



WALLIX gibt Ausblick auf die Cybersecurity-Trends und Technologien von 2026

Paris, 8. Januar 2026 – WALLIX (Euronext ALLIX), europäischer Cybersecurity-Spezialist und führender Anbieter für Identity-, Access- und Privileged-Access-Management, stellt seine technologische Vision für das Jahr 2026 vor. Präsentiert wird der Ausblick von Julien Cassignol, Chief Product & Technology Officer (CPTO).

Vor dem Hintergrund geopolitischer Spannungen und einer sich weiter beschleunigenden digitalen Transformation identifiziert das Unternehmen vier zentrale Kräfte, die die Cybersicherheitslandschaft nachhaltig verändern: verschärfte regulatorische Anforderungen, KI-gestützte intelligente Automatisierung, das exponentielle Wachstum digitaler Identitäten – sowohl menschlicher als auch maschineller – sowie den Beginn des Post-Quanten-Zeitalters.

Regulierung als Fundament vertrauenswürdiger digitaler Umgebungen

Die europäischen Cybersecurity-Vorgaben entwickeln sich kontinuierlich weiter – mit dem Ziel, digitale Umgebungen zu schaffen, in denen Datenschutz und Resilienz im Mittelpunkt stehen. Richtlinien und Regularien wie NIS2, DORA, IEC 62443, der Cyber Resilience Act oder der AI Act setzen inzwischen hohe Anforderungen. In einem geopolitisch instabilen Umfeld, in dem Cyberangriffe zunehmend auf die Grundpfeiler von Wirtschaft und Gesellschaft zielen, gehen diese Rahmenwerke weit über reine Compliance hinaus. Sie stehen für den gemeinsamen Anspruch, vertrauenswürdige digitale Ökosysteme im Interesse von Staaten, Organisationen und Anwendern zu etablieren.

Im Fokus steht dabei der Schutz sensibler Daten – insbesondere personenbezogener und industrieller Informationen, die zu den kritischsten Vermögenswerten zählen. Ebenso entscheidend ist es, kryptografische Schlüssel unter lokaler Kontrolle zu halten und digitale Zugriffe innerhalb von Organisationen strikt zu steuern. Diese operative Souveränität lässt sich nur mit skalierbaren Identity- und Access-Management-Plattformen erreichen. Bis 2026 müssen solche Lösungen regulatorische Anforderungen bereits „by design“ erfüllen, zugleich effizient arbeiten und sich flexibel in On-Premises-, Hybrid- und Cloud-Umgebungen einsetzen lassen – ohne unerwünschte extraterritoriale Abhängigkeiten zu schaffen.

Digitale Souveränität ist dabei ein strategisches Kernanliegen. Mit der modularen Plattform WALLIX One erhalten Organisationen die Möglichkeit, die Kontrolle über digitale Zugriffe sowie über menschliche und nicht-menschliche Identitäten gezielt zu stärken – bei voller Freiheit in



der Wahl des Betriebsmodells. Damit positioniert sich das Unternehmen im Einklang mit der regulatorischen Vision widerstandsfähiger, interoperabler und vertrauenswürdiger digitaler Ökosysteme.

Machine Identity Management: Zugriffe im großen Maßstab kontrollieren

Die Zahl digitaler Identitäten wächst rasant. Neben menschlichen Nutzern entwickeln sich insbesondere nicht-menschliche Identitäten – etwa Maschinen und agentenbasierte Systeme – zu einer zentralen sicherheitstechnischen Herausforderung. Service Accounts, SPS/PLCs, Roboter, medizinische Geräte sowie laut Gartner bis zu 30 Milliarden vernetzte Objekte bis 2030 bilden eine Vielzahl „unsichtbarer“ Identitäten, die bei fehlender Kontrolle erhebliche Sicherheitsvorfälle verursachen können. Gerade für die Stabilität industrieller Umgebungen sowie die Resilienz kritischer und systemrelevanter Organisationen ist dieses Thema von entscheidender Bedeutung.

Bis 2026 wird Machine Identity Management zu einer festen Säule moderner Sicherheitsstrategien. Maschinenidentitäten müssen dann mit derselben Konsequenz verwaltet und abgesichert werden wie menschliche Nutzer. Sämtliche Secrets, Zertifikate und kryptografischen Schlüssel sind vollständig zu inventarisieren, zu schützen und automatisiert zu erneuern. Doch der Schutz von Zugangsdaten allein reicht nicht aus. Ebenso entscheidend ist es, die Prozesse zu identifizieren, zu verifizieren und zu autorisieren, die diese Secrets verwenden. Selbst häufig rotierte Credentials bieten keinen ausreichenden Schutz, wenn der legitim zugreifende Prozess kompromittiert oder durch schädlichen Code ersetzt wurde.

WALLIX verfolgt diesen Ansatz konsequent und entwickelt offene, innovative Lösungen, mit denen sich Maschinenidentitäten sicher und skalierbar verwalten lassen. Ein konkretes Beispiel ist das Engagement des Unternehmens in der Open-Source-Community OpenBao, die sich der Absicherung von Secrets in hybriden und Multi-Cloud-Umgebungen widmet.

Dieser offene Ansatz ermöglicht es Organisationen, die Kontrolle über kryptografische Schlüssel und Zugriffe zu behalten, ohne sich an einen einzelnen proprietären Anbieter zu binden – und dabei gleichzeitig sicher zu skalieren. Er unterstreicht das klare Bekenntnis von WALLIX zu offenen Standards als Grundlage für Vertrauen, Interoperabilität und langfristige technologische Unabhängigkeit.

