

- /Administration
- /Human Resources
- /Legal
- /Accounting
- /Finance
- /Marketing
- /Publicity
- /Promotion
- /Research
- /Business
- /Development
- /Engineering
- /Manufacturing
- /Planning

DIGITAL Trust.
Mastering business security


Computacenter

DIGITAL TRUST

Vertrauen in die IT ist Voraussetzung
für Digitalisierung

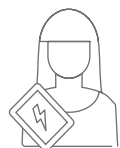
DIE ROLLE DER IT-SECURITY IM DIGITALEN ZEITALTER

Bots, die Zehntausende von IoT-Geräten befallen, Kundendaten, die auf dem Schwarzmarkt gehandelt werden, manipulierte Steuergeräte in der Produktion – fast täglich dringen neue Cyberattacken an die Öffentlichkeit. Laut einer Studie des Digitalverbands Bitkom wurden in den vergangenen zwei Jahren mehr als die Hälfte aller Unternehmen in Deutschland Opfer von Wirtschaftsspionage, Sabotage oder Datendiebstahl. Die cyberkriminelle Bedrohung ist omnipräsent und eine sichere IT wird geschäftskritisch.

DIE HERAUSFORDERUNGEN SIND KOMPLEX:



Cyberkriminelle arbeiten heute hochprofessionell. Sie sind finanziell und technologisch bestens ausgestattet und bereiten ihre Angriffe von langer Hand vor, um sich über Monate in Unternehmensnetze einzunisten und sensible Daten abfischen zu können.



Die digitale Angriffsfläche der Unternehmen vergrößert sich durch die zunehmende Vernetzung und den Einsatz neuer Technologien. Alle Firmen, die es ihren Mitarbeitern beispielsweise ermöglichen, unterwegs oder im Homeoffice mobil zu arbeiten oder ihre Produktion im Sinne von Industrie 4.0 digital vernetzen, schaffen damit eine Vielzahl neuer Einfallstore für Cyberkriminelle.



