IDC Info Snapshot, gesponsert von Akamai | Februar 2024

Transformation der öffentlichen Dienste in Deutschland: Erweiterte Sicherheit für mehr Effizienz und Vertrauen


Massimiliano Claps
Research Director


Remi Letemple
Senior Research Analyst,
IDC Government Insights


Romain Fouchereau
Research Manager,
European Security

Top-Prioritäten:

Verbesserung der Nutzererfahrung und des Vertrauens der Bürger:innen bei der Nutzung staatlicher Dienstleistungen (56 % der Befragten)

Strategischer Fokus:

Zero-Trust-Ansatz als oberste Priorität, wird als vorteilhaft angesehen und in neuen Initiativen integriert (89 % – Top 2 der Antworten)

Herausforderungen:

52 %

Fähigkeiten von Mitarbeitern im öffentlichen Dienst in Bezug auf Cybersicherheitsrisiken

41%

Mangelndes Verständnis seitens des Managements

Quelle: IDC EMEA, *Digital Transformation and Security Survey 2023*

Um öffentliche Dienste der nächsten Generation anbieten zu können, müssen die Regierung und Kommunalverwaltungen in Deutschland in moderne, intelligente Sicherheitsarchitekturen investieren. Damit können sie die Resilienz gegen Cyberangriffe verbessern und Vertrauen aufbauen. Dieser strategische Ansatz zielt darauf ab, praktische Ergebnisse zu liefern. Die Einführung moderner Sicherheits-Frameworks ermöglicht den Bürger:innen sichere und nahtlose Interaktionen beim Zugriff auf eGovernment-Services, wodurch Vertrauen aufgebaut und die Zuverlässigkeit erhöht wird. Fortschrittliche Sicherheitsmaßnahmen werden integriert, um die betriebliche Effizienz und Resilienz gegen immer ausgefeiltere Bedrohungen zu verbessern. Dies gewährleistet eine kontinuierliche Servicebereitstellung und schützt geschäftskritische Betriebsabläufe.

Die Umfrage von IDC zur digitalen Transformation und Sicherheit (Digital Transformation and Security Survey) ergab die folgenden drei größten Herausforderungen bei der Reaktion auf Cyberbedrohungen von heute:

- Geringes Bewusstsein und geringe Fähigkeiten im Zusammenhang mit Cybersicherheitsrisiken bei Mitarbeitern im öffentlichen Dienst (48 % der Befragten)
- Nicht in der Lage sein, zeitnah auf aufkommende Bedrohungen zu reagieren (52 %)
- Digitalisierung und höhere Datenmengen, die online übertragen werden, was zu neuen Angriffsflächen und vermehrten Schwachstellen führt (48 %)

Eine effiziente Lösung, um diese Herausforderungen zu bewältigen, ist die Einbeziehung von Servicepartnern. Sie stellen das erforderliche Fachwissen und die Ressourcen zur Verfügung, um Kompetenzlücken zu überwinden, die Reaktionsfähigkeit zu verbessern und um die digitale Infrastruktur vor Bedrohungen zu schützen.

Derartige Modernisierungsmaßnahmen bringen ihre eigenen Herausforderungen mit sich. Die digitale Transformation erhöht die Angriffsfläche und zwingt Unternehmen im öffentlichen Sektor dazu, die Sicherheitsmaßnahmen zu verbessern, um eine größere Bandbreite an komplexen Cyberbedrohungen zu bewältigen. Diese erweiterte Bedrohungslandschaft erfordert einen strategischen und ganzheitlichen Sicherheitsansatz, um die Integrität und Vertraulichkeit sensibler Informationen zu schützen.

Mit der Einführung neuer Vorschriften und Compliance-Standards müssen Unternehmen den sicheren und effizienten Einsatz von Technologie im öffentlichen Dienst gewährleisten. Dazu gehört nicht nur, aktuelle Compliance-Anforderungen zu erfüllen, sondern auch zukünftige regulatorische Rahmenbedingungen zu antizipieren und vorzubereiten.

Zu den Modernisierungsmaßnahmen gehören Fortschritte bei der Transformation von Sicherheitprozessen: Technologien werden kombiniert, um die Sicherheit zu verbessern und gleichzeitig die Nutzererfahrung der Bürger:innen zu verbessern. Mit Cloud-Sicherheit wird gewährleistet, dass die in der Cloud gespeicherten und verarbeiteten Daten sicher bleiben und Bedenken hinsichtlich Datenschutz und -souveränität berücksichtigt werden. Letzteres ist für 30 Prozent der Befragten in Deutschland eine wichtige betriebliche Priorität. Die Netzwerksicherheit sorgt für einen zuverlässigen Schutz der Umgebung und schützt vor unbefugtem externem Zugriff.

Das Zero-Trust-Framework, ein grundlegender Wandel in der Philosophie der Cybersicherheit, basiert auf dem Prinzip „Niemals vertrauen, immer überprüfen“. Dieser Ansatz stellt das herkömmliche perimeterbasierte Sicherheitsmodell in Frage und erfordert eine kontinuierliche Überprüfung aller Nutzer:innen, Geräte und Netzwerkflüsse. Durch die Einführung von Zero Trust schaffen Regierungen ein Umfeld, in dem Vertrauen nicht angenommen wird, sondern erst durch kontinuierliche Überprüfung gewonnen wird. Damit werden Sicherheitsmaßnahmen an die dynamische Natur der heutigen Cyberbedrohungen angepasst.

Als Reaktion auf die häufigsten Angriffe im letzten Jahr – insbesondere Ransomware (41 %), Phishing (37 %) und Fake-Webseiten (33 %) – ist eine umfassende Strategie unerlässlich. Diese erfordert die Implementierung robuster Maßnahmen gegen derartige Angriffe sowie die Umsetzung von Cloud-Migrationsstrategien und die Optimierung von Compliance-Maßnahmen, um Innovationen zu ermöglichen und Vertrauen aufzubauen.

Für 37 Prozent der IT-Sicherheitsteams ist die Visibilität und Minimierung von Sicherheitsrisiken, die von Drittanbietern herrühren, eine der top operativen Prioritäten. Regierungsbehörden sollten mit Sicherheitsanbietern zusammenarbeiten, um Zugang zu hochmodernen Technologien zu erhalten. Mit diesen Lösungen können Umgebungen visualisiert und vor Ransomware und anderen Bedrohungen geschützt werden, ein nahtloser Zugriff auf Anwendungen und Daten bereitgestellt und das gesamte Nutzererlebnis verbessert werden.

Zusammenfassend lässt sich sagen: Die öffentliche Hand in Deutschland setzt die digitale Transformation fort, und die Integration fortschrittlicher Sicherheitsmaßnahmen ist nicht nur eine Reaktion auf unmittelbare Bedrohungen, sondern auch eine strategische Investition in einen zukunftssicheren öffentlichen Dienst. Es ist ein Weg hin zu effizienten, sicheren und auf die Bürger:innen ausgerichteten Abläufen. Diese Herausforderungen bieten gleichzeitig auch Chancen für Innovation und Verbesserung. Wenn sie richtig angegangen werden, kann die Regierung in Zukunft auf optimierte Cyberresilienz und Technologie bauen.