

Interview

Fundament des mobilen Arbeitsplatzes

[18.08.2026] Materna Virtual Solution bietet mit SecurePIM einen mobilen Arbeitsplatz, der den hohen Sicherheitsanforderungen von Behörden entspricht. Nun kooperiert das Unternehmen mit Wire, einem Anbieter souveräner Kommunikationslösungen. move – moderne verwaltung sprach mit Daniel Zimmermann von Materna Virtual Solution und Oliver Brown von Wire über die Vorteile der Zusammenarbeit für die Kunden der beiden Unternehmen.

Herr Zimmermann, Herr Brown, was war der Auslöser für die Zusammenarbeit zwischen [Materna Virtual Solution](#) und [Wire](#), und welche Anforderungen von Behörden und sicherheitskritischen Organisationen möchten Sie damit adressieren?

Daniel Zimmermann: Wir richten uns beide an dieselbe Zielgruppe: Behörden und Organisationen mit hohen Sicherheitsanforderungen. Beide Unternehmen bieten sichere Lösungen für mobiles Arbeiten und mobile Kommunikation an. Irgendwann haben wir gesagt: Warum sollten unsere Lösungen nebeneinander existieren? Warum schaffen wir keine engere Verbindung zwischen ihnen? Unsere Kunden wünschen sich integrierte, nahtlose Lösungen. Sie möchten nicht ständig zwischen verschiedenen Anwendungen wechseln, die im schlimmsten Fall inkompatibel zueinander sind.

Oliver Brown: Dem kann ich mich nur anschließen. Der Impuls kam eindeutig von unseren Kunden. Hinzu kommt ein weiterer Aspekt: Wenn wir über digitale Souveränität und die aktuelle geopolitische Lage sprechen, dann ist jetzt der richtige Zeitpunkt für europäische Technologieanbieter, enger zusammenzuarbeiten und ein integriertes Ökosystem aufzubauen. Dieses entspricht genau den Erwartungen und Anforderungen europäischer IT-Entscheider. Letztlich geht es aber vor allem darum, gemeinsam einen größeren Mehrwert für unsere Kunden zu schaffen.

Warum gewinnt das Thema sichere und souveräne mobile Kommunikation derzeit so stark an Bedeutung?

Zimmermann: In den vergangenen Jahren hat sich das Arbeiten grundlegend verändert. Es wird immer mobiler – wir sprechen häufig sogar von „ultramobilem Arbeiten“. Viele unserer Kunden, insbesondere im öffentlichen Sektor, arbeiten inzwischen viel mit Tablets oder Smartphones. Gleichzeitig hat sich die Sicherheitslage deutlich verändert. Die politischen Rahmenbedingungen haben sich verschärft, Bedrohungen nehmen zu und auch die Diskussion um digitale Souveränität gewinnt an Bedeutung. Ich ergänze dabei gerne den Begriff der Datensouveränität. Es geht darum, Daten auf dem Endgerät während ihrer Übertragung und auf den Backendsystemen zu schützen. Deshalb bündeln wir unsere Kompetenzen und verfolgen gemeinsam das Ziel, eine wirklich souveräne und sichere mobile Arbeitsumgebung für Bundesbehörden, Landesverwaltungen und Kommunen bereitzustellen – also für genau die Einrichtungen, die wir heute bereits betreuen oder künftig unterstützen möchten.

Brown: Wenn wir mit Führungskräften und IT-Verantwortlichen im öffentlichen Sektor sprechen, stehen im Wesentlichen vier Risikobereiche im Vordergrund: Cybersicherheit, Compliance, Governance sowie digitale und datentechnische Souveränität. Mobile Endgeräte und mobile Kommunikation gehören heute zu den wichtigsten Angriffspunkten für Cyberangriffe. Kommunen und Behörden in Deutschland und im gesamten DACH-Raum waren in den vergangenen Jahren immer wieder Ziel von Ransomware- oder

Hacking-Angriffen. Hinzu kommen regulatorische Anforderungen wie NIS2 oder die Datenschutz-Grundverordnung, die umfangreiche Berichtspflichten und Sicherheitsmaßnahmen verlangen. Ein weiterer Punkt ist die Nutzerfreundlichkeit. Mitarbeitende erwarten heute dieselbe einfache Bedienung, die sie von privaten Kommunikationsanwendungen kennen. Werden solche Anforderungen im beruflichen Umfeld nicht erfüllt, entstehen häufig sogenannte Schatten-IT-Strukturen, weil Beschäftigte auf nicht freigegebene Anwendungen ausweichen. Zusammen mit den aktuellen geopolitischen Entwicklungen und der zunehmenden Bedeutung von Datenhoheit führt all dies dazu, dass sichere und souveräne mobile Kommunikation immer wichtiger wird.

