Intelligent Host – Schluss mit Sicherheits-lücken bei Guest Usern

Automatisierte Lösung für sicheres Guest User Management mittels der Power Platform auf Azure

Produkt: Intelligent Host
Umsetzung: Corporate Software AG
Technologie: Microsoft Azure, Microsoft Power Automate, Microsoft Power Apps und Microsoft SharePoint

Corporate Software

Microsoft Partner
Microsoft

Gold Cloud Platform
Gold Cloud Productivity
Gold Data Analytics
Gold DevOps
Gold Collaboration and Content
Gold Project and Portfolio Management
Gold Data Platform
Gold Application Integration
Gold Application Development
Gold Datacenter

Corporate Software AG
Schöneggstrasse 5, 2503 Biel, T +41 32 322 67 05, www.corporatesoftware.ch, info@corporatesoftware.ch

Inhaltsverzeichnis

Darum geht es

Einer der grossen Vorteile von M365 ist es, einfach externe Personen als Gäste in die eigene M365-Umgebung einzuladen, gemeinsame Meetings abzuhalten und Dokumente sowie Ressourcen zu teilen. Dies ermöglicht eine effiziente Online-Zusammenarbeit über Organisationsgrenzen hinweg.

Die Benutzer können passende Rechte vergeben und so den Austausch selbstständig gestalten – diese Selbstbefähigung macht Spass, erzeugt Motivation und ergibt Sinn in einer Welt, in der die Komplexität ständig steigt. Es ist gut, wenn die Business User mehr und mehr Verantwortung in der IT übernehmen und ihre Arbeitsumgebung entsprechend mitentwerfen.

Die Kunden von Corporate Software nutzen diese Möglichkeit intensiv. In mittleren und grossen Azure Active Directories (AAD) führt dies schnell zu vielen Gastbenutzern im Verzeichnis. Microsoft selbst bietet keine Lösung, die die Guest User übersichtlich anzeigt und auch keine Workflows, um allenfalls inaktive Guest User zu erkennen und zu deaktivieren. Da ein unkontrollierter Wildwuchs an Guest Usern, mit zugewiesenen Berechtigungen auf Ressourcen, ein Sicherheitsrisiko darstellt, ist es empfehlenswert, einen Mechanismus zu implementieren, der zur Kontrolle befähigt. Somit kann vermieden werden, dass Artefakte entstehen, von denen niemand den Status kennt, die Ressourcen binden und Sicherheitslücken darstellen.

Corporate Software hat für dieses sehr konkrete Problem das Produkt «Intelligent Host» entwickelt. Basierend auf der Microsoft Power Platform und in Zusammenarbeit mit verschiedenen Pilot-Kunden ist eine Lösung entstanden, die zum kontrollierten Umgang mit bereits bestehenden sowie allen zukünftig hinzugefügten Guest Usern befähigt.

Power Automate regelt die Workflows bezüglich Erstellung, Verlängerung und Löschung der Gastbenutzer, Power Apps funktioniert als Eingabe- und Anzeigemaske, SharePoint-Online-Tabellen dienen als Datenspeicher. Der Wildwuchs hört auf, die Azure AD ist immer auf dem aktuellen Stand und potenzielle Sicherheitslücken werden geschlossen.

«M365 und Azure AD bieten wunderbare Möglichkeiten, um unsere Zusammenarbeit den heutigen Anforderungen an Geschwindigkeit und Komplexität anzupassen. Mit «Intelligent Host» überblicken wir nun auch die Guest User in unserem AD.»

Matthias Gessenay, Corporate Software

Die Intelligent-Host-Lösung im Detail

Wir beleuchten die unterschiedlichen Perspektiven von Intelligent Host. Technik steht im Vordergrund, wir werfen zudem Licht auf Architektur, Sicherheit, Wirtschaftlichkeit, Benutzerinterface, die administrative Seite und schauen, was Intelligent Host mit «Lernen» zu tun hat.

Die Technik hinter der Lösung

Intelligent Host setzt sich aus mehreren Komponenten zusammen, die nahtlos zusammenarbeiten. Eine Power-Apps-Applikation bietet internen Endbenutzern ein einfaches Interface zur Erfassung von Gastbenutzern. Benutzer können über die Power App die erforderlichen Informationen angeben, wie z. B. Gastname, Besitzername, E-Mails, Telefonnummern, Zweck und Gültigkeitsdauer. Die Gültigkeitsdauer kann zwischen 1, 3, 6 oder 12 Monaten betragen. Zusätzlich können die Nutzer Gäste auch im Namen einer Drittperson aus dem entsprechenden Tenant anlegen.