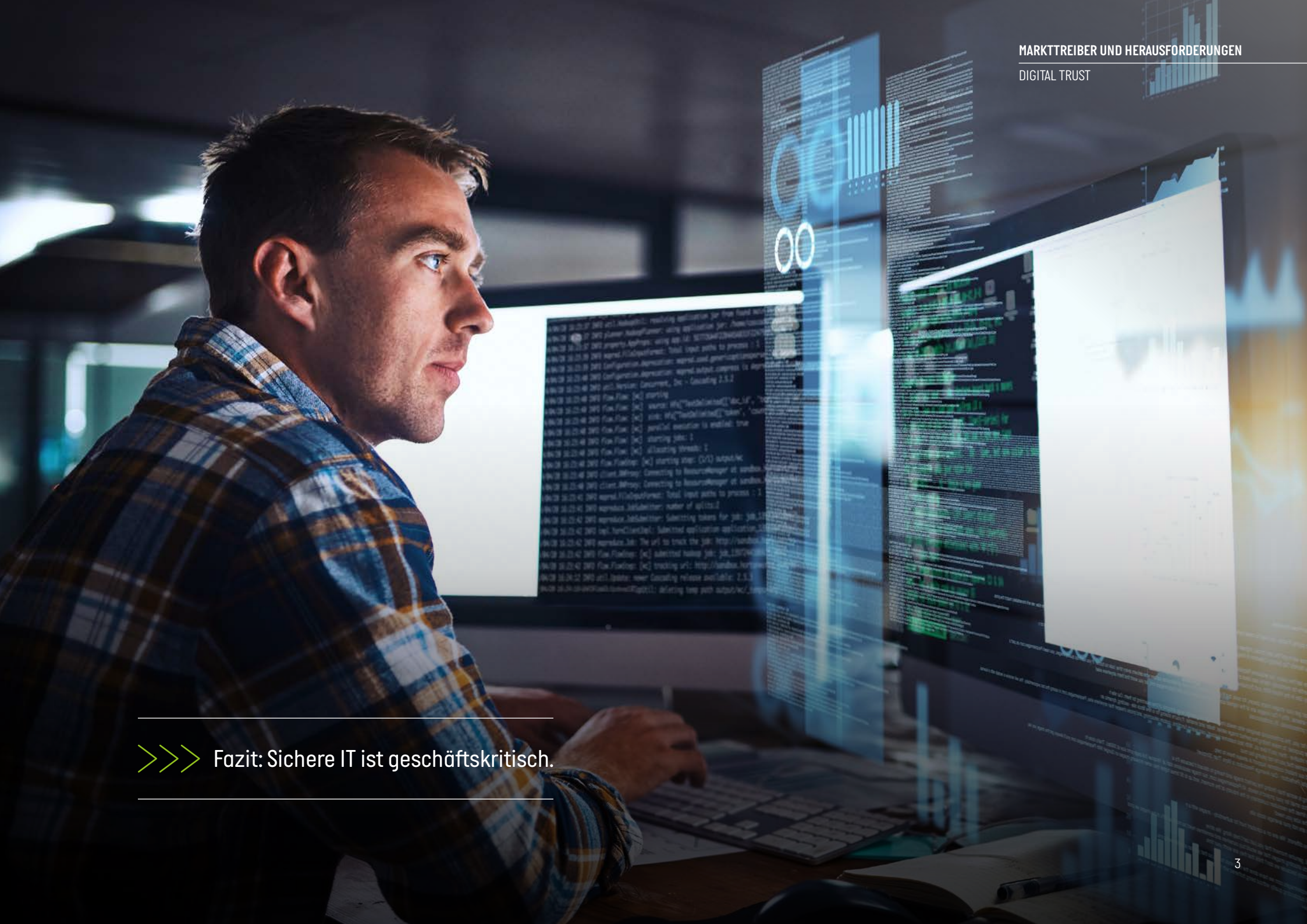
Dennoch versäumen es die meisten, im gleichen Zuge ihre Cyberabwehr aufzurüsten – was nicht nur den Nutzen der neuen Technologien erheblich schmälert, sondern sich im Fall eines Cyberangriffs auch negativ auf Image, Umsatz und Wettbewerbsfähigkeit auswirken kann.



Hinzu kommt, dass allen Unternehmen Cyber-Security-Experten fehlen, die zum Beispiel aus kleinsten Anomalien die ersten Anzeichen eines Hackerangriffs herauslesen und die vorhandenen Sicherheitslösungen optimal einsetzen können.



Und als wäre das noch nicht genug, stellen die Compliance-Vorschriften der neuen EU-Datenschutzgrundverordnung – kurz DSGVO oder GDPR – alle Unternehmen vor zusätzliche Herausforderungen in puncto Datensicherheit.



➤➤➤ Fazit: Sichere IT ist geschäftskritisch.

VERTRAUEN SCHAFFEN

VON DER DIGITALISIERUNG PROFITIEREN – OHNE NEBENWIRKUNGEN

Wer sich der aktuellen Bedrohungslage bewusst ist, könnte den Eindruck gewinnen: Digitalisierung ist brandgefährlich für mein Unternehmen. Ist sie aber eben nicht – vorausgesetzt, man setzt auf wirksame Schutzkonzepte und vertrauenswürdige Partner wie Computacenter. Denn nur auf der Basis sicherer Prozesse können Unternehmen von innovativen Trends profitieren – von mobilem Arbeiten über Cloud Computing und Big Data bis zu Industrie 4.0 und Internet of Things.

Unser Ziel ist, neue Technologien ohne Nebenwirkungen nutzbar zu machen. Daher begreifen wir IT-Security nicht als notwendiges Übel oder Hürde, die den Fortschritt blockiert und Skepsis vor neuen Technologien säht – ganz im Gegenteil.

Unsere Security-Lösungen schaffen Vertrauen: in die eigene IT, in die eigene Innovationsfähigkeit, in die eigenen Mitarbeiter und ihre Produktivität.

