BASEL LANDSCHAFT
REGIERUNGSRAT

Vorlage an den Landrat

Beantwortung der Interpellation 2022/167 von Christine Frey: «Cybercrime im Kanton Basel-Landschaft»
2022/167

vom 14. Juni 2022

1. Text der Interpellation

Am 24. März 2022 reichte Christine Frey die Interpellation 2022/167 «Cybercrime im Kanton Basel-Landschaft» ein. Sie hat folgenden Wortlaut:

Die Zahl der Cyberangriffe ist 2021 in der Schweiz drastisch gestiegen. Durch die Corona-Pandemie wich die Gesellschaft zunehmend auf die digitale Welt aus - ein perfekter Nährboden für Cyberkriminelle. Die Digitalisierung bietet zwar unzählige Vorteile und eröffnet der Wirtschaft neue Wachstumschancen und Beschäftigungsmöglichkeiten.

Leider bringt die zunehmende Abhängigkeit einer funktionierenden IT-Infrastruktur aber auch grosse Nachteile mit sich: Kriminelle nutzen die IT-Abhängigkeit aus und hacken nicht nur Privatpersonen, sondern auch KMU. Von der kleinen Bäckerfirma bis zum Grossbetrieb mit mehreren Tausend Mitarbeitenden – es kann jeden treffen. Bei einem Hacker-Angriff kann das gesamte Netzwerk eines Unternehmens betroffen sein. Beispielsweise sind Websites nicht mehr erreichbar und vertrauliche Daten gelangen an die Öffentlichkeit. Meist erleiden die Firmen auch finanzielle Schäden. Inzwischen ist jede dritte Firma von solchen Hackerangriffen betroffen, wie eine aktuelle Studie der Hochschule für Wirtschaft der Fachhochschule Nordwestschweiz FHNW zeigt. Der volkswirtschaftliche Schaden, der durch Cyberangriffe auch für KMU entsteht, ist enorm.

Um die Cyberkriminalität wirkungsvoll zu bekämpfen, wurde im Kanton Basel-Landschaft im April 2020 das «Kompetenzzentrum Cybercrime» von Staatsanwaltschaft und Polizei in Betrieb genommen. Cyberdelikte sollen effizient und effektiv verhindert, verfolgt und geahndet werden. Die Strategie basiert auf den vier Pfeilern Aus- und Weiterbildung, Spezialisierung, Prävention und Repression. Während die Prävention fast ausschliesslich eine polizeiliche Aufgabe darstellt, betreffen die drei anderen Schwerpunkte die Polizei und die Staatsanwaltschaft gleichermassen.

Das Kompetenzzentrum Cybercrime ist wichtig für den wirkungsvollen Schutz der regionalen KMU. Daher bitte ich den Regierungsrat, zu prüfen und zu berichten:

1. *wie viele Cybercrime-Fälle seit Inbetriebnahme des Kompetenzzentrums bearbeitet wurden;*
2. *welche Arten von Cyberangriffen registriert wurden;*
3. *wie viele der registrierten Fälle Privatpersonen und wie viele KMU betreffen und*
4. *welche Branchen wie stark betroffen sind;*

5. *wie sich die Corona-Pandemie auf die Cyberaktivität im Kanton Basel-Landschaft ausgewirkt hat;*
6. *ob Homeoffice einen Einfluss auf die Cybercrime-Aktivität hatte und wenn ja, wie sich dieser äusserte;*
7. *ob die kantonale Verwaltung Opfer von Cyberangriffen wurde und wie sich diese generell gegen Cyberangriffe schützt;*
8. *ob die Seite «Kompetenzzentrum Cybercrime» auf der Website des Kantons Basel-Landschaft ansprechender und nutzerfreundlicher gestaltet werden kann (Beispiel Kanton Zürich https://www.zh.ch/de/sicherheit-justiz/delikte-praevention/gefahren-im-internet.html#25031585) und ob geplant ist, dort einen jährlichen Bericht über die Aktivitäten des Zentrums zu veröffentlichen;*
9. *ob aufgrund des Ukraine-Konflikts vermehrt Cyberattacken auf Firmen im Kanton registriert wurden (bspw. in der Energiebranche).*

2. Beantwortung der Fragen

1. Wie viele Cybercrime-Fälle wurden seit Inbetriebnahme des Kompetenzzentrums bearbeitet?

Das Kompetenzzentrum Cybercrime hat per 1. April 2020 seinen operativen Betrieb aufgenommen und ist in die zwei Dienste IT-Forensik und IT-Ermittlung gegliedert. Die Hauptsachbearbeitung von Cybercrimefällen findet vorwiegend im Dienst IT-Ermittlung statt. Innerhalb des Dienstes sind aktuell 3 Mitarbeitende mit der Aufgabe IT-Ermittlung tätig. Aufgrund der geringen Personalressourcen im IT-Ermittlungsbereich bearbeitet das Kompetenzzentrum Cybercrime vorwiegend komplexe Cybercrimefälle.

	2020	**2021**
Anzahl bearbeitete Cybercrimefälle	34	35

Des Weiteren ist anzumerken, dass im Jahre 2020 und 2021 ein Schwergewicht auf die Schulung und Unterstützung der mehreren Hundert Frontmitarbeitenden der Polizei Basel-Landschaft gelegt wurde. Im Bereich der Prävention wurden zudem zahlreiche Präventionsveranstaltungen (Cybercrime und Cybermobbing an den Berufsbildungