valantic

DORA & TLPT

Digitale Resilienz durch Threat-Intelligence-Analysen und simulierte Cyberangriffe

So erfüllen Finanzinstitute die Anforderungen des Digital Operational Resilience Act (DORA)

Inhalt

Mit DORA (Digital Operational Resilience Act) zielt die EU darauf ab, einen universellen Rahmen für das Management und die Minderung von ICT-Risiken im kritischen Finanzsektor zu etablieren. Durch die Harmonisierung der Risikomanagementregeln in der gesamten EU verfolgt DORA das Ziel, die Lücken, Überlappungen und Konflikte zu beseitigen, die zwischen unterschiedlichen Vorschriften in verschiedenen EU-Staaten entstehen könnten. Wichtig: Für sicherheitskritische Unternehmen in Deutschland und Europa sind die DORA-Direktiven obligatorisch.

Thomas Lang

thomas.lang@mc.valantic.com

Nach über 20 Jahren als Berater und Unternehmer ist für Thomas Lang das schnelle Einarbeiten auch in kritische Situationen in „Fleisch und Blut" übergegangen. Er bewahrt in jeder Lage Ruhe, kann Wichtiges von Unwichtigem trennen und gibt Dingen Struktur. Das hilft ihm, um in schwierigen Situationen den Überblick zu bewahren. Zu seinen Beratungsschwerpunkten gehören neben den Themen Cybersicherheit & Compliance unter anderem die Themen IT-Strategie, Projekt-Governance und -Controlling, Krisenmanagement sowie IT-Infrastruktur & Betrieb.

DORA ist verpflichtend, ansonsten drohen Bußgelder

Für Unternehmen folgt daraus: DORA ist seit dem 17. Januar 2025 verpflichtend und gilt für alle Finanzinstitutionen in der EU.

> Das umfasst traditionelle Finanzakteure wie Banken, Investmentfirmen und Kreditinstitute sowie nicht-traditionelle Akteure, einschließlich Anbietern von Krypto-Asset-Dienstleistungen und Crowdfunding-Plattformen. Alle Vorgaben von DORA sind vollständig einzuhalten.

Und Vorsicht: Führende Aufsichtsstellen können Bußgelder von bis zu einem Prozent des durchschnittlichen weltweiten Tagesumsatzes des Anbieters im vorangegangenen Geschäftsjahr verhängen. Diese Strafen können täglich bis zu sechs Monate lang fortgesetzt werden.

Darüber hinaus sieht DORA vor, dass Mitglieder des Managements bei grober Fahrlässigkeit oder vorsätzlichen Verstößen persönlich haftbar gemacht werden können.

Cybersicherheit: Allianz Risk Barometer 2025 und Bitkom

Der Grund für die verschärften Sicherheitsanforderungen: Cybervorfälle wie Ransomware-Angriffe, Datenschutzverletzungen und IT-Ausfälle rangieren zum Beispiel im Allianz Risk Barometer (2025) an erster Stelle der globalen Risiken – und das zum wiederholten Male. Konkret heißt das:

- **Cyberangriffe bedrohen die Existenz ganzer Unternehmen**, zum Beispiel kommt die Produktion zum Stillstand, Lieferungen, Zahlungen oder der Zugriff auf eigene Systeme oder Daten sind nicht mehr möglich
- Neben den finanziellen Auswirkungen entsteht zudem Schaden durch die **Veröffentlichung interner Daten, geistigem Eigentum, Geschäftsgeheimnissen von Partnern**, vertraulichen **Daten natürlicher Personen** usw.

