ZERO TRUST: VERTRAUEN IST GUT, EXPLIZITE SICHERHEIT IST BESSER

MIKRO-SEGMENTIERUNG UND SCHWACHSTELLENMANAGEMENT: EIN STARKES DUO

Die steigende Nutzung von Cloud-Services führt zu einer wahren Datenexplosion. Während die Gefahren durch Cyber-Angriffe stetig zunehmen, erhöhen neue hybride Arbeitsmodelle und eine Vielzahl an Geräten gleichzeitig die Komplexität. All das sorgt dafür, dass alte Security-Ansätze ausgedient haben. Mit einem Zero-Trust-Konzept und kontextbasierter Mikro-Segmentierung in Verbindung mit Schwachstellenmanagement schützen Behörden ihre IT – ohne modernes Arbeiten einzuschränken.

KLASSISCHE SECURITY – HEUTE EIN OFFENES SCHEUNENTOR

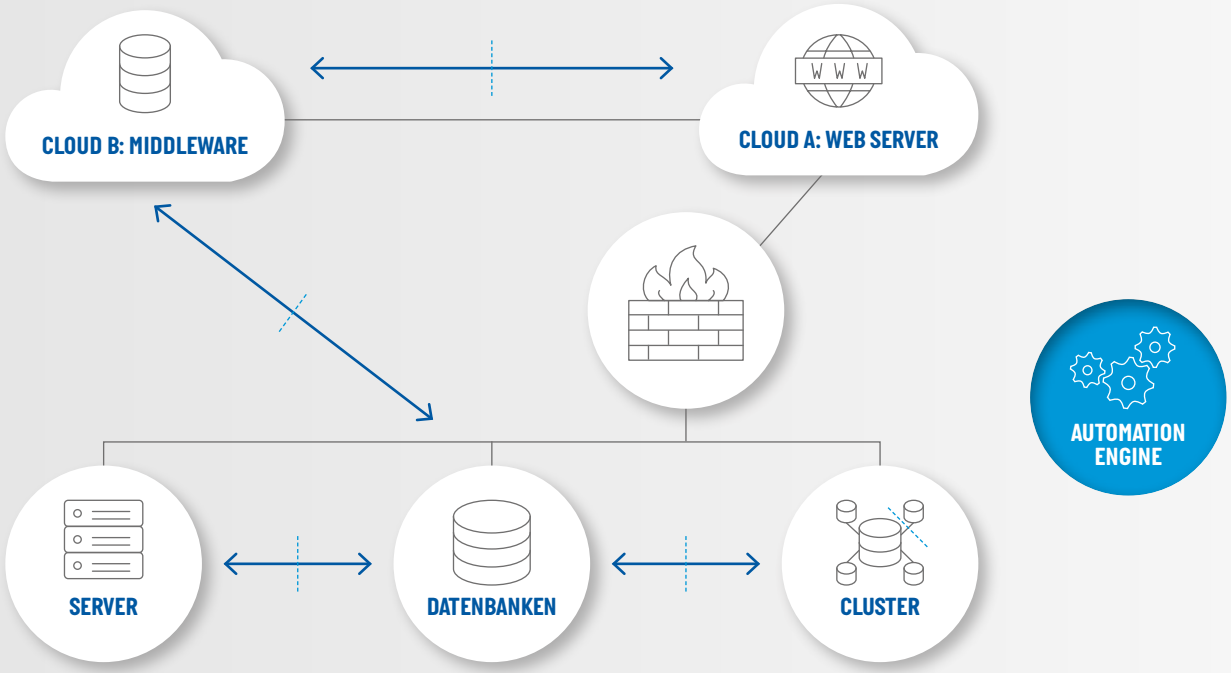
Der bisherige, starre Security-Ansatz basiert auf einer Umgebung, deren definierter Perimeter – etwa die Grenze des eigenen Netzwerks – durch eine Firewall vor Zugriffen von außen geschützt wird. Allen Menschen und Endgeräten, die sich innerhalb des Perimeters hinter dieser Firewall befinden, wird aufgrund ihres Standortes, Gerätetyps oder ihrer User-ID implizit vertraut. Dies gilt für Mitarbeiter:innen gleichermaßen wie auch beispielsweise für Lieferanten oder Techniker:innen, die Wartungsarbeiten durchführen. Sprich: wer es hinter die Firewall geschafft hat, dem stehen Tür und Tor in das Unternehmensnetzwerk offen.

