Schluss mit Chaos & Datenlecks in Teams und M365.

SecureWork für Microsoft 365 – powered by Swiss IT Security AG.

Ob Dateifreigabe, Wissensmanagement, Videokonferenzen oder einfache Gruppenchats: Moderne Unternehmen setzen auf Kollaborationstools wie Teams, SharePoint sowie OneDrive – und geraten damit ins Visier digitaler Angreifer.

Die Swiss IT Security AG sichert Ihre Microsoft 365-Umgebung mit dem neuen Servicepaket SecureWork vollständig ab: Es vereint hauseigene Sicherheitssoftware mit ausgereiften Security & Govenance-Strategien und sorgt zudem für eine produktivere Zusammenarbeit.

Knotenpunkt Teamarbeit: Wenn Chaos zu Sicherheitslücken führt.

Die Stärke von Kollaborationstools wie Teams, Sharepoint oder OneDrive ist auch ihre grösste Schwäche:
Als zentraler Knotenpunkt für Daten, Chats oder Transkripts von Videokonferenzen erhält ein Angreifer mit nur einem ausgespähten Login sofortigen Zugriff auf weitreichende Unternehmensinterna.

Die Verbreitung von M365 und Teams ohne Governance führt ausserdem zu unkontrolliertem Wildwuchs: Zahlreiche Teams Workspaces werden zu bestimmten Zwecken und von verschiedenen Mitarbeitern erstellt. Doch was, wenn der Zweck erfüllt ist und sich niemand verantwortlich fühlt? Was, wenn die Verantwortlichen das Unternehmen verlassen?

Das sorgt für Chaos und bremst die Produktivität aus. Im Ernstfall erhalten Unbefugte durch verwaiste Teams Workspaces Zugriff auf Inhalte, die sie keinesfalls haben dürften.

Hier setzt die Swiss IT Security AG an:
Unser **SecureWork**-Paket verbessert die Sicherheit Ihrer Kollaborationstools mit einer Kombination aus neuen Governance-Strategien und hauseigener Software zur sicheren Dateiübertragung, Verwaltung von Gastkonten und Microsoft Teams Governance – alles aus einer Hand.

Swiss IT Security AG
Etzelmatt 3, 5430 Wettingen, Schweiz
Telefon: 0848 088 088
info@sits.ch – www.sits.ch

Wenn Sie Interesse oder Fragen zu unserem Angebot haben, dann rufen Sie uns gern direkt an. Wir freuen uns auf Sie!

SecureWork – Die 3 Kern-Komponenten

#1 – TEAMS GOVERNANCE MIT VALO TEAMWORK

Die Experten der Swiss IT Security AG implementieren vollumfängliche Governance-Strategien basierend auf Valo Teamwork, IAM, Lifecycle-Management & mehr in nur drei Phasen:

- Phase I – Schwachstellendefinition
- Phase II – Umsetzung der Sicherheitsstrategie
- Phase III – Umsetzung, Go-Live & Support

#2 – GÄSTE-MANAGEMENT MIT GUEST LIFECYCLE FOR AZURE AD

Unsere Guest Lifecycle for Azure AD-Lösung sorgt für die sichere Verwaltung und Enrollment von Gästen, Partnern und externen Dienstleistern. Die Lösung umfasst die Erstellung von Gastkonten in Azure AD, Zuweisungen an verantwortliche Personen sowie die automatische Sperrung und Löschung von Gastkonten nach Inaktivität.

#3 – SICHERER DATEIAUSTAUSCH MIT INDIVIDUAL FILESHARING

Die hauseigene Lösung Individual Filesharing for SharePoint Online (IF4SPO) erlaubt eine sichere Dateifreigabe über SharePoint Online. Sie umfasst die Speicherung von Ordnern in anonymen Libraries, verhaltens- und zugriffsbasierte Privilegien sowie Regeln zur automatischen Löschung oder Archivierung.

Alle Details zu den drei Komponenten finden Sie unten. Bei uns stehen Ihre Bedürfnisse an erster Stelle: Alle drei Lösungen können wir vollständig oder völlig massgeschneidert und passgenau auf Ihr Unternehmen umsetzen.