In Unternehmen herrscht oft die Meinung: Uns trifft es schon nicht. Aber angegriffene Unternehmen sind keine Einzelfälle. Der Digitalverband Bitkom führt jährlich eine für die Gesamtwirtschaft repräsentative Studie durch, die im Jahr 2024 zu folgenden Ergebnissen kam:

- 8 von 10 Unternehmen sind von Datendiebstahl, Spionage oder Sabotage betroffen
- Insgesamt entsteht ein jährlicher Schaden von 267 Mrd. EUR.
- 31% der betroffenen Unternehmen berichten von Schäden durch Ransomware
- Zwei Drittel der Unternehmen fühlen sich in ihrer Existenz bedroht

Die aktuellen Risiko-trends für Finanzins-titute

Zuerst die gute Nachricht. Weniger relevant sind nach den Analysen von valantic derzeit Advanced Persistent Threats (APTs) – also staatlich-kontrollierte Akteure. Diese Analyse ist jedoch stark abhängig von geopolitischen Entwicklungen und kann sich schnell ändern.

Ransomware führt seit Jahren kontinuierlich die Liste der Top-Bedrohungen für die meisten Unternehmen in Deutschland an. Auch Finanzunternehmen werden immer wieder Opfer von Erpresser-Software, die Daten stiehlt, verschlüsselt und erst nach Zahlung eines Lösegeldes wieder freigibt. So wurde beispielsweise 2023 die Deutsche Leasing, ein Partner der Kreissparkasse Köln, Opfer der Ransomware-Gruppe BlackBasta.

Hacktivismus, insbesondere durch DDoS-Angriffe, ist mittlerweile Teil des Alltags für die deutsche Finanzindustrie und wird dies nach Einschätzung der Sicherheitsexpert*innen von valantic auch vorerst bleiben. DDoS-Angriffe dauern in der Regel nur kurz an und verursachen kaum langfristige Schäden.

Die Verflechtungen des Finanzsektors – gerade bei den Sparkassen – erhöht außerdem das Risiko von Supply-Chain-Vorfällen durch die Kompromittierung von Dienstleistern und Geschäftspartnern. Gerade durch die hohe regulatorische Absicherung des Finanzsektors versuchen Bedrohungsakteure zunehmend, Organisationen über Partnerunternehmen zu kompromittieren.

Diese Angriffsmuster bedrohen zurzeit die Finanzindustrie

Besonders auffällig für den Finanzsektor ist **Social Engineering**, eine Technik, bei der Cyberkriminelle gezielt menschliche Schwächen ausnutzen, um an **vertrauliche Informationen zu gelangen, Systeme zu kompromittieren** oder **Personen zu bestimmten Handlungen zu bewegen**. Dabei manipulieren sie das Vertrauen, die Hilfsbereitschaft oder die Unachtsamkeit ihrer Opfer durch **Täuschung und psychologische Tricks**.

Auch der Einsatz von **Stealer Malware** erfährt eine **zunehmende Relevanz** für das gesamte cyberkriminelle Ökosystem einschließlich Ransomware- und APT-Gruppen. Der Kauf von Zugangsdaten bietet in der Regel einen **einfacheren Zugang zu Unternehmensnetzwerke** als eine Erforschung und Ausnutzung einer technischen Schwachstelle. Angriffe auf Banking-Zugänge bieten nach der Kompromittierung der Konten durch Angreifer insbesondere über simple Überweisungen eine besonders attraktive Angriffsfläche.

In den meisten Fällen nutzen geopolitisch motivierte Angreifergruppen **(D)DoS-Attacken**, um Webseiten und Dienste im Finanzsektor für eine kurze Zeit lahmzulegen.

Unmittelbare potenzielle Folgen von (D)DoS-Angriffen sind **Dienstunterbrechungen**. Eine Überlastung der Server führt womöglich dazu, dass Online-Dienste der Bank, wie **Internetbanking, mobile Apps und Kundensupport, gar nicht mehr erreichbar sind**.

Vertrauensverlust:

Kunden sind insbesondere betroffen, da sie keinen Zugriff auf ihre Konten haben und keine Transaktionen durchführen können, was zu Frustration und Vertrauensverlust führen kann.

Absoluter Stillstand wichtiger Prozesse:

Je nach Intensität und Schutz können wichtige Geschäftsprozesse gestört werden, darunter Transaktionen, die Abwicklung von Zahlungen und das Kundeneinlagegeschäft, was zu einem direkten finanziellen Verlust führen kann.

