LANline

9,– €

Januar 2017
19. Dezember 2016

ITP VERLAG

IT ■ Network ■ Datacenter www.lanline.de

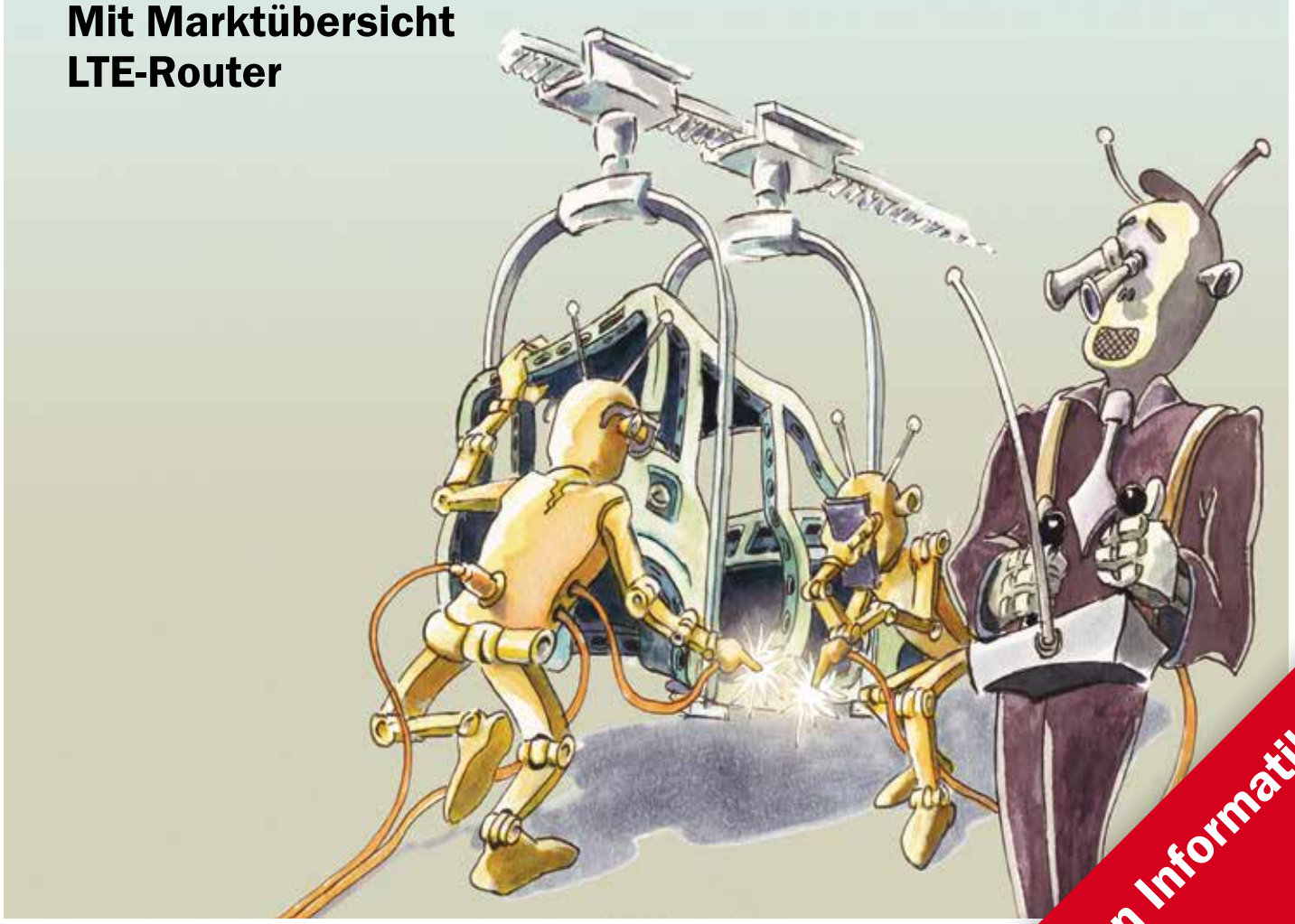
Wireless-Technik für IT und Industrie

WLAN als Zentralverteiler

Juristische Blockaden im Hotspot

Business Access Points

Mit Marktübersicht LTE-Router



Datenklau im Rechenzentrum
Schwachstelle Admin-Zugriff

Testserie Monitoring Teil 6: Netbrain
Dynamic Maps für die Fehleranalyse

Schwer… und …
Mi…

Consumer-IAM-Lösungen

Skalierbar authentifizieren

Anders als bei klassischen Lösungen für das Identity- und Access-Management (IAM) ist bei einer CIAM-Lösung (Consumer-IAM) besonders hohe Flexibilität gefragt: Kunden-Login-Systeme müssen hochskalierbar sein und dürfen Anwender, die sich zum ersten Mal an einem System anmelden möchten, nicht überfordern. Damit ist CIAM prädestiniert für das Cloud-Service-Zeitalter.

