Zero-Trust-Architektur

Ein neuer Ansatz für die IT-Sicherheit

Die IT-Sicherheit ist eine der größten Herausforderungen für Unternehmen und Organisationen in der heutigen digitalen Welt. Angesichts der zunehmenden Anzahl und Komplexität von Cyberangriffen, die Daten, Anwendungen und Netzwerke bedrohen, reichen traditionelle Sicherheitsmodelle heute nicht mehr aus, um einen effektiven Schutz zu gewährleisten. Ein neuer Ansatz, der in den letzten Jahren an Popularität gewonnen hat, ist die Zero-Trust-Architektur (ZTA).

Zero Trust, 2010 von Forrester postuliert, basiert auf dem Prinzip, dass kein Element innerhalb oder außerhalb eines Netzwerks als vertrauenswürdig angesehen werden kann, ohne vorher überprüft zu werden. Das bedeutet, dass jede Anfrage, jeder Zugriff und jede Transaktion kontinuierlich validiert und autorisiert werden muss, basierend auf einer Reihe von Faktoren wie Identität, Kontext, Risiko und Verhalten. Die ZTA erfordert eine radikale Umgestaltung der Sicherheitsarchitektur, die von einem perimeterbasierten Modell zu einem datenzentrierten Modell übergeht und umfasst folgende Kernelemente:

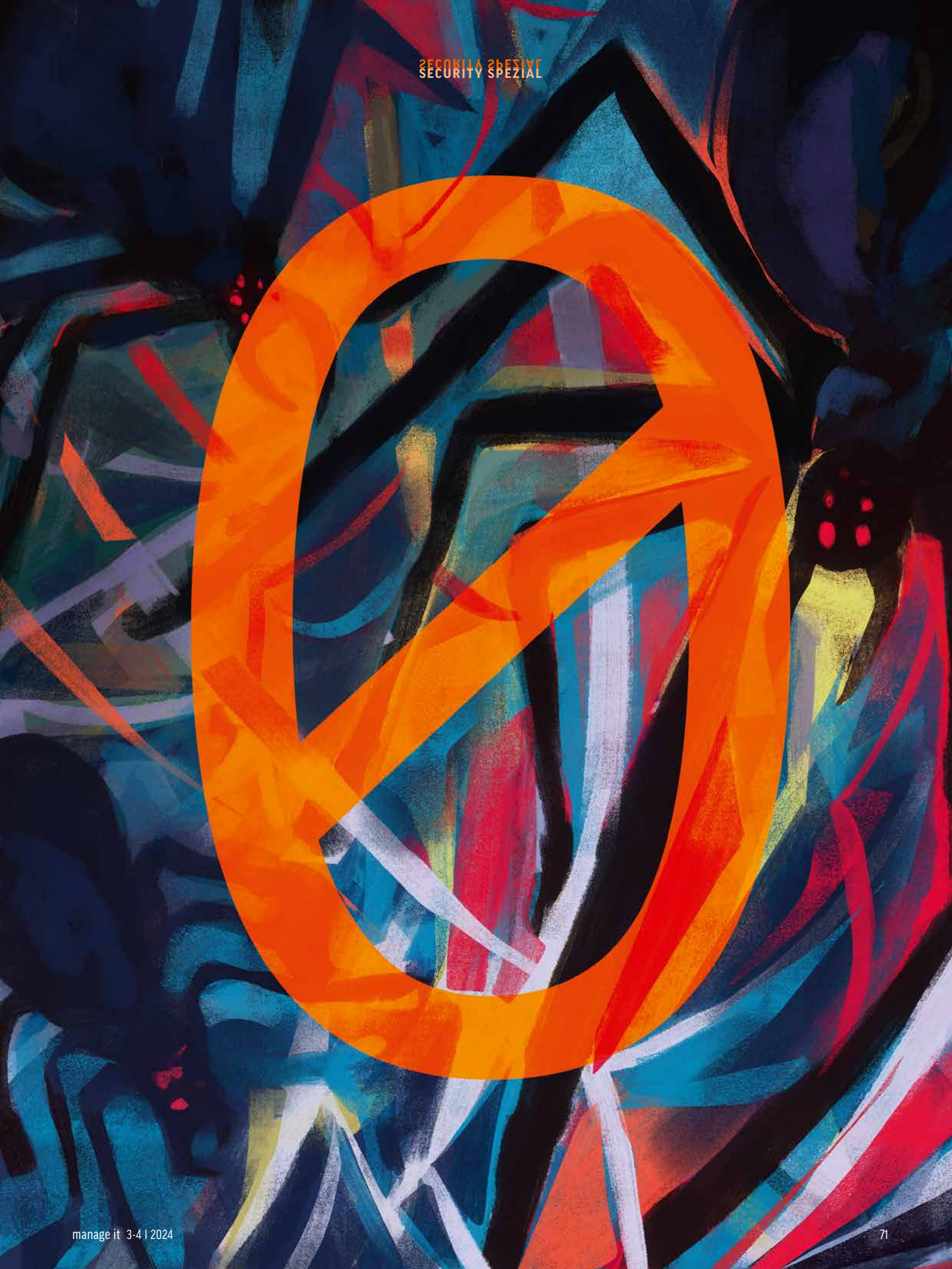
Identitäts- und Zugriffsmanagement (IAM):
IAM ist der Prozess, der sicherstellt, dass nur autorisierte Benutzer, Geräte und Anwendungen auf die benötigten Ressourcen zugreifen können, basierend auf ihrer Rolle, ihrem Standort, Gerätetyp, Sicherheitsstatus und anderen Attributen. IAM umfasst die Verwendung von Multi-Faktor-Authentifizierung (MFA), Single Sign-On (SSO), Privileged Access Management (PAM) und anderen Technologien, um die Identität zu verifizieren und den Zugriff zu steuern.

