## Überprüfung der organisatorischen und technischen Resilienz des Gesundheitsamtes gegen Cyberangriffe

Gesundheitsamt Bochum

Das Gesundheitsamt Bochum ließ im Rahmen des Paktes für den Öffentlichen Gesundheitsdienst seine organisatorische und technische Widerstandsfähigkeit gegen Cyberangriffe prüfen. Ein IT-Sicherheitsunternehmen führte dazu mehrere Analysen durch: die Überprüfung mobiler Dienstgeräte, Social-Engineering-Tests an verschiedenen Standorten, einen Penetrationstest im internen Netzwerk sowie eine erneute Bewertung der mobilen Endgeräte mit Fokus auf das Mobile Device Management. Ergänzend wurden technische Prüfungen und physische Sicherheitskontrollen durchgeführt, etwa zu Passwörtern, Verschlüsselung, Zugriffsschutz und Mitarbeitendenverhalten.

Die Analyse ergab verschiedene Schwachstellen. Kritische Probleme wie unzureichende physische Sicherungen, veraltete Software oder fehlende Sperrmechanismen wurden sofort behoben. Hoch eingestufte Sicherheitslücken – unter anderem schwache Passwörter oder fehlerhafte Konfigurationen – wurden zeitnah adressiert. Mittlere und niedrigere Schwachstellen, etwa in der Netzwerksegmentierung oder beim Sichtschutz, wurden schrittweise bearbeitet. Parallel wurden organisatorische Maßnahmen gestärkt, darunter Sensibilisierungstrainings zu Social Engineering, klare Verhaltensregeln und Übungen zu Reaktionsabläufen bei Sicherheitsvorfällen. Zudem wurde ein Notfallhandbuch in Auftrag gegeben.

Die Untersuchungen führten zu deutlichen Fortschritten im Sicherheitsreifegrad. Das IT-Sicherheitsmanagement erreichte ein deutlich höheres Niveau, ebenso das Identitäts- und Zugangsmanagement. Die Ergebnisse zeigen, dass mit zunehmender Digitalisierung auch die Folgen eines möglichen Cyberangriffs wachsen und daher ein hohes Sicherheitsniveau notwendig ist.

Im Bereich mobiler Geräte wurden einige hoch-, mittel- und niedrig priorisierte Schwachstellen festgestellt, während grundlegende Schutzmechanismen wie BitLocker funktionierten. Social-Engineering-Tests offenbarten mehrere kritische und hochgradige Risiken, etwa offenen Zugang zu Technikbereichen. Im internen Netzwerk wurde eine schwerwiegende Schwachstelle durch veraltete Software gefunden, die eine vollständige Kompromittierung ermöglichen konnte, sowie weitere hoch- bis niedriggradige Probleme wie unsichere Verschlüsselungsalgorithmen oder unzureichende Netztrennung.