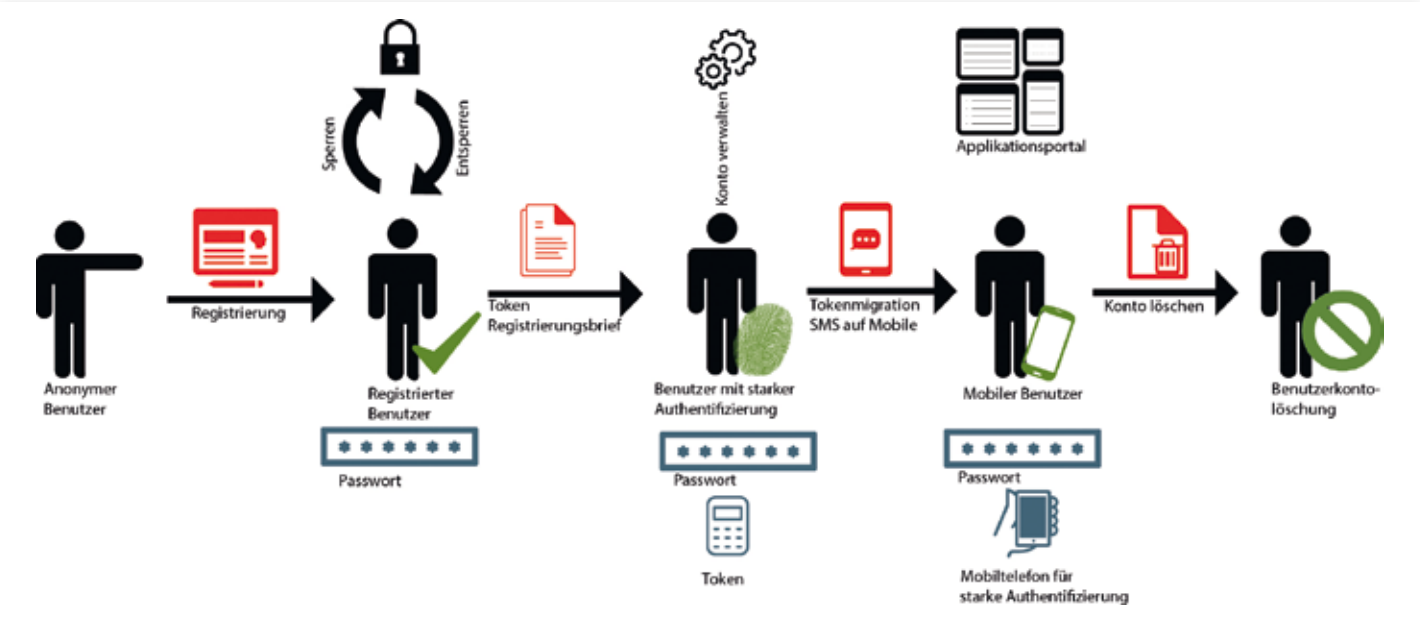
Im Gegensatz zu IAM-Lösungen für Unternehmensmitarbeiter müssen CIAM-Lösungen mit einer größeren Anzahl von Identitäten und entsprechend vielen gleichzeitigen Sessions umgehen können. CIAM-Software ist deshalb darauf ausgelegt, bei hoher Performance bis auf Millionen von Nutzern zu skalieren. Zusätzlich bietet eine CIAM-Lösung gegenüber einer klassischen IAM-Lösung auch einen Preisvorteil, da bei diesen eine hohe Zahl zu schützender Identitäten meist bei den Lizenzgebühren ins Gewicht fällt.

Setzt ein Unternehmen eine CIAM-Lösung ein, hat der Anwender einen großen Vorteil: Er kann die Anmeldung und die Erweiterung seines Kundenprofils ohne Eingriff des Administrators oder eines Helpdesks selbst bewerkstelligen. Dieser User-Self-Service entlastet die Support-Mitarbeiter, senkt die Kosten und verkürzt Wartezeiten für Nutzer signifikant. Beispielsweise lassen sich so Passwörter schnell und einfach jederzeit selbst zurücksetzen.

Falls dennoch eine Helpdesk-Unterstützung notwendig wird, kann der Support-Mitarbeiter über delegierte Administrationsrechte auf das Endanwenderkonto zugreifen. Mittels sogenannten Co-Browsings lassen sich einzelne Arbeitsschritte sogar in Zusammenarbeit mit dem Endanwender erledigen – vorteilhaft für die Effizienz und die Zufriedenheit des Anwenders.

Bei der Registrierung neuer Accounts ist im Consumer-Umfeld eine niedrige Eintrittsbarriere wichtig, damit Interessenten nicht frühzeitig abspringen. Das Einbeziehen bestehender Social-Media-Accounts vereinfacht die Eröffnung von Konten und kürzt den Vorgang ab. Dabei bringen Endanwender ihre bestehenden digitalen Identitäten gleich mit („Bring Your Own Identity“). Das ist einfach, verständlich und steigert letztlich die Zahl der Registrierungen.