Mikrosegmentierung:
Bei der Mikrosegmentierung handelt es sich um die Aufteilung eines Netzwerks in kleinere, isolierte Segmente, die jeweils eine bestimmte Funktion oder einen bestimmten Dienst erfüllen. Mikrosegmentierung ermöglicht es, den Datenverkehr zwischen den Segmenten zu beschränken und zu überwachen, um die Angriffsfläche zu reduzieren und die Erkennung und Eindämmung von Bedrohungen zu erleichtern.

Verschlüsselung:
Verschlüsselung ist die Umwandlung von Daten in eine »unleserliche« Form, die sich nur mit einem geheimen Schlüssel entschlüsseln lässt. Verschlüsselung schützt die Vertraulichkeit, Integrität und Verfügbarkeit von Daten, indem sie verhindert, dass unbefugte Personen auf die Daten zugreifen oder diese manipulieren können. Es ist ratsam, Verschlüsselung sowohl für Daten in Ruhe (auf Speichermedien) als auch für Daten in Bewegung (über Netzwerke) anzuwenden.

Endpunkt- und Cloud-Sicherheit:
Endpunkt- und Cloud-Sicherheit sind die Maßnahmen, die ergriffen werden, um die Sicherheit von Geräten und Anwendungen zu gewährleisten, die außerhalb des traditionellen Netzwerkperimeters liegen. Endpunkt- und Cloud-Sicherheit umfassen die Verwendung von Antiviren-, Firewall-, Patch- und Konfigurationsmanagement-Software und schützen die Endgeräte vor Malware, Exploits und anderen Angriffen. Cloud-Sicherheit beinhaltet die Verwendung von Cloud Access Security Brokers (CASB), Cloud Workload Protection Platforms (CWPP) und anderen Technologien, um die Sicherheit von Cloud-Diensten und Cloud-Ressourcen zu gewährleisten.

Sicherheitsanalyse und Automatisierung:
Sicherheitsanalyse und Automatisierung sind die Prozesse, die Daten aus verschiedenen Quellen sammeln, korrelieren und analysieren, um Anomalien, Bedrohungen und Schwachstellen zu identifizieren und darauf zu reagieren. Sicherheitsanalyse und Automatisierung umfassen die



Verwendung von Security Information and Event Management (SIEM), Security Orchestration, Automation and Response (SOAR), künstlicher Intelligenz (KI) und maschinellem Lernen (ML) und erlauben es, Sicherheitsvorfälle zu reduzieren, zu priorisieren und zu lösen.