#1 – Risiko verwaiste Teams und Sites: 7 Strategien zur sicheren Produktivität

Ab Werk bieten Microsoft Teams und SharePoint noch grosses Potential zur sicheren Kollaboration, aber auch ein grosses Potential für Sicherheitslücken: Denn schon nach kurzer Nutzungszeit entstehen verwaiste Teams Workspaces und SharePoint Sites, Zugriffsrechte sind oft nur mässig verwaltet (sprich: Unbefugte erhalten Zugriff) und alte Daten werden nicht sauber abgesichert. Hier setzen wir mit einer vollumfänglichen MS Teams Security & Governance-Strategie an:

1. Sicherheit Ihres Tenants:
Assessment aller sicherheitskritischen Komponenten von M365, etwa Tenant-Einstellungen, Conditional Access oder PIM und Erstellung eines Anforderungskatalogs, der alle aktuellen Sicherheitsstandards (CIS-Benchmark und etablierte Best Practices) erfüllt. So können Teams und SharePoint sicher bedient werden.

2. Sicherheit für Kollaboration:
Zur Verstärkung der Sicherheit (Hardening) von Teams, SharePoint Online und OneDrive for Business erstellen wir gemeinsam einen Anforderungskatalog. Er beinhaltet Spezifikationen, etwa Regelungen zur Nutzung von Chats, Apps in Teams oder Freigaben.

3. Datenräume für sensitive Inhalte:
Da nicht alle Daten gleich schützenswert sind, definieren wir Datenräume mit unterschiedlich strengen Vertraulichkeitsstufen. Pro Datenraum werden Zugriffsrechte und Freigaben für externe Personen definiert. Nur so gewährleisten Sie eine gesunde Balance zwischen Schutz und Produktivität.

4. Teams und SharePoint Governance:
Erstellung von Governance-Strategien, die eine sichere Nutzung von Teams sowie SharePoint ermöglichen und die Produktivität durch eine einfachere Übersicht und Verwaltung mitbringen.

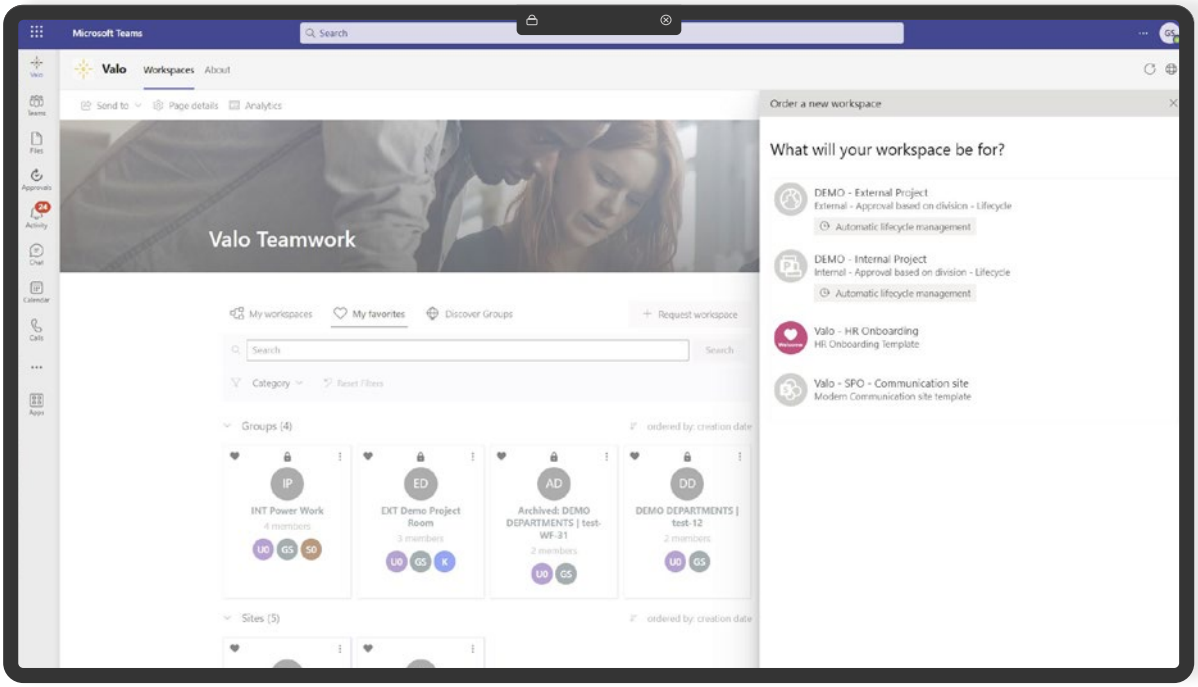
5. Zugriffsverifizierung:
In regelmässigen Abständen werden Teams-Owner aufgefordert, Zugriffsrechte Ihrer Workspaces und Inhalte zu prüfen und entsprechend anzupassen. Das sorgt dafür, dass zu jedem Zeitpunkt nur Personen auf Inhalte Zugriffe haben, die sie auch wirklich benötigen.