AUS IMPLIZITEM TRUST WIRD EXPLIZITER TRUST

Während sich interne IT-Systeme durch den Schutz der Netzwerkgrenze relativ einfach absichern ließen, verschwimmen die unter anderem durch Bring-Your-Own-Device-Konzepte, Home-Office, Verwendung mobiler Geräte und Cloud-Anwendungen zunehmend. Die Folge: Das Risiko, dass unbekannte, ungeprüfte IT-Systeme und Nutzer:innen auf das Netzwerk zugreifen, steigt an. Gleichzeitig lassen sich grundlegende Schutzmaßnahmen wie Patching, Schutz der Arbeitsplatzrechner und der Infrastruktur sowie eine wirksame Cyber-Abwehr nicht mehr überall kontrolliert umsetzen. Daher reicht es nicht mehr aus, Verbindungen am Perimeter zu schützen.

Um seine IT-Infrastruktur zu schützen, empfiehlt sich auch für die öffentliche Hand der Zero-Trust-Ansatz – ein Konzept, das stets einen erfolgreichen Angriff unterstellt und einen optimalen Schutz für diese Bedingungen anstrebt. Zero Trust stellt die Datenverbindung in den Mittelpunkt und prüft anhand einer Policy, ob diese Verbindung erlaubt ist. Weiterhin wird ständig geprüft, ob die Verbindung riskant ist und ob es Hinweise auf eine bereits erfolgte Kompromittierung gibt. Dazu werden so viele Informationen wie möglich über den

ABLAUF DER MIKRO-SEGMENTIERUNG



Kontext, beispielsweise Schwachstellen oder Konfigurationsschwächen, ausgewertet. Auf diese Weise entsteht aus dem impliziten Trust – einem Ansatz, der auf einer Sicherung des Perimeters basiert – für jede einzelne Verbindung expliziter Trust.

SEGMENTIERUNG UND DURCHGÄNGIGE KONTROLLE

Zero Trust umfasst eine Reihe von Prinzipien, die in der NIST Sonderveröffentlichung 800-207 beschrieben sind: Identitäts- und Zugriffsmanagement, Governance, Risk und Compliance, Cyber-Defense-Fähigkeiten, Infrastruktur- und Workplace-Absicherung sowie ein ganzheitlicher Security-Ansatz, der auch Datenverschlüsselung und Monitoring umfasst. Alle diese Prinzipien zielen darauf ab, sich von dem Konstrukt des impliziten Vertrauens zu lösen.

Zentrale Anforderung ist dabei die Einführung von Zero-Trust-Architekturen mit einer durchgängigen Kontrolle der Verbindungen und des Datenverkehrs innerhalb eines Netzwerks, der Anwenderberechtigungen und des Kontextes, ganz unabhängig vom Ursprung der Kommunikation. So gewährleisten Behörden Sicherheit in modernen Rechenzentrums- und Applikationsumgebungen und setzen regulatorische Vorgaben flexibel und mit hoher Effizienz um.

