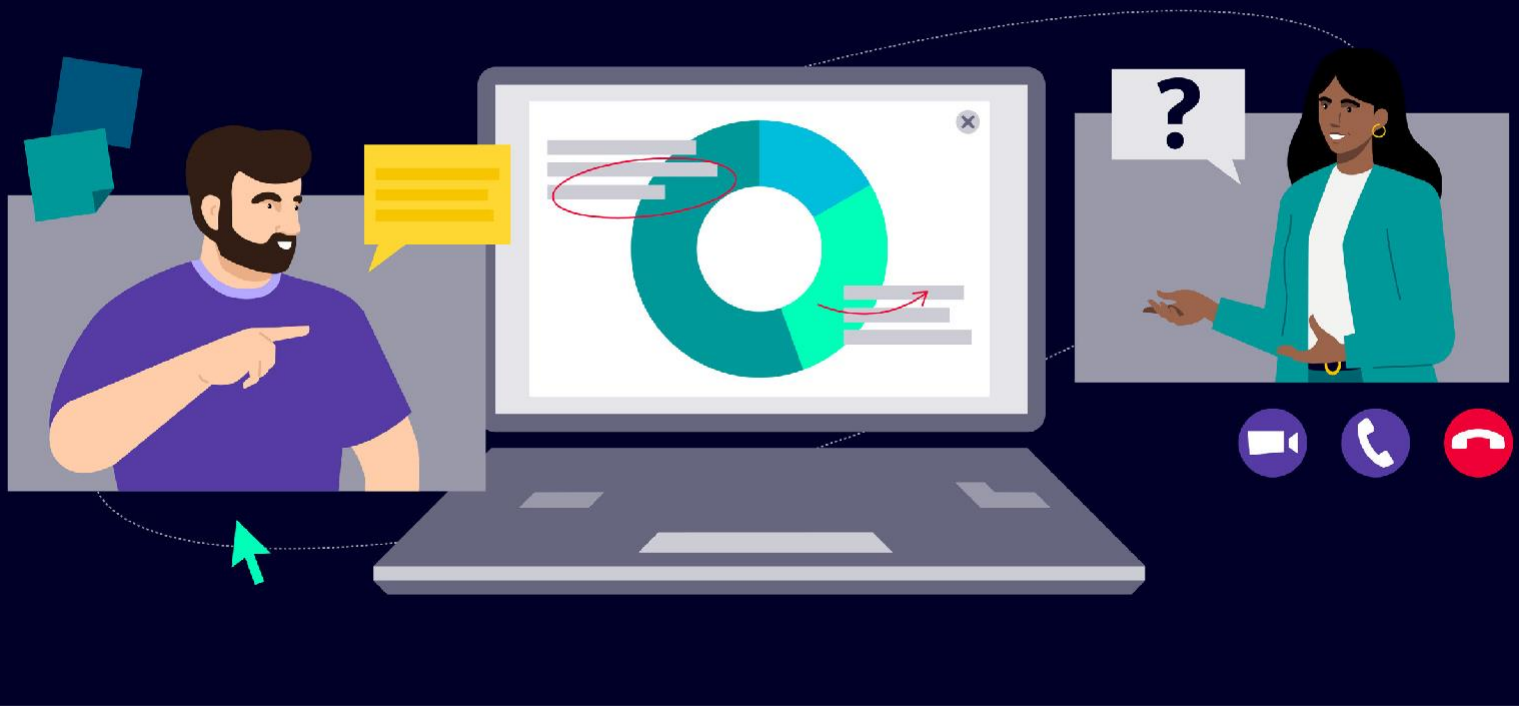

CYBERSECURITY CARD

Sichere Datenübertragung

IT-Services für die sichere Kommunikation und Zusammenarbeit externer Geschäftspartner mit Siemens

Definition

Geschäftspartner (GP): In diesem Zusammenhang handelt es sich um jede externe Partei, die in einer Geschäftsbeziehung zu Siemens steht, aber keinen autorisierten Zugriff auf das Siemens Intranet (z. B. über Business Partner Access) hat und damit auch keinen Zugriff auf die internen IT-Services von Siemens.

Situation

Der Austausch von Informationen mit Geschäftspartnern ist Teil unseres Geschäftsalltags. In einigen Fällen werden Daten und Dokumente (z. B. Kosten, Verträge oder technische Unterlagen) als „vertraulich" oder sogar „streng vertraulich" eingestuft. Zur Sicherstellung einer sicheren Kommunikation und Zusammenarbeit mit solchen Informationen wurde diese anwendungsfallbasierte IT-Service-Übersicht erstellt. Sie hilft sowohl dem Endanwender bei Siemens als auch seinen Geschäftspartnern bei der Ermittlung, Bestellung und Nutzung des jeweils geeigneten Siemens IT-Services. Bitte beachten Sie, dass IT-Services für bestimmte Geschäftsprozesse (z. B. elektronischer Datenaustausch über EDI) nach wie vor Priorität haben und die Übersicht nur die verbleibenden Anwendungsfälle (z. B. Fälle, in denen bisher unverschlüsselte E-Mails ausgetauscht wurden) abdecken sollte.

Bedrohung

Vertraulichkeitsvereinbarungen (NDAs) und die „Rules for Business Partners" (Richtlinie nur in englisch verfügbar) von Siemens legen zwar den richtigen Umgang mit vertraulichen Informationen fest, enthalten aber keine Angabe, mit welcher konkreten IT-Lösung die Vorschriften umgesetzt werden sollen.

