

Anfrage

der Abgeordneten Katharina Kucharowits,

Genossinnen und Genossen

an den Bundesminister für Inneres

betreffend Vorbereitung auf Cyberangriffe innerhalb der österreichischen Bundesverwaltung

Die Gefahren von Cyberkriminalität werden von vielen immer noch extrem unterschätzt, zu diesem Schluss kommt eine Studie von KPMG, über die der ORF ÖO im April diesen Jahres berichtete (<https://ooe.orf.at/stories/3153580/>). Dass Cyberattacken – auch aufgrund der Covid-19 Pandemie und der Verlagerung großer Teile des täglichen Lebens ins Virtuelle – rasant zunehmen werden, davor warnten die Vereinten Nationen bereits im Mai 2020 (<https://unicri.it/news/cyber-crime-during-covid-19-pandemic>).

Dabei betreffen Cyberangriffe und Cyberkriminalität längst nicht mehr nur große, medial präsente Unternehmen in Wirtschaft und IT. Neben kleineren Unternehmen und Einzelpersonen geraten auch öffentliche Einrichtungen immer mehr ins Blickfeld der Angreifer*innen.

So sorgte Anfang 2020 ein breitflächig angelegter Cyberangriff auf das österreichische Außenministerium für großes Aufsehen. Erst nach Wochen konnte die virtuelle Gefahr eingedämmt werden. Weitere Cyberangriffe auf die öffentlichen Verwaltungen von Bundesländern und Gemeinden in den vergangenen zwei Jahren zogen ähnliche Folgen nach sich: Wochenlange Unsicherheit, Chaos und vor allem Gefahr. Denn Cyberattacken können über den immanenten, rein virtuellen Angriff hinaus zu einer ganzen Reihe praktischer Schäden führen. So könnten Angriffe auf sensible Daten von Bürger*innen dazu führen, neben der enormen Verletzung des Datenschutzes und damit einhergehender Missbrauch, dass notwendige finanzielle Leistungen wie das Arbeitslosengeld oder die Mindestsicherung nicht ausbezahlt werden können. Oder wie zuletzt ein Fall in Frankreich, bei dem ein Krankenhaus nahe Paris Ziel eines großflächigen Angriffs war und hunderte Patient*innen in teils lebensbedrohliche Gefahr brachte.

Dass Cyberkriminalität auch für die öffentliche Verwaltung eine ernstzunehmende Priorität sein sollte, zu diesem Schluss kommt auch ein Rechnungshofbericht aus dem April 2022. Während die Prüfer*innen die Cyberattacke auf das Außenministerium als „grundsätzlich erfolgreich“ bewerten, sehen sie zeitgleich jedoch eine ganze Reihe an „To-Dos“, um öffentliche Stellen auf künftige Angriffe vorzubereiten (<https://bit.ly/3cEOpHK>).

In Anbetracht dieser Entwicklungen und auf Basis des Berichts des Rechnungshofes stellt sich die Frage, wie gut die Ressorts der österreichischen Bundesregierung tatsächlich für den virtuellen Ernstfall gewappnet sind.

Die unterfertigten Abgeordneten stellen daher folgende

ANFRAGE

1. Gab es in Ihrem Ressort bereits Cyberangriffe?
 - a. Falls ja, bitte um detaillierte Schilderung des Angriffs/der Angriffe, welche Schäden daraus resultierten und welche Gegenmaßnahmen ergriffen wurden?