WIE MIKRO-SEGMENTIERUNG BEDROHUNGEN ISOLIERT

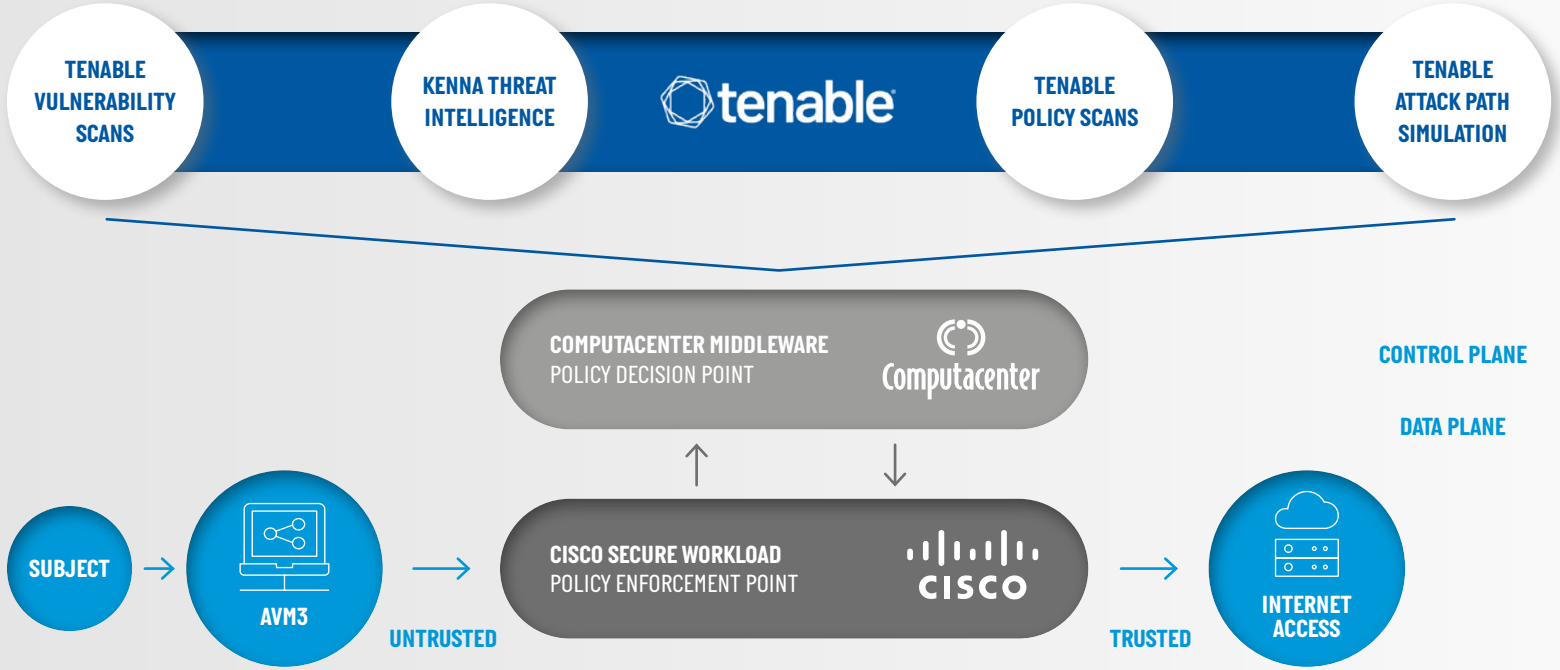
Eine beispielhafte Infrastruktur kann aus Datenbanken sowie Servern im Rechenzentrum, Webservern, Middleware und Applikationen in der Cloud bestehen. Der Webserver nimmt Anfragen von Anwender:innen entgegen, kommuniziert mit der Middleware, die diese Anfragen bearbeitet und hierfür wiederum die notwendigen Informationen beispielsweise aus einer Datenbank im Rechenzentrum abfragt. Die Antwort wird über den Webserver zurück zu den Anwender:innen gespielt.

Im Rahmen der Mikro-Segmentierung werden all diese Verbindungen mit Hilfe von Agenten überwacht und bewertet. Dazu werden Programme auf den Instanzen installiert, die kontinuierlich im Hintergrund arbeiten und die Kommunikationsbeziehungen überprüfen. Zur Automatisierung dieses Prozesses leiten die Agenten Informationen an eine Automation-Engine weiter, die lernt, welche Kommunikationsbeziehungen erforderlich sind, um normalen Datacenter-Traffic abzubilden. Nach einigen Wochen des Lernens erstellt die Automation-Engine Policies, nach denen künftig direkt entschieden werden kann, ob eine Kommunikationsbeziehung notwendig ist oder unterbunden werden muss, weil sie von der Policy abweicht.

WIRKUNG VON MIKRO-SEGMENTIERUNG

1. Instanzen und Kommunikationsbeziehungen identifizieren und visualisieren
2. Policies auf Grundlage identifizierter Kommunikationsanforderungen festlegen
3. Policies durch automatisierte Analyse und Regelwerkserstellung durchsetzen

VULNERABILITY-MANAGEMENT IN EINER ZERO-TRUST-ARCHITEKTUR ALS CONTEXT-DELIVERY



FÜR DAS PLUS AN SICHERHEIT: SCHWACHSTELLENMANAGEMENT UND MIKRO-SEGMENTIERUNG INTEGRIEREN

Um die Sicherheit weiter zu erhöhen, hat Computacenter eine Lösung entwickelt, mit der die Mikro-Segmentierung durch Daten aus dem Schwachstellenmanagement ergänzt wird. Ein modernes Schwachstellenmanagement-System besteht in der Regel aus einem Server, der mit verschiedenen Scan-Engines kommuniziert, die im Netzwerk verteilt sind. Diese Scan-Engines, beispielsweise der Schwachstellen-Scanner von Tenable, prüfen die Systeme und identifizieren Schwachstellen.