HANDLUNGSEMPFEHLUNGEN

So verbessern Sie Ihren Schutz

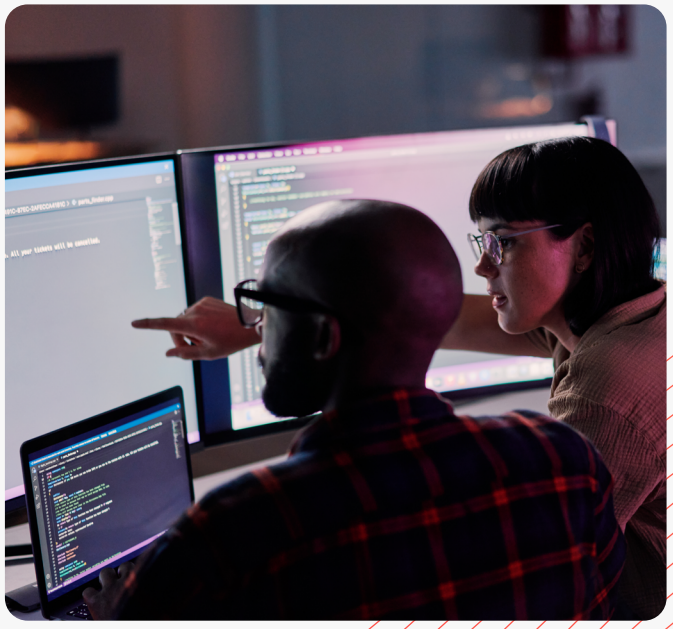
Bedrohung: Social Engineering

Sensibilisierungsschulungen: Regelmäßige Schulungen für Mitarbeiter zur Erkennung und Abwehr von Social-Engineering-Versuchen.

Verifizierungsprozesse: Implementierung von Verfahren, die wichtige Transaktionen und Änderungen durch mehrfache Bestätigung absichern.

Zero-Trust-Prinzip: Minimierung von Vertrauen intern und extern, sowie Begrenzung der Zugriffsrechte auf das Notwendigste.

Threat Intelligence: Kontinuierliche Beschaffung von Informationen zu aktuellen Trends und Angreifergruppen, um drohenden Gefahren einen Schritt voraus zu sein.



Bedrohung: Stealer Malware

Endpoint-Sicherheit: Einsatz von Anti-Malware und Anti-Viren-Software mit Echtzeitschutz und automatischer Erkennung.

Zwei-Faktor-Authentifizierung (2FA): Einführung von 2FA für alle Mitarbeiter und Kunden zur Sicherung von Zugangsdaten.

Darknet Monitoring: Alarmierung bei zum Verkauf angebotenen (Zugangs-)Daten in einschlägigen Darknet-Foren, -Marktplätzen oder in Telegram-Kanälen

Bedrohung: DDoS-Angriffe

DDoS-Abwehrdienste: Einsatz von Cloud-basierten Lösungen zur Filterung und Abwehr von DDoS-Datenverkehr.

Netzwerksegmentierung: Isolierung kritischer Systeme, um die Auswirkungen eines Angriffs zu minimieren.

Last- und Stresstests: Durchführung regelmäßiger Last- und Belastungstests zur Prüfung der Infrastrukturstabilität.

SIMULIERTE CYBERANGRIFFE

Threat-led Penetration Tests (TLPT)

Um resilient zu werden und zu bleiben, empfiehlt DORA unter anderem, systemische technologische Risiken über **TLPT (Threat-led Penetration Testing)**, also simulierte, auf die jeweilige Organisation individuell angepasste Cyberangriffe, zu bewerten. Für besonders kritische Unternehmen im Finanzbereich sind TLPTs von der BaFin und der Deutschen Bundesbank alle drei Jahre zwingend vorgeschrieben und die betroffenen Unternehmen sind dazu aufgerufen, sich selbst um zertifizierte und qualifizierte externe Dienstleister zu kümmern.

