PROSTEP
integrate the future

WHITEPAPER

DATEN AUSTAUSCHEN MUSS SICHERER WERDEN

Viele Unternehmen vernachlässigen die Datensicherheit beim Datenaustausch und kompromittieren damit ihr geistiges Eigentum oder – schlimmer noch – das ihrer Kunden. Dabei ist die Implementierung einer sicheren Datenaustauschlösung nicht zuletzt dank der Cloud kein Hexenwerk mehr und auch nicht sehr teuer. Aber der Teufel steckt wie immer im Detail. Worauf Sie bei der Auswahl von Anbieter und Datenaustauschlösung achten sollten, verrät Ihnen das neue PROSTEP-Whitepaper zum Thema Datensicherheit im Datenaustausch.

Einleitung

Bei der Zusammenarbeit in verteilten Entwicklungsprozessen ist es notwendig, die erforderlichen Daten allen beteiligten Partnern zeitnah zur Verfügung zu stellen. Das stellt sehr hohe Anforderungen an den Datenaustausch. Sicherheit ist eine dieser Anforderungen, die nicht immer von beliebigen Datenaustauschlösungen erfüllt wird. Welche Anforderungen Unternehmen bei der Auswahl einer entsprechenden Lösung an die Software, aber auch an den Hersteller und seine Entwicklungsprozesse stellen sollten, erfahren Sie in dem neuen PROSTEP-Whitepaper zum Thema Datensicherheit im Datenaustausch.

Datenaustausch als Einfallstor für Cyber-Attacken

Die meisten Unternehmen schützen ihre Daten intern durch Firewalls, restriktive Zugriffsberechtigungen und Backups vor Cyber-Attacken. Sie vernachlässigen jedoch die Sicherheit beim Datenaustausch. Erhebungen zufolge setzen nur wenige Unternehmen eine Lösung für den sicheren Datentransfer ein. Grund dafür sind neben fehlenden personellen Ressourcen, hohen Kosten und der vermeintlichen Komplexität einer solchen Lösung die Tatsache, dass die Unternehmen die Risiken eines unverschlüsselten Datenversands unterschätzen.

Der Datenaustausch entwickelt sich dadurch immer mehr zur Achillesferse der Cyber-Sicherheit und zum Einfallstor für Datenpiraten. Unternehmen riskieren durch den unverschlüsselten Datenversand den Verlust ihrer Daten oder, schlimmer noch, von Kundendaten und laufen Gefahr, dass ihre Reputation Schaden nimmt und sie das Vertrauen ihrer Kunden verspielen. Laut Digitalverband Bitkom hat die Gefahr von Cyber-Attacken, die der organisierten Kriminalität zugeschrieben werden, deutlich zugenommen. Allein im Jahr 2023 entstand der deutschen Wirtschaft durch Cyber-Kriminalität ein Schaden von 206 Milliarden Euro.

Die Unternehmen müssen sich deshalb ernsthaft mit der Frage auseinandersetzen, wie sie ihre Daten auf dem Weg durch die weltweiten Datennetze optimal schützen können. Mit der Einführung einer beliebigen Datenübertragungssoftware ist es nicht getan. Diese Lösungen können Sicherheitslücken aufweisen, die von Hackern genutzt werden, um Kundendaten abzugreifen.

Bei der Auswahl einer entsprechenden Lösung sind deshalb eine Reihe von Kriterien zu berücksichtigen, angefangen von der Frage, wie vertrauenswürdig der Software-Hersteller ist und wie er die IT-Sicherheit in seiner Organisation gewährleistet. Eine wichtige Rolle spielt dabei vor allem die Konformität der Prozesse in der Software-Entwicklung mit den einschlägigen Normen und Standards.

Im Unterschied zu anderen Herstellern hat es mit den Datenaustauschlösungen OpenDXM und OpenDXM GlobalX von PROSTEP dank entsprechender Vorkehrungen in 30 Jahren keinen einzigen Sicherheitsvorfall gegeben. Warum das so ist, erfahren Sie in diesem Whitepaper.

