Stadt Laatzen
Der Bürgermeister

Laatzen, den 10.02.2022

Mitteilung
- öffentlich -

Beratungsfolge: **Drucksachen-Nr.: 2022/024/1**

Ausschuss für Wirtschaft, Vermögen, Digitalisierung	am 15.02.2022	TOP:

Erfolgreiche Digitalisierung braucht Schutz vor Cyber-Kriminalität
- Anfrage der Gruppe SPD-Grüne-Linke im Rat
- Stellungnahme der Verwaltung

Die Anfrage der Gruppe SPD-Grüne-Linke im Rat zum Schutz vor Cyberkriminalität wird wie folgt beantwortet:

(1) Welche technischen, organisatorischen und personellen Maßnahmen (TOP-Prinzip) wurden zur Abwehr von IT-Sicherheitsrisiken ergriffen?

- Es wurde ein IT-Sicherheitsbeauftragter bestellt
- Es wurde eine IT-Sicherheitsrunde eingerichtet (Beteiligte: Prozess/Organisation, IT, IT-Sicherheit)
    - Protokolle an DSB Puschmann
- Es sind diverse technische Maßnahmen zur Abwehr von Cyber-Angriffen aktiv
    - Präventive Maßnahmen zur Vermeidung einer Schadsoftware-Infektion
        - E-Mail-Sicherheit (PDF-Umwandlung von Office-Dok. / Nur-Text-Darstellung / div. Anti-Virus und –Spam Automatismen / etc.)
        - Netzwerksicherheit (USB-Sperre / 2-Faktor-VPN / VLAN / etc.)
        - Administration (Einschränkung von Admin. Rechten / Protokollierung / Einführung einer Access-Rights-Management Software / etc.)
        - etc.
    - Maßnahmen zur Erkennung von Angriffen
        - Automatisches Server Monitoring
        - Aktivitätserkennung (autom. Erkennung und Stopp von Ransomware-Aktivitäten)
        - Etc.

Vorlage gefertigt von	SV Team	Mitzeichnungen			
Diktatz.: 10 LPs					

Besteht ein Notfallplan und wenn ja, innerhalb welcher Zeit können organisatorische und technische Maßnahmen zur Wiederherstellung des Betriebes umgesetzt werden?

- Es bestehen Notfall- und Wiederanlaufpläne für zentrale Anwendungen und Systeme
- Es besteht ein übergeordneter Disaster-Recovery-Plan (DRP)
- Ein IT-Notfallhandbuch, ist in Bearbeitung (inkl. Überarbeitung / Aktualisierung des DRP)
- Zeiträume unterscheiden sich je nach Art eines Sicherheitsvorfalls. Abläufe zu Identifikation von Sicherheitsvorfällen und Einleitung technischer und organisatorischer Maßnahmen werden im IT-Notfallhandbuch beschrieben.

(2) Werden regelmäßig IT-Notfallübungen durchgeführt, um sicherzustellen, dass die Verwaltung auch bei einem Ausfall der IT handlungsfähig bleibt?

- Verwaltungsweite IT-Notfallübungen finden noch nicht statt
- IT-interne Notfallübungen finden individuell geplant statt
- Überprüfungen der Wiederherstellbarkeit von Datensicherungen finden automatisiert laufend statt
- Recovery-Simulationen finden individuell geplant statt (derzeit ca. jährlich)

(4) Werden die Mitarbeiter der Verwaltung regelmäßig zur Abwehr von Sicherheitsrisiken aus z.B. Spam und Phishing geschult und sensibilisiert?

- Regelmäßige Information und Sensibilisierung über internen Blog - Bereitstellung des Behörden-Sicherheitstrainings (Bits)
- Bereitstellung interner E-Mail-Sicherheitshinweise
- Automatische Warnung vor externen Mails mit Verweis auf interne E-Mail-Sicherheitshinweise
- Angebot zur regelmäßigen direkten Sensibilisierung über Teambesprechungen in Vorbereitung
- Gezielte Sensibilisierung spezieller Fachteams in Vorbereitung (Bsp. Social-Engineering bei direkten Bürgerkontakt im Bürgerbüro)

(5) Ergeben sich aus der zunehmenden Arbeit im Home-Office zusätzliche Risiken? Wie wird diesen entgegnet?

- Die Stadt Laatzen verfügte bereits vor Beginn der Pandemie über eine technisch und organisatorisch geregelte Vereinbarung zum HomeOffice. Im Zuge des gestiegenen Bedarfs wurden die betreffenden Ressourcen erweitert
- Die Vereinbarung wurde überarbeitet. Zur Risikominimierung beinhaltet diese auch eine Umstellung auf Thin-Client-Technologie (Technische Umstellung in Vorbereitung)

(6) Werden die IT-Infrastrukturen durch Sicherheitsanalysen externer Spezialisten regelmäßig geprüft?

- Keine Regelmäßigkeit
- Letzte Analyse:
  - AD-Schwachstellenanalyse 10/2021

Im Auftrag

Stefan Zeilinger