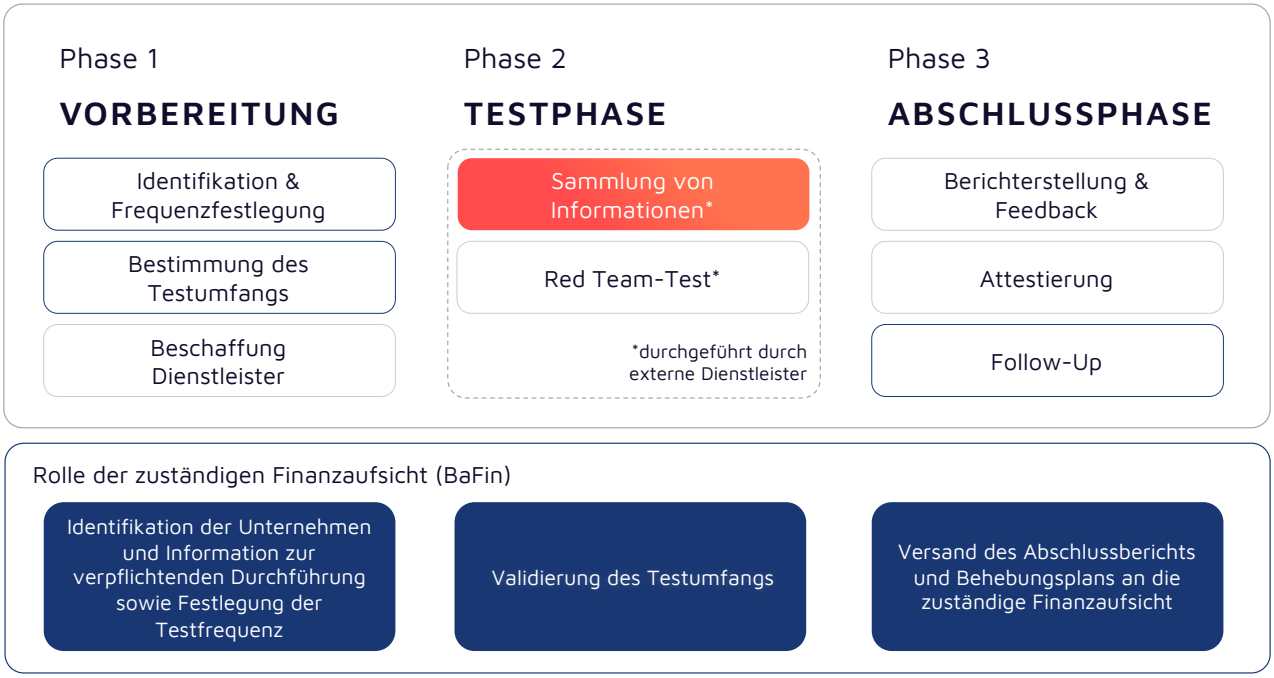
Eine gute Vorbereitung zum Beispiel mit Unterstützung eines erfahrenen Cybersecurity-Dienstleisters ist dabei erfolgsentscheidend und die Zeit drängt. Die Messlatte wird von der BaFin und der Deutschen Bundesbank hoch aufgehängt: Externe Dienstleister müssen mit Threat Intelligence- und Täterprofilen, Bedrohungsanalysen und Open-Source-Erfahrung haben und darüber hinaus unabhängig sein. Diese Qualifikationen müssen, inklusive entsprechender Referenzen, alle nachgewiesen werden. Das Controlling-Team wird von der BaFin gestellt. Das Ziel besteht darin, einen individualisierten Targeted Threat Intelligence Report aufzustellen.