Die App speichert die erfassten Daten in einer SharePoint-Online-Tabellenstruktur und löst einen Power-Automate-Flow aus, der mit Hilfe einer Azure-Funktion den Gastbenutzer im Azure AD erstellt. Intelligent Host überwacht regelmässig die bestehenden Gastbenutzer hinsichtlich ihres Ablaufdatums. Wenn ein Gastbenutzer kurz vor dem Ablaufdatum steht, erhält der Owner 10 Tage vor Ablauf der Frist ein E-Mail mit der Aufforderung zur Verlängerung oder Löschung des Gastbenutzers.

Wenn der Besitzer den Gastbenutzer verlängert, schreibt Intelligent Host das neue Erinnerungsdatum in die SharePoint-Datenstruktur. Das Azure AD wird in diesem Fall jedoch nicht aktualisiert. Wenn der Besitzer den Gastbenutzer zur Löschung freigibt, löscht ihn die Azure Function aus dem Active Directory. Wenn keine Antwort auf die Genehmigung erfolgt, sperrt Intelligent Host das Login und verschickt erneut das Genehmigungs-E-Mail. Wenn nach erneuter Anfrage keine Antwort erfolgt, streicht Intelligent Host den Gastbenutzer definitiv aus dem Azure AD.

©unsplash

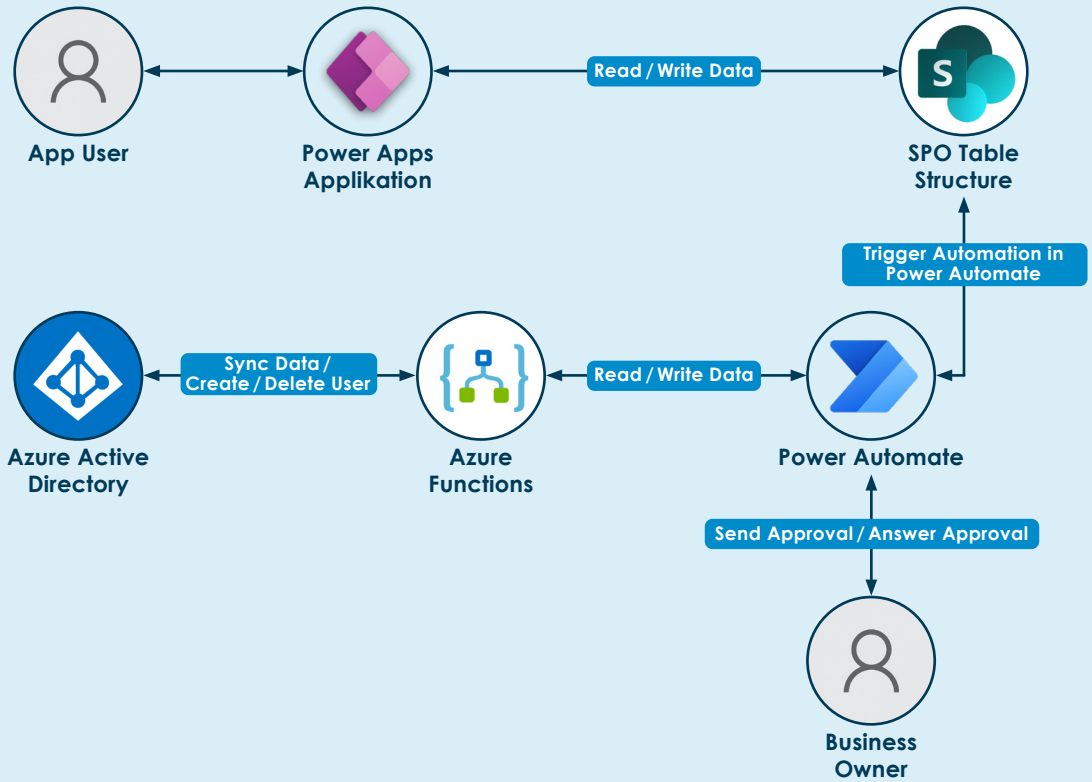
Architektur – das Zusammenspiel

Die Architektur der Lösung ist einfach gehalten und passt auf jedes bestehende Azure-Verzeichnis. Intelligent Host hat nur eine einzige Schnittstelle zum Azure AD, alles weitere ist in das Produkt selbst verpackt. Power Apps dient der Erfassung der Guest User, SharePoint speichert die Daten und Power Automate regelt den Workflow der Bewilligung und Löschung.

