WBD news 04/2023

Cyberangriffe als Risiko für die Wirtschaftsbetriebe Duisburg

Liebe Kolleginnen und Kollegen,

laut neusten Studien, war jedes dritte Unternehmen in Duisburg bereits Opfer eines Cyberangriffs. Bei diesen Angriffen wurde meist versucht, Daten durch Phishing-Mails zu stehlen.

Cyberangriffe können zu Ausfallzeiten und damit verbundenen Serviceunterbrechungen unserer Dienstleistungen am Bürger, Datenverlust oder Manipulationen, Imageverlust sowie monetären Verlusten aufgrund Lösegeldern führen. **Alle Beschäftigten** der Wirtschaftsbetriebe sollten der IT-Sicherheit im Unternehmen eine hohe Bedeutung entgegenbringen und bei der Nutzung von Anwendungen entsprechende Regelungen beachten.

In letzter Zeit wurden Beschäftigte von Behörden und Einrichtungen des Landes gezielt – teilweise auch privat – angegriffen, um in interne Netzwerke einzudringen, wie z.B. beim Cyberangriff auf die Universität Duisburg-Essen. Gemäß Presseberichterstattung hatten unbekannte Hacker im Dezember 2022 Systeme der Uni lahmgelegt und Lösegeld gefordert. Es kam in der Folge zu gravierenden Problemen für den Lehr- und Forschungsbetrieb. Die Behebung der Schäden soll noch bis zum Sommer 2023 andauern. Auch bei direkten Vertragspartnern der Wirtschaftsbetriebe wie z.B. Heubeck AG, SSI Schäfer Shop GmbH und Technolit GmbH waren Cyberangriffe erfolgreich und führten zu erheblichen Störungen im Geschäftsbetrieb.

Mit dieser WBD news möchten wir erneut auf die besondere risikobehaftete Lage hinweisen und vor Angriffen mit Schadsoftware, die oftmals über E-Mail-Anhänge oder -Links verteilt werden, warnen. Bitte beachten Sie in diesem Zusammenhang die generellen Verhaltensregeln im Zusammenhang mit der IT-Sicherheit, um die Wirtschaftsbetriebe Duisburg und sich selbst zu schützen.

Vorsicht ist bei allen E-Mails geboten, die

1. von **unbekannter Quelle** stammen und einen **Anhang** enthalten. Hierbei wird meist aus Gründen der **Dringlichkeit** (z.B. Handlung muss zwingend heute abgeschlossen werden) oder der **Wichtigkeit** (z.B. direkte Anweisung des Vorstands) zum Öffnen der manipulierten Anlage aufgefordert. Diese Gründe können auch emotional behaftet sein, wie beispielsweise, dass etwas mit der eigenen Gehaltsabrechnung nicht stimmen würde.

2. auf **externe Seiten** leiten, auf denen **Zugangsdaten** eingegeben werden sollen. Besondere Vorsicht gilt auch dann, wenn die E-Mail von einem vermeintlich bekannten Kontakt verschickt wurde. Hierzu gehören auch allgemein bekannte Absender wie z.B. die IT oder die Unternehmenskommunikation.

Wirtschaftsbetriebe DUISBURG

Bei Nachfragen wenden Sie sich bitte an die IT-Koordination im Fachbereich.

3. auf externe Seiten leiten, von denen eine **Datei heruntergeladen** werden soll. Hier gilt, jede Datei (z.B. *.jpg, *.pdf) kann potentiell einen Schadcode enthalten und sollte daher nicht heruntergeladen und ausgeführt werden.

   ⇨ Wenn Sie unsicher sind, ob eine E-Mail bzw. deren Inhalt potentiell gefährlich ist, können Sie z.B. folgendes tun: Prüfen Sie Absenderadresse, Mailtext und Ziel des Hyperlinks genau, bevor Sie Anhängen oder Hyperlinks vertrauen. Bewegen Sie die Maus über den Hyperlink **ohne** zu klicken, dann sehen Sie wohin der Hyperlink wirklich führen würde.

Möchten Sie Ihre Kenntnisse zur IT-Sicherheit bzw. zum Umgang mit E-Mails weiter vertiefen, können Sie das mit folgendem praktischen Training (BITS – Behörden-IT-Sicherheitstraining (E-Mail)
https://www.bits-training.de/training/030-lektion-e-mail/
oder mit dem (Phishing-Quiz)
https://phishingquiz.withgoogle.com/?hl=de

Im Zweifel sprechen Sie bitte Ihre IT-Koordination und/oder die Beschäftigten aus dem Fachbereich WBD-T 23 an.

Übrigens sind diese einfachen Regeln auch sehr hilfreich für Ihren privaten Umgang mit E-Mails bzw. für die IT-Sicherheit Ihrer privaten Geräte.

Duisburg, den 06.01.2023

Thomas Patermann
Sprecher des Vorstands

i. A.

Andreas Benstem
Geschäftsbereichsleitung
Technische Services

Wirtschaftsbetriebe Duisburg

Bei Nachfragen wenden Sie sich bitte an die IT-Koordination im Fachbereich.