2. Welche Rolle und welche konkreten Aufgaben fallen Ihrem Ressort in der gesamtstaatlichen Bekämpfung von Cyberkriminalität zu?
3. Ergreift Ihr Ressort aktiv konkrete Maßnahmen, um sich präventiv gegen Cyberattacken und Cyberkriminalität angemessen zu schützen?
 - a. Falls ja, welche Maßnahmen sind das im Detail?
 - b. Falls ja, wird in der Vorbereitung auf einen potenziellen Cyberangriff auch die Expertise externer Expert*innen, etwas Personen auf Wissenschaft oder Zivilgesellschaft, hinzugezogen?
 - c. Falls nein, warum gibt es keine Pläne, sich für den Ernstfall eines potenziellen Cyberangriffs zu schützen?
4. Durch die unterschiedlichen Zuständigkeitsbereiche aller Ressorts der Bundesregierung ergeben sich auch unterschiedliche Risiken in Bezug auf Cyberangriffe, beispielsweise wird es im Bundesministerium für europäische und internationale Angelegenheiten aller Wahrscheinlichkeit nach andere Herausforderungen und Risiken in Bezug auf Cyberkriminalität geben als beispielweise im Bundesministerium für Justiz.
 - a. Gab es eine ressortspezifische Risikoanalyse in Ihrem Ressort?
 - i. Falls nein, warum nicht?
 - b. Welche konkreten Maßnahmen setzen Sie, um den spezifischen Risiken Ihres Ressorts gerecht zu werden?
5. Gibt es eine Person oder einen Personenkreis in Ihrem Ressort, die dezentriert als „Cybersicherheitsbeauftragte(r)“ fungiert/fungieren?
 - a. Falls ja, über welche Expertise verfügt/verfügen diese Person(en)?
 - b. Falls nein, warum gibt es keine(n) „Cybersicherheitsbeauftragte(n)“ in Ihrem Ressort?
6. Bietet Ihr Ressort spezielle Trainings, Webinare, Kurse etc. an, um alle Mitarbeiter*innen im Umgang mit potenziellen Cyberangriffen und der daraus resultierenden Gefahrenlage zu sensibilisieren?

Die folgenden Fragen ergeben sich aus dem Bericht des Rechnungshofs (<https://bit.ly/3cE0pHK>), der einige Aufholbedarf im Bereich der Cybersicherheit verortet.

7. Der Rechnungshofbericht bemängelt unter anderem, dass Krisen-, Kontinuitäts- und Einsatzpläne in Bezug auf Cybersicherheit gänzlich fehlen. Zum Zeitpunkt der Beantwortung dieser Anfrage, wurden diese von Ihrem Ressort mittlerweile erstellt?
 - a. Falls ja, wurden zur Erstellung dieser Pläne auch externe Expert*innen hinzugezogen?
 - b. Falls nein, wann ist mit der Fertigstellung dieser Pläne in Ihrem Ressort zu rechnen?
8. Der Rechnungshof sah zudem die Etablierung eines permanent verfügbaren Cyber-Einsatzteam („Rapid Response Team“) sowie die Schaffung eines ebenso permanenten Cyber-Lagezentrums zur Bearbeitung von Notfällen als essentiell. Wurden dieses Einsatzteam und das Lagezentrum zum Zeitpunkt der Beantwortung dieser Anfrage bereits geschaffen?
 - a. Falls ja, in welchem Ressort sind diese Strukturen angesiedelt und der Zuständigkeit welcher/welchen Bundesministerin/Bundesministers unterliegen diese?

9. Zudem forderte der Rechnungshof ein regelmäßig zu erstellendes Cyber-Lagebild, um laufende Bedrohungen und potentielle Gefahrenquellen schneller und effektiver zu identifizieren. Wird ein solches Cyberlagedbild in Ihrem Ressort zum Zeitpunkt der Beantwortung dieser Anfrage bereits regelmäßig erstellt?
- a. Falls ja, seit wann wird ein solches Lagebild in Ihrem Ressort erstellt und in welchen Abständen findet das statt?
 - b. Falls nein, warum wird bisher kein Cyber-Lagebild in Ihrem Ressort erstellt und ab wann planen Sie, ein solches regelmäßig zu erstellen?
10. Der Rechnungshof bemängelt weiters, dass zum Ende des Untersuchungszeitraums Ende Mai 2021 das „NIS-Meldeanalysesystem“, dass im Netz- und Informationssystemsicherheitsgesetz (NISG) bereits 2018 beschlossen wurde und im Bundesministerium für Inneres angesiedelt sein soll, noch nicht in Betrieb ist. Das Meldesammelsystem ist zwar seit dem dritten Quartal 2021 etabliert, dabei handle es sich aber nur um eine Vorstufe zum Meldeanalysesystem. Zum Zeitpunkt der Beantwortung dieser parlamentarischen Anfrage, ist das finale Cyber-Meldeanalysesystem bereits im Einsatz?
- a. Falls ja, seit wann ist das finale Meldeanalysesystem im Einsatz?
 - b. Falls nein, warum nicht und ab wann wird das Meldeanalysesystem im Einsatz sein?
11. Wer – welche Stellen der öffentlichen Verwaltung, welche privatwirtschaftlichen Unternehmen, Organisationen etc. waren an der Konzipierung und Ausarbeitung der in Frage 10 erwähnten Meldesammel- bzw. Meldeanalysesysteme beteiligt?
- a. Welche(s) Unternehmen, Organisationen etc. wurde(n) mit der Konzipierung und Ausarbeitung der Meldesammel- bzw. Meldeanalysesysteme betraut? Weshalb wurde(n) diese(s) Unternehmen gewählt?
 - b. Wie hoch waren die Kosten für die Konzipierung und Ausarbeitung der Meldesammel- bzw. Meldeanalysesysteme?
 - c. Wie hoch sind (werden) die laufenden Betriebskosten der Meldesammel- bzw. Meldeanalysesystem (sein)?
 - d. Gab es eine öffentliche Ausschreibung für die Konzipierung und Ausarbeitung dieser Systeme?
 - i. Falls ja, wie viele Unternehmen, Organisationen etc. haben sie für diese Ausschreibung beworben?
 - ii. Falls nein, warum gab es keine öffentliche Ausschreibung dazu?
 - e. Welche Stellen der öffentlichen Verwaltung, Zivilgesellschaft etc. nehmen zum Zeitpunkt der Beantwortung dieser parlamentarischen Anfrage bereits am Meldesammel- bzw. Meldeanalysesystems teil? Gibt es Pläne, auch noch andere Stellen miteinzubinden?
12. Neben dem Meldeanalysesystem soll es ein Frühwarnsystem geben, ebenfalls im Bundesministerium für Inneres angesiedelt. Laut Rechnungshofbericht war dieses Frühwarnsystem 2021 erst in einer ersten Konzipierungsphase, obwohl bereits 2019 Investitionen und 2020 auch schon Betriebskosten dafür veranschlagt wurden.

