



oplon®

SECURE ACCESS

NIS2

Oplon Secure Access ist ein entscheidendes Element, um die Einhaltung der NIS2-Richtlinie in mehrfacher Hinsicht zu unterstützen. Im Folgenden wird erläutert, wie Oplon Secure Access zur Einhaltung der Richtlinie beitragen kann:

Verwaltung des privilegierten Zugriffs

ZUGANGSKONTROLLE

Oplon Secure Access PAM hilft bei der Kontrolle und Überwachung des Zugriffs von Benutzern mit erhöhten Privilegien und stellt sicher, dass nur autorisierte Personen auf kritische Systeme und sensible Informationen zugreifen können.

GRUNDSATZ DES MINDESTPRIVILEGS

Es setzt das Prinzip der minimalen Privilegien um, indem es den Benutzern nur die Berechtigungen zuweist, die sie für die Ausführung ihrer spezifischen Funktionen benötigen.



2. Überwachung und Prüfung



AKTIVITÄTSVERFOLGUNG

Es zeichnet alle Aktivitäten privilegierter Benutzer auf und liefert einen detaillierten Prüfpfad, der zur Erkennung verdächtigen Verhaltens und zur Reaktion auf Sicherheitsvorfälle verwendet werden kann.

BERICHTERSTATTUNG ÜBER VORFÄLLE

Oplon Secure Access erleichtert die rechtzeitige Meldung von Sicherheitsvorfällen, wie von NIS2 gefordert, durch seine Fähigkeit, die Aktionen von privilegierten Benutzern in Echtzeit zu überwachen und aufzuzeichnen.

3. Sicherheit der Berechtigungsnachweise

VERWALTUNG DER PASSWORTERS

Es automatisiert die Passwortverwaltung für privilegierte Konten und stellt sicher, dass die Anmeldedaten sicher sind und regelmäßig aktualisiert werden.

PASSWORT-ROTATION

Es implementiert eine automatische Passwortrotation, um das Risiko der Kompromittierung von Zugangsdaten zu verringern.



4. Rollenbasierte Zugangskontrolle (RBAC)

ROLLENDEFINITION

Es ermöglicht die Definition und Verwaltung von Rollen und Berechtigungen auf der Grundlage der spezifischen Anforderungen der verschiedenen Funktionen innerhalb der Organisation.

TEMPORÄRER ZUGANG

Es erleichtert die Gewährung eines zeitlich begrenzten Zugangs für bestimmte Aktivitäten, indem es die Dauer des privilegierten Zugangs begrenzt.

5. Compliance und Berichterstattung

BERICHTERSTELLUNG

Es liefert detaillierte Berichte über den Zugriff und die Verwendung von privilegierten Zugangsdaten, die für Compliance-Audits und zum Nachweis der Einhaltung der NIS2-Anforderungen nützlich sind.

COMPLIANCE-RICHTLINIE

Es hilft bei der Implementierung und Pflege von Sicherheitsrichtlinien, die den Anforderungen von NIS2 entsprechen, und stellt sicher, dass die besten Praktiken der Zugriffsverwaltung eingehalten werden.



6. Reaktion auf Vorfälle



UNFALLISOLIERUNG

Oplon Secure Access ermöglicht es Ihnen, kompromittierte Konten oder verdächtige Aktivitäten schnell zu isolieren und so die möglichen Auswirkungen eines Sicherheitsvorfalls zu begrenzen.

FORENSISCHE ANALYSE

Es liefert detaillierte Daten für die forensische Analyse nach einem Unfall und erleichtert so das Verständnis der Ursachen und die Durchführung von Korrekturmaßnahmen.

Die Implementierung von Oplon Secure Access trägt nicht nur zum Schutz kritischer Informationen und Systeme bei, sondern ist auch ein wichtiger Schritt in Richtung **NIS2-Konformität**, der dazu beiträgt, die allgemeine Sicherheit des Unternehmens zu stärken und das Risiko von Sicherheitsvorfällen zu verringern.

oplon®

Oplon Networks ist ein im Jahr 2010 gegründetes Unternehmen für Computertechnik.

Unser Ziel ist es, Produkte und Dienstleistungen zu entwickeln, die eine hohe Zuverlässigkeit und Sicherheit auf Infrastrukturebene bei der Bereitstellung von Dienstleistungen mit außergewöhnlichen Qualitätsstandards garantieren. Exzellenz ist unser oberstes Ziel! Aus diesem Grund entwickeln wir Cybersecurity-Tools und integrierte Lösungen zum Schutz moderner Rechenzentren, Netzwerke, Clouds und Hybrid-Clouds.

Daten und Funktionen können sich jederzeit ohne vorherige Ankündigung ändern.

Weitere Informationen finden Sie auf unserer Website <https://www.oplon.net> oder schreiben Sie uns an info@oplon.net