Vorgelagerte IAM-Funktionaliät ermöglicht ein zentrales Single Sign-on, was die Akzeptanz starker Authentisierung durch die Benutzer erheblich verbessert. Eine starke Authentifizierung für hohe Sicherheits- oder Compliance-Anforderungen lässt sich dabei durch ein sogenanntes Step-up-Verfahren umsetzen. Für beste-



Self-Service- und Sicherheitsfunktionen erleichtern das Management digitaler Identitäten über deren gesamten Lebenszyklus hinweg. Bild: Ergon Informatik

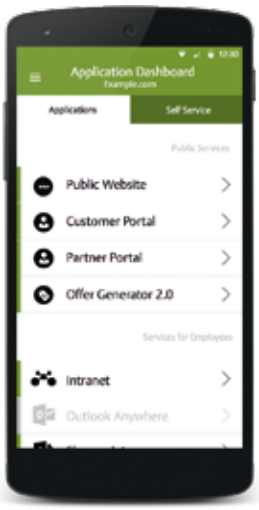
hende Applikationen sinkt durch vorgelagerte IAM-Funktionalität zudem die Komplexität, da sie selbst keine Routinen für Authentifizierung und Grobautorisierung bereitstellen müssen. Dies ermöglicht nicht nur Single Sign-on, sondern entlastet zugleich die Applikationslandschaft.

Sicherheit plus Benutzerfreundlichkeit

Unternehmen können mit CIAM zwischen verschiedenen Authentifizierungsformen wählen und wechseln. Ob ein einfaches Passwort oder ein modernes, starkes Authentifizierungsverfahren erforderlich ist: Der IT-Administrator oder Helpdesk muss nicht unbedingt eingreifen. Benutzer empfinden hauptsächlich interaktive Authentifizierungsschritte als störend. Denn hierbei müssen sie wiederholt einen weiteren Handlungsschritt tätigen, damit das System ihre Identität verifizieren kann.

Bei der risikobasierten Authentifizierung hingegen berücksichtigt eine intelligente Sicherheitssoftware Kontextinformationen während des Zugriffs auf eine Anwendung, zum Beispiel die Tageszeit, den Zugriffsort, die Geräte-ID sowie verschiedene Browser-Informationen. Die Kombination dieser gesammelten Informationen ergibt eine gute Einschätzung, ob der Zugriff regulär erfolgt oder betrugsverdächtig ist. Auf diese Weise lässt sich ein hohes Sicherheitsniveau erreichen und zugleich die Anzahl der interaktiven Authentifizierungsschritte reduzieren.

In allen Unternehmen und Organisationen gibt es Bereiche mit verschiedenen Sicherheitsanforderungen. Der Hypothekenrechner einer Bank beispielsweise ist nicht sicherheitskritisch; ein persönlicher Börsenticker aber erfordert eine einfache Authentifizierung, während das E-Banking-System eine starke Authentifizierung voraussetzt. In CIAM-Systemen



CIAM-Lösungen bieten Endanwendern schnellen Zugriff auf alle Applikationen. Bild: Ergon Informatik

schafft Single Sign-on eine nahtlose Bedienbarkeit, wenn eine höhere Sicherheitsstufe gefordert ist. Der Benutzer tippt zum Beispiel einen SMS-Code ab und erhält dann für eine längere Zeit Zugriff auf alle relevanten Anwendungen. Dies vermeidet, dass dem Endanwender eine Applikationen mit vielen unterschiedlichen Login-Aufforderungen zu kompliziert wird und er deshalb nach Alternativen sucht.

CIAM-Lösungen sind häufiger Ziel von Hackerangriffen als klassische Enterprise-IAM-Lösungen, da sie nach außen gerichtet sind. Hier kann die Kombination mit einer Web Application Firewall (WAF) ein CIAM und die Applikationen gegen Angriffe wie etwa Cross-Site Scripting oder Session Hijacking schützen. Zudem kann die WAF zulässige Werte von Benutzereingaben dynamisch verifizieren. Mittels Dynamic Value Endorsement ist dies auch für JSON-Objekte möglich, was den Schutz auf REST-APIs ausweitet. REST-APIs kommen oft für Smartphone-Apps zum Einsatz und sind daher ein wichtiger Pfeiler, wenn es um die Sicherheit mobiler Applikationen geht. Gezielte Web-basierte Betrugsversuche („Web Fraud“) lassen sich dabei früh in der Benutzerinteraktion erkennen, sodass man dann die nötigen Gegenmaßnahmen ergreifen kann.

Eine CIAM-Lösung lässt sich über technische Schnittstellen in andere Lösungen integrieren. Dies ermöglicht den flexiblen Zugriff auf bestehende Services sowie eine Integration in existierende Lösungen wie Portale. Schließlich ist es mit CIAM möglich, verschiedene Directory-Services zu synchronisieren, um Identitäten aus verschiedenen Benutzerverzeichnissen zusammenzuführen. Token-Lösungen von Drittherstellern lassen sich auf einfache Weise zusätzlich zur bestehenden Directory-Authentisierung in Betrieb nehmen, ohne dass geschützte Applikationen anzupassen wären. Dr. Martin Burkhart/wg

Dr. Martin Burkhart ist Produktmanager bei Ergon Informatik in Zürich, www.ergon.ch.