Absicherung von Organisation und Prozessen

Sichere IT-Lösungen können nur in einer sicheren Umgebung entstehen. Deshalb ist es zwingend erforderlich, das Thema Datensicherheit durch eine effektive Sicherheitsstrategie und die Unterstützung entsprechender Sicherheitsstandards fest in der Organisation und den IT-Prozessen zu verankern. Außerdem müssen die Mitarbeiter*innen regelmäßig über die Bedeutung der Datensicherheit geschult und für die immer größer werdenden Sicherheitsrisiken sensibilisiert werden, denn sie sind die erste Verteidigungslinie im Kampf gegen mögliche Cyber-Attacken.

Bei PROSTEP ist das Thema Datensicherheit fester Bestandteil unserer DNA. Wir analysieren regelmäßig die potenziellen Risiken und Bedrohungen, denen wir ausgesetzt sind, und haben entsprechende Sicherheitsmaßnahmen implementiert. Wir haben klare Richtlinien und Verfahren für den Umgang mit sensiblen Daten festgelegt, einschließlich entsprechender Passwortrichtlinien, Zugriffskontrollen und Kommunikationswege. Aus diesem Grund nutzen wir für die Kommunikation sensibler Kundendaten unsere eigene sichere Datenaustauschplattform OpenDXM GlobalX. Außerdem gibt es einen klar definierten Prozess für die Meldung und Behandlung von Sicherheitsvorfällen, um schnell auf Gefahrensituationen reagieren zu können.

Um das Vertrauen unserer Kunden und Partner in unser Sicherheitsmanagement zu stärken, lassen wir uns regelmäßig nach ISO 27001 zertifizieren. Das Zertifikat bescheinigt uns, dass wir die Anforderungen der international wichtigsten Norm zur Informationssicherheit erfüllen, nicht nur was die Sicherheit unserer IT-Systeme, sondern auch was unsere Prozesse und das Verhalten unserer Beschäftigten angeht. Ein weiterer Baustein in unserer Sicherheits-Architektur ist die TISAX-Zertifizierung, die bei vielen Automobilherstellern und -zulieferern heute Grundlage für die Organisation der Zusammenarbeitsprozesse ist. Der vom VDA definierte Standard baut auf der ISO 27001 auf und definiert einheitliche Anforderungen für den Umgang mit vertraulichen und personenbezogenen Daten und den Schutz der IT-Infrastruktur.

Darüber hinaus entsprechen unsere Geschäftsprozesse den Anforderungen der Qualitätsnorm ISO 9001, die ebenfalls Aspekte der Datensicherheit beinhaltet und explizit die Entwicklung unserer Standardsoftwareprodukte (OpenPDM, OpenCLM und OpenDXM GlobalX) einschließt. Und wir erfüllen auch die Datenschutz-Bestimmungen der Datenschutz-Grundverordnung (DSGVO). Abgerundet wird dieses Paket an Sicherheitsmaßnahmen durch eine Software-Entwicklungsumgebung, die durch Automatismen ein hohes Maß an Sicherheit gewährleistet.

Kontinuierliches Monitoring der Sicherheitsvorfälle

Eine der aktuell wohl bedeutendsten Anforderungen zum Schutz des eigenen Know-Hows ist die Sicherheit der eingesetzten Software-Produkte. Die Software-Entwicklungsumgebung und die Organisation des Entwicklungsprozesses für solche Produkte haben maßgeblichen Einfluss auf die inhärente Sicherheit der Anwendungen. Wir arbeiten in der Software-Entwicklung für unsere Produkte nach zertifizierten Prozessen, um den vielfältigen Qualitätsanforderungen zu entsprechen.

Durch die kontinuierliche Integration von Werkzeugen und die automatisierten Prozesse beim Bilden und Testen unserer Software-Produkte lassen sich Sicherheitslücken in verwendeten OpenSource-Komponenten schneller erkennen und beheben. Automatisierte Tests und Prüfungen gegen Datenbanken helfen, Schwachstellen zu erkennen, sobald sie als solche gemeldet werden.