Somit bleibt architektonisch die gesamte Organisations-Infrastruktur beibehalten, während die Logik und Bedienung der Erstellung, Genehmigung und Löschung von Guest Usern auf Intelligent Host ausgelagert ist. Beide Systeme können unabhängig voneinander gewartet und weiterentwickelt werden.

Es besteht die Möglichkeit, die Automatisierungen entsprechend den individuellen Präferenzen und Anforderungen entweder in Power Automate, mit Azure Functions oder Logic Apps umzusetzen.

Intelligent Host: Schema der Lösung



Sicherheit – alles säuberlich getrennt

Die Zulassung von Gastbenutzern in Azure Active Directories kann potenzielle Sicherheitsrisiken darstellen, da externe Gastbenutzer zu Ihrer Organisation gehören und möglicherweise nicht denselben Sicherheitsrichtlinien und -kontrollen wie interne Benutzer unterliegen. Einige der Sicherheitsbedenken, die mit der Zulassung von Gastbenutzern in Azure AD einhergehen, sind folgende:

- Guest User können unbefugt auf Ressourcen Ihrer Organisation zugreifen. Dies kann sensible Informationen, geistiges Eigentum oder Finanzdaten betreffen.
- Datenverlust: Gastkonten können versehentlich oder absichtlich Daten Ihrer Organisation mit unbefugten Parteien teilen, was zu einem Datenverlust führen kann.
- Compliance-Risiken: Gastkonten unterliegen möglicherweise nicht denselben Compliance-Anforderungen wie interne Benutzer, was Compliance-Risiken für Ihre Organisation schaffen kann.
- Account-Übernahme: Gastkonten können anfälliger für Account-Übernahme-Angriffe sein, da sie möglicherweise schwächere Passwörter oder Sicherheitskontrollen haben.

Offene Guest User Accounts, die nicht mehr genutzt werden, stellen also ein hohes potenzielles Sicherheitsrisiko dar. Um diese Risiken zu minimieren, ist es wichtig, den Gastzugriff in Azure AD sorgfältig zu verwalten. Dazu gibt es verschiedene Möglichkeiten wie beispielsweise die Zugriffsbegrenzung auf bestimmte Ressourcen, Implementierung von Multi-Faktor-Authentifizierung (MFA), Überwachung auf verdächtige Aktivitäten sowie die regelmässige Überprüfung und Aufhebung von nicht mehr benötigten Gastkonten. Für letzteres allerdings gibt es aktuell Built-in von Microsoft noch keine Lösung.

Genau hier greift unsere Lösung «Intelligent Host». Solange eine Organisation nicht weiss, welche Guest User nicht mehr aktiv sind, ist es schwierig, diese zu bereinigen. Mit Intelligent Host kann der Gastzugriff in Azure AD sorgfältiger verwaltet werden, um so die Vorteile in Bezug auf Zusammenarbeit und Produktivität so sicher wie möglich nutzen zu können und potenzielle Sicherheitsrisiken zu minimieren.

Intelligent Host schafft Klarheit, indem es die Guest User übersichtlich listet, gesamthaft und für jeden einzelnen internen Mitarbeitenden. Es bietet einen sauberen, sicheren Workflow, um regelmässig alle Guest User zu überprüfen und gegebenenfalls zu löschen.

Zu Beginn synchronisiert Intelligent Host einmalig alle bestehenden Guest User aus dem Azure AD in die Tabellenstruktur in SharePoint. Basierend auf diesen Daten versendet die App automatisiert E-Mails an die Guest User, um Informationen (Name, Firma, verantwortlicher interner Mitarbeiter usw.) in Erfahrung zu bringen. Den bestehenden Guest Usern wird initial ein Gültigkeitszeitraum zugewiesen und anschliessend der Prozess zum zyklischen Überprüfen bestehender Guest User gestartet.

Falls von einem Guest User keine verwertbare Reaktion kommt und dieser infolgedessen nicht korrekt zugeordnet werden kann, wird das Login blockiert und bei weiterhin ausbleibender Reaktion wird der User gelöscht.

