Omada

Identity Security Breach Management

IdentityPROCESS+

79%

have had an identity-related breach within the last two years

Only 26%

of enterprises today are very confident they can prevent identity breaches

206 days

Average time it takes after initial intrusion to identify a data breach

73 days

Average time to then remediate the impact of a data breach

$1.23M

Average reduction in breach-related costs for companies able to detect and contain a breach in fewer than 200 days

Source: 2021 Trends in Securing Digital Identities, Identity Defined Security Alliance

A breach is something that no security leader likes to think about, nevermind deal with in real-time. Breaches can be particularly damaging when they are identity-related, both in terms of how long it takes to identify that a breach has occurred and in overall economic damage.

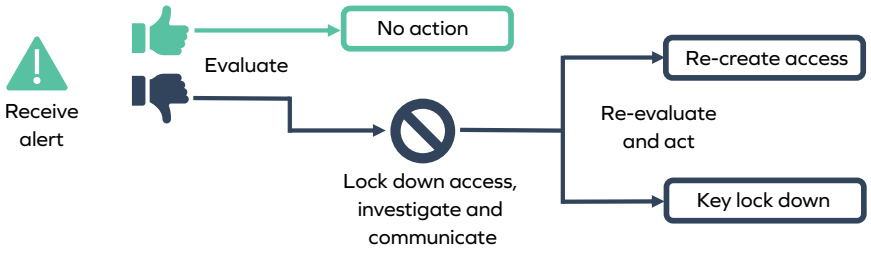
As part of Omada IdentityPROCESS+, there are several key components to Identity Security Breach Management. These are critical to follow best practices, to ensure that business efficiency is optimized, security is tight, and compliance is met.

Background

Having a defined procedure for when an Identity Security breach occurs can help limit the loss or corruption of sensitive data, limit lateral movement, and enable automation of emergency lockout. If not planned out in advance these can be incredibly lengthy processes. Identity Security Breach Management processes outlined in IdentityPROCESS+ provide administrators with the ability to suspend all accounts associated with an identity that is suspected to be breached. This allows the administrator to reactivate access once the situation is under control.

IdentityPROCESS+ allows the breach processes to be initiated manually, but also provides the background needed to curate a more advanced solution by giving and receiving triggers from SIEM, UEBA, or threat analytics tools.

The Security Breach



Simplified identity security breach management

The use of the security breach process must be considered carefully as it involves removing access from individuals. The possible negative implications of using this process includes unnecessarily restricting a user's access to critical business systems or resources due to a suspected external or internal security breach.

Identity Security Breach Questions to consider:

- Is the security breach policy written down?
- Which stakeholders should be involved?
- Is there a process to limit who knows about the triggering of the security breach process?
- What is the process to roll back the emergency lockout in the event of the initial suspicion being incorrect?

Process Stakeholders

Within IGA processes, it is critical that multiple stakeholders are aligned and working together. For Identity Security Breach Management, the following teams must be involved in the following capacities:

HR

- Ensure that corporate policies are being followed
- Write down policies in place to govern the breach process

IGA Team

- Initiate emergency lockout procedure when necessary
- Return access when all is restored

This then would prevent users from performing their roles. However, as there are instances when disabling a user's access is legitimate - such as when a security breach is detected or when inappropriate use of the systems is evident - there are times when this process needs to be used. It is therefore important for the organization to have a formal policy governing how this process should be used and what should be taken into consideration.

Emergency Lockout

As prescribed in IdentityPROCESS+, organizations can disable user accounts belonging to an individual if the security or IT team suspect they have been compromised. In the event of compromise, the emergency lockout process is used to set an identity to 'locked' which disables access to all systems to which that identity is normally entitled. This automatic process shortcuts the need for permission from a manager, which can sometimes slow the process if someone needs to manually intervene. This drastic action should only be used in a true emergency where there is a high degree of certainty that a breach has occurred. A manager or security practitioner can manually start the emergency lockout process in Omada by selecting the identity they want to lock, then enter a reason why. Omada then sets that identity to 'locked' and the assignment is set to 'disabled'.

When lockout is no longer needed, the manager selects the identity to unlock and enters a reason why. Omada then sets the identity to 'unlocked' and the assignment parameter is set back to 'active.' More on this below.

Revoke Emergency Lockout

When an emergency lockout for an identity is no longer needed, or a remedy has been found, managers and operations administrators need to quickly unlock the identities so that work can continue. This process reenables previous access to all target systems for the identity. To do so, a manager or operations administrator starts the 'revoke emergency lockout' process in Omada and selects the identity they want to unlock. For auditing purposes, they must input a reason why the identity is to be unlocked. Omada then sets the identity to 'unlocked' and the assignment parameter is set back to 'active'.