Ganz gleich, ob Fachkräftemangel, sorglose Mitarbeiter oder ein undurchdringlicher Compliance-Dschungel, der mit GDPR noch dichter ist als je zuvor. Als Europas bevorzugter Secure IT-Provider vereinen wir die Expertise für alle IT-Bereiche, um unsere Kunden bei diesen Herausforderungen zu unterstützen. Vom schlagkräftigen Cyber Defence Center bis zu jedem einzelnen Endpoint, für die Office- genauso wie für Produktions-IT.



„ONE-STOP-SHOP“ IT-SECURITY AUS EINEM GUSS

Warum können wir IT-Infrastrukturen bestmöglich absichern? Weil wir sie von A bis Z verstehen.

Computacenter verfügt über eines der umfangreichsten IT-Security-Portfolios am Markt, denkt das Thema in jedem Kundenprojekt mit und integriert Security-Lösungen immer nahtlos in die bestehende IT-Landschaft. Dadurch können wir Unternehmen und Behörden optimal dabei unterstützen, trotz verschärfter Bedrohungslage ihr Business abzusichern und das Vertrauen ihrer Kunden und Partner sicherzustellen. Dafür bringen wir in unserem Portfolio alle Komponenten digitaler Geschäftsstrategien und -modelle zusammen: den auf jeden einzelnen Mitarbeiter zugeschnittenen digitalen Arbeits-

platz (Digital Me), IT-Services aus Multi- und Hybrid-Clouds (Digital Power) – und über alle Bereiche hinweg das Sicherheitsnetz unseres umfanglichen, nahtlos integrierten IT-Security-Lösungsangebots: **DIGITAL TRUST.**

Das macht uns zu Ihrem „One-Stop-Shop“ für eine sichere IT. Sie erhalten alle Services und Lösungen aus einer Hand und müssen keine zusätzlichen Leistungen von Dritten kaufen. Selbstverständlich gewährleisten wir als Secure IT-Provider bei allem, was wir tun, dass die Security-Anforderungen auch bei unseren eigenen Services erfüllt sind. Mit unserem Information Security Management und Cyber Defence Center sichern wir uns und unsere Managed Services ab.

#MAKINGDIGITALWORK

DIGITAL
Cloud accelerating business
Power.

DIGITAL
Mastering business security
Trust.

DIGITAL
IT designed for people
me.



DIGITAL TRUST

CYBERSICHERHEIT SCHAFFT DIGITALES VERTRAUEN

Digitale und mobile Arbeitsweisen sind gang und gäbe: Mitarbeiter arbeiten von zuhause und loggen sich von unterwegs ins Firmennetz ein. Sie tauschen Dokumente über Cloud-Dienste aus, organisieren sich mithilfe von Apps und kommunizieren via Social Media. All diese in den vergangenen Jahren neu entstandenen Angriffspunkte müssen gegen Cyberattacken abgesichert werden – genauso wie die, die noch kommen werden. Denn spätestens dann, wenn Roboter und Autos autonom agieren, kommt der IT-Security auch eine Safety-Funktion zu und sie muss Leib und Leben schützen. Dabei muss klar sein: Hundertprozentig sicher vor Cyberangriffen ist heute (und morgen) kein Unternehmen mehr.

Auch der Austausch mit anderen Unternehmen wird im digitalen Industriezeitalter intensiver. Zulieferer, Partner und Kunden vernetzen sich – was neben allen Vorteilen auch das wachsende Risiko birgt, Opfer eines Cyberangriffs zu werden, sobald ein Akteur in der Wertschöpfungskette angegriffen wurde. Daher sind heute Cyber-Security-Lösungen essenziell, die wie unser umfassendes Portfolio bei allen vernetzten Parteien für Sicherheit und Vertrauen sorgen.