- a. Zum Zeitpunkt der Beantwortung dieser parlamentarischen Anfrage, ab wann wird das genannte Frühwarnsystem zum Einsatz kommen?
 - b. Wieso wurden – gemäß Rechnungshofbericht und wirkungsorientierter Folgenabschätzung zum NISG – bereits Investitionen bzw. Betriebskosten für ein System veranschlagt, das erst in der ersten Phase der Konzipierung ist?
 - c. Welche(s) Unternehmen, Organisationen etc. wurde(n) mit der Konzipierung und Ausarbeitung des Frühwarnsystems betraut? Weshalb wurde(n) diese(s) Unternehmen gewählt?
 - d. Wie hoch waren die bisherigen Kosten für Konzipierung und Ausarbeitung des Frühwarnsystems? Wie hoch werden die weiteren Kosten für Konzipierung und Ausarbeitung des Frühwarnsystems bis zu Fertigstellung geschätzt sein?
 - e. Wie hoch sind (werden) die laufenden Betriebskosten des Frühwarnsystems (sein)?
 - f. Gab es eine öffentliche Ausschreibung für die Konzipierung und Ausarbeitung des Frühwarnsystems?
 - i. Falls ja, wie viele Unternehmen, Organisationen etc. haben sie für diese Ausschreibung beworben?
 - ii. Falls nein, warum gab es keine öffentliche Ausschreibung dazu?
 - g. Sofern das Frühwarnsystem bereits im Einsatz ist: Welche Stellen der öffentlichen Verwaltung, Zivilgesellschaft etc. nehmen zum Zeitpunkt der Beantwortung dieser parlamentarischen Anfrage bereits am Frühwarnsystem teil? Gibt es Pläne, auch noch andere Stellen miteinzubinden?
13. Schließlich sieht der Rechnungshof bei den „Personalressourcen, um die Cyber-Sicherheit aufrecht zu erhalten“ konkret im Bundesministerium für Inneres großen Aufholbedarf.
- a. Zum Ende des vom Rechnungshof überprüften Zeitraums, nämlich Mai 2021, wie viele Personen waren im Bundesministerium für Inneres deziert im Bereich Cybersicherheit tätig?
 - b. Wurde zum Zeitpunkt der Beantwortung dieser Anfrage bereits zusätzliches Personal im Bereich der Cybersicherheit im Bundesministerium für Inneres aufgenommen?
 - i. Falls ja, wie viele Personen sind zum Zeitpunkt der Beantwortung dieser Anfrage im Bundesministerium für Inneres im Bereich Cybersicherheit tätig?
 - ii. Falls nein, wann planen Sie, mehr Personen für den Bereich Cybersicherheit im Bundesministerium für Inneres einzustellen?

