



---

## Application Management Services für KMU

---

## EINLEITUNG

**Viele kleinere und mittlere Unternehmen (KMU), die eigene Softwareanwendungen im Hause selbst entwickeln oder warten, haben häufig mit mehreren Herausforderungen zu kämpfen, die schnell geschäftskritisch werden können.**

Das vielleicht größte Risiko liegt im **Verlust der Handlungsfähigkeit** in Bezug auf die eigenen Geschäftsanwendungen sowie im **Verlust des bestehenden Know-hows**. Ist das IT-Team sehr klein oder wird die Anwendungsentwicklung und -wartung von einzelnen externen Freelancern geleistet, kann ein plötzlicher Wegfall der zuständigen Person – ob krankheitsbedingt oder durch Arbeitgeberwechsel – meist nur unzureichend kompensiert werden. Die Folge: Störungen und Fehler in den Anwendungen lassen sich nur mit starker Verzögerung beheben – oft mit unmittelbaren negativen Auswirkungen auf den laufenden Geschäftsbetrieb. Und selbst mit guter Dokumentation kann es schwierig werden, verlorenes Know-how adäquat und zeitnah zu ersetzen.

Daneben werden **Sicherheitsrisiken** durch mögliche Angriffe aufgrund von Schwachstellen in den Anwendungen immer relevanter. Cyberattacken sind inzwischen sehr professionell geworden und erfolgen unter anderem auch durch die organisierte Kriminalität. Immer häufiger ist das Ziel, Lösegeld zu erpressen, um wieder Zugriff auf die eigenen Daten/Programme zu erhalten. Selbst bei nicht öffentlich im Internet aufrufbaren Geschäftsanwendungen sind Angriffsszenarien bei automatischer Datenverarbeitung, z.B. aus E-Mails oder Dokumenten, denkbar. Ein Angriff kann aber auch aus dem internen Netz erfolgen, wenn es den Cyberkriminellen zuvor gelungen ist, über Schadprogramme, wie beispielsweise einem Trojaner, einzudringen.

Compliance ist ein weiteres Thema mit dem sich zunehmend mehr kleinere und mittelständische Unternehmen befassen müssen. Vor allem im Finanzdienstleistungssektor sind die gesetzlichen und regulatorischen Anforderungen an die IT in den letzten Jahren massiv gestiegen (z.B. mit BaIT, VaIT, DORA). Aber auch andere Branchen sind hiervon nicht ausgenommen. Mit NIS2 (eine Weiterentwicklung der „EU-Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union“) verschärfen sich u.a. die Anforderungen für alle Unternehmen, die einem der wesentlichen Sektoren zugeordnet sind, und dies betrifft nicht nur große Organisationen. Sauber dokumentierte IT-Prozesse, die Sicherstellung ihrer Einhaltung sowie die erforderliche Dokumentation hinsichtlich Security und Qualitätssicherung werden damit zukünftig noch wichtiger.

**Blieben Sie handlungsfähig und behalten Sie die Kontrolle – mit Cegeka als starkem Partner an Ihrer Seite**

Mit **Application Management Services** unterstützt Cegeka kleine und mittlere Unternehmen dabei, diese Herausforderungen zu bewältigen. Wir kümmern uns um Entwicklung, Management und Wartung Ihrer Anwendungen und halten Ihnen den Rücken frei – damit Sie sich ganz auf Ihr Business konzentrieren können.

# Handlungsfähig bleiben und Know-how sichern

## Was ist zu tun?

Um die Handlungsfähigkeit in Bezug auf die eigenen Geschäftsanwendungen langfristig sicherstellen zu können, ist es entscheidend **Skills und Know-how redundant vorzuhalten**. Es wäre nicht das erste Mal, dass ein Unternehmen unter Druck gerät, weil die einzige Person, die die Geschäftsanwendung seit 20 Jahren betreut, in Ruhestand geht und es niemanden mehr gibt, der sich damit ausreichend auskennt. Konkret bedeutet das: Sie benötigen immer mehrere Softwareentwickler/Innen in Ihrem Team, die in der Lage sind, sich bei etwaigen Personalausfällen gegenseitig zu vertreten. Hinzu kommt, dass sich Technologien fortlaufend weiterentwickeln. Eine **kontinuierliche Weiterbildung** des Teams ist daher Pflicht, um mit den Neuerungen Schritt halten zu können. Darüber hinaus gehendes Spezialwissen muss zusätzlich oft über externe Unterstützung ergänzt werden.