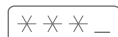
Das Beste, was wir tun können, ist es den Angreifern so schwer wie möglich zu machen, sich unerkannt in Unternehmensnetzen auszubreiten und dort einzunisten. Das erreichen wir mit Security-Frameworks, die präventive mit detektiven und reaktiven Lösungen vereinen. Wichtig dabei:

Security-Lösungen dürfen nicht einfach „oben drauf gepackt“, sondern müssen direkt und nahtlos in alle Anwendungen und Systeme integriert werden.

Das garantieren wir durch unseren Best-Integrated-Ansatz, mit dem wir sicherstellen, dass die eingesetzten Security-Komponenten bestmöglich zur bestehenden IT-Infrastruktur passen – von sicheren Netzwerken über sichere Rechenzentren bis hin zu sicheren Arbeitsplätzen. Dadurch schaffen wir in einem Klima der täglich neuen Cyberbedrohung eine sichere Arbeitsatmosphäre, in der Mitarbeiter ihr volles Potenzial abrufen können und Unternehmen ihre digitalen Ziele erreichen. Damit tragen unsere Security-Lösungen zu weit mehr bei als „nur“ einer sicheren IT: Sie helfen dabei, Vertrauen zu schaffen, sichern den Geschäftsbetrieb und die Wettbewerbsfähigkeit. Gleichzeitig senken wir Betriebskosten, verbessern die Servicequalität und schützen Daten, Identitäten und Arbeitsplätze. Das verstehen wir unter Digital Trust: Vertrauen, das ein Unternehmen jeden Tag sichert.

UNSER PORTFOLIO

VERTRAUEN DURCH KOMPETENZ



INFORMATION SECURITY MANAGEMENT

Wir unterstützen nicht nur bei der Steuerung der Informationssicherheit nach ISO 27001 und BSI IT-Grundschutz, sondern integrieren auch regulative Anforderungen in ein umfassendes Rahmenwerk. Wir vermessen Compliance und Risiken der IT-Systeme per Knopfdruck. Unsere Security Assessment Services industrialisieren manuelle Erhebungen zu Compliance und Risiken dort, wo keine Automatisierung möglich ist.



CYBER DEFENCE SERVICES

Um sich gegen Cyberangriffe zu wappnen, um sie frühzeitig zu erkennen und aus erfolgreichen Angriffsmustern für die Zukunft zu lernen, brauchen Unternehmen heute zusätzlich spezielle Cyber-Abwehrmaßnahmen, die wir in unseren Infrastrukturangeboten SIEM, UEBA, VM und AMP bündeln und durch Threat Intelligence und Frühwarnsysteme ergänzen. Und wenn Ihnen IT-Sicherheitsspezialisten fehlen, „leihen“ wir Ihnen unsere Security-Analysten on top aus.



IDENTITY & ACCESS MANAGEMENT

Mit zunehmender Digitalisierung wächst die Anzahl digitaler Identitäten in Unternehmen sprunghaft an. Jeder Mitarbeiter, jedes Endgerät, jedes System, das sich im Unternehmensnetz anmeldet, muss mit individuellen Informationen zur Autorisierung und Authentifizierung verknüpft und verwaltet werden. Diese Anforderungen erfüllen wir mit Identity- und Access-Management-Lösungen, die auch speziell neue Use Cases aus dem Consumer- und IoT-Bereich abdecken. Lösungen zum Privileged Account Management, zu starker Authentifizierung und Public-Key-Infrastrukturen runden das Portfolio ab.



ENDPOINT SECURITY

Mitarbeiter nutzen mittlerweile eine Vielzahl unterschiedlicher Endgeräte, auf denen berufliche und private Daten gespeichert sind. Gleichzeitig werden auf dem Endgerät zahlreiche Daten aus dem Internet verarbeitet und stellen damit ein besonderes sensibles Einfallstor für Angreifer dar. Neben den klassischen Maßnahmen wie Antivirus, Firewall, Patch Management und Verschlüsselung bietet Computacenter mit neuen Advanced-Endpoint-Security-Lösungen, wie Applikations-Isolation, Exploit-Mitigation, Client-Verhaltensanalyse oder Deception auch Lösungen an, die aktuellen Angriffen Widerstand leisten.



