

Umfrage zeigt Trend: Schweizer Unternehmen wollen europäische IT-Sicherheit

Immer mehr Schweizer Unternehmen stellen sich die Frage: Wem kann man bei der IT-Sicherheit noch vertrauen? Eine neue Umfrage zeigt: Die Herkunft der eingesetzten Lösungen rückt zunehmend in den Mittelpunkt strategischer Entscheidungen.

DER AUTOR
Rainer Schwegler
Senior Territory Manager
Schweizland, East Deutschland

Datensouveränität und digitale Abhängigkeit sind für Schweizer Unternehmen längst keine abstrakten Themen mehr. Eine aktuelle, repräsentative Umfrage des Analytischen Hauses Technoconsult im Auftrag des europäischen IT-Sicherheitsanbieters Eset zeigt: Die Mehrheit der befragten Unternehmen in der Schweiz denkt und hinterfragt die Herkunft ihrer IT-Sicherheitslösungen.

Laut der Studie würden 72 Prozent der Unternehmen bei einer Neuschaffung gezielt einen Anbieter aus Europa bevorzugen. Knapp 44 Prozent setzen bereits auf europäische oder schweizerische Lösungen. US-amerikanische Hersteller folgen mit 22 Prozent, Anbieter aus Asien oder anderen Weltregionen spielen in der Schweiz kaum eine Rolle.

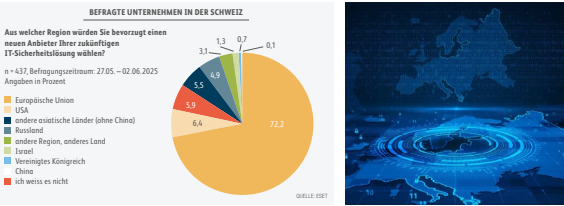
Anbieterwechsel wird aktiv erwogen
Auffällig ist vor allem die hohe Wechselbereitschaft: Zwei Drittel der befragten Unternehmen gaben an, mässig bis sehr stark über einen Anbieterwechsel nachzudenken. Dabei dürfen nicht allein technische oder wirtschaftliche Gründe die Befragten zu einem Wechsel bewegen, sondern zunehmend auch Aspekte wie Datenschutz, rechtliche Sicherheit und geopolitische Unabhängigkeit. Die Ergebnisse lassen darauf schliessen, dass sich der Trend zur europäischen IT-Sicherheit weiter verstärken wird. Denn die Umfrage wurde noch vor der jüngsten Affäre rund um den Schweizer Nachrichtendienst und die vermutete Weitergabe sensibler

Daten an einen russischen IT-Anbieter durchgeführt: ein Vorfall, der in Medien und Politik für Diskussionen über die digitale Souveränität der Schweiz sorgt.

Rechtsrahmen als Argument für Europa
Ein zentrales Argument der befragten Unternehmen: Europäische Anbieter unterliegen einem klar definierten Rechtsrahmen, der mit dem revidierten Schweizer Datenschutzgesetz (revDSG) weitgehend kompatibel ist. Das schafft Vertrauen, vor allem im Hinblick auf Compliance-Anforderungen, Zertifizierungen und Kundenbeziehungen im europäischen Wirtschaftsraum.

Im Gegensatz dazu stehen Anbieter aus Drittstaaten, die teils Grenzen unterliegen, die Zugriff auf Daten auch ohne Zustimmung der Betroffenen ermöglichen (etwa dem US Cloud Act). Für viele Unternehmen sind solche rechtlichen Unsicherheiten zunehmend ein Ausschlusskriterium.

Souveränität wird strategisch
Die Studienergebnisse zeigen auch, dass IT-Sicherheit heute strategischer bewertet wird als noch vor wenigen Jahren. Es geht nicht mehr nur um technische Funktionen, sondern um Kontrolle, Transparenz und Verlässlichkeit. Digitale Souveränität ist für viele Unternehmen in der Schweiz ein erklärtes Ziel und die Wahl des richtigen Anbieters ein erster Schritt dorthin.



netzwoche.ch © netzmedien ag

Beispiel online:
<https://www.netzwoche.ch/news/2025-08-25/umfrage-zeigt-trend-schweizer-unternehmen-wollen-europaeische-it-sicherheit>

« Digitale Souveränität beginnt bei der Wahl der Sicherheitslösung »

Immer mehr Schweizer Unternehmen entscheiden sich für IT-Sicherheit aus Europa. Rainer Schwegler, Senior Territory Manager Switzerland bei Eset, erklärt im Gespräch, warum «Made in Europe» mehr ist als ein Label und was Unternehmen jetzt beachten sollten. Interview: Jodi Orant



tativen Auswertung viele Befragte explizit den Wunsch nach mehr Transparenz in der Lieferkette und nach Produkten nannten, die im europäischen Rechtsraum entwickelt und betreut werden. Wir sehen darin ein Umdenken, das vor allem durch Erfahrungen in den letzten zwei Jahren beschleunigt wurde.