Viele unserer Kunden, insbesondere im öffentlichen Sektor, arbeiten inzwischen ausschließlich mit Tablets oder Smartphones.

Welche Auswirkungen haben regulatorische Vorgaben wie NIS2 auf die Anforderungen an mobile Arbeitsplätze in der öffentlichen Verwaltung?

Brown: Aus unserer Sicht bringen Regelwerke wie NIS2 vor allem strengere Anforderungen an das Risikomanagement, die Zugriffskontrolle und die Verschlüsselung mit sich. Die Kombination der Lösungen von Materna Virtual Solution und Wire adressiert genau diese Anforderungen. Gleichzeitig ermöglichen wir eine hohe Benutzerfreundlichkeit und steigern die Produktivität der Anwender. Wie bereits erwähnt, stellen mobile Endgeräte einen besonders kritischen Angriffsvektor dar. Sie müssen deshalb systematisch abgesichert werden. Selbst wenn einzelne Kommunen möglicherweise nicht unmittelbar unter NIS2 fallen, erhöhen Datenschutzbehörden und Aufsichtsstellen die Anforderungen kontinuierlich. Dadurch verändert sich die Art und Weise, wie digitale Arbeitsplätze künftig gestaltet werden müssen.

Zimmermann: Viele Organisationen haben zunächst ihre IT-Infrastruktur abgesichert und anschließend klassische Arbeitsplatzrechner geschützt. Mobile Endgeräte wurden dagegen lange Zeit nicht mit derselben Konsequenz in Sicherheitskonzepte einbezogen. Das hat sich inzwischen grundlegend geändert. Heute besteht weitgehend Einigkeit darüber, dass private und dienstliche Daten auf mobilen Geräten strikt voneinander getrennt und entsprechend geschützt werden müssen – nicht nur aus Datenschutzgründen, sondern vor allem aus Sicht der Informationssicherheit.

Der Begriff „digitale Souveränität“ wird häufig verwendet. Was bedeutet er aus Ihrer Sicht konkret für Behörden und andere Organisationen mit hohen Sicherheitsanforderungen?

Zimmermann: Digitale Souveränität bedeutet für mich, dass Behörden, Unternehmen und andere Organisationen jederzeit handlungsfähig bleiben und die vollständige Kontrolle über ihre Systeme behalten. Ich verwende in diesem Zusammenhang gerne den deutschen Begriff der Selbstbestimmung. Aktuell wird in der medialen Berichterstattung häufig über sogenannte „Kill Switches“ gesprochen – also die Möglichkeit, dass ein Anbieter den Zugriff auf Systeme oder Anwendungen aus der Ferne unterbindet. Lange Zeit wurde das eher als theoretisches Szenario betrachtet. Heute wissen wir, dass solche Risiken real sind. Deshalb ist es entscheidend, jederzeit die Kontrolle über die eigenen Geräte und vor allem über die eigenen Daten zu behalten. Das betrifft sowohl Daten, die auf einem Endgerät gespeichert sind, als auch Daten, die während der Kommunikation übertragen werden. Genau dafür stehen wir – ebenso wie Wire – mit unserer hochsicheren Verschlüsselungstechnologie. Für uns gehört dazu auch, dass unsere Sicherheitslösungen aus Europa beziehungsweise – im Fall von Materna Virtual Solution – aus Deutschland stammen. Aus politischer Sicht verstehen wir uns als Unternehmen, das Deutschland und Europa mit sicheren Technologien unterstützt.