Das alles selbst im Haus zu organisieren, erfordert einen hohen Zeitaufwand und dennoch ist die Lösung oft nicht ideal: Teilweise sind die Softwareentwickler/Innen nicht ausgelastet, teilweise fehlen Kapazitäten im Team, um aktuelle Anforderungen aus dem Business kurzfristig umzusetzen. Wird mit wechselnder externer Unterstützung gearbeitet, kommt jeweils noch ein signifikanter Einarbeitungsaufwand hinzu, der die Umsetzung verzögert.

## Unser Angebot

Damit Unternehmen sich über diese Herausforderungen keine Gedanken mehr machen müssen, stellt Cegeka **dedizierte Softwareentwicklungsteams als Team-as-a-Service** bereit. Ein solches Team arbeitet exklusiv für Sie und übernimmt sowohl die laufende Wartung als auch die künftige Weiterentwicklung. Dabei stellen wir sicher, dass Ihre Anwendungen langfristig zukunftsfähig und wartbar sind, indem wir ältere IT-Systeme modernisieren und alle Anwendungen technologisch immer up-to-date halten.

Für die Zusammenstellung des Teams ermitteln wir zunächst gemeinsam mit Ihnen den individuellen Bedarf und prüfen, welche unserer verfügbaren Mitarbeiter/Innen am besten zu Ihrem Unternehmen und Ihren Anforderungen passen. Alle Teams bestehen aus qualifizierten IT-Fachkräften, die **bewährte Standards, agile und DevSecOps-Methoden sowie die Best Practices** von Cegeka aus den Bereichen Security, Tests und Dokumentation anwenden.

Daneben besteht zudem die Möglichkeit, ein Team anteilig für weitere Kundenprojekte einzusetzen, wenn das Team von einem Kunden nur partiell ausgelastet wird. Auch in diesem Fall sorgen wir dafür, dass stets mehrere Teammitglieder mit dem entsprechenden Wissen um Ihre Anwendungen zur Verfügung stehen und die Vertretung sowie Handlungsfähigkeit zu jeder Zeit sichergestellt ist. Alternativ können wir je nach Bedarf zudem die Teamstärke an die Ihnen benötigte Kapazität anpassen.



# Schwachstellen in Anwendungen beseitigen und Sicherheitsrisiken mindern

## Was ist zu tun?

Je digitaler unsere Welt wird, desto mehr nehmen Angriffe durch Cyberkriminelle zu. Kein Unternehmen ist davor gefeit, das Ziel eines solchen Angriffs zu werden. Es ist daher unabdingbar, sich angemessen auf den Ernstfall vorzubereiten und potenzielle Schwachstellen in Ihren Anwendungen zu beseitigen, um möglichst wenig Angriffsfläche zu bieten.

Es gibt verschiedene Wege, wie Sie diese Risiken durch den Einsatz von entsprechenden Tools und Vorgehensweisen mindern können. Eine **statische bzw. dynamische Codeanalyse** analysiert zum Beispiel den eigenen Sourcecode. Das Ziel ist es, die häufigsten Programmierfehler, die zu Sicherheitsrisiken führen, zu vermeiden und einen **gut lesbaren, verständlichen Code** zu gewährleisten (Clean Code).

Im Rahmen der Softwareentwicklung ist es heutzutage üblich, bestehende Open Source-Komponenten bzw. Bibliotheken zu nutzen, da sie helfen, den eigenen Entwicklungsaufwand zu verringern. Durch die verbreitete Nutzung und eine intensive Analyse werden innerhalb von Open Source Bibliotheken immer wieder Schwachstellen gefunden und behoben. Sobald Informationen zu diesen Schwachstellen öffentlich gemacht werden, bietet dies Cyberkriminellen die Möglichkeit für gezielte Angriffe. Jetzt zählt jede Minute. Daher ist es wichtig, dass Sie **schnell reagieren** und dafür sorgen, dass stets die **neuesten, korrigierten Versionen in** den eigenen Anwendungen zum Einsatz kommen.