Swiss IT Security AG
Etzelmatt 3, 5430 Wettingen, Schweiz
Telefon: 0848 088 088
info@sits.ch – www.sits.ch

Wenn Sie Interesse oder Fragen zu unserem Angebot haben, dann rufen Sie uns gern direkt an. Wir freuen uns auf Sie!

6. Schutz vor Datenverlust:
Erstellung oder Ergänzung existierender Data Loss Prevention-Regeln auf Basis der Datenraumkonzepte. Sind diese noch nicht vorhanden, entwickeln wir gemeinsam neue Richtlinien, damit Daten auch in offenen Workspaces nicht verloren gehen oder in unbefugte Hände geraten.

7. Lifecycle Management:
Jeder Teams-Workspace und jede SharePoint-Site wird für einen bestimmten Zweck aufgesetzt, dessen Ziel, Umfang und Mitglieder sich oft mit der Zeit ändern. Ist der Zweck erfüllt, sollte der Workspace oder die Site entsprechend archiviert oder vollständig gelöscht werden. So wird verhindert, dass nicht mehr verwendete Inhalte in falsche Hände geraten.



Das Expertenteam der Swiss IT Security AG kümmert sich um jeden Schritt – von der Erstberatung über das Aufsetzen oder Anpassung einer Strategie an Ihre Bedürfnisse bis hin zur Implementierung mittels Valo Teamwork und der Konfiguration entsprechender M365-Dienste sowie fortlaufendem Support und Überwachung. Die Umsetzung erfolgt in drei Phasen:

PHASE I	PHASE II	PHASE III
Gemeinsam identifizieren wir Schwachstellen und Problemherde in Ihrer Umgebung mit Teams Workspaces und SharePoint Online Sites. Ist MS Teams (noch) nicht im Einsatz, erstellen wir gemeinsam ein Konzept zur sicheren Einrichtung.	Umsetzung der im Sicherheitskonzept festgelegten Anforderungen und der Einrichtung der Teams & SharePoint-Governance Strategie mittels Valo Teamwork.	Unterstützung des Go-Live von MS Teams und unserer Governance-Lösung mittels Schulung und Anleitung des Kunden sowie 2nd / 3rd Level Support.

Swiss IT Security AG
Etzelmatt 3, 5430 Wettingen, Schweiz
Telefon: 0848 088 088
info@sits.ch – www.sits.ch

Wenn Sie Interesse oder Fragen zu unserem Angebot haben, dann rufen Sie uns gern direkt an. Wir freuen uns auf Sie!

#2 – Das Risiko verwaister Gastkonten: Mit Guest Lifecycle for Azure AD sicher verwaltensicher verwalten

Die Zusammenarbeit mit Partnern, Gästen und externen Dienstleistern über Microsoft 365 erfolgt oft über verschiedene Tools wie OneDrive, SharePoint Online oder Teams. Um Datenlecks und unberechtigte Zugriffe zu vermeiden, müssen Gastkonten in Azure AD gesondert behandelt werden.

Die Swiss IT Security AG hat dazu eine Eigenlösung namens Guest Lifecycle for Azure AD (GL4AAD) entwickelt. Basierend auf der Microsoft Power Platform und entsprechenden Azure-Diensten wird es leicht in Ihren Microsoft 365 Tenant eingebunden und übernimmt die folgenden Aufgaben:

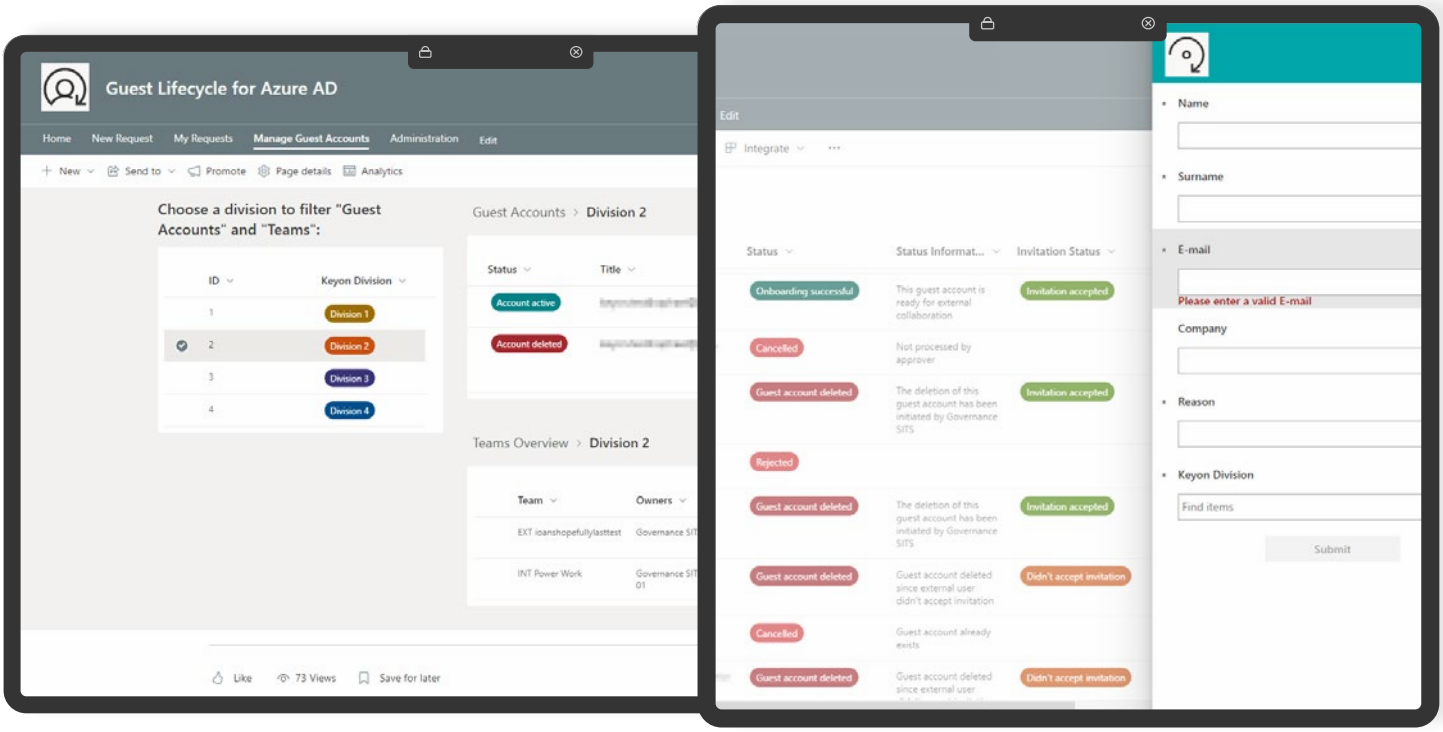
1. Onboarding:
Gäste werden automatisch eingebunden und auf Wunsch über das 4-Augen-Prinzip zugelassen. Im Rahmen dessen müssen Gäste kritische Richtlinien rund um Sicherheit, Vertraulichkeit und Verhaltensnormen beim Benutzen Ihrer Infrastruktur akzeptieren. Dies beinhaltet die entsprechende Konfiguration und Absicherung von Azure AD.

2. Verantwortung
Zuweisung jedes Gastkontos an eine Abteilung und Person, die fortan für dessen Lifecycle und Abläufe verantwortlich ist.

3. Multi-Faktor Authentifizierung:
Einrichtung und Verwaltung von MFA-Richtlinien zur sicheren Anmeldung und Eingrenzung von externen Benutzern.

4. Löschung nicht mehr existierender Nutzer:
Nicht mehr benötigte Gastkonten werden aufgrund Inaktivität oder Ablaufdatum gesperrt und anschliessend gelöscht. Sie können auch manuell gelöscht werden: zur Erleichterung des Entscheides werden Teams Workspaces aufgeführt, auf welche das betreffende Gastkonto noch Zugriff hat.

GL4AAD kann ganz an Ihre Anforderungen angepasst und mit Azure AD Access Packages kombiniert werden.



Die Highlights von Guest Lifecycle for Azure AD (GL4AAD) im Überblick

- Einfache Verwaltung von Azure AD Gastkonten
- Schnelle Festlegung von Verantwortlichkeiten für Gäste, Freigabeprozesse und Lifecycle-Vorgaben, sodass Gastkonten nach bestimmter Inaktivität oder Ablaufdatum automatisch gelöscht werden

Swiss IT Security AG
Etzelmatt 3, 5430 Wettingen, Schweiz
Telefon: 0848 088 088
info@sits.ch – www.sits.ch