INFRASTRUCTURE SECURITY

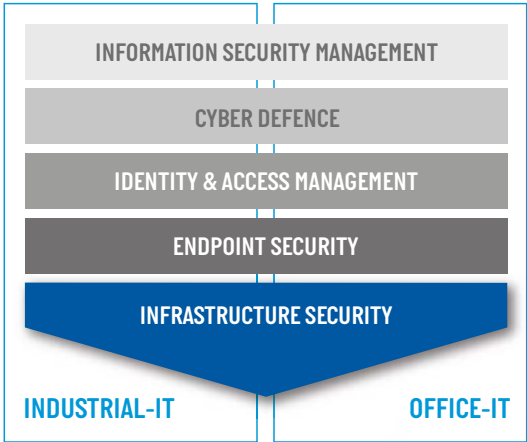
Die IT-Infrastruktur ist das digitale Rückgrat eines Unternehmens, die sowohl im lokalen Netzwerk und Datacenter, mobil als auch in der Cloud vor vielfältigen Angriffsformen geschützt werden muss. Unser Portfolio umfasst daher Firewalls, Intrusion-Detection/Prevention-Systeme, VPN-Lösungen, Application Delivery Controller, Web- und E-Mail-Sicherheit, Analysesysteme sowie Lösungen zum erweiterten Malwareschutz, IPAM- und DNS-Sicherheit. Aus diesen vielfältigen Bausteinen designen und implementieren wir eine für Ihre Umgebung passende und umfassende Sicherheitsarchitektur.



INDUSTRIAL SECURITY

Fertigungsunternehmen, die ihre Produktion digital vernetzen, brauchen spezielle, auf die industrielle Fertigung ausgelegte Sicherheitslösungen. Wir beraten Sie und implementieren genau solche Schutzmaßnahmen: Firewalls für die Produktion, IPS, Netzwerksegmentierung, Application Whitelisting, Fernwartung, SIEM und Cyber Defence für die Produktion. Damit sichern wir nicht nur Ihre Produktion, sondern bieten gleichzeitig innovative Lösungen zur Extraktion und Auswertung von Maschinen- und Produktionsdaten zur Störungsvorhersage und Ursachenidentifikation. Damit sichern wir nicht nur die Produktion, sondern tragen auch zur Effizienzsteigerung mit Return on Investment (ROI) dieser bei.

PORTFOLIO



METHODIK



VORTEILE



Zusammenhängender und ganzheitlicher Security-Ansatz



Security für den Erfolg des Unternehmens



Umgang mit Anbieter-/Lösungskomplexität



Entwicklung von Security-Lösungen für die komplexe, dynamische digitale Welt



Schutz von Daten, Identität und Geräten



MASTERING BUSINESS SECURITY

EINE SICHERE IT MACHT DEN UNTERSCHIED

Unser umfassendes Security-Lösungsportfolio erstreckt sich über alle Unternehmensbereiche – von Rechenzentren, Cloud Services und Netzwerken bis hin zu jedem einzelnen Arbeitsplatz. Damit sichern wir Ihr Unternehmen und schaffen Vertrauen bei allen Stakeholdern und Zielgruppen:



ALS CIO, CISO ODER IT-SICHERHEITSVERANTWORTLICHER können Sie sich darauf verlassen, dass Ihre Investitionen auf die Unternehmensziele einzahlen – was Ihnen den Rücken für die Einführung neuer Technologien stärkt. Sie können nachts ruhig schlafen, weil Ihr Unternehmen von neuen Technologien sicher profitiert und wir Sie so unterstützen, dass Sie interne Ressourcen optimal einsetzen und das eigene Know-how weiterentwickeln können.



IHRE MITARBEITER können sich auf die Sicherheit ihrer Geräte, Anwendungen und Cloud Services verlassen – wo immer sie arbeiten und sich im Firmennetz anmelden. Das motiviert – und steigert ihre Flexibilität und Produktivität.