Nicht jede Schwachstelle ist kritisch, daher muss mittels Threat-Intelligence-System bewertet werden, ob eine Schwachstelle durch eine bestehende Schadsoftware ausgenutzt werden kann. Zur Einstufung des Risikos können Bewertungen von Tenable eingesetzt sowie weitere Datenquellen herangezogen werden, wie beispielsweise die Daten von Kenna-Security von Cisco. Wird eine hochkritische Schwachstelle gefunden – das kann ein Client sein, der länger nicht gepatcht wurde oder auf dem eine nicht vertrauenswürdige Software installiert ist – erzeugt das System ein Ticket, das anschließend von Administrator:innen, beispielsweise durch das Einspielen eines Patches, behoben werden muss.

Mit Hilfe einer von Computacenter entwickelten Middleware, werden diese Informationen aus dem Schwachstellenmanagement an den Policy-Decision-Point transferiert. Die Middleware ermöglicht es, über Maßnahmen zur weiteren Absicherung zu entscheiden – beispielsweise das Kappen einer Verbindung, solange die Schwachstelle nicht behoben wurde. Der Policy-Decision-Point (PDP) basiert auf einem Regelwerk und prüft kontinuierlich die Kontextinformationen, also welches Gerät kommuniziert von welcher Location mit welcher Berechtigung, sowie das Risiko der Verbindung.

Wird beispielsweise eine kritische Schwachstelle identifiziert, erfolgt das Kappen der Verbindung über den Policy-Enforcement-Point (PEP), beispielsweise durch das Tool zur Mikro-Segmentierung: Cisco-Secure-Workload. Dieses ist auch für die Durchsetzung der Regeln, die im Rahmen der Mikro-Segmentierung bereits von der Automation-Engine erstellt wurden, zuständig. Er überwacht kontinuierlich alle Aktivtäten. Sobald ein Risikowert zu hoch ist, sorgt der PEP dafür, dass das System dynamisch von der Kommunikation ausgeschlossen wird und schafft so explizites Vertrauen.

ZUSAMMENSPIEL VON NETZWERK- UND SECURITY-OPERATING-TEAMS

Der Vorteil dieses Ansatzes ist, dass kritische Schwachstellen schneller behoben werden, weil IT-Disziplinen zusammengebracht werden, die sonst nichts miteinander zu tun haben. Denn typischerweise wird die Mikro-Segmentierung von Netzwerk-Teams durchgeführt, das Schwachstellenmanagement liegt in den Security-Operating-Teams während das Beheben der Schwachstellen wiederum durch die jeweiligen Administator:innen (Linux, Windows, Netzwerk etc.) erfolgt.

Durch das Zusammenspiel von Schwachstellenmanagement und Mikro-Segmentierung erhalten Unternehmen eine größere Kontrolle über das Risiko von Verbindungen. Während die Mikro-Segmentierung einzelne Verbindungen prüft und beurteilt, ob sie „normal" sind, erkennt man über das Schwachstellenmanagement auch, warum eine augenscheinlich „normale" Kommunikation trotzdem unterbunden werden sollte. All diese Informationen laufen am Policy Decision Point zusammen und werden entsprechend gesteuert.