Die SharePoint-Tabelle speichert Metadaten der Guest User wie Name, E-Mail, Telefon, Laufzeit und Owner. Auf Azure AD liegen lediglich die für die Erstellung nötigen Daten der Guest User. So werden deren Daten gesondert geschützt.

Intelligent Host speichert die Daten auf der jeweiligen Azure Cloud der Organisation oder auf der Schweizer Azure Cloud von Corporate Software. Es besteht auf Wunsch die Möglichkeit, Intelligent Host auf der eigenen On-Premise-Infrastruktur zu hosten.

Wirtschaftlichkeit – die Zahlen müssen stimmen

Intelligent Host skaliert mit der Anzahl Benutzer in einem einfachen Lizenzmodell. Dies garantiert überschaubare, monatliche Kosten. Es entstehen dabei keine Wartungs- oder Entwicklungskosten, wenn Kunden die von Corporate Software gemanagte Power App und Power Automate in der Microsoft Cloud nutzen.

Um Intelligent Host aufzusetzen, benötigen wir zunächst einen geringen Setup-Aufwand, um Ihre Wünsche zu parametrisieren. Der Workflow startet zu Beginn mit einem vollständigen Scan aller Guest User und deren Verifizierung durch die entsprechenden internen Owner. Diese Arbeiten des initialen Scans und der Parametrisierung der Bedürfnisse können durch Corporate Software, durch Sie selbst oder in Zusammenarbeit geleistet werden.

«Intelligent Host ist ein low-code, low-cost Add-on zu bestehenden Azure und M365 Subscriptions. Mit einem Franken pro Benutzer pro Monat und minimalem Initialaufwand können es sich alle unsere Kunden leisten – das ist uns wichtig.»

Matthias Gessenay, Corporate Software

Benutzerinterface – geräteunabhängige Visualisierung

Das Benutzerinterface von Intelligent Host wurde bewusst simpel gehalten, um den Endanwendern ein möglichst intuitives Nutzungserlebnis zu bieten. Dabei kann die Applikation auf verschiedenen Geräten wie Mobile, Tablet oder Desktop verwendet werden. Durch die schnelle und unkomplizierte Entwicklung mit Power Apps lassen sich auch individuelle Anpassungen problemlos umsetzen, wie beispielsweise das Anpassen des Layouts an Ihr Corporate Design oder das Ändern der Menüführung. So können Ihre Anwender beispielsweise über die Mobile-App neue Guest User direkt während eines Meetings genehmigen. Dank der nahtlosen Integration von Power Apps in das gesamte Microsoft-Ökosystem lässt sich die Applikation praktisch überall integrieren und somit einfach verfügbar machen.

Das GUI entspricht dem Microsoft Look and Feel und wird dadurch von den Benutzern gut akzeptiert. Sie kennen die Syntax der Applikation und verstehen intuitiv, wie die Workflows ineinander greifen. Alles in allem setzen wir grössten Fokus auf Einfachheit.

Administration – alles aus einer Hand

Die Wartung und Weiterentwicklung dieser Cloud-App erledigt Corporate Software. Sie beziehen «Software as a Service». Das spart Zeit und hält den Fokus auf das Wesentliche – Ihr Geschäft. Wartung und Weiterentwicklung sind in den Lizenzkosten bereits eingeschlossen. Nur für das erstmalige Setup benötigen wir Ihre Zeit. Die Initiierung geschieht in Zusammenarbeit mit der IT der Kundenorganisation, um die entsprechenden Credentials sicher abzubilden.

Eine Installation auf Ihrer eigenen Azure-Umgebung ist ebenfalls möglich. Dies hat den Vorteil, dass wir die Lösung auf spezifische Anforderungen eines einzelnen Kunden anpassen können. Der Nachteil besteht darin, dass wir Updates und Weiterentwicklungen jeweils auch separat in der Umgebung der Kund:innen nachvollziehen müssen, was zusätzliche Aufwände und damit Kosten generiert.

Lernen – die Zukunft im Blick

Corporate Software entwickelt die App «Intelligent Host» kontinuierlich weiter. Im Dialog mit unseren Kund:innen entdecken wir neu gewünschte Features wie doppelte Bewilligung, automatische Verzögerung der Löschung, semi-automatische Erstellung oder Anreicherung der Daten mit individuellen Dritt-Datenquellen. Die App lernt mit den Usern und die Entwickler von Corporate Software entwickeln sich – technisch, kommunikativ und wirtschaftlich.