Agentic AI: auf dem Weg zur autonomen Cyberabwehr

Mit zunehmender Geschwindigkeit und Komplexität von Bedrohungen wird intelligente Automatisierung zu einer zentralen Säule der Cybersicherheit. Während Angreifer generative KI gezielt einsetzen, um ihre Angriffsmethoden zu verfeinern, setzen Verteidiger zunehmend auf agentenbasierte KI, die in der Lage ist, in komplexen Umgebungen autonom zu agieren. In Security Operations Centern (SOCs) eingebettet, analysiert diese Technologie Sicherheitsvorfälle ganzheitlich, priorisiert Alarme und entlastet Teams von permanenter manueller Überwachung.



Damit vollzieht die Cybersicherheit den Wandel von einer reaktiven hin zu einer proaktiven Verteidigung, die innerhalb von Sekunden reagieren oder Angriffe sogar antizipieren kann. Intelligente Automatisierung macht es möglich, Aufgaben zu bewältigen, die bislang als nicht beherrschbar galten – etwa die Verwaltung von Millionen sich kontinuierlich verändernder Zugriffsrechte. Durch die Kombination von Machine Learning zur Anomalieerkennung mit der Analyse großer Datenmengen aus Millionen von Ereignissen kann KI ungewöhnliches Verhalten kompromittierter oder unsicherer Service Accounts in Echtzeit erkennen und neutralisieren – bevor es zu einem Sicherheitsvorfall kommt. Prozesse, die früher Tage in Anspruch nahmen, lassen sich so auf Sekunden verkürzen.

WALLIX investiert kontinuierlich in die Verbindung von KI und menschlicher Expertise, um eine wirklich proaktive Cyberabwehr zu ermöglichen. Der Einsatz agentenbasierter KI erfordert dabei eine strikte Governance: Sie darf ausschließlich auf die für ihre Aufgabe notwendigen Daten zugreifen. Dadurch gewinnt Machine Identity Management weiter an strategischer Bedeutung, insbesondere bei der Kontrolle nicht-menschlicher Identitäten und ihrer Berechtigungen. Die kürzlich erfolgte Übernahme von Malizen stärkt die Fähigkeiten von WALLIX in der Erkennung anomalen Verhaltens und der automatisierten Datenanalyse – und hilft Organisationen, immer schnelleren und ausgefeilteren Angriffen einen Schritt voraus zu sein.

Post-Quanten-Kryptografie und digitale Souveränität

Quantencomputing stellt ein langfristiges strategisches Risiko für die Sicherheit von Daten, industriellen Systemen, IoT-Netzwerken und anderen vernetzten Umgebungen dar. Seine Fähigkeit, heutige kryptografische Verfahren zu brechen, bedeutet, dass Daten, die heute verschlüsselt werden, morgen offengelegt werden könnten, wenn Organisationen nicht rechtzeitig vorsorgen. Betroffen sind unter anderem industrielle Netzwerke, medizinische Geräte in Krankenhäusern sowie intelligente Gebäude.

Der Übergang zu Post-Quanten-Kryptografie ist daher sowohl eine technische als auch eine strategische Priorität. Unternehmen müssen bereits heute auf **Krypto-Agilität** setzen, um Verschlüsselungsmechanismen und Sicherheitsrichtlinien flexibel anpassen zu können, sobald neue Standards reifen und etabliert werden.

Über die Plattform WALLIX One wird WALLIX künftig Post-Quanten-Verschlüsselungsstandards integrieren, um quantenresistente Algorithmen zu unterstützen. Dazu gehört die Absicherung von Backups, interner Kommunikation und privilegierten Zugriffen mit Verfahren, die auch zukünftigen Quantenangriffen standhalten. Indem Organisationen bei der Migration ihrer Schlüssel, Zertifikate und Protokolle auf diese neuen Standards unterstützt werden, leistet WALLIX einen weiteren Beitrag zum Aufbau einer europäischen kryptografischen Souveränität.

Über WALLIX

WALLIX (Euronext: ALLIX, seit 2015 börsennotiert) ist ein europäischer Anbieter von Cybersecurity-Lösungen und führend im Bereich Privileged Access Management (PAM). Das Unternehmen unterstützt Organisationen dabei, ihre Sicherheit und digitale Souveränität nachhaltig zu stärken. Verwurzt in europäischen Werten wie Sicherheit und Freiheit und von führenden Analystenhäusern für die technologische Leistungsfähigkeit der Plattform **WALLIX One** anerkannt, begleitet



WALLIX heute mehr als 4.000 Organisationen weltweit.

Die Mission ist klar: Identitäten, Zugriffe und privilegierte Berechtigungen in sämtlichen IT- und OT-Umgebungen zu schützen – und Unternehmen so die Freiheit zu geben, sich sicher und selbstbewusst in einer zunehmend digitalen Welt zu bewegen.

www.wallix.com | info@wallix.com

PRESSEKONTAKTE

Finanzkommunikation

ACTUS Finance & Communication

Investor Relations – Hélène de Watteville

+33 (0)1 53 67 36 33 / WALLIX@actus.fr

Pressekontakt

Déborah Schwartz +33 (0)6 27 09 05 73 / dschwartz@actus.fr