Cybersicher und resilient in einer vernetzten Welt

In fünf Schritten zur digitalen Souveränität

31.01.2025 · Von Thierry Kramis · 5 min Lesedauer ·

Die Wettbewerbsfähigkeit kleiner und mittlerer Unternehmen (KMU) im digitalen Zeitalter steht und fällt mit ihrer digitalen Souveränität. Fünf Aspekte sind ausschlaggebend, um die IT-Infrastruktur zukunftssicher zu gestalten, unabhängiger von Drittanbietern zu werden und Cyberrisiken zu minimieren.

Digitale Souveränität: KMU sichern mit Monitoring und hybriden Infrastrukturen Kontrolle und Unabhängigkeit. (Bild: Dätwyler IT Infra)

Ob Unternehmen, Staat oder Privatperson: Wer digital souverän ist, bleibt Herr seiner Daten und IT-Systeme, kann diese also unabhängig von externen Einflüssen wie Drittanbietern

steuern und nutzen. Die digitale Souveränität gewinnt geopolitisch und wirtschaftlich immer mehr an Bedeutung – aber auch an Komplexität. Vor diesem Hintergrund schaffen Richtlinien wie die DSGVO und NIS-2 sowie die im Oktober 2024 veröffentlichte CER-Richtlinie einen regulatorischen Rahmen für mehr Sicherheit und Resilienz in der digitalen Infrastruktur im EU-Raum.

Cyberresilienz – die Achillesferse der KMU?

Cyberangriffe sind das größte Risiko fürs Geschäft – davon waren 48 Prozent der KMU überzeugt, die im Rahmen einer einschlägigen Studie der Gothaer Versicherungen 2024 befragt worden sind. Die zunehmende Vernetzung und Globalisierung hat zur Folge, dass Anbieter von Komponenten und Infrastrukturen über Ländergrenzen hinweg tätig sind. Der Überblick über komplexe IT-Infrastrukturen wird so schwieriger zu wahren. Diese Intransparenz birgt erhebliche juristische und finanzielle Risiken, insbesondere für KMU, die nicht immer über die nötigen Ressourcen und Kapazitäten verfügen, um ihre IT-Infrastruktur auf diesem Detailgrad proaktiv und umfassend zu überwachen. Eine zusätzliche Komplexitätsebene kommt durch den Einsatz von Künstlicher Intelligenz (KI) hinzu. Diese eröffnet viele Möglichkeiten der Automatisierung, fordert jedoch mehr Performance von der IT-Infrastruktur und kann Cyberkriminellen zu neuen Exploits verhelfen.

Welche Maßnahmen können IT-Verantwortliche konkret ergreifen, um KMU digital fit für die Zukunft zu machen und Risiken inmitten eines intransparenten Marktes zu minimieren?

1. Hybrid Cloud als Kompromiss zwischen Sicherheit und Flexibilität

Digitale Souveränität beginnt bei der Wahl des Cloud-Anbieters. Für KMU oft ein strategischer Spagat: Während der Betrieb einer vollständig On-Premise-basierten IT-Infrastruktur ab einer gewissen Größe ressourcenintensiv und personell oft nicht tragbar ist, hat auch das Outsourcing an externe Cloud-Dienstleister seine Schattenseiten.

Zwar reduziert ein Managed-Service-Ansatz den internen IT-Aufwand, doch gehen KMU potenziell Kompromisse bei der Datenhoheit ein – gerade, wenn sie auf internationale Hyperscaler setzen. Kritisch sind insbesondere Fragen zur Datenverarbeitung: Wo werden die Daten physisch gespeichert, und wie weit reichen die Zugriffs- und Verarbeitungsmöglichkeiten des Anbieters? Bei Providern aus Drittstaaten können unterschiedliche Rechtslagen, etwa zur Herausgabe von Daten an Behörden, zusätzliche Unsicherheiten schaffen. Nicht zuletzt machen sich KMU in einer Full-Managed-Beziehung

abhängig von einem Anbieter und können nicht ohne weiteres migrieren, sollten Preissteigerungen oder andere veränderte Rahmenbedingungen die Zusammenarbeit mit diesem Dienstleister unattraktiver gestalten.

Für KMU bietet die Hybrid-Cloud einen gangbaren Mittelweg. Sensible Daten bleiben in der privaten Cloud, während weniger kritische Anwendungen in der Public Cloud laufen. Das reduziert die Abhängigkeit von einzelnen Anbietern und ermöglicht eine schnelle Skalierung bei Bedarf. Edge Computing verleiht dieser Strategie ein Plus an Effizienz. Daten werden direkt dort verarbeitet, wo sie entstehen. Das spart Zeit, reduziert Latenz und entlastet zentrale Ressourcen.

2. Dezentralisierung zur Risikodiversifizierung

Der hybride Ansatz birgt für KMU einen weiteren Vorteil hinsichtlich der Ausfallsicherheit. Wer seine IT-Infrastruktur in die Hände eines einzigen Anbieters legt, riskiert einen Totalausfall, sollte dieser Anbieter beispielsweise Opfer eines Cyberangriffs werden. Eine solche Abhängigkeitsbeziehung ist ein klassischer „Single Point of Failure“ (SPOF). Redundante Systeme, verteilt auf verschiedene geografische Standorte, können die Cyberresilienz stärken – vorausgesetzt, alle Komponenten sind nahtlos integriert und lassen sich zentral verwalten, um im „Ernstfall“ schnell einsatzfähig zu sein. Zur Dezentralisierung gehört es auch, den Anbieterwechsel so reibungslos wie möglich zu gestalten. Lösungen wie Containerisierung oder Multi-Cloud-Management-Plattformen sorgen hier für mehr Flexibilität.