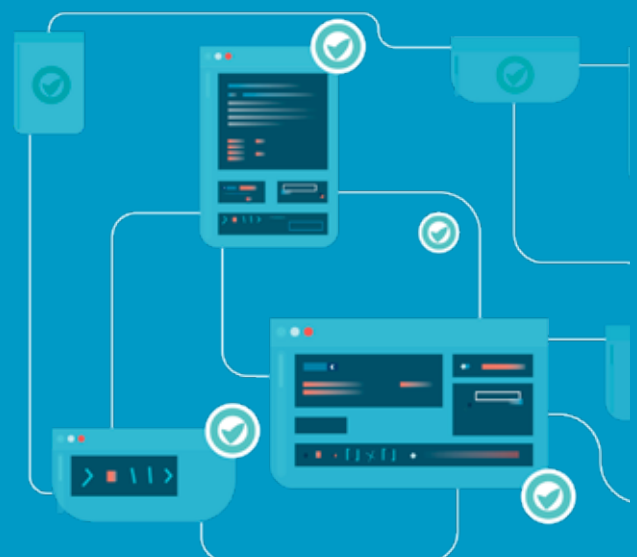
## Unser Angebot

Unsere Entwicklungsteams achten bereits bei der Implementierung darauf, **potenzielle Schwachstellen im Code zu vermeiden (Secure Coding)**, wenden **DevSecOps-Methoden** an und unterstützen Sie beim Aufbau einer **Build-Automatisierung über eine CI/CD Pipeline** (Continuous Integration/ Continuous Delivery). Um die Kosten gering zu halten, greifen wir hierbei häufig auf Open-Source Tools zu.

Einige **Beispiele für Open Source Tools**, mit denen wir in zahlreichen Kundenprojekten bereits sehr gute Erfahrungen gemacht haben, sind

- CI/CD-Pipeline: Jenkins
- Überprüfung des eigenen Source-Codes: SonarQube
- Überprüfung von OpenSource-Komponenten/Bibliotheken: OWASP Dependency-Check
- Überprüfung von Docker Containern: Trivy-, Clair-Scanner
- Überwachung von Lizenzen: OWASP Dependency-Track

Je nach Anforderung unterstützen wir Sie selbstverständlich ebenso bei dem Einsatz weiterer bzw. **kommerzieller Tools**, wie Microsoft DevOps, Github Actions, Bitbucket Pipelines, GitLab etc.



# Gesetzliche und regulatorische Vorschriften umsetzen und einhalten

## Was ist zu tun?

Auch wenn Ihre Prozesse sauber dokumentiert sind und es entsprechende Anweisungen an die handelnden Personen gibt, ist damit leider noch nicht zwangsläufig sichergestellt, dass diese Prozesse tatsächlich eingehalten werden. Insbesondere, wenn es mal schnell gehen muss und manuelle Prozesse länger dauern oder umständlich sind, kann es in der Softwareentwicklung passieren, dass z.B. Anwendungen aus der Entwicklungsumgebung ohne ausreichende Tests direkt produktiv eingesetzt werden.

Ein weiteres Thema ist, sicherzustellen, dass nur **Open Source-Komponenten mit passenden Lizenzen** genutzt werden. Nur weil eine Komponente öffentlich verfügbar ist, heißt das noch lange nicht, dass sie auch kommerziell im Rahmen eigener Lösungen verwendet werden darf. Im Open Source-Umfeld gibt es eine Vielzahl von Lizenzmodellen, die unterschiedlichste Rechte einräumen (z.B. von LGPL = freie Verwendung über GPL zu AGPL = freie Verwendung, aber mit Quelloffenheit des Codes) und nicht jeder Entwickler und jede Entwicklerin ist sich dessen immer bewusst.

Um zu **gewährleisten, dass die definierten Prozesse eingehalten werden**, sollten Sie entsprechende Vorkehrungen treffen:

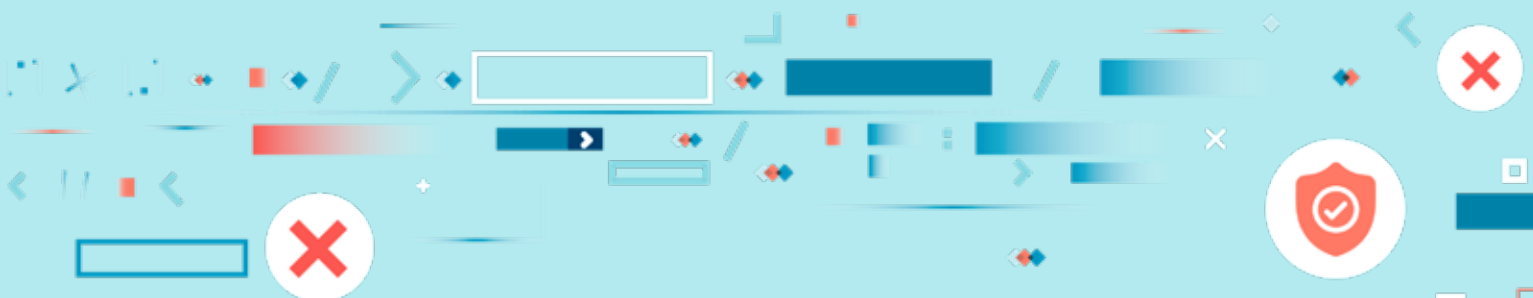
- Eine strikte Trennung der Entwicklungs-/Testumgebung von der Produktivumgebung
- Keine manuellen Eingriffe bei der Installation zulassen (ausschließlich über die CI/CD Pipeline).

