Sicherheitsstrategien für den effektiven Schutz in Kommunalverwaltungen

ZERO TRUST PRAKTISCH UMSETZEN: EIN LEITFADEN FÜR KOMMUNALE IT-VERANTWORTLICHE

Kommunaler IT-Sicherheitskongress (KITS)
Dr. Anna Lena Fehlhaber, Technology Strategy Lead - AI and Security

AGENDAÜBERSICHT

- **Grundlagen** des Zero Trust Sicherheitsprinzips
- Schrittweises Vorgehen **zur Einführung** von Zero Trust
- Technische und organisatorische Maßnahmen im Zero Trust Modell
- **Herausforderungen** und **Best Practices** bei der Umsetzung in Kommunen

GRUNDLAGEN DES ZERO TRUST SICHERHEITSPRINZIPS

DEFINITION UND ZENTRALE PRINZIPIEN VON ZERO TRUST

Grundprinzipien von Zero Trust

Zero Trust setzt auf geringstmögliche Rechtevergabe und strenge Authentifizierung für alle Nutzenden und Geräte

Kontinuierliche Zugriffskontrolle

Jeder Zugriff wird kontinuierlich überprüft, um Sicherheit unabhängig vom Standort zu gewährleisten

Paradigmenwechsel in IT-Sicherheit

Zero Trust ersetzt traditionelle perimeterbasierte Sicherheitsansätze durch segmentierte und kontrollierte IT-Betriebsmodelle

UNTERSCHIEDE ZU KLASSISCHEN SICHERHEITS-MODELLEN

Klassische Sicherheitsmodelle

Setzen auf ein stark abgesichertes Netzwerk-Perimeter und vertrauen internen Nutzenden und Geräten überwiegend

Prinzip von Zero Trust

Verzichtet auf implizite Vertrauenszonen und validiert jede Zugriffsanfrage kontinuierlich und standortunabhängig

Moderne Resilienz gegen Angriffe

Zero Trust bietet eine deutlich höhere Sicherheit gegen gezielte Angriffe und Insider-Bedrohungen als klassische Modelle

WARUM ZERO TRUST FÜR KOMMUNEN RELEVANT IST

Komplexität kommunaler IT

Kommunale IT umfasst viele Nutzendengruppen und heterogene Systeme, die hohe Sicherheitsanforderungen stellen

Zunahme von Cyberangriffen

Kommunen sind vermehrt Ziel von Cyberangriffen auf kritische Infrastrukturen, was einen erhöhten Schutzbedarf schafft

Schutz sensibler Bürgerdaten

Zero Trust schützt Bürgerdaten effektiv und unterstützt die Einhaltung gesetzlicher Vorgaben

Betriebssicherheit und Resilienz

Zero Trust Modelle verbessern die Betriebssicherheit und erhöhen die Widerstandsfähigkeit gegen moderne Bedrohungen

SCHRITTWEISES VORGEHEN ZUR EINFÜHRUNG VON ZERO TRUST

BESTANDSAUFNAHME DER BESTEHENDEN IT-INFRASTRUKTUR

Gründliche IT-Inventarisierung

Alle IT-Komponenten, Nutzendenrollen und Datenflüsse müssen vollständig erfasst werden

Transparenz zur Risikominimierung

Ohne vollständige Transparenz entstehen Lücken in der Zugriffskontrolle und Risiken für unerkannte Angriffe

Automatisierte Asset-Erkennung

Empfohlene Tools zur automatischen Erkennung von Assets und Netzwerk-Mapping schaffen belastbare Daten(!)

IDENTIFIKATION SCHÜTZENS-WERTER RESSOURCEN UND NUTZENDER

Kategorisierung kritischer Assets

Wichtige Daten und Systeme werden nach Schutzbedarf klassifiziert, um gezielte Sicherheitsmaßnahmen zu ermöglichen

Nutzendengruppen Zuordnung

Unterschiedliche Nutzendengruppen wie Verwaltungsmitarbeitende oder externe Dienstleister werden eindeutig zugeordnet

Fokus auf sensible Kontrollpunkte

Durch Identifikation sensibler Kontrollpunkte wird Komplexität reduziert; der Fokus liegt dann auf besonders sensiblen Sicherheitsbereichen

FESTLEGUNG VON ZUGRIFFS-RICHTLINIEN UND KONTROLL-MECHANISMEN

Granulare Zugriffsregeln

Implementierung von feingliedrigen Zugriffsregeln basierend auf Prinzipien wie Least Privilege zur Minimierung von Risiken

Kontextbasierte Zugriffskontrollen

Zugriffsentscheidungen werden dynamisch anhand von Kontextfaktoren wie Standort und Zeit getroffen

Automatisierte Kontrollmechanismen

Nutzung von RBAC und ABAC zur automatischen und sicheren Verwaltung von Benutzendenrechten in komplexen Umgebungen

