

Informationsvorlage	
- öffentlich -	
MI-11/2024	
Fachbereich	Dezernat I
Federführendes Amt	Fachdienst Informationstechnik und digitale Verwaltung
Datum	03.04.2024

Beratungsfolge	Termin	Beratungsaktion
Kreistag	29.04.2024	

Betreff:

Cybersicherheit

- Große Anfrage der AfD-Fraktion

Mitteilung / Information:

Frage 1:

„Wie viele Cyber-Angriffe auf IT-Systeme der Kreisverwaltung und kreiseigenen Einrichtungen gab es seit dem 01.01.2021? (Bitte aufschlüsseln nach Jahr, Abteilung und Straftatbeständen)“

Antwort:

Eine Beantwortung der Frage in der gewünschten Form ist nicht möglich, da entsprechende Jahresdaten nicht vorliegen. Aus der Datensicherung der jeweiligen Jahre wurde jeweils ein Zeitraum von 50 Tagen analysiert und auf einen allgemeinen Jahresdurchschnittswert über alle vier Jahre hochgerechnet.

Folgende Kategorien wurden gebildet:

- Blockierte Malware mit Ziel eines PC's – 137 Vorfälle jährlich
- Blockierte Angriffe/Anomalien mit Ziel eines PC's – 1.252 Vorfälle jährlich
- Blockierte eingehende E-Mails – 624.491 Vorfälle jährlich
- Blockierte Malware mit Ziel aus dem Internet erreichbare Server – 834 Vorfälle jährlich
- Blockierte Angriffe/Anomalien mit Ziel eines aus dem Internet erreichbaren Servers – 7.030 Vorfälle jährlich
- Blockierte Versuche von Botnetzen, auf aus dem Internet erreichbare Server zuzugreifen – 32 Vorfälle jährlich

Frage 2:

„In wie vielen Fällen konnten die konkreten Angreifer ermittelt werden? (Bitte aufschlüsseln nach Jahr, Abteilung und Straftatbeständen)“

Antwort:

Konkrete Angreifer sind nicht bekannt.

Frage 3:

„In wie vielen Fällen haben derartige Angriffe zu einer Beeinträchtigung des Betriebsablaufs geführt? (Bitte aufschlüsseln nach Jahr, Abteilung)“

Antwort:

Im März 2021 kam es zu einem Angriff auf den Microsoft Mail Exchange Server der Kreisverwaltung. Dies führte von Freitag bis Sonntag zu einem Ausfall der E-Mail-Erreichbarkeit auf allen Endgeräten und Mobiltelefonen der Kreisverwaltung.

Frage 4:

„Welche Maßnahmen zur Erhöhung der IT-Sicherheit wurden innerhalb dieser Zeit umgesetzt, um das Risiko eines erfolgreichen Cyberangriffs zu minimieren?“

Antwort:

Die Sicherheitsrichtlinien der Firewall werden laufend nachjustiert, die Erreichbarkeit von Servern aus dem Internet wurde auf ein Mindestmaß reduziert, die Mitarbeiterschaft wurde zu einem jährlichen IT-Sicherheitstraining verpflichtet und die Stelle des Informationssicherheitsbeauftragten im Jahr 2023 neu geschaffen. Darüber hinaus wurde ein externer Dienstleister mit der 24/7 Überwachung der IT-Systeme und Netzwerke beauftragt, um in Echtzeit potentielle Sicherheitsbedrohungen und Cyberangriffe erkennen und abwehren zu können.

Frage 5:

„Welche weiteren Maßnahmen zur Erhöhung der IT-Sicherheit sind in Umsetzung oder geplant, um die Wahrscheinlichkeit eines erfolgreichen Cyberangriffs weiter zu minimieren?“

Antwort:

Der Landkreis Waldeck-Frankenberg strebt eine Zertifizierung nach dem BSI-IT-Grundschutz an.

Frage 6:

„Welche Institutionen unterstützen bei Bedarf die Kreisverwaltung?“

Antwort:

Bei einem Cybersicherheitsvorfall würde der Landkreis Waldeck-Frankenberg von folgenden Institutionen unterstützt:

- Polizeidirektion Waldeck-Frankenberg
- Hessen3C Cyber Competence Center
- BSI (Bundesamt für Sicherheit in der Informationstechnik)
- Zentrale Ansprechstelle Cybercrime Hessen
- Hessischer Datenschutzbeauftragter
- Externe Dienstleister abhängig vom spezifisch betroffenen Produkt
- ekom21

Frage 7:

„War oder ist der Landkreis Waldeck-Frankenberg Mitglied im Cybersicherheitsrat Deutschland e.V.?“

Antwort:

Nein.

Anlage(n):

AfD Große Anfrage Cybersicherheit