Region der Zukunft
Landkreis Darmstadt-Dieburg

Fraktionsvorlage

Vorlage-Nr.: **2931-2020/DaDi**
Aktenzeichen: 029-013

Fachbereich: Fraktion der Alternative für Deutschland
Seiler, Ulf, Prof.

Beteiligungen:

Produkt: **1.01.01.02 Gremienmanagement**

Beschlusslauf:

Nr.	*Gremium*	*Status*	*Zuständigkeit*
1.	Kreistag	Ö	Zur Kenntnisnahme

Betreff: **Cyber-Angriffe – Anfrage AfD**

Anfrage der Fraktion der AfD:

Während der letzten Wochen wurden mehrere Cyber-Angriffe in Hessen bekannt. Unter anderem wurden die Universität Gießen sowie die Städte Frankfurt, Bad-Homburg und Alsfeld Opfer solcher Angriffe.

Im Juli 2019 waren mehrere Krankenhäuser und Einrichtungen des DRK in Rheinland-Pfalz und dem Saarland von Cyber-Angriffen betroffen. Auch in Bayern wurden in den letzten Jahren Angriffe auf Kliniken bekannt (z. Bsp. Fürstenfeldbruck).

2017 wurde bekannt, dass das Computersystem des MVZ Ober-Ramstadt durch einen Hackerangriff lahmgelegt wurde.

Die AfD-Fraktion stellt die folgenden Fragen:

1. Wie viele Cyber-Angriffe gegen kommunale Einrichtungen wurden seit dem Jahr 2017 im Landkreis Darmstadt-Dieburg festgestellt?

   Die Zahl ist nicht quantifizierbar. Die Systeme der Kreisverwaltung werden dauerhaft von außen „angegriffen". Unsere Schutzsysteme wie z.B. Firewall, Mailgateway usw. „machen ihren Job" und blocken diese Angriffe.

   Im Web-Umfeld werden ständig – den Access-Logs nach zu urteilen - oft mehrmals täglich - Versuche unternommen, Schwachstellen und Einfallstore auszumachen.

   Dieses Phänomen beschränkt sich nicht auf öffentliche Einrichtungen sondern ist in der Regel internetweit bei allen Webservern zu beobachten.

   Üblicherweise wird automatisch versucht, mit Default-Zugangsdaten auf Backends von häufig genutzten Webapplikationen zuzugreifen (phpmyadmin, wordpress, typo3 etc.)

   Erfolgreich waren solche Angriffe was die System der Kreisverwaltung betrifft bisher nicht.

2. Welcher Natur waren diese Cyber-Angriffe?

   - *Brute-Force-Attacken bei häufig genutzten Web-Applikationen (s.o.)*
   - *Denial-of-Service-Attacke via SQL-Injection im GET-Parameter der Webanwendung.*
   - *Portscans auf die von außen erreichbare System*
   - *Schadsoftware per Mail*

3. Welche Kommunen, Verwaltungen (inklusive Kreisverwaltung) sowie kommunale Einrichtungen waren konkret betroffen? Bitte aufschlüsseln nach Jahren seit 2017.

   Systeme der Kreisverwaltung (Für andere Institutionen ist der Fachbereich 222 nicht zuständig)

4. Wie viele Cyber-Angriffe konnten erfolgreich abgewehrt werden? Bitte aufschlüsseln nach Jahren seit 2017 und betroffenen Einrichtungen.

   Die Zahl ist nicht quantifizierbar (siehe Punkt 1)

5. Wie viele Cyber-Angriffe waren „erfolgreich“? Bitte aufschlüsseln nach Jahren seit 2017 und betroffenen Einrichtungen.

   Ein erfolgreicher Angriff auf das BürgerGIS Portal im September 2019.

6. Welche konkrete Schäden resultierten aus den Cyber-Angriffen?

   Die Bürger des Landkreises konnten mehrere Stunden das BürgerGIS Portal nicht nutzen, weil die Datenbank ausgelastet war und somit die Webseite nicht mehr reagiert hat.

   Der Software-Hersteller wurde kontaktiert und dieser hat umgehend die Sicherheitslücke behoben. Außerdem wurde die IP des Angreifers gesperrt.

7. Welche konkreten Vorsichtsmaßnahmen wurden nach dem Angriff auf das MVW in Ober-Ramstadt, und werden nach Bekanntwerden der aktuellen Cyber-Angriffe gegen hessische Kommunen und die Universität Gießen zum Schutz der IT-Systeme in den Kommunen, kommunalen Einrichtungen und Verwaltungen des Landkreises getroffen?

   Anlassbezogen wurden keine konkreten Maßnahmen initiiert.

   Die Mitarbeiter der Kreisverwaltung werden schon seit Jahren zu diesem Thema sensibilisiert. U.a. gab es hierzu Infoplakate im Kreishaus, Warnungen/Aufklärungen im Intranet, Schulungsvideos sowie Vorträge.

   Die Schutzsysteme (z.B. AnitVirus) werden auf einen aktuellen Stand gehalten und die etablierten Maßnahmen (z.B. die nicht Zustellung von ausführbaren Dateien und veralteten Office Dokumenten) werden ständig auf Aktualität und Sinnhaftigkeit überprüft und ggf. angepasst.

   Unsere Web-Infrastruktur ist auf Grund einer DMZ, SSH-Verschlüsselung, komplexen Passwörtern, Firewall gut geschützt.

   Sobald Sicherheitslücken bekannt werden, überprüfen wir unser System auf diese Lücken und schließen diese ggf. nach vorliegenden „Best Practices“ des BSI.

8. Wurden und werden zum Schutz der IT-Systeme externe Berater bzw. externe Unternehmen

eingesetzt?

Es wurde ein Sicherheitsaudit durch die ekom21 durchgeführt.
Turnusmäßig werden die IT-Systeme von unseren externen Dienstleister im Rahmen der Wartung auf IT-Sicherheit getestet.

9. Falls Frage 8 mit „ja“ beantwortet wird, wie hoch belaufen sich die Kosten? Bitte aufschlüsseln nach Jahren seit 2017.

   Die Kosten lassen sich nicht explizit aufschlüsseln, weil diese Tätigkeiten im Rahmen der Wartungsverträge inkludiert sind.

10. Falls Frage 8 mit „nein“ beantwortet wird, warum nicht?

    Entfällt. Siehe Antwort zu Frage 9.