DAS MANAGEMENT weiß, dass das Unternehmen sicher ist vor allen Folgen, die ein Cyberangriff mit sich bringt, vom Imageschaden bis zum Umsatzeinbruch – weil die IT sicher und gut gerüstet ist für aktuelle und zukünftige Herausforderungen.




UND IHRE KUNDEN können darauf vertrauen, dass ihre Daten bei Ihnen in sicheren Händen sind.

Damit tragen unsere Security-Lösungen zu weit mehr bei als „nur“ einer sicheren IT: Wir helfen Ihnen dabei, Vertrauen zu schaffen, sichern Ihren Geschäftsbetrieb und Ihre Wettbewerbsfähigkeit.

WARUM SIE UNS VERTRAUEN KÖNNEN

10 GRÜNDE FÜR COMPUTACENTER

- 
- 01 Wir sind Ihr „One-Stop-Shop“ für eine sichere IT. Sie erhalten alle Services und Lösungen aus einer Hand und müssen keine zusätzlichen Leistungen von Dritten kaufen.
 - 02 Als herstellerübergreifender IT-Dienstleister wählen wir immer die beste aller Lösungen, die haargenau zu Ihren Anforderungen und Zielen passt.
 - 03 Wir haben mehr als 40 Jahre Erfahrung mit Enterprise-IT, mehr als 20 Jahre mit Information Security und allein über 150 ausgewiesene Security-Experten. Wir verstehen Ihre IT-Infrastruktur und bieten pragmatische, bodenständige Lösungen, die sich nahtlos in die bestehenden Systeme integrieren lassen.
 - 04 Unser Security-Portfolio ist nicht nur eines der breitesten und ausgereiftesten am Markt. Es überzeugt vor allem auch durch unseren „Best-Integrated“-Ansatz.
 - 05 Wir vereinen umfassendes Expertenwissen in allen IT-Bereichen – vom Rechenzentrum bis zum Arbeitsplatz.
 - 06 Unser Kundenstamm schließt mehr als die Hälfte der DAX-30-Unternehmen und viele weitere multinationale Konzerne ein.
 - 07 Mithilfe unseres eigenen Compliance Frameworks helfen wir Ihnen, den Überblick über alle aktuellen Regulierungsanforderungen zu behalten – und stellen sicher, dass Ihr Unternehmen alle Compliance-Auflagen erfüllt.
 - 08 Wir schützen unsere eigene IT – damit Ihre Daten bei uns sicher sind.
 - 09 Wir ermöglichen es Ihnen, die Anforderungen Ihrer Mitarbeiter an mobile Arbeitsplätze, neue Endgeräte, flexible Arbeitsplatz- und -zeitmodelle umzusetzen und sich damit auch als Arbeitgeber im Kampf um die besten Köpfe vom Wettbewerb zu differenzieren.
 - 10 Wir begreifen getreu unserer Philosophie „Making Digital Work“ IT-Security nicht als notwendiges Übel, als defensiven Schutz vor Bedrohungen, sondern als aktiven Katalysator, der Sie in die Lage versetzt, aus IT-Trends wie Cloud Computing, Big Data oder dem Internet of Things für Ihr Unternehmen den größten Nutzen zu ziehen.

Enabling users and their business

Computacenter ist Europas führender herstellerübergreifender Dienstleister für eine Informationstechnologie, die Anwender und deren Geschäft erfolgreich macht. Wir beraten Organisationen hinsichtlich ihrer IT-Strategie, implementieren die am besten geeigneten Technologien, optimieren ihre Performance oder managen die IT-Infrastruktur unserer Kunden.

Verwurzelt in europäischen Kernländern verbindet Computacenter globale Reichweite mit lokaler Kompetenz.



Computacenter AG & Co. oHG
Europaring 34-40, 50170 Kerpen

computacenter.de
+49 (0)2273 5970