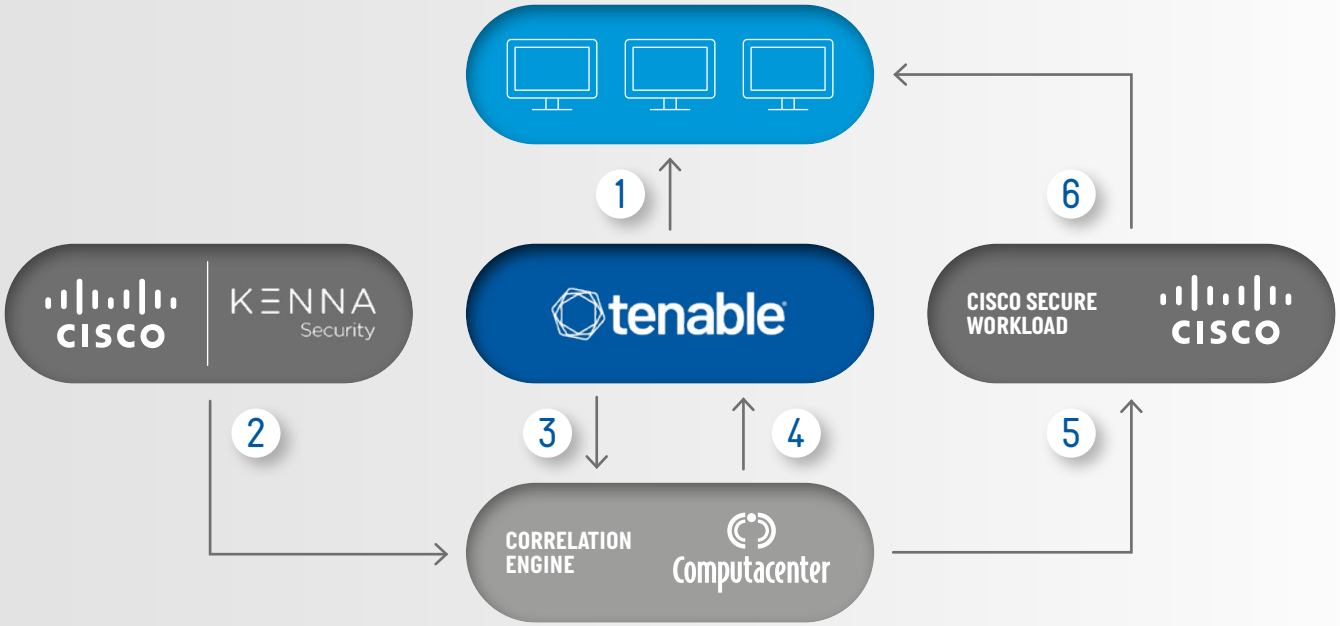
KONTEXTBASIERTE MIKRO-SEGMENTIERUNG IN DER PRAXIS

Wie ein solches Zusammenspiel des Tenable-Vulnerability-Scanners, Cisco-Kenna-Security, Cisco-Secure-Workload und der Computacenter-Middleware erfolgreich in der Praxis aussieht, können Sie sich in einer Live-Demo in unserem Solution Center ansehen.

In einer Testumgebung zeigen wir, wie der Tenable-Vulnerability-Scanner IT-Systeme prüft, während Cisco-Secure-Workload die Mikrosegmentierung durchführt und einzelne Verbindungen überprüft. Wir demonstrieren, wie beim Schwachstellen-Scan die entsprechenden Schwachstellen der Systeme erkannt und von einer Threat-Intelligence-Software bewertet werden. Im letzten Schritt zeigt die Demo, wie auf der Grundlage erkannter, kritischer Schwachstellen die Policies in Cisco-Secure-Workload angepasst werden, damit das kritische System von der Kommunikation ausgeschlossen wird und somit gesichert wird.

Zero Trust ist eine Geisteshaltung. Wir unterstützen unsere Kund:innen mit unserem umfassenden Prozess-, Change- und Security-Know-how bei der organisatorischen und technischen Umsetzung.