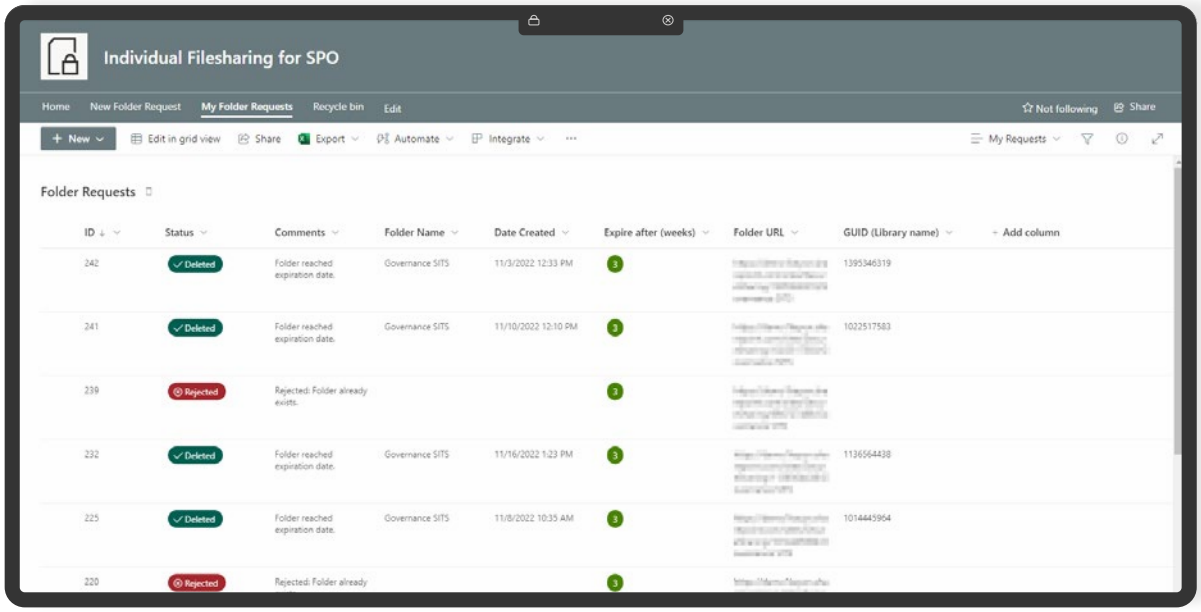
Wenn Sie Interesse oder Fragen zu unserem Angebot haben, dann rufen Sie uns gern direkt an. Wir freuen uns auf Sie!

#3 – Risiko unbefugter Zugriff: Mit Individual Filesharing zur sicheren Dateiübertragung

Ganz gleich ob intern oder extern: Der Empfang und Versand vertraulicher Daten zählt zu den grössten Risiken für Unternehmen. Mit **Individual Filesharing for SharePoint Online (IF4SPO)**, einer Entwicklung der Swiss IT Security AG, erweitern Sie Ihre existierende Microsoft 365-Umgebung um eine sichere Dateifreigabe, sodass Sie etwa Mitarbeitern oder externen Partnern sorgenfrei streng vertrauliche Informationen zuschicken oder einen sicheren Ablageort bieten können.

Mit **Individual Filesharing for SharePoint Online (IF4SPO)** werden Ordner in einer anonymen Library basierend auf vordefinierten Freigaben erstellt. Nutzer können schnell festlegen, wer diese Dateien sehen kann und ab welchem Zeitpunkt Daten gelöscht oder archiviert werden.

Kurzum: **IF4SPO** sorgt für sichere und einfache Berechtigungen beim Teilen und Zugriff Ihrer streng vertraulichen Daten.



Die Features im Überblick

- Speicherung von Ordnern in anonymer Library (Name verrät nichts über Verwendungszweck)
- Strikte und klar definierte Zugriffsrechte basierend auf dem entsprechenden Grund des Zugriffs
- Automatische Löschung oder Archivierung basierend auf Ihren Definitionen
- Optional: Integration mit Individual Filesharing for SharePoint Online (IF4SPO) und Microsoft 365 Data Loss Prevention-Richtlinien

Das Resultat: SecureWork.

Mit unseren Governance-Konzepten, Sicherheitslösungen und Tools **arbeiten Ihre Teams ab sofort sicher und schneller zusammen. Neugierig? Wir schnüren Ihnen gerne ein massgeschneidertes Paket zur sicheren Kollaboration.**

Jetzt loslegen: Mit SecureWork – powered by Swiss IT Security AG

Swiss IT Security AG
Etzelmatt 3, 5430 Wettingen, Schweiz
Telefon: 0848 088 088
info@sits.ch – www.sits.ch

Wenn Sie Interesse oder Fragen zu unserem Angebot haben, dann rufen Sie uns gern direkt an. Wir freuen uns auf Sie!