Was bringt Unternehmen das Label «Made in Europe» konkret?
Zum einen Rechtssicherheit: Europäische und schweizerische Datenschutzgesetze definieren klare Regeln, die für beide Seiten gelten. Es gibt keine Grauzonen oder aussergerichtliche Zugriffe. Zum anderen stärken Unternehmen mit europäischen Lösungen ihre digitale Souveränität. Sie behalten die Kontrolle über ihre Systeme, Datenflüsse und Updates. Drittens bieten europäische Anbieter oftmals eine höhere Transparenz hinsichtlich Produktentwicklung, Sicherheitsarchitektur und Betriebsführung. Und nicht zuletzt: Wer sich für einen europäischen Hersteller entscheidet, sendet ein starkes Signal an Kunden, Partner und Öffentlichkeit.

Wie wichtig ist aus Ihrer Sicht der rechtliche Rahmen für die tägliche Praxis?
Sehr wichtig – aber oft unterschätzt. In der Praxis hängen viele Prozesse davon ab, dass man auf rechtlich eindeutige Grundlagen bauen kann. Mit einem Anbieter, der dem europäischen oder schweizerischen Datenschutzrecht unterliegt, lassen sich Audits, Zertifizierungen oder Sicherheitsnachweise deutlich einfacher bewältigen. Man spricht grossmühsam die gleiche Sprache. Bei Anbietern aus Drittstaaten wird es schnell komplexer: etwa durch divergierende Gesetzeslagen, mögliche Zugriffsansprüche fremder Behörden oder Unsicherheiten im Haftungsfall. Wer diese Risiken reduzieren will, muss sie aktiv im Beschaffungsprozess berücksichtigen.

Was können Sie Unternehmen sonst noch empfehlen?
Unternehmen, die sich mit dem Thema auseinandersetzen, sollten sich vor allem Klarheit über ihre individuellen Sicherheitsbedürfnisse und regulatorischen Anforderungen verschaffen. Es beginnt mit der Frage: «Betreibe ich meine Infrastruktur via Cloud oder On-Premise?» und reicht bis zu politischen und rechtlichen Einflussfaktoren, die die eigene Security betreffen. Wer langfristig plant, sollte IT-Sicherheit als strategisches Erfolgsfaktor begreifen und damit auch Herkunft, Datenschutzkonformität und Transparenz zur Chef-sache machen. Es lohnt sich, genau hinzuschauen und nicht nur auf Funktionalität, sondern auch auf Vertrauenswürdigkeit zu setzen.

Haben Schweizer Unternehmen die Vorteile von «Made in Europe» erkannt?
Ja, und zwar zunehmend differenzierter. Unsere aktuelle Umfrage zeigt, dass viele Unternehmen ihre bisherigen Anbieterbeziehungen überdenken. Das betrifft nicht nur die Herkunft der eingesetzten Lösungen, sondern auch Fragen der Verfügbarkeit im Krisenfall und politische Neutralität. Besonders interessant ist, dass in der quali-



netzwoche.ch © netzmedien ag

netzwoche.ch © netzmedien ag

Text

Spezifikationen

Grundtext Fachbeitrag
1 Seite: 3000–3500* Zeichen**
Titel: max. 80 Zeichen**
Lead: 250–300* Zeichen**

Angaben inkl. 1 Abbildung;
pro jede weitere Abbildung
ca. 500 Zeichen weniger

Grundtext Interview
1 Seite: 3000–3500* Zeichen** (inkl. Fragen)
*Minimum–Maximum | **inklusive Leerzeichen

Inhalt

Fachbeitrag: muss firmen- und produkt neutral verfasst sein.
Kein Marketing – kein Advertorial!

Grundtext: Titel, Lead, Fliesstext
Bild: neutrales Themenbild
Autor: Name, Funktion, Firma, Farbfoto

*Nutzen Sie die digitalen Möglichkeiten!
Senden Sie uns einen **Call-to-Action** mit!*

Interview: Fragen werden von der Redaktion gestellt
Interviewpartner: Name, Funktion, Firma, Farbfoto

Bitte beachten Sie, dass wir bei Firmenschreibungen keine Marketing-schreibweisen berücksichtigen (kleine Anfangsbuchstaben, Binnenmajuskel, Versalschreibung etc.).

Bild

Porträtbilder: Farbfotos
Auflösung: mind. 1500 Pixel breit
(Bilder online haben ein Format von 16:9)
Bildformat: JPG, PNG

Preise – Print + online

	Netzwoche	IT-Markt	ICTjournal (FR)
2 Seiten	6950.–	6250.–	6250.–

Bitte senden Sie alle Daten an: produktion@netzmedien.ch
Netzmedien AG · Heinrichstrasse 235 · 8005 Zürich · Tel: 044 355 63 63