Finanziert von der Europäischen Union
NextGenerationEU

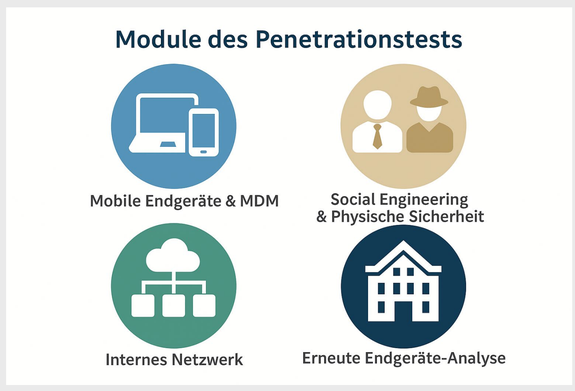
Landesamt für Gesundheit
und Arbeitsschutz
Nordrhein-Westfalen

Überprüfung der organisatorischen und technischen Resilienz des Gesundheitsamtes gegen Cyberangriffe

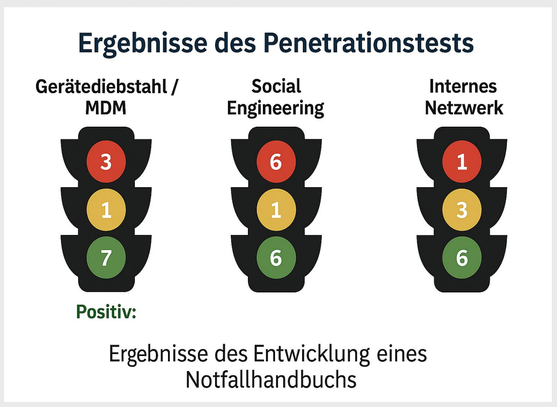
Je digitaler das Arbeiten im Öffentlichen Gesundheitsdienst wird, desto größer sind die potenziellen Datenverluste bei einem Ausfall oder Angriff auf die IT-Infrastruktur.

Hintergrund und Zieldimensionen

- Der ÖGD in Bochum hat im Rahmen des Paktes für den öGD ein IT-S Start-up mit einer vierstufigen Sicherheitsanalyse beauftragt:
- **Diebstahl-Szenario & Prüfung mobiler Dienstgeräte (iPhone, iPad, Laptop)**
  Social-Engineering-Test an drei Standorten
  Interner Netzwerk-Penetrationstest
  Erneute Bewertung mobiler Endgeräte (MDM)
- **Gesamtdimension:**
  Sicherstellung der Informationssicherheit (Vertraulichkeit, Integrität, Verfügbarkeit) und Aufbau eines belastbaren Sicherheitsniveaus im digitalen Transformationsprozess.



Quelle: Eigene Darstellung



Quelle: Eigene Darstellung

Maßnahmen und Methoden

Blackbox- und Greybox-Penetrationstests
(u. a. nach Stand der Technik, NIST, OWASP, gängigen Angriffsvektoren)

- **MDM-Konfigurationsanalyse** auf iOS-Geräten

Technische Prüfungen

- Schwache Passwörter, Unsichere Verschlüsselung, Gerätediebstahl-Szenario, Man-in-the-Middle-Angriffe, Weboberflächen-Analysen (XSS, Authentifizierung)

Physische Sicherheitsüberprüfung

- Zugangskontrollen, Verhalten von Mitarbeitenden, Dokumentenschutz

Social-Engineering-Simulationen

- Vorwandtests, Batch-Dateien / Malware-Simulation, Angriffe in öffentlich zugänglichen Bereichen

Stufensprünge im Reifegrad

- IT-Sicherheitsmanagement von 1 auf 4
- Umgang mit IT-Sicherheitsrisiken/ Angriffen von 1 auf 2
- Identitäts- und Zugangsmanagement von 1 auf 4

Hauptbefunde

1. Gerätediebstahl / MDM
3 × Hoch: z.B. Schwache Geräte-Codes möglich
1 × Mittel: z.B. Unkontrollierte VPN-Profile möglich
7 × Niedrig: z.B. fehlende Sichtschutzfolien
Positiv: BitLocker & BIOS-Schutz wirksam

2. Social Engineering
6 × Kritisch: z.B. Offener Zugang zu Serverschränken
1 × Hoch: z.B. Verkeilte Außentür/Kellertür
4 × Niedrig: z.B. Drucker-Login-Verfahren

3. Internes Netzwerk
1 × Kritisch: z.B. Veraltete Software → Remote Code Execution → vollständige Systemkompromittierung
3 × Hoch: z.B. Unsichere Verschlüsselungsalgorithmen
6 × Mittel: z.B. Unzureichende VLAN-Trennung im Gäste-WLAN
1 × Niedrig: z.B. SSH-Passwort-Login aktiv

Ergebnisse und Schlussfolgerungen

Kritische Schwachstellen wurden sofort behoben
Physische Zutrittssicherung (Serverschränke, Türen, Räume), Veraltete Software sofort patchen, PC-Sperrmechanismen und Passwortsicherheit erzwingen

Hoch eingestufte Schwachstellen wurden zeitnah adressiert
Starke Passwörter, sichere Verschlüsselung, Konfigurationsfehler in MDM, Telefonen, Servern

Mittlere und niedrige Schwachstellen wurden sukzessive behoben
Netzsegmentierung, IDS/IPS, Druckermanagement, Sichtschutz, Zertifikatsmanagement

Awareness und Organisationsmaßnahmen wurden und werden weiterhin gestärkt
Schulungen zu Social Engineering, Klare Verhaltensregeln (Sperren von PCs, Umgang mit Besuchern), Incident Response Szenarien simulieren

Beauftragung der Entwicklung eines Notfallhandbuches

Korrespondenzadresse:
Gesundheitsamt der Stadt Bochum
Telefon: 0234 910 3201
E-Mail: gesundheitsamt@bochum.de

STADT BOCHUM