Gleichzeitig binden wir Kunden auf Wunsch aktiv in die Produktentwicklung ein, um das Wissen über die Microsoft Power Platform zu erhöhen. Diese relativ neue Low-Code-Technologie kann unglaublich viel leisten – wir und unsere Kund:innen entdecken jeden Tag neue Anwendungsfälle und bauen entsprechende Szenarien auf. «Intelligent Host» ist nur ein Zwischenschritt zu mehr Autonomie bezüglich selbstentwickelter Applikationen, Workflows und BI-Reportings.

Ausblick

Die Verwendung von Microsoft Teams wird weiter zunehmen. Gleichzeitig werden Organisationen mehr denn je miteinander zusammenarbeiten. Dies führt automatisch dazu, dass sich in den Azure ADs in Zukunft mehr Gäste befinden werden als heute. Intelligent Host überblickt die Guest User Accounts, bereinigt diese und sorgt so dafür, dass keine Sicherheitslücken entstehen oder Ressourcen verschwendet werden.

Für die Zukunft planen wir, Intelligent Host als Standardlösung für Guest User Management auf dem Markt zu positionieren – am liebsten zukünftig integriert in die offizielle Version der Azure AD. Microsoft Azure powered by Corporate Software – dafür entwickeln wir Intelligent Host jeden Tag weiter.

«Ein Produkt wie 'Intelligent Host' von der Idee bis zur Marktreife zu entwickeln, hat mir viel Freude bereitet. Teamarbeit, Lernen, Spass, Wirkung und Business Case standen im Vordergrund. Die Schnittstellen der verschiedenen Disziplinen reizen mich – dort liegen wunderbare Produktivitätsgewinne für unsere Kunden.»

Maxim Lavoie, Entwickler Intelligent Host, Corporate Software

Porträts Projektbeteiligte

Thomas von Mentlen
Product Owner «Intelligent Host», Consultant, Developer und Trainer in Power Platform & Azure, Corporate Software

«Es erfüllt mich mit grosser Freude, die Rolle als Product Owner für das innovative Produkt «Intelligent Host» zu übernehmen. Ich blicke gespannt auf die bevorstehenden Herausforderungen und Möglichkeiten, die wir gemeinsam meistern werden, um dieses Produkt zum Erfolg zu führen.»

Maxim Lavoie
Entwickler «Intelligent Host», Microsoft Certified Functional Consultant, Consultant und Trainer Power Platform, Corporate Software

«Die Entwicklung von Intelligent Host fühlt sich wie eine coole Reise mit meinem Motorrad an: Immer schön im Flow, nicht zu schnell und nicht zu langsam, gute Etappenplanung mit Drive am Tag und Erholung während der Nacht und immer mal wieder treffen wir auf Überraschungen hinter der nächsten Kurve, oft erfreulich, manchmal halt auch nicht.»

Sebastian Steer
Entwickler «Intelligent Host», Consultant und Trainer Power Platform, Mitglied der Geschäftsleitung, Corporate Software

«Im Entwicklungsteam von Intelligent Host entscheiden wir mit unserem Product Owner und den Stakeholdern über die Features, die wir im nächsten Sprint entwickeln. Dieser Dialog bringt tolle Ideen zur Umsetzung und schliesslich in die Live-Umgebung. Diese Drehscheibe zu verkörpern, bereitet mir Freude und bringt mich weiter.»

Matthias Gessenay
CEO und CO-Gründer, Senior-Consultant, Microsoft Azure MVP, Corporate Software

«Ich freue mich auf den Moment, wenn Intelligent Host offiziell Teil der Microsoft Azure AD wird. Das Produkt schliesst eine Lücke im Guest User Life Cycle Management – etwas, das praktisch alle Organisationen benötigen.»