Wir prüfen OpenDXM GlobalX und die in der Software verwendeten OpenSource-Komponenten jede Nacht auf Sicherheitsvorfälle. Werden durch diese Tests, Sicherheitsvorfälle erkannt, sichern unsere internen Prozesse die sofortige Analyse und Bewertung der Sicherheitslücken ab. Bei kritischen Sicherheitslücken wie der Schwach-

stelle, die Ende 2021 in der Java-Bibliothek Log4j entdeckt wurde, informieren wir unsere Kunden umgehend und stellen ihnen schnellstmöglich einen Sicherheits-Patch zur Verfügung. Bei weniger kritischen Sicherheitslücken werden die notwendigen Maßnahmen eingeplant und in den Release Prozess übernommen.

Vertrauen ist gut, Kontrolle ist besser. Nach diesem Prinzip lassen wir alle größeren Releases unserer Datenaustauschplattform OpenDXM GlobalX zusätzlich durch externe Penetrationstests absichern. Bislang sind dabei keine größeren Sicherheitslücken entdeckt worden. Gute Noten für Datensicherheit erhalten wir auch von unseren großen Kunden aus der Automobilindustrie, die ebenfalls Penetrationstests der bei ihnen eingesetzten Software-Lösungen durchführen.

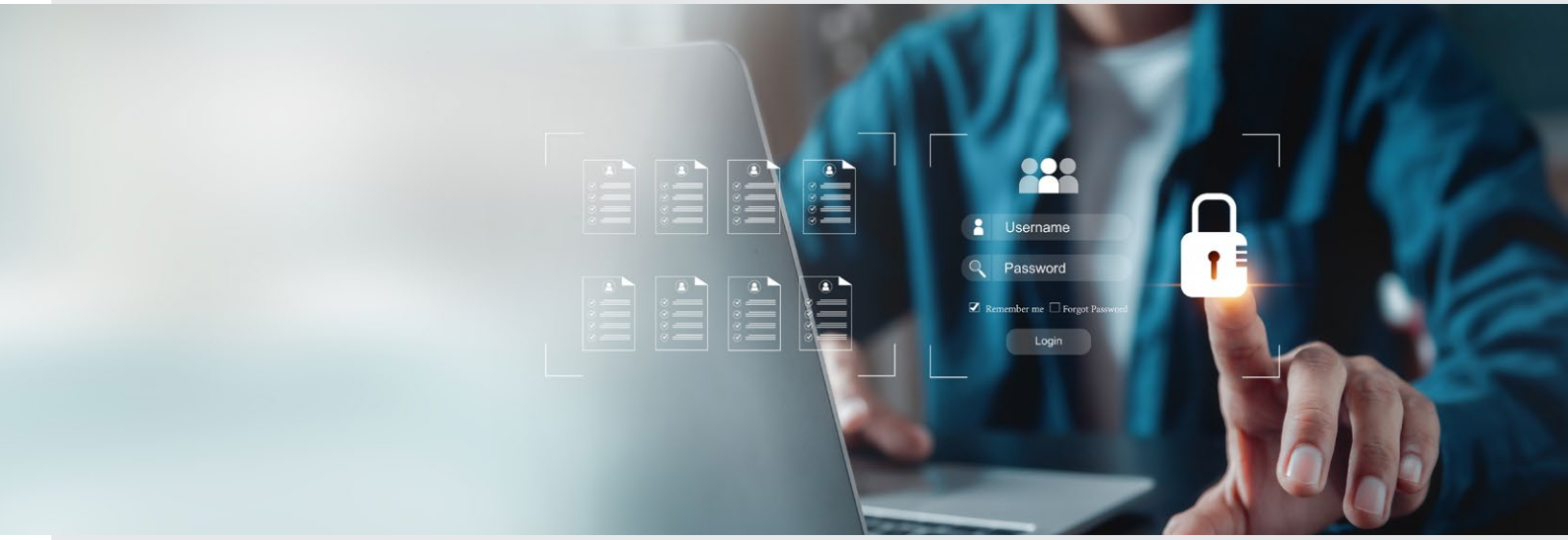
Software mit mehrstufiger Verschlüsselung

Die Sicherheit des Datenaustauschs hängt wesentlich davon ab, wie gut die Daten auf dem Weg durch die globalen Netze vor Missbrauch und unbefugten Zugriffen geschützt sind. Das fängt bei einem umfassenden Rollen- und Rechtemanagement an, das dafür sorgt, dass nur berechtigte Anwender*innen Daten versenden können, und vor dem Zugriff auf die Daten die Identität der Empfänger*innen prüft, und endet bei der sicheren Verschlüsselung der auszutauschenden Daten und Datenverbindungen.