Dies führt zu dem Risiko, dass die Anforderungen an die Informationssicherheit zwar bekannt sind, aber nicht korrekt oder vollständig umgesetzt werden.

In dieser Liste werden wichtige Themen hervorgehoben.
Bitte beachten Sie jedoch, dass die Liste keinen Anspruch auf Vollständigkeit erhebt und zusätzlich alle allgemeinen Cybersicherheitsvorschriften gelten.
Aufgrund der besseren Lesbarkeit wird im Text das generische Maskulinum verwendet, gemeint sind jedoch immer alle Geschlechter.

SIEMENS

Verhalten

Was Sie als Geschäftspartner beim Versenden einer E-Mail mit SecuFEx beachten sollten:

Der Geschäftspartner benötigt für den Versand von Daten an einen Mitarbeiter von Siemens ein temporäres SecuFEx-Konto. Dieses temporäre Konto kann von jedem Siemens-Mitarbeiter angelegt und verwaltet werden. Die Nutzer des SecuFEx-Dienstes sind verpflichtet, alle anwendbaren nationalen und internationalen (Wieder-) Ausfuhrkontrollvorschriften einzuhalten.

Was Sie als Geschäftspartner beachten sollten, wenn Sie eine Einladung zu einer virtuellen Konferenz oder einer MS Teams-Besprechung von einem Siemens-Mitarbeiter erhalten:

Der Geschäftspartner muss sicherstellen, dass während der virtuellen Besprechung keine unbefugten Personen Besprechungsinhalte sehen und/oder mithören können. Darüber hinaus ist es dem Geschäftspartner nicht gestattet, Ausdrucke oder Screenshots von Bildschirminhalten zu erstellen, wenn vertrauliche Informationen angezeigt werden. Öffnen Sie während virtueller Besprechungssitzungen nur die Anwendungen und Dokumente, die für Ihre jeweilige Besprechung relevant sind, und vermeiden Sie es, den gesamten Desktop freizugeben. Darüber hinaus dürfen keine vertraulichen Dokumente auf den Server für die virtuelle Besprechung hochgeladen werden.

Anwendungsfall	Empfohlener IT-Service	Max. Schutzklasse	Technische Voraussetzungen	Benutzeranweisungen und Ansprechpartner für technische Fragen
Einmaliger sicherer Dokumentenaustausch				
 "Wir wollen **ein Dokument einmalig *sicher*** austauschen	Secure File Exchange (SecuFEx)	C2 – Vertraulich 	Es muss ein temporäres Benutzerkonto für das Versenden von Dateien durch den Ansprechpartner des Siemens-Geschäftspartners angelegt werden	SecuFEx-Website →
Kontinuierlicher sicherer Dokumentenaustausch				
 "Wir wollen **Dokumente kontinuierlich *sicher*** austauschen	MS OneDrive	C2 – Vertraulich[1] 	Keine	MS OneDrive-Website →
Kontinuierlicher sicherer Daten- und Dokumentenaustausch				
 "Wir wollen **Daten und Dokumente kontinuierlich *sicher*** austauschen	E-Mail-Verschlüsselung	C3 – Streng vertraulich 	• Voraussetzungen → • Implementierungs-Leitfaden zur E-Mail-Verschlüsselung →	Siemens PKI Website →
Sichere Zusammenarbeit				
 "Wir wollen **gemeinsam** an den gleichen Dokumenten **arbeiten**	SharePoint Global Collaboration Service-Portal	C2 – Vertraulich	• PC-Einstellungen • Mobiltelefon oder Token zur Authentifizierung	SharePoint-Website →
	Workspace Strictly Confidential / High Secure-Dateifreigabe	C3 – Streng vertraulich 	Bitte wenden Sie sich an Ihren Cybersicherheitsbeauftragten oder Ansprechpartner bei Siemens	
Sichere Zusammenarbeit im PLM-Umfeld				
 "Wir wollen an **gleichen Dokumenten / Daten im PLM-Bereich** arbeiten, darunter an integrierten, komplexen Szenarien (z. B. Digital Twin)	Siemens Teamcenter (TC)	C2 – Vertraulich[2] 	TC Supplier Collaboration Foundation (SCF) →	SCF-Website →
Zusammenarbeit in Echtzeit				
 "Wir wollen eine ***sichere* virtuelle Besprechung** abhalten	MS Teams	C2 – Vertraulich[3] 	Die Besprechung wird durch einen Ansprechpartner bei Siemens eingerichtet	MS Teams →

[1] Die Schutzklasse „Vertraulich" ist möglich, wenn alle Teilnehmer einen Account auf dem Siemens-Mandanten haben oder die Dokumente ordnungsgemäß mit MIP geschützt sind. In allen anderen Fällen ist nur die Schutzklasse „Intern" möglich.

[2] Abhängig von der lokalen Installation und Konfiguration, maximal bis zu „Intern". Die genaue Schutzklasse muss mit Ihrem Ansprechpartner bei Siemens geklärt werden.

[3] Die Schutzklasse „Vertraulich" ist möglich, wenn alle Teilnehmer einen Account auf dem Siemens-Mandanten haben. Wenn ein Teilnehmer keinen Account auf dem Siemens-Mandanten hat oder sich per Telefon einwählt, ist nur die Schutzklasse „Intern" möglich.

Weitere Informationen (Links):

Siemens Global Webpage →

Zusammenarbeit mit Siemens →