3. Monitoring und Updates automatisieren

Die IT-Abteilung als One-Man-Show – das ist immer noch die Realität, gerade in Kleinstunternehmen. Ein engmaschiges Monitoring aller Systeme und Prozesse innerhalb der IT-Infrastruktur, wie die Cybersicherheit und digitale Souveränität es erfordern, wird so uferlos. Ein systematischer Ansatz, gepaart mit Automatisierungslösungen, entlastet auch kleine IT-Teams und schafft Cyberresilienz.

Durch den Einsatz von proaktivem Monitoring in Kombination mit automatisierten Sicherheitslösungen können Probleme frühzeitig und effizient erkannt werden. Automatisierte Systeme liefern Echtzeit-Insights zu potenziellen Störungen, während regelmäßige Sicherheitsprüfungen – etwa durch Penetrationstests oder Schwachstellen-Scans – den IT-Betrieb zusätzlich absichern. Das automatisierte Management von

Sicherheitspatches und Updates sollte in cyberresilienten Unternehmen ebenfalls zum IT-Alltag gehören.

Jetzt Newsletter abonnieren

Täglich die wichtigsten Infos zu Netzwerktechnik, IP-Kommunikation und UCC

Geschäftliche E-Mail

Mit Klick auf „Newsletter abonnieren“ erkläre ich mich mit der Verarbeitung und Nutzung meiner Daten **gemäß Einwilligungserklärung (bitte aufklappen für Details)** einverstanden und akzeptiere die Nutzungsbedingungen. Weitere Informationen finde ich in unserer Datenschutzerklärung.

Aufklappen für Details zu Ihrer Einwilligung

4. IT-Normen leben, nicht nur dokumentieren

Gerade die ISO 27001 und die DSGVO assoziieren viele KMUs mit Bürokratie und Regulierungsdruck. Dabei können diese Normen wirksame Instrumente der digitalen Souveränität sein – vorausgesetzt, sie werden von der grauen Theorie zur gelebten Praxis im Unternehmen. Dazu gehört auch: Das Audit und die Zertifizierung sind nicht das Ende, sondern der Beginn eines lebenden Prozesses.

Es gilt also, alle Datenflüsse und implementierten Sicherheitsmaßnahmen fortlaufend und gewissenhaft zu dokumentieren. Dazu gehören auch Firewalls, Verschlüsselungen oder Intrusion-Detection-Systeme. So bleiben IT-Experten nicht nur auf rechtssichere Weise auskunftsfähig in Audits, sondern sichern sich auch das Vertrauen von Kunden und Partnern – mit verlässlicher IT-Sicherheit als Wettbewerbsvorteil. Auch diese kontinuierliche Dokumentation muss heutzutage nicht mehr in „Handarbeit“ geschehen. Automatisierte Monitoring- und Reporting-Tools entlasten IT-Verantwortliche und minimieren das Risiko menschlicher Fehler.

5. Mündige Mitarbeiter als Schlüssel zur Resilienz

Apropos menschliche Fehler: Der Faktor Mensch ist entscheidend für die digitale Souveränität. IT-Verantwortliche sollten deswegen ein Grundverständnis für IT-Sicherheit und Datenschutz in der gesamten Belegschaft verankern. Dazu gehört, Cybergefahren wie Phishing-Angriffe oder Social-Engineering-Methoden frühzeitig zu erkennen und konsequent zu melden. Simulierte Cyberangriffe oder interaktive Schulungen mit realitätsnahen Beispielen helfen bei der Sensibilisierung. Die Multi-Faktor-Authentifizierung (MFA) oder der sichere Umgang mit Passwörtern sollte ein selbstverständlicher Teil der „IT-Hygiene“ sein. Cybersicherheit profitiert von emotionaler Sicherheit, sprich: Mitarbeiter sollten sich sicher genug fühlen, um IT-Probleme oder Sicherheitsvorfälle zeitnah zu melden, ohne aus Angst vor Konsequenzen zu zögern. Das spart wertvolle Zeit bis zur Reaktion auf eine Cybergefahr.

Digitale Souveränität ist daher mehr als ein Schutzschild gegen Risiken – sie ist ein strategischer Vorteil. KMU, die ihre IT-Infrastruktur proaktiv gestalten und stetig weiterentwickeln, wahren ihre Resilienz und die Agilität, um in einem dynamischen Marktumfeld wettbewerbsfähig zu bleiben.

Thierry Kramis.
(Bild: Seabix)

Über den Autor

Thierry Kramis ist Gründer und Head of Seabix ICT Services der Seabix AG . Er verfügt über umfassende Erfahrungen in der Produkte- und Strategiedefinition im Bereich von IT und Telekommunikation. Auf dieser Basis entwickelt der diplomierte Wirtschaftsinformatiker (Universität Zürich, Schweiz) mit der Seabix AG ein Ökosystem aus universell zugänglichen und flexiblen digitalen Geschäftslösungen speziell für den Mittelstand. Der Fokus liegt dabei auf effizienter, tief in die Geschäftsprozesse integrierter Bereitstellung von ICT.

(ID:50284876)