OpenDXM GlobalX verfügt über ein leistungsfähiges Rollen- und Rechtemanagement mit einer voll integrierten Zwei-Faktor-Authentifizierung (2FA). Das bedeutet, dass die Anwender*innen bei der Anmeldung am Datenaustausch-Portal nicht nur ihre User-IDs und ihr Passwort eingeben müssen, sondern außerdem einen zeitbasierten Token, der auf einem beliebigen Endgerät erzeugt werden kann. Das 2FA-Verfahren lässt sich problemlos mit etablierten Authentifizierungsverfahren nach LDAP/AD- oder durch ein externes IAM-System (Identity Access Management) zum Single-Sign-On (SSO) kombinieren.

Um ein Maximum an Datensicherheit zu bieten, nutzt OpenDXM GlobalX ein mehrstufiges Verschlüsselungskonzept. Sowohl die interne Datenübertragung als auch der Transfer über das Internet erfolgen immer über eine verschlüsselte https-Verbindung. Falls trotzdem jemand versuchen sollte, die Daten abzufangen, kann er mit ihnen nichts anfangen, da sie beim Upload auf die Plattform nach dem Public-Private-Key-Verfahren mit bis zu 4.096 Bit verschlüsselt werden. Darüber hinaus lassen sich besonders schützenswerte Daten durch einen separaten, individuell erzeugten Schlüssel schützen, den nur der/die Empfänger*in kennt. Die Schlüssel können getrennt von den verschlüsselten Daten auf einem Server in einem Land verwaltet werden, in dem die Nachrichtendienste kein Recht haben, ihre Herausgabe zu fordern.

Voraussetzung für den sicheren Datenaustausch ist eine kontrollierte Datenhaltung in den Unternehmen selbst, beispielsweise durch Einsatz einer PDM/PLM-Lösung. Nur so lässt sich sicherstellen, dass keine Daten ohne Autorisierung oder falsche Versionsstände das Unternehmen verlassen. Um den Datenaustausch noch sicherer zu machen, muss die Datenaustauschlösung in die bestehende System- und IT-Infrastruktur integrierbar sein.



Integration in die bestehende Systemlandschaft

Der Mensch wird gerne als schwächstes Glied in der Sicherheitskette bezeichnet, und tatsächlich haben die Gefahren für die Datensicherheit mit der Arbeit im Homeoffice zugenommen. Häufig ist der unsichere Umgang mit Daten aber auch darauf zurückzuführen, dass die Sicherheitsmaßnahmen sich nicht mit den Prozessanforderungen und Arbeitsweisen der Mitarbeiter*innen vertragen. Die Verankerung der Sicherheitsmechanismen in ihrer Arbeitsumgebung erleichtert ihnen die Einhaltung der Sicherheitsvorgaben.

Was unsere Datenaustauschlösung OpenDXM GlobalX so sicher macht, sind nicht nur die Verschlüsselungsmechanismen, das leistungsfähige Rollen- und Rechtekonzept oder die Integration in IAM-Systeme (Identity Access Management). Das bieten andere Lösungen auch. Das Besondere ist, dass sie sich nahtlos in die bestehenden Geschäftsprozesse und Unternehmensanwendungen integrieren lässt. Dadurch kommen die Anwender*innen gar nicht in Versuchung, ihre Daten über andere Wege auszutauschen als über die sichere Datenaustauschplattform.