Über Corporate Software

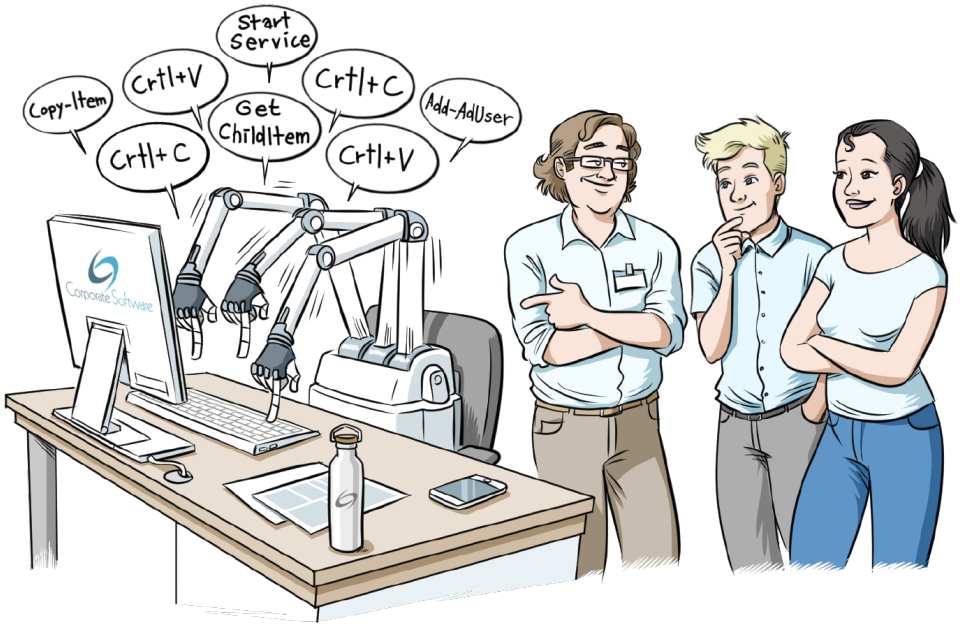
Corporate Software entwirft intelligente Cloud-IT-Lösungen für Unternehmen. Als unsere Kundin oder unser Kunde profitieren Sie langfristig und erhalten individuelle Lösungen in den Bereichen Collaboration, Data & Artificial Intelligence und Automation.

CoSo begeistert als Schweizer Unternehmen seit 2011 Kund:innen mit nachhaltigen Lösungskonzepten an der Schnittstelle zwischen Business und IT.

Was die Mitarbeitenden von Corporate Software gemeinsam haben, ist das Interesse an der stetigen Verbesserung von Technik, Wirtschaft und sich selbst. «Wir gehen voran, um den nächsten Schritt zu ermöglichen» ist unser Motto.

Aktuell sind wir 10-facher Microsoft Gold Partner: Gold Application Integration, Gold Application Development, Gold Cloud Platform, Gold Cloud Productivity, Gold Collaboration and Content, Gold Data Analytics, Gold Data Platform, Gold Datacenter, Gold DevOps, Gold Project and Portfolio Management.

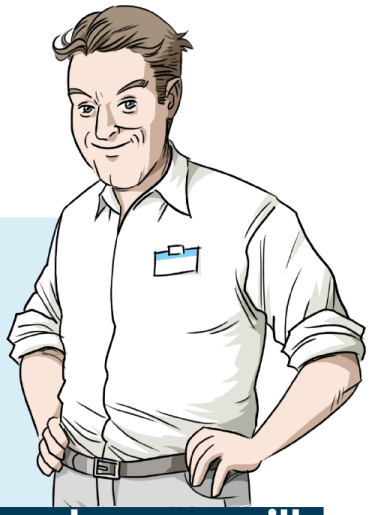
Zudem wurden wir von Microsoft mit den neuen Advanced Specializations «Adoption und Change Management» und «Calling for Microsoft Teams» ausgezeichnet.



Corporate Software begleitet seine Kunden bei der Entdeckung von neuen Gebieten und befähigt sie, mit Technologie neue Prozesse, neues Zusammenarbeiten und neue Produkte für sich zu entdecken.

Sind Sie an Intelligent Host für das Management Ihrer Guest User interessiert?

Nehmen Sie mit uns Kontakt auf!



Ihre Ansprechperson:

Matthias Gessenay
matthias.gessenay@corporatesoftware.ch
Telefon: +41 32 315 03 60

«Wer schwimmen lernen will, muss ins Wasser.»

Microsoft Partner
Microsoft

Gold Cloud Platform
Gold Cloud Productivity
Gold Data Analytics
Gold DevOps
Gold Collaboration and Content
Gold Project and Portfolio Management
Gold Data Platform
Gold Application Integration
Gold Application Development
Gold Datacenter

Corporate Software

Wir gehen voran, um den nächsten Schritt zu ermöglichen!

Corporate Software AG
Schöneggstrasse 5, 2503 Biel, T +41 32 322 67 05, www.corporatesoftware.ch, info@corporatesoftware.ch