

PROVITAKO: KOMMUNALE CYBERSICHERHEIT ALS EXISTENZFRAGE

Die Digitalisierung des öffentlichen Sektors ist kein reines IT-Projekt – sie ist das Fundament für das Vertrauen der Bürger in den demokratischen Staat.

Wenn kommunale Systeme von Ransomware-Wellen getroffen werden, steht weit mehr auf dem Spiel als temporäre IT-Ausfälle. Es drohen massiver Datenabfluss ins Darknet, Identitätsdiebstahl und monatelange Lähmungen der kritischen Infrastruktur. Ein solcher Systemkollaps beschädigt das gesellschaftliche Vertrauen nachhaltig. Für die ProVitako ist vorausschauende Cybersecurity daher kein optionaler Schutz, sondern die Existenzbedingung für eine handlungsfähige kommunale Familie.

Als Einkaufsgemeinschaft und Innovationsnetzwerk bündeln wir die Kräfte der kommunalen IT-Dienstleister, damit sie dieser Bedrohung mit maximaler

technologischer Souveränität begegnen können. Unser breit gefächertes Portfolio bildet das softwareseitige Fundament für resiliente Betriebsinfrastrukturen unserer Mitglieder. Durch europaweite Beschaffung mit Marktführern wie Palo Alto Networks, Fortinet und Check Point etablieren wir in unseren Rahmenverträgen modernste Next-Generation-Sicherheitsstandards. Flankiert wird dies durch ganzheitliche Ansätze mit Red Hat, VMware by Broadcom sowie zukunftsfähigen Open-Source-Virtualisierungsalternativen.

Um den Schutzschirm lückenlos zu schließen, erweitern wir das Portfolio aktuell um dedizierte Resilienz-Pro-

dukte im Endpoint-Security-Segment. Zudem befindet sich ein Beschaffungsvorhaben „Managed Detection and Response“ (MDR) in der aktiven Vorbereitung. Damit befähigen sich unsere Mitglieder, Angriffe nicht nur abzuwehren, sondern proaktiv in Echtzeit zu erkennen und zu isolieren – ein wichtiger Baustein für einen dauerhaft resilienten, digitalen Staat.



Stefan Pauly
ist Teamleiter
Anforderung
bei ProVitako.