Der Einsatz einer Zero-Trust-Architektur bietet der IT-Sicherheit enorme Vorteile:

- **Erhöhte Sichtbarkeit und Kontrolle:** Eine ZTA ermöglicht es, alle Aktivitäten und Ereignisse im Netzwerk zu erfassen, zu überprüfen und zu verwalten, unabhängig davon, wo sie stattfinden. Dies verbessert die Transparenz und die Verantwortlichkeit und ermöglicht eine schnellere Erkennung und Reaktion auf Sicherheitsvorfälle.

- **Reduzierte Komplexität und Kosten:** Eine ZTA vereinfacht die Sicherheitsarchitektur, indem sie die Abhängigkeit von veralteten und ineffizienten Sicherheitslösungen reduziert, die oftmals schwer zu verwalten und zu warten sind. Darüber hinaus wird eine bessere Nutzung der vorhandenen Ressourcen und eine Optimierung der Sicherheitsinvestitionen erzielt, indem sie eine konsistente und skalierbare Sicherheitspolitik über alle IT-Umgebungen hinweg anwendet.

- **Verbesserte Benutzererfahrung und Produktivität:** Eine ZTA kann die Benutzererfahrung und die Produktivität verbessern, indem sie einen nahtlosen und sicheren Zugriff auf die benötigten Daten und Anwendungen ermöglicht, unabhängig vom Standort, Gerät oder Netzwerk. Ebenso lassen sich Reibung und Frustration reduzieren, die in der Regel durch häufige Passwortänderungen, Captchas, VPNs und andere Sicherheitsmaßnahmen verursacht werden.

Eine Zero-Trust-Architektur ist jedoch kein einfacher Schalter, den man umlegen kann, um die IT-Sicherheit zu verbessern. Sie erfordert eine strategische Planung, eine schrittweise Implementierung und eine kontinuierliche Überwachung und Anpassung, um die gewünschten Ergebnisse zu erzielen. Zudem setzt Zero Trust kulturelle Veränderungen voraus, damit eine enge Zusammenarbeit zwischen den verschiedenen Stakeholdern wie IT, Sicherheit, Geschäftsführung, Compliance und Benutzern erfolgen kann. Eine ZTA ist kein Endziel, sondern ein fortlaufender Prozess, der ständige Verbesserungen und Innovationen erfordert.

Fazit. Zusammenfassend lässt sich feststellen: Bei der Zero-Trust-Architektur handelt es sich um einen neuen Ansatz im Rahmen der IT-Sicherheit, der das Potenzial hat, die Art und Weise, wie Unternehmen und Organisationen ihre Daten, Anwendungen und Netzwerke schützen, zu revolutionieren. Eine ZTA bietet erhebliche Vorteile – unter anderem erhöhte Sichtbarkeit und Kontrolle, reduzierte Komplexität und Kosten, verbesserte Benutzererfahrung und Produktivität. Gleichzeitig ist jedoch auch eine sorgfältige Planung, Implementierung und Überwachung notwendig, um die Herausforderungen und Risiken zu bewältigen, die mit der digitalen Transformation einhergehen. Wichtig ist: Eine Zero-Trust-Architektur ist kein einmaliges Projekt, sondern eine kontinuierliche Reise, die eine kollaborative und adaptive Sicherheitskultur erfordert.

*/ Bei der Zero-Trust-Architektur handelt es sich um einen neuen Ansatz im Rahmen der IT-Sicherheit, der das Potenzial hat, die Art und Weise, wie Unternehmen und Organisationen ihre Daten, Anwendungen und Netzwerke schützen, zu revolutionieren.

Als IT-Dienstleister und Managed Service Provider ist Controlware der ideale Partner für die Planung und Realisierung einer effektiven Zero-Trust-Strategie. Neben der Entwicklung einer bedarfsgerechten IT-Architektur, der Bestimmung des Reifegrads und der Implementierung übernehmen die Controlware IT- und Security-Experten auf Wunsch auch den teilweisen oder kompletten Betrieb der Systemkomponenten.

Christoph Schmidt,
Lead Architect Information Security,
Controlware GmbH

www.controlware.de
blog.controlware.de