Die Akteure, die für bedrohungsgesteuerten Penetrationstests gemäß Artikel 26 Absatz 11 der DORA benötigt werden, im Überblick

- **TLPT Cyber Team (TCT)**: das Personal innerhalb der TLPT-Behörde, das den TLPT-Betrieb überwacht.
- **Kontrollteam**: Verwaltet den TLPT des Finanzunternehmens und kümmert sich um die Beschaffung, die Risikobewertung und das Betriebsmanagement unter Wahrung der Vertraulichkeit der Tests.
- **Blue Team Verteidiger**: Das Verteidigungsteam, das versucht, simulierte oder reale Cyberbedrohungen abzuwehren.
- **Threat Intelligence Provider**: Ein externer Dienstleister, der das Sammeln von Informationen durch Hacker anhand zuverlässiger Quellen simuliert.
- **Red Team Angreifer**: Tritt entweder als interner oder als externer Dienstleister an und fungiert als angreifendes Team.

So laufen Pentests ab: Planung, Test- und Abschlussphase

Die einzelnen Phasen eines obligatorisch von DORA vorgeschriebenen Threat-led Penetrationtests im Überblick, von der Planung bis zur Auswertung der Ergebnisse und der Lessons learnt:



Quelle: valantic – Darstellung nach Bundesbank und BaFin

Die Pentests simulieren auf Basis eines vorab erstellten Risikoprofils einen Cyberangriff durch das Red Team, werten die Ergebnisse aus und schließen danach die durch den Test herausgefundenen Lücken und Sicherheitsdefizite. Sie erhöhen dadurch deutlich die Resilienz des Unternehmens.

Denken wie ein Cyberkrimineller

Penetrationstests selbst, also der eigentliche Angriff, läuft vereinfacht nach einem genauen „Plan" ab, den nicht nur Pen-Tester, sondern auch Cyberkriminelle so verfolgen.

1 Erkundung

Sammeln wichtiger Informationen über ein Zielsystem, um das betroffene Unternehmen besser angreifen zu können. Ziel könnte zum Beispiel sein, Informationen ausfindig zu machen, die für einen Social-Engineering-Angriff verwendet werden können.

2 Scannen

Verwendet technische Tools, um das Wissen des Angreifers über das System zu erweitern. Zum Beispiel dient der Sicherheitsscanner Nmap dazu, nach offenen Ports zu scannen.

3 Zugang erlangen

Mithilfe der in der Erkundungs- und Scanphase gesammelten Daten kann der Angreifer in das System eindringen und Teile unter seine Kontrolle bringen. Die Penetration-Testing-Plattform Metasploit kann beispielsweise verwendet werden, um Angriffe auf bekannte Schwachstellen wie offene, ungeschützte Ports zu automatisieren.

4 Aufrechterhaltung des Zugangs

Die Aufrechterhaltung und Verschleierung des Zugriffs ist wichtig, um sich dauerhaft in der Zielumgebung aufhalten und so viele Daten wie möglich sammeln zu können. In der Vergangenheit waren Zielsysteme monate- oder sogar jahrelang kompromittiert, ohne dass das Opfer, also das angegriffene Unternehmen, davon wusste.

5 Spuren verwischen

Der Angreifer beseitigt alle Spuren und alle Arten von gesammelten Daten und Protokollereignisse, um anonym zu bleiben.

Den Cyberkriminellen einen Schritt voraus sein

Viele Cyberattacken passieren in der Regel nicht aus heiterem Himmel, sondern sozusagen mit Ansage. Denn Cyberkriminelle sind mittlerweile wie Unternehmen organisiert und wirtschaften arbeitsteilig. Das „Geschäft" hat sich zunehmend kommerzialisiert. Insbesondere in der ersten Erkundungsphase (siehe oben: Denken wie ein Cyberkrimineller) machen sich Cyberkriminelle, die einen Angriff planen, in Foren und Marktplätzen auf die Suche nach Informationen, Passwörtern, Zugangsdaten und Leaks, die bereits erbeutet und nun weiterverkauft werden.

Denn etwa 95% des Internets sind „verborgen". Dieses sogenannte **Deepweb** umfasst Inhalte, die nicht von herkömmlichen Suchmaschinen indexiert werden. Darunter fallen **sensible** oder **vertrauliche** Informationen, die nicht öffentlich zugänglich sind. Das **Darkweb** beherbergt **Foren, Marktplätze** und **Communities**, wo wertvolle, kritische Daten gehandelt werden, die für einen Cyberangriff nützlich sind.