Ralf Nemeyer
Solution Manager bei Computacenter



COMPUTACENTER – IHR PARTNER FÜR DIE INTEGRATION VON ZERO TRUST

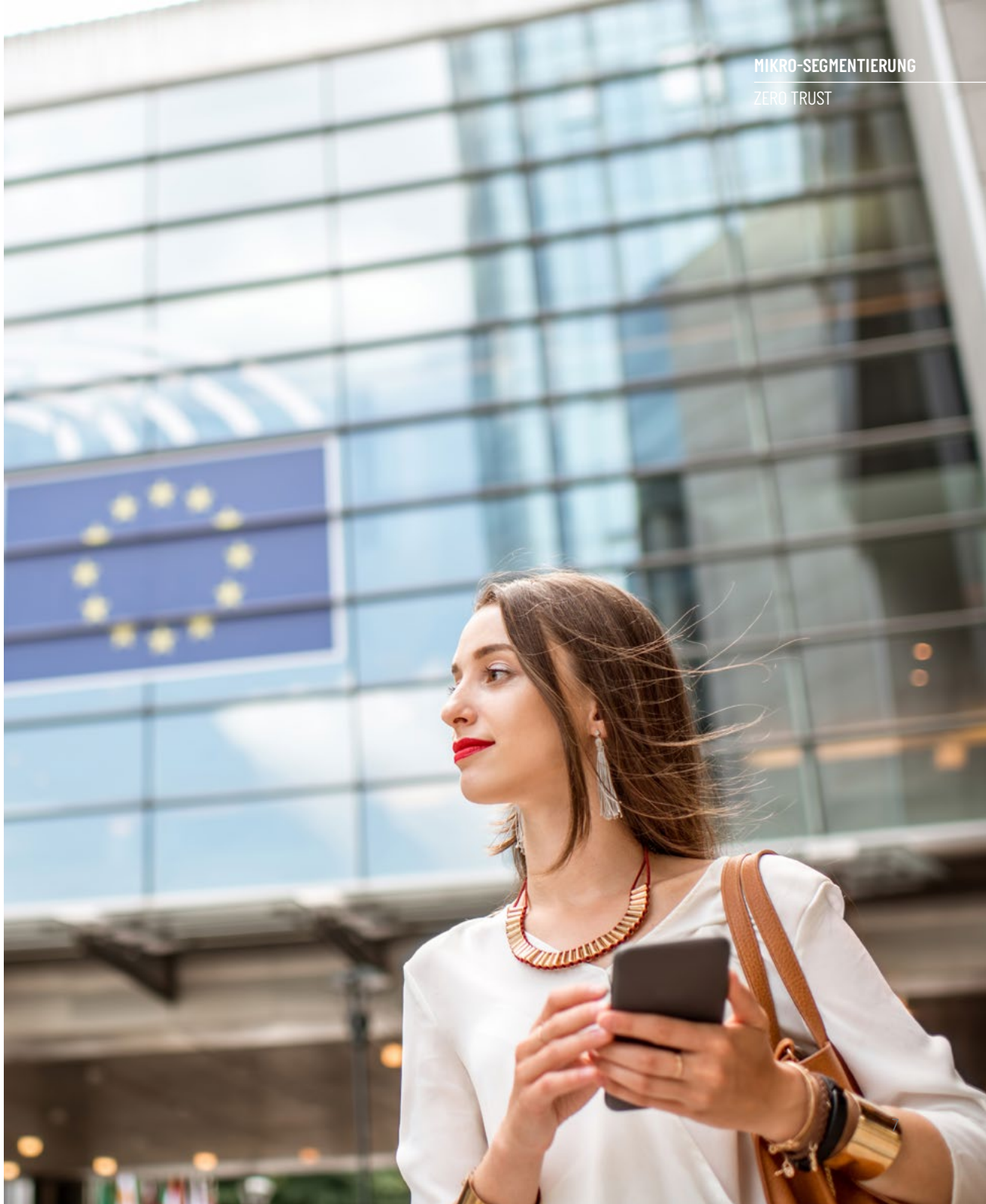
Unsere Leistungen umfassen neben der Entwicklung einer Zero-Trust-Roadmap und der Analyse der vorhandenen Sicherheitsmaßnahmen auch die Architekturberatung, Planung sowie Konzeption und einen reibungslosen Betrieb. Darüber hinaus führen wir eine Marktanalyse sowie Proof-of-Concepts durch. Wir implementieren Zero-Trust-Bausteine und integrieren diese in bestehende oder neue IT-Systeme und -Prozesse. Zudem migrieren wir Bestandssysteme, führen Schulungen Ihrer Fachabteilungen durch und unterstützen beim Kulturwandel.

Wir haben nicht nur Expert:innen im Schwachstellenmanagement, sondern auch im Bereich der Mikro-Segmentierung und in der Threat-Intelligence. Darüber hinaus sind unsere Entwickler:innen in der Lage, die notwendige Software zu programmieren und auf Ihre individuellen Bedürfnisse anzupassen.

Ein weiteres Plus sind unsere langjährigen Partnerschaften mit führenden Herstellern wie Tenable und Cisco. Wir haben bereits zahlreiche Zero-Trust-Konzepte anhand eines eigens entwickelten Blueprints ganzheitlich und erfolgreich umgesetzt. Damit sorgen wir für den notwendigen Schutz der IT-Infrastruktur in der öffentlichen Verwaltung.

SIND NOCH FRAGEN OFFEN?

Sie wollen die Sicherheit in Ihrer Behörde erhöhen? Sie möchten Zero Trust in Ihrer Organisation einführen oder sind an weiteren Informationen dazu interessiert? Dann sprechen Sie gerne Ihr Account-Team an.



Unternehmensprofil

Computacenter ist ein führender, unabhängiger Technologie- und Servicedienstleister, dem große Unternehmen und öffentliche Auftraggeber vertrauen. Wir helfen unseren Kunden bei der Beschaffung, der Weiterentwicklung und dem Betrieb ihrer IT-Infrastruktur, um eine digitale Transformation zu ermöglichen, die Anwender und deren Geschäft erfolgreich macht.

Computacenter ist ein an der Londoner Börse notiertes Unternehmen und beschäftigt über 20.000 Mitarbeiterinnen und Mitarbeiter weltweit.

Computacenter

Computacenter AG & Co. oHG
Computacenter Park 1, 50170 Kerpen

computacenter.de
+49 (0)2273 5970