Identity And Access Management Strategies against Ransomware Risks

Least Privilege

- ✓ Grants only the minimum access needed for each user or system
- ✓ Limits ransomware spread if credentials are compromised
- ✓ Reduces overall damage by containing access scope
- ✓ Minimizes attack surface by restricting unnecessary permissions and privileges

Role-Based Access Control

- ✓ Assigns permissions based on defined user roles within the organization
- ✓ Ensures access is granted strictly on necessity, not convenience
- ✓ Reduces insider risk and limits damage from compromised credentials
- ✓ Improves security governance through consistent and structured access control

Multi-Factor Authentication

- ✓ MFA Even if login credentials are stolen, attackers still face additional authentication barriers.
- ✓ This extra layer makes unauthorized access significantly more difficult.
- ✓ MFA is effective in reducing ransomware risks linked to compromised accounts

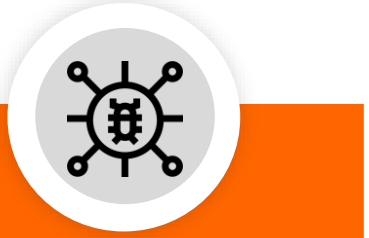
Regular Audits and Compliance Checks

- ✓ Regular audits and access reviews help detect outdated or inappropriate permissions early
- ✓ These checks ensure that unnecessary or excessive access rights are updated or removed quickly
- ✓ Ongoing monitoring supports compliance with internal security policies and regulations
- ✓ Reduces opportunities for ransomware attacks by limiting exploitable access rights

Identity And Access Management Strategies against Ransomware Risks

Automated Provisioning and Deprovisioning

- ✓ Automated systems adjust user access rights quickly when roles change within an organization
- ✓ Ensures that access is immediately removed when employees leave the company
- ✓ Reduced risk of unused or outdated credentials remaining active
- ✓ Limit potential entry points for ransomware attacks



Segregation of Duties (SoD)

- ✓ SoD ensures that no single person has full control over sensitive actions
- ✓ It requires multiple individuals to complete critical processes, reducing individual risk
- ✓ This prevents unauthorized or malicious use of excessive access rights
- ✓ Lowers the chance of ransomware being introduced into critical systems

User Behavior Analytics

- ✓ UBA helps identify unusual activity that may indicate compromised accounts or insider threats
- ✓ It monitors access patterns to detect deviations from normal user behavior
- ✓ Early detection allows security teams to respond before incidents escalate
- ✓ This helps prevent data breaches and the deployment of ransomware

Incident Response Preparedness

- ✓ A clear incident response plan defines roles, responsibilities, and step-by-step actions during a security event.
- ✓ Rapid detection and escalation processes help limit the spread of an attack
- ✓ Coordination between IT, security, and business units ensures an effective and structured response
- ✓ Post-incident analysis supports continuous improvement and strengthens future resilience