Um den Cyberangreifern einen Schritt voraus zu sein, bietet valantic einen Darknet-Monitoring-Service an. Werden zum Beispiel sensible Zugangsinformationen des Unternehmens xy im Darknet zum Verkauf angeboten, dann ist damit zu rechnen, dass in nächster Zeit ein Angriff auf das betroffene Unternehmen erfolgt. Aus Gründen der Cybersicherheit, primär im Bereich der **Threat Intelligence**, sind Blicke ins Dark- und Deepweb daher **unumgänglich**.

Das Sicherheitspaket von valantic

Professionell durchgeführte Threat-led Penetrationstests bieten echte, datenbasierte Erkenntnisse und identifizieren technologische und organisatorische Schwachstellen, von denen Ihr Unternehmen bislang noch nichts wusste. Die Testresultate geben wertvolle Insights und helfen Ihnen dabei, Ihr Unternehmen sicherer und resilienter gegen Cyberangriffe zu machen.

Valantic als erfahrener, externer Threat Intelligence Provider unterstützt Sie entlang des gesamten TLPT-Prozesses. Damit vermeiden Sie unangenehme Überraschungen, wenn die Ergebnisse der obligatorischen Tests an die Bundesbank gemeldet werden.

Jede Industrie hat eigene Besonderheiten. Wir analysieren Branchen und leiten ggfs. vorhandene besondere Angriffsrisiken, Vorgehensmuster oder erkennbare Bedrohungen ab und berücksichtigen diese in unseren Analysen. Höchste Qualitätsansprüche sind nur durch Experten erreichbar. In unserem Team kommen ehemalige Hacker, SOC-Spezialisten, Admins, Berater, Ermittler uvm. zusammen.

Unser Lösungsangebot geht weit über TLPTs hinaus: Mit regelmäßigen Bedrohungsanalysen und Echtzeit-Monitoring halten wir Ihre Sicherheitsmaßnahmen stets auf dem neuesten Stand und unterstützen Sie proaktiv bei der Identifikation und Schließung von Sicherheitslücken. Durch kontinuierliches Monitoring sind unsere Kunden jederzeit optimal auf TLPTs vorbereitet – ohne böse Überraschungen.

