Identitäts- und Zugriffsmanagement-Strategien gegen Ransomware-Risiken

Prinzip der geringsten Berechtigungen

- ✓ Gewährt jedem Benutzer oder System nur den unbedingt erforderlichen Mindestzugriff
- ✓ Verhindert die Ausbreitung von Ransomware, wenn Zugangsdaten kompromittiert wurden
- ✓ Reduziert potenzielle Schäden durch die Einschränkung von Zugriffsrechten
- ✓ Reduziert die Angriffsfläche durch die Begrenzung unnötiger Rechte und Privilegien

Rollenbasierte Zugriffskontrolle

- ✓ Weist Berechtigungen basierend auf definierten Benutzerrollen innerhalb der Organisation zu
- ✓ Sichert eine strikt bedarfsorientierte Vergabe von Zugriffsrechten.
- ✓ Reduziert Insider-Risiken und begrenzt Schäden durch kompromittierte Zugangsdaten
- ✓ Verbessert die Security Governance durch eine konsistente und strukturierte Zugriffskontrolle

Multi-Faktor-Authentifizierung

- ✓ MFA stärkt die Sicherheit durch die Anforderung mehrerer Verifizierungsmethoden.
- ✓ Selbst wenn Zugangsdaten gestohlen werden, stehen Angreifer vor zusätzlichen Authentifizierungshürden
- ✓ Diese zusätzliche Schutzschicht macht unbefugten Zugriff deutlich schwieriger
- ✓ MFA reduziert effektiv Ransomware-Risiken, die mit kompromittierten Konten verbunden sind

Regelmäßige Audits und Compliance-Prüfungen

- ✓ Regelmäßige Audits und Zugriffsprüfungen helfen, veraltete oder unangemessene Berechtigungen frühzeitig zu erkennen
- ✓ Die Prüfungen stellen sicher, dass unnötige oder übermäßige Zugriffsrechte schnell aktualisiert oder entfernt werden
- ✓ Kontinuierliches Monitoring unterstützt die Einhaltung von Richtlinien und Vorgaben
- ✓ Verringert Ransomware-Risiken durch die Einschränkung ausnutzbarer Zugriffsrechte

Identitäts- und Zugriffsmanagement-Strategien gegen Ransomware-Risiken

Automatisierte Benutzer- und Rechteverwaltung

- ✓ Automatisierte Systeme passen Zugriffsrechte bei Rollenänderungen in der Organisation schnell an
- ✓ Stellt sicher, dass Zugriffe beim Verlassen des Unternehmens sofort entfernt werden
- ✓ Reduziert das Risiko, dass alte oder ungenutzte Credentials aktiv bleiben
- ✓ Begrenzt potenzielle Einstiegspunkte für Ransomware-Angriffe

Funktionstrennung (SoD)

- ✓ SoD stellt sicher, dass keine einzelne Person die vollständige Kontrolle über sensible Vorgänge hat
- ✓ IEs erfordert mehrere Personen zur Durchführung kritischer Prozesse und reduziert so das individuelle Risiko
- ✓ Dies verhindert die unbefugte oder böswillige Nutzung übermäßiger Zugriffsrechte
- ✓ Senkt die Wahrscheinlichkeit einer Ransomware-Infektion kritischer Systeme

Analyse des Nutzerverhaltens

- ✓ UBA unterstützt die Erkennung ungewöhnlicher Aktivitäten, die auf kompromittierte Konten oder Insider-Risiken hinweisen
- ✓ Überwacht Zugriffsmuster, um Abweichungen vom normalen Benutzerverhalten zu erkennen.
- ✓ Früherkennung erlaubt es Sicherheitsteams, zu handeln, bevor sich Vorfälle eskalieren
- ✓ Dies trägt dazu bei, Datenverletzungen und Ransomware-Angriffe zu verhindern

Incident-Response-Vorbereitung

- ✓ Ein klarer Incident-Response-Plan legt Rollen, Verantwortlichkeiten und konkrete Schritte bei Sicherheitsvorfällen fest
- ✓ Schnelle Erkennung und Eskalation tragen dazu bei, die Ausbreitung eines Angriffs zu begrenzen.
- ✓ Die Abstimmung zwischen IT-, Sicherheits- und Fachbereichen sorgt für eine effektive und strukturierte Reaktion
- ✓ Post-Incident-Analysen tragen zur kontinuierlichen Verbesserung und höheren Resilienz bei