Als ein Produkt von PROSTEPs Digital Thread-Plattform stellt OpenDXM GlobalX gemeinsam mit den Produktfamilien OpenPDM und OpenCLM standardisierte und gewartete Integrationsbausteine für viele PLM- und ERP-Systeme zur Verfügung. Systeme, zu denen es keine Integrationsbausteine gibt, können über die offiziellen Programmierschnittstellen angebunden werden. Dadurch kann der sichere und vollautomatisierte Datenaustausch aus zahlreichen Backendsystemen realisiert werden. Die Integrationen ermöglichen es den Anwender*innen, ihre Daten direkt aus ihrer gewohnten Arbeitsumgebung zu versenden und auch nur die Daten, für die sie berechtigt sind. In der Automobilindustrie lassen sich die Datenaustauschprozesse mit Hilfe der OFTP/ENGDAT-Komponenten sogar komplett automatisieren.

Um Mitarbeiter*innen außerhalb des Engineerings den sicheren Versand und Empfang von vertraulichen Daten per E-Mail zu ermöglichen, lässt sich OpenDXM GlobalX außerdem in MS Outlook integrieren. Dateianhänge einer bestimmten Größe, eines bestimmten Dateityps oder für bestimmter Empfänger*innen werden dann beim Versand automatisch verschlüsselt im Datenaustauschportal bereitgestellt bzw. beim Empfang verschlüsselt in Outlook zum Download angezeigt. Dank Windows Explorer-Integration lassen sie sich auch per Drag & Drop sicher austauschen.

Die Integration in die bestehende IT-Infrastruktur ist absolut kompatibel mit der Nutzung von OpenDXM GlobalX als SaaS-Angebot. Die Frage ist, wie sich der Einsatz in der Cloud auf die Datensicherheit auswirkt.

Sicherheitsvorteile beim Einsatz in der Cloud

Die Nutzung von OpenDXM GlobalX als SaaS-Angebot (Software as a Service) aus der Cloud bietet Kunden viele Vorteile: Sie sparen sich die Anschaffung von Hard- und Software, die Datenaustauschplattform ist praktisch aus dem Stand einsetzbar und sie lässt sich flexibel skalieren, wenn Anwenderzahl oder Austauschvolumen zunehmen oder sinken. Vor allem aber bietet der Cloud-Einsatz im Vergleich zu den On Premises-Installationen vieler Unternehmen oft ein Mehr an Sicherheit, was die IT-Infrastruktur und die verfügbaren Ressourcen anbelangt.

Die Zeiten, in denen viele Unternehmen aus Sicherheitsbedenken vor dem Einsatz von Cloud-Anwendungen zurückschreckten, sind vorbei. Nach zahlreichen, zum Teil spektakulären Cyber-Attacken setzt sich allmählich die Erkenntnis durch, dass die Daten in der IT-Infrastruktur eines vertrauenswürdigen Cloud-Providers oder SaaS-Anbieters oft sicherer aufgehoben sind als im eigenen Rechenzentrum. Hier kümmert sich deutlich mehr Personal um den sicheren und performanten Betrieb der Anwendungen, und die Zugriffe werden kontinuierlich überwacht, um mögliche Sicherheitsvorfälle schnell erkennen und beheben zu können.

OpenDXM GlobalX ist auf den Cloud-Stacks beliebiger Provider lauffähig und kann auch in hybriden On Premises- /Cloud-Szenarien eingesetzt werden. Die Architektur einer OpenDXM GlobalX-Umgebung und die bereitgestellten Schnittstellen bieten genau diese Möglichkeiten. Der Betrieb in einer Cloud-Infrastruktur stellt darüber hinaus besondere Anforderungen an die browserbasierte Anwenderoberfläche, die eine sichere Interaktion über Internet ermöglichen muss. Die netzwerkübergreifende Kommunikation zwischen den Client-Server-Komponenten erfolgt via Webservice-Schnittstellen auf Basis des HTTPS Protokolls.

In der Cloud betriebene Anwendungen werden üblicherweise automatisch installiert und kontinuierlich aktualisiert. Dadurch können auch Patches und empfohlene Sicherheitskonfigurationen schneller eingespielt werden als in einer On Premises-Installation, deren Updates aufgrund der vielen Anpassungen oft eine monatelange Vorbereitung erfordern. Dass keine manuellen Eingriffe der Administratoren mehr erforderlich sind, sorgt ebenfalls für ein höheres Maß an Sicherheit.

