BÜNDNIS 90/DIE GRÜNEN, Adolfstr. 67, 65307 Bad Schwalbach

Herrn Kreistagsvorsitzenden
André Stolz
Heimbacher Str.7
65307 Bad Schwalbach

BÜNDNIS 90
DIE GRÜNEN
RHEINGAU-TAUNUS

Kreistagsfraktion
Adolfstr. 67
65307 Bad Schwalbach
✆ 06124 / 720 060
gruene-rtk-fr@online.de

Bad Schwalbach, den 22.08.2021

28/21

Antrag: IT-Sicherheit der kritischen Verwaltungsinfrastruktur

25/08/2021

Sehr geehrter Herr Kreistagsvorsitzender Stolz,

bitte nehmen Sie den nachstehenden Antrag mit auf die Tagesordnung der nächsten Kreistagssitzung.

Mit freundlichen Grüßen

Günter Linke

Günter Linke
Fraktionsvorsitzender

Antragstext:

Die Kreisverwaltung wird beauftragt, einen Penetrationstest der Verwaltungs-IT-Systeme durchführen zulassen. Dieser soll extern erfolgen und sich auf die kritische Infrastruktur konzentrieren.

Zur kritischen Infrastruktur zählen in diesem Zusammenhang das Kreisgesundheitsamt, der Katastrophenschutz und dessen Warnsysteme sowie die Rettungsleitstelle.

Anschließend soll dem Kreistag ein Bericht über die Ergebnisse des externen Penetrationstest vorgelegt werden.

Begründung:

Mitte Juli dieses Jahres berichtete der *Wiesbadener Kurier* über einen erfolgreichen Trojaner-Angriff auf die Verwaltung der Stadt Geisenheim.[1] Im Anschluss wurde von massiven Beeinträchtigungen des Verwaltungsbetriebs berichtet. Die Auswirkungen waren auch für andere Kommunen spürbar. Ein schwerwiegenderer Vorfall traf im Juli den bayrischen Landkreis Anhalt-Bitterfeld. Dort wurde durch einen Trojaner-Angriff der Verwaltungsbetrieb kreisweit lahmgelegt. Der Landrat sah sich gezwungen den „Cyber-Katastrophenfall" auszurufen.[2] Diese beiden Vorfälle illustrieren, dass kommunale Verwaltungen immer mehr ins Visier von Hacker*innen gelangen oder zumindest zum „Kollateralschaden" eines großflächigen Angriffs werden können.

Es gibt keine sicheren IT-Systeme, sondern nur solche, deren Schwachstellen unbekannt sind. Entscheidend im Kampf gegen IT-Kriminalität ist folglich, wer die Schwachstellen zuerst aufdeckt. Hier setzten externe Penetrationstests an.

Im Rahmen von externen Penetrationstests wird ein Team von IT-Sicherheitsexpert*innen beauftragt, gezielt nach Angriffsvektoren im IT-System zu suchen. Aufgedeckte Angriffsvektoren werden anschließend dokumentiert oder direkt – in Zusammenarbeit mit der Verwaltung – geschlossen. Vereinfacht dargestellt simuliert ein externer Penetrationstest einen gezielten Hackerangriff, nur dass die gefundenen Schwachstellen nicht ausgenutzt, sondern „verantwortungsvoll offengelegt" (*responsible disclosure*) werden.

Externe Penetrationstests werden unter anderem von TÜV Rheinland angeboten.[3] Hier variieren die Kosten – je nach Umfang – zwischen 2000 und 7000 EUR. Diese Kosten stellen allerdings in keinem Verhältnis zu den Kosten, die anfallen, wenn die Verwaltung durch einen böswilligen Hackerangriff wochenlang lahmgelegt würde. Weiterhin gilt es zu berücksichtigen, dass die Kosten-Nutzen-Ratio bei Penetrationstests tangential verläuft und entsprechend schon für geringe Kosten ein großer Nutzen entsteht, der mit steigenden Kosten sukzessive aus dem Verhältnis gerät.[4]

---

[1] https://www.wiesbadener-kurier.de/lokales/rheingau/geisenheim/edv-netz-der-stadt-geisenheim-gehackt_24110761

[2] https://www.br.de/nachrichten/netzwelt/hacker-legen-anhalt-bitterfeld-lahm-sind-bayerns-aemter-sicher,Sd9LmmW

[3] https://www.tuv.com/germany/de/penetrationstest-und-it-sicherheitsanalyse.html

[4] https://turingpoint.de/en/blog/cost-and-pricing-for-a-pentest/