TECHNISCHE UND ORGANISATORISCHE MAßNAHMEN IM ZERO TRUST MODELL

IMPLEMENTIERUNG VON MULTI-FAKTOR-AUTHENTIFIZIERUNG

Mehrdimensionale Identitätsprüfung

Kombination aus mindestens zwei Faktoren: Wissen (Passwort), Besitz (Authenticator-App, FIDO2-Security-Key, Hardware-Token) und ggf. Biometrie

Wirksame Reduzierung von Angriffsrisiken

Sicherheitsbehörden und Fachgremien empfehlen MFA als eine der effektivsten und schnell umsetzbaren Maßnahmen zur Stärkung der IT-Sicherheit in Verwaltung und kritischer Infrastruktur

Praxistaugliche Implementierung für Kommunen

Integration über etablierte Standards (z.B. SAML, OpenID Connect, RADIUS) ermöglicht eine schrittweise Einführung mit überschaubarem Aufwand und hohem Sicherheitsgewinn für kommunale IT-Systeme

SEGMENTIERUNG DES NETZWERKS UND MIKRO-SEGMENTATION

Netzwerksegmentierung

Netzwerksegmentierung teilt das Netz in abgeschottete Zonen und begrenzt so die laterale Ausbreitung von Angriffen

Mikro-Segmentation

Mikrosegmentierung kontrolliert Zugriffe auf Workload- und Anwendungsebene nach Zero-Trust-Prinzipien

Vorteile für komplexe Netzwerke

In komplexen kommunalen Netzen erhöht Mikrosegmentierung die Transparenz und Steuerbarkeit der Datenflüsse deutlich

MONITORING UND KONTINUIERLICHE ÜBERPRÜFUNG DER ZUGRIFFE

Kontinuierliches Monitoring

SIEM-Systeme ermöglichen die ständige Überwachung von Zugriffen und erkennen ungewöhnliche Aktivitäten

Automatisierte Analysetools

Automatisierte Tools analysieren Datenmuster und unterstützen die Identifikation von potenziellen Bedrohungen

Schnelle Erkennung von Angriffen

Proaktives Monitoring hilft, Angriffsversuche frühzeitig zu identifizieren und reduziert Ausfallzeiten sowie Schäden

HERAUSFORDERUNGEN UND BEST PRACTICES BEI DER UMSETZUNG IN KOMMUNEN

TYPISCHE STOLPERSTEINE UND LÖSUNGSANSÄTZE

Häufige Schwierigkeiten

Fehlende IT-Transparenz, begrenzte Ressourcen und Widerstände erschweren Veränderungsprozesse

Klare Projektplanung

Eine strukturierte Planung und Einbindung aller Stakeholder ist entscheidend für den Projekterfolg(!)

Graduelle Einführung

Pilotprojekte und schrittweise Einführung helfen Risiken zu minimieren und Akzeptanz zu fördern

MITARBEITENDEN SENSIBI-LISIERUNG UND CHANGE MANAGEMENT

Schulung und Sensibilisierung

Gezielte Schulungen stärken das Bewusstsein und fördern die Einhaltung von Sicherheitsrichtlinien im Unternehmen

Regelmäßige Kommunikation

Kontinuierlicher Informationsaustausch unterstützt die Anpassung an neue Sicherheitskonzepte und Prozesse

Erfolg durch Change Management

Organisationen mit starkem Change Management erleben höhere Sicherheit und reibungslose Umstellungen

ERFOLGSFAKTOREN FÜR ZERO TRUST IN DER KOMMUNALEN IT-PRAXIS

- Konkrete, priorisierte Sicherheitsziele geben kommunalen IT-Projekten klare Richtung und machen Fortschritte beim Schutzniveau messbar
- Dashboards, Monitoring- und Ticketsysteme schaffen technikgestützte Transparenz und erleichtern die Abstimmung zwischen IT, Fachämtern und Leitung
- Ein kontinuierlicher Sicherheitsprozess mit regelmäßigen Reviews und angepassten Maßnahmen verankert IT-Sicherheit dauerhaft im Verwaltungsalltag
- Weniger Sicherheitsvorfälle, kürzere Ausfallzeiten und höhere Zufriedenheit der Nutzenden mit IT-Services belegen den Erfolg kommunaler Sicherheitsprojekte

VOM SCHLAGWORT ZUR PRAXIS: ZERO TRUST IM KOMMUNALEN ALLTAG

Schrittweise Umsetzung

Ein schrittweises Vorgehen erleichtert die Einführung von Zero Trust in kommunalen IT-Strukturen effektiv und nachhaltig

Technische Maßnahmen

Technische Lösungen wie Zugangskontrollen und kontinuierliche Überwachung stärken die Sicherheit kritischer kommunaler Ressourcen

Einbindung aller Beteiligter

Die Einbeziehung der Mitarbeitenden fördert das Sicherheitsbewusstsein und unterstützt die erfolgreiche Umsetzung von Zero Trust

Nachhaltige IT-Sicherheit

Zero Trust ermöglicht eine resilientere und nachhaltige digitale Infrastruktur in kommunalen IT-Umgebungen