Brown: Wenn wir Europa insgesamt betrachten, fließen bislang rund 80 Prozent der Cloud-Ausgaben in Angebote amerikanischer Hyperscaler. Vor dem Hintergrund geopolitischer Entwicklungen und gesetzlicher Regelungen wie dem US Cloud Act stellt dies ein erhebliches Risiko dar. Deshalb ist es entscheidend, die vollständige Kontrolle über Daten, Identitäten und die zugrunde liegende Infrastruktur zu behalten. Gerade in einer Zeit, in der Künstliche Intelligenz immer wichtiger wird, sind Daten zur eigentlichen Währung geworden. Wenn diese Daten nicht unter der richtigen nationalen oder europäischen Gesetzgebung stehen oder außerhalb des entsprechenden Rechtsraums gespeichert werden, entsteht ein erhebliches Problem – sowohl für die europäische Unabhängigkeit als auch für den Schutz unserer Daten und unseres geistigen Eigentums.

Herr Zimmermann, welche Rolle spielt SecurePIM heute bei der Umsetzung sicherer mobiler Arbeitsplätze?

Zimmermann: Seit rund 15 Jahren konzentrieren wir uns auf ein Thema: SecurePIM. SecurePIM bildet das Herzstück des sicheren mobilen Arbeitsplatzes und wurde über zwei Jahrzehnte kontinuierlich weiterentwickelt. Die Lösung ermöglicht sämtliche zentralen Arbeitsprozesse auf mobilen Endgeräten. Dazu gehören E-Mail, Kalender, Kontakte, die Bearbeitung und der Austausch von Dokumenten sowie viele weitere Funktionen. Kurz gesagt: SecurePIM stellt den vollständigen mobilen Arbeitsplatz auf Smartphones und Tablets bereit. Von Anfang an lag unser Fokus ausschließlich auf mobilen Endgeräten. Ebenso wichtig war es für uns, höchste Sicherheitsstandards einzuhalten. Deshalb arbeiten wir seit vielen Jahren eng mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zusammen. Unser Ziel ist es, eine vollständig souveräne Lösung anzubieten. Die von uns eingesetzte Kryptografie wurde in Deutschland entwickelt. Unsere Kunden wissen deshalb genau, woher die Technologie stammt. Es gibt keine versteckten Hintertüren oder vergleichbare Risiken. Wir verstehen SecurePIM als das Fundament des mobilen Arbeitsplatzes. Gleichzeitig sehen wir Wire als Spezialisten für sichere Kommunikation – also Messaging, Telefonie und Videokonferenzen. Statt diese Funktionen selbst neu zu entwickeln, integrieren wir eine bereits etablierte und leistungsfähige Lösung.

Herr Brown, wodurch unterscheidet sich Wire von anderen Messaging- und Kollaborationsplattformen im Markt?

Brown: Wire wurde in Berlin gegründet und hat dort bis heute seinen Hauptsitz. Mehr als 90 Prozent unserer Forschung und Entwicklung finden in Deutschland statt und werden überwiegend von deutschen beziehungsweise europäischen Mitarbeitenden getragen. Mit Wire Bund betreiben wir die einzige Messaging-, Sprach- und Kollaborationsplattform, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für den Einsatz bis zum Geheimhaltungsgrad VS-NfD zertifiziert wurde. Ein weiterer wichtiger Unterschied ist, dass Wire als Open-Source-Plattform entwickelt wird. Dadurch schaffen wir Transparenz und Vertrauen. Wie Daniel bereits sagte, gibt es keine versteckten Hintertüren. Vor allem aber wurde Wire von Anfang an konsequent unter Sicherheits- und Datenschutzgesichtspunkten entwickelt. Viele bekannte Kommunikationsplattformen wie Microsoft Teams, Slack oder auch WhatsApp wurden zunächst für die Zusammenarbeit entwickelt. Sicherheitsfunktionen kamen häufig erst später hinzu. Bei Wire war es genau umgekehrt: Sicherheit und Datenschutz standen von Beginn an im Mittelpunkt.

Wie wird Wire künftig in SecurePIM integriert sein, und welche Vorteile ergeben sich daraus für die Anwenderinnen und Anwender?

