-time basis. After the task is completed, the elevated privileges from the endpoint are revoked. EPM significantly reduces threats arising from uncontrolled access to business-critical applications.

**Password change**

One serious mistake we often tend to make is that passwords are not frequently changed. The greater the number of end-users, including privileged users, the higher the risk of password theft. It is extremely important to reset passwords at regular intervals.

ARCON | Privileged Access Management can schedule password changes for social media apps such as Gmail/LinkedIn by creating its services and changing the password through the RPA bot.
Conclusion

Social media applications are as vulnerable as any other business-critical applications. Access controls and policy enforcements are must to keep them safe and secure. Restricted endpoint elevation, resetting passwords at regular intervals and due diligence on security framework implemented by a third-party digital marketing agency can significantly reduce the risks associated with social media applications.
About ARCON

ARCON is a leading enterprise information risk control solution provider, specializing in Privileged Access Management (PAM) and continuous risk assessment solutions. Our mission is to help enterprises identify emerging technology risks and help mitigate them by robust solutions that predict, protect and prevent.

PAM: ARCON | Privileged Access Management (PAM) is a highly effective solution that helps in managing, controlling and monitoring privileged user activities. The solution provides IT security team with a centralized policy framework to authorize privileges based on roles and responsibilities ensuring rule-based restricted access to target systems.

UBA: ARCON | User Behaviour Analytics (UBA) is a highly effective risk predictive & analytics tool built for daily enterprise use cases. It breaks the traditional approach of ‘restrictive’ access and is capable of crunching large lakes of enterprise data, spot anomalous activity and trigger alerts in real-time.

SCM: ARCON | Security Compliance Management (SCM) allows an enterprise to prioritize security and compliance efforts based on risk level. The tool enables continuous risk assessment for critical technology platforms and ensuring desired compliance levels.

Connect with us  

All rights reserved by ARCON
This document or any part of the document may not be reproduced, distributed or published in any form without the written consent of the copyright owner under any circumstances. Any kind of infringement in the owner’s exclusive rights will be considered unlawful and might be subject to penalties. This document was made in good faith with all the available information at the time of publishing. For the latest updates, please get in touch with our sales team.