- Durch die Automatisierung Ihrer Prozesse über eine CI/CD Pipeline können Sie des Weiteren sicherstellen, dass diese nun deutlich schneller sind und somit keine Abkürzungen nötig sind.
- Ablage der Ergebnisse aus dem automatischen Build zur Dokumentation
- Automatisierte Testfälle
- Security Scans
- Automatisierte Überprüfung ob alle Lizenzen zum Einsatzszenario passen.

Eine Automatisierung Ihrer Build-/Deployment-Prozesse bietet Ihnen aber noch weitere Vorteile. Durch die **Vermeidung manueller Schritte** werden Ihre Prozesse auf Dauer **weniger fehleranfällig** und **schneller**, was Kosten spart.

## Unser Angebot

Wir beraten Sie, wie Sie die gesetzlichen und regulatorischen Anforderungen technisch am besten umsetzen können. Zudem unterstützen Sie bei der Anpassung oder Erweiterung Ihrer bestehenden Infrastruktur sowie dem Aufbau einer zusätzlichen getrennten Entwicklungs-/Testumgebung. Mit Umsetzung einer Build-Automatisierung, sorgen wir für die **Rückverfolgbarkeit Ihrer Prozesse**: Sämtliche Ergebnisse der einzelnen Schritte werden für eine **saubere und vollständige Dokumentation** automatisch abgelegt und archiviert.



# Unsere Application Management Services im Überblick:



## ASSESSMENT

Analyse Ihrer Ist-Situation & Anforderungen  
Handlungsempfehlungen zur Verbesserung



## BEREITSTELLUNG EINES DEDIZIERTEN SOFTWAREENTWICKLUNGSTEAM

(Team-as-a-Service)



### Weiterentwicklung, Wartung & Betrieb Ihrer Anwendungen

Wir sorgen dafür, dass Ihre Anwendungen reibungslos laufen und den Anforderungen Ihres Business entsprechen.



- **Kontinuität und Stabilität**
- **Sie behalten die Kontrolle über Ihr Projekt**
- **Planungssicherheit**
- **Skalierbarkeit**



### Automatisierung Ihrer Build- und Deployment-Prozesse

Wir automatisieren Ihre Prozesse, um Fehlerquellen auszuräumen und qualitativ hochwertige Software bereitzustellen.



- **Sicherheit**
- **Qualität**
- **Geschwindigkeit**
- **Kostensenkung**



### Richtlinien & Dokumentation zur Professionalisierung Ihres Entwicklungsprozesses

Wir nutzen bewährte Standards, agile sowie DevSecOps-Methoden und stellen eine vollständige, saubere Dokumentation sicher.



- **Sicherheit**
- **Rückverfolgbarkeit**
- **Compliance**

---

Konzentrieren Sie sich ganz darauf, worin Sie gut sind – Ihr Business. Lassen Sie Ihre Anwendungen unsere Sorge sein. Wir kümmern uns darum, dass Ihre IT reibungslos läuft, sicher und state-of-the-art ist.

**Sie haben Fragen zu unserem Angebot und möchten mehr erfahren?**

Vereinbaren Sie jetzt unverbindlich einen (Online-)Termin für ein persönliches Gespräch mit unseren Experten. Senden Sie uns einfach eine E-Mail mit Ihrem Terminwunsch an [de.contact@cegeka.com](mailto:de.contact@cegeka.com)

**Mehr über unsere Application Management Services unter**

**[WWW.CEGEKA.COM/DE-DE/SOLUTIONS/APPLICATIONS/  
APPLICATION-MANAGEMENT-SERVICES](http://WWW.CEGEKA.COM/DE-DE/SOLUTIONS/APPLICATIONS/APPLICATION-MANAGEMENT-SERVICES)**