Zimmermann: Wir verfolgen bewusst einen schrittweisen Ansatz. Es wird keinen großen Umbruch geben. Beide Lösungen sind bereits heute bei zahlreichen Kunden im Einsatz. Deshalb entwickeln wir die Integration gemeinsam mit Referenz- und Pilotkunden Schritt für Schritt weiter. Der erste Ausbauschnitt ist vergleichsweise einfach: Öffnet ein Nutzer in SecurePIM seine Kontakte, werden künftig auch die Wire-Kontaktdaten angezeigt. Tippt er beispielsweise auf einen Wire-Kontakt, öffnet sich unmittelbar die Wire-Anwendung und der Chat oder Anruf kann direkt gestartet werden. Darüber hinaus planen wir weitere Funktionen. SecurePIM verfügt bereits über die Zulassung für die Bearbeitung von Dokumenten bis zum Geheimhaltungsgrad VS-NfD. Künftig sollen beispielsweise verschlüsselte PDF-Dokumente, die über Wire ausgetauscht werden, direkt in SecurePIM geöffnet und bearbeitet werden können.

Die Partnerschaft zielt auf Lösungen bis zum VS-NfD-Niveau. Welche technischen und organisatorischen Voraussetzungen müssen dafür erfüllt werden?

Zimmermann: Sowohl Wire als auch Materna Virtual Solution verfügen bereits über die erforderlichen Zulassungen für den Einsatz bis zum Geheimhaltungsgrad VS-NfD. Um diese Zertifizierung zu erhalten, ist eine sehr enge Zusammenarbeit mit dem Bundesamt für Sicherheit in der Informationstechnik erforderlich. Das BSI definiert mit der Verschlusssachen-Architekturspezifikation (VSA) sehr detaillierte technische Anforderungen. Diese betreffen die gesamte Systemarchitektur, die eingesetzten Technologien und zahlreiche weitere Sicherheitsaspekte. Die BSI-Zertifizierung bestätigt, dass die Anwendung so entwickelt wurde, dass Nutzer keine sicherheitskritischen Umgehungsmöglichkeiten schaffen können und Datenlecks technisch verhindert werden.

Mitarbeitende erwarten heute dieselbe einfache Bedienung, die sie von privaten Kommunikationsanwendungen kennen.

Brown: Aus Sicht von Wire kommt noch ein weiterer Punkt hinzu. Für den Einsatz bis VS-NfD entwickeln wir ein separates Produkt, das sich deutlich von unserer Standardlösung unterscheidet und den höheren Sicherheitsanforderungen gerecht wird. Beide Unternehmen verfügen zwar bereits über entsprechende Zertifizierungen. Das bedeutet allerdings nicht automatisch, dass auch die gemeinsame integrierte Lösung unmittelbar zertifiziert ist. Genau daran werden wir in den kommenden Monaten gemeinsam arbeiten und die Integration entsprechend weiterentwickeln.

Die aktuelle Integration ist der Auftakt einer engeren Zusammenarbeit. Welche weiteren Entwicklungen und Innovationen planen Sie gemeinsam für die Zukunft des sicheren mobilen Arbeitens?

Zimmermann: Wir kennen uns bereits seit mehreren Jahren, ich würde sogar sagen, dass wir eine ähnliche DNA haben. Beide Unternehmen sind mittelständisch geprägt und verfolgen dasselbe Ziel: Wir möchten unseren Kunden hochwertige Technologien anbieten, die einfach zu bedienen sind und den Arbeitsalltag erleichtern. Gleichzeitig teilen wir dieselben Werte. Beide Unternehmen stehen für digitale Souveränität und für den sicheren Umgang mit schutzbedürftigen Informationen. Außerdem konzentrieren wir uns beide auf das mobile Arbeiten. Dabei verfolgen wir nicht das Ziel, unsere Produkte zu einer einzigen Anwendung zusammenzuführen. Vielmehr wollen wir unsere jeweiligen Stärken miteinander verbinden und unsere Entwicklungs-Roadmaps aufeinander abstimmen.

Brown: Wir gehen bewusst Schritt für Schritt vor. Zunächst schaffen wir eine Integration, die einen einheitlichen digitalen Arbeitsplatz ermöglicht. Dabei orientieren wir uns konsequent an den Anforderungen unserer Kunden und an den Entwicklungen, die wir im Markt beobachten – sei es im Hinblick auf digitale Souveränität, regulatorische Vorgaben, Cybersicherheit oder Governance. Ich bin überzeugt, dass dies

erst der Anfang ist. Wir haben noch viele Ideen und werden in Zukunft sicher weitere gemeinsame Entwicklungen vorstellen können.

()

Stichwörter: IT-Infrastruktur, Materna Virtual Solution, SecurePIM, Wire