valantic

Über uns

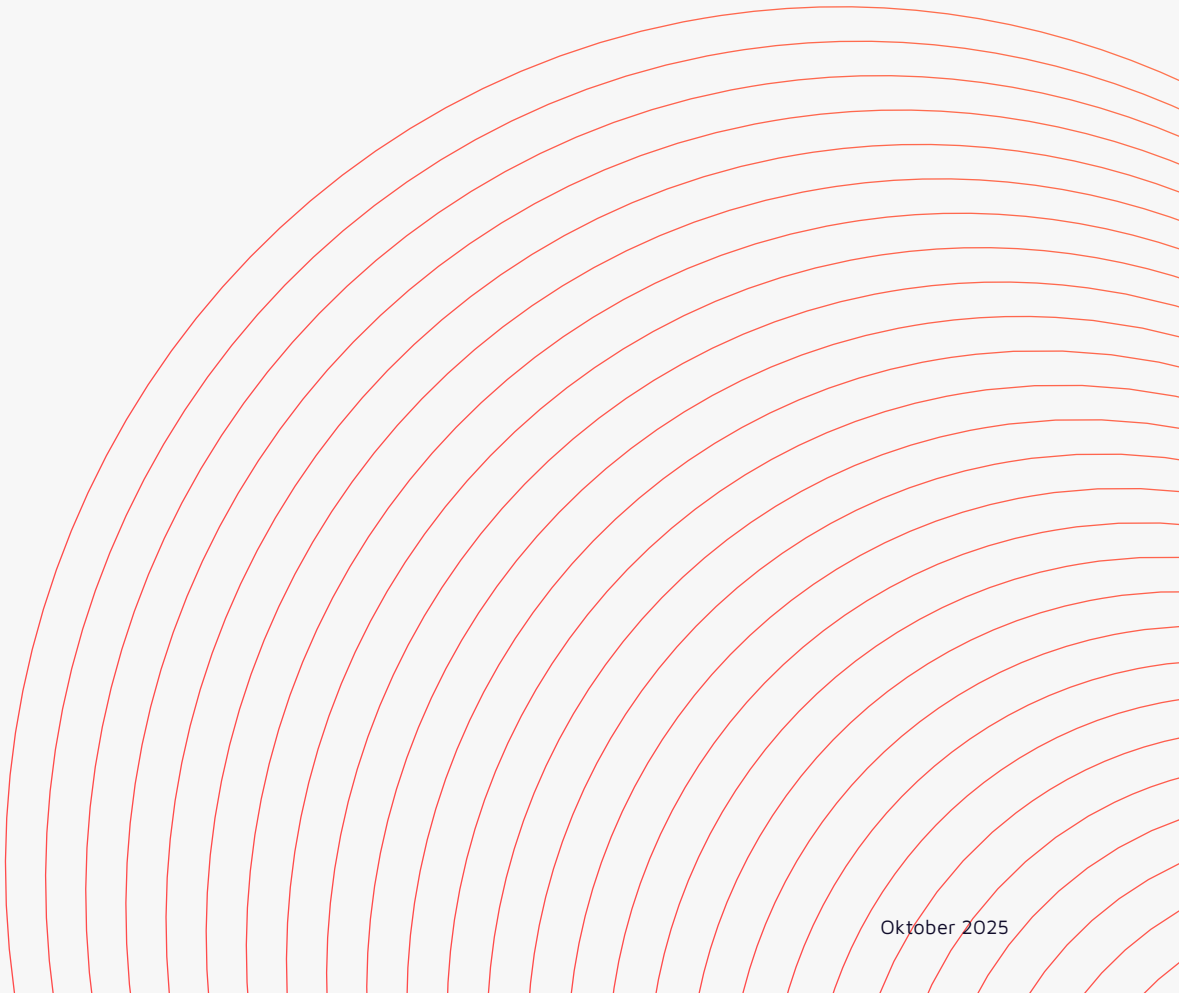
valantic zählt zu den am schnellsten wachsenden Digital Consulting-, Solutions- und Software-Gesellschaften am Markt. Über 500 Blue-Chip-Kunden vertrauen bereits auf valantic – davon 33 von 40 DAX-Konzernen sowie eine Vielzahl internationaler Marktführer. Mit mehr als 4.000 Digitalisierungs-Expertinnen und -Experten ist valantic in 18 Ländern weltweit vertreten.

Etwa 2.000 erfolgreiche Digitalisierungsprojekte in den letzten fünf Jahren haben gezeigt, dass die Expertinnen und Experten von valantic die Herausforderungen ihrer Kunden genaustens verstehen. Von der Strategie bis zur handfesten Umsetzung verfügen diese über die notwendige Expertise, Projekte von Anfang bis Ende zu begleiten und erfolgreich zu machen. Dabei verbinden sie technologische Kompetenz mit Branchenkenntnis und Menschlichkeit.

valantic berät Unternehmen zu allen Herausforderungen der Digitalen Transformation, hilft diesen, ihre Corporate Performance besser zu managen und die Potenziale von Daten und Künstlicher Intelligenz zu heben. Darüber hinaus unterstützt valantic seine Kunden dabei, die Customer Experience optimal zu gestalten, Kerntechnologien der Digitalisierung gewinnbringend einzusetzen und Unternehmensprozesse durchgängig zu optimieren.

valantic
Management Consulting GmbH
Dreieich Plaza 2A
63303 Dreieich
Deutschland
Telefon +49 6103 50 86 0
Mail info@mc.valantic.com

www.valantic.com



Oktober 2025