IDENTITY SECURITY BREACH MANAGEMENT

LIMIT YOUR BREACH EXPOSURE

To limit the impact of a potential breach exposure in the event of security breaches or cyber-attacks action must be taken quickly and efficiently. The breach must be contained so that the damage is limited and the lateral spread to other systems is minimized. Lack of automated identity security breach processes makes it difficult to create an overview of which access a compromised identity has and to lock these down immediately across the relevant business systems.

CROSS-SYSTEM ACCESS SUSPENSION

Omada's IdentityPROCESS+ framework provides best practice processes for identity security breach management including an emergency lockout which enables administrators to disable a user's access to all on-premises and cloud-based systems. Cross-system access suspension limits exposure to further breaches while an investigation is carried out and the user's passwords are reset.

Processes for identity security breach management:

- **Suspend access:** Gives administrators the ability to suspend all accounts associated with an identity
- **Reactivate access:** Allows the administrator to reactivate the access once the situation is under control

Suspending the access quickly stops an attacker from continuing to perform any network reconnaissance, stealing confidential or sensitive data, or causing disruption to operations by corrupting data or making critical business systems unusable.

Suspending breached accounts gives the company time to perform a technical investigation and to deal with the non-technical aspects of critical security incidents such as internal and external communications management, protecting the company's reputation and brand, and fielding external calls from customers and the press.

Why identity security breach management is important:

1. To limit the loss or corruption of sensitive data
2. To limit lateral movement through the network by an attacker
3. To enable automation of an emergency lockout due to information from other security monitoring tools

EMERGENCY LOCKOUT

In the event of a user account being compromised, the emergency lockout process is used to set an identity to "locked" which disables access to all systems for that identity. To reduce the time to implement the lockout, this process shortcuts the need for permission of the employee's manager which would be the normal procedure. As a result, it should only be used in emergency cases or if requested by authorities and therefore a process should be defined in written company policies.

REVOKE EMERGENCY LOCKOUT

The process to reactivate access ensures that once investigations have established the causes of the breach and the security administrators have taken the necessary steps to ensure the breach will not reoccur. The locked identities can be quickly reactivated so that business operations can continue and users can access their systems to continue working.

Once the situation causing an organization to lock out an account has been resolved, managers and operation administrators can reactivate the locked identities and reenable previous access to all target systems.

Omada

Omada is a market leading provider of IT security solutions for identity management and access governance. Omada delivers services within identity and access governance, risk management, compliance, role-based access management, and process governance. Omada enables organizations to achieve compliance, reduce risk exposure, and maximize efficiency – providing policies, processes, and solutions for fulfillment of governance demands. Established in 2000, Omada has operations in Europe and North America, delivering its solution via a network of skilled partners and system integrators. **www.omada.net | info@omada.net**

DO MORE WITH IDENTITY