Rundum sicher mit OpenDXM GlobalX

Zusammenfassend lässt sich festhalten, dass viele Unternehmen die Sicherheit beim Datenaustausch immer noch vernachlässigen und dadurch Gefahr laufen, Opfer von Cyber-Attacken zu werden. Um ihre Daten auf dem Weg durch die weltweiten Datennetze effektiv zu schützen, benötigen sie eine sichere Datenaustauschlösung, die sich nahtlos in ihre IT-Infrastruktur und Geschäftsprozesse einfügt. Bei der Auswahl einer entsprechenden Lösung ist auch zu berücksichtigen, wie vertrauenswürdig der Software-Hersteller ist und wie er die IT-Sicherheit in seiner Organisation gewährleistet.

PROSTEP hat das Thema Sicherheit durch eine effektive Sicherheitsstrategie und die Unterstützung entsprechender Sicherheitsstandards fest in der Organisation und den IT-Prozessen verankert. Wir haben klare Richtlinien für den Umgang mit sensiblen Daten festgelegt und einen klaren Prozess für die Behandlung von Sicherheitsvorfällen definiert.

Um das Vertrauen unserer Kunden und Partner in unser Sicherheitsmanagement zu stärken, lassen wir uns regelmäßig nach ISO 27001 und dem darauf aufbauenden TISAX-Standard zertifizieren. Wir erfüllen auch die Anforderungen der Qualitätsnorm ISO 9001 und der Datenschutz-Grundverordnung (DSGVO). Unsere Software-Entwicklung orientiert sich an diesen Sicherheitsstandards. Wir scannen OpenDXM GlobalX und die in der Software verwendeten Open-Source-Komponenten jede Nacht auf Sicherheitsvorfälle und führen regelmäßig Penetrationstests durch.

OpenDXM GlobalX bietet ein Maximum an Datensicherheit durch ein leistungsfähiges Rollen- und Rechtemanagement mit Zwei-Faktor-Authentifizierung, die mit externen IAM-Verfahren kombiniert werden kann, sowie ein mehrstufiges Verschlüsselungskonzept. Nicht nur die auszutauschenden Daten werden beim Upload auf die Plattform verschlüsselt, sondern auch die Übertragung selbst erfolgt über eine verschlüsselte Verbindung.

Eine besondere Stärke der Lösung ist, dass sie sich komfortabel in die bestehenden PLM/ERP-Landschaften, aber auch in MS Outlook oder den Windows Explorer integrieren lässt. Dadurch können die Anwender*innen den Datenaustausch direkt aus ihrer gewohnten Arbeitsumgebung veranlassen und kommen gar nicht auf die Idee, ihre Daten über andere Wege auszutauschen.

OpenDXM GlobalX wird bei Kunden in unterschiedlichen Branchen genutzt, die sehr hohe Anforderungen in punkto Datensicherheit haben. Die Datenaustauschplattform kann sowohl on premises installiert als auch als SaaS-Angebot genutzt werden. Der Cloud-Einsatz sorgt für zusätzliche Sicherheit, da die Daten in der Infrastruktur eines vertrauenswürdigen Cloud-Providers oder SaaS-Anbieters in der Regel sicherer aufgehoben sind als in den Rechenzentren vieler Unternehmen.

PDF Version des Whitepapers:
www.prostep.com/whitepaper
oder scannen Sie den QR Code

PROSTEP
integrate the future

Sie haben Anmerkungen oder Fragen?

Wir freuen uns auf Ihr Feedback an
infocenter@prostep.com

PROSTEP AG
Dolivostraße 11 · 64293 Darmstadt · Deutschland
Telefon +49 6151 9287-0 · E-Mail infocenter@prostep.com

IMPRESSUM

Herausgeber
PROSTEP AG

Ansprechpartner:
Daniel Wiegand
daniel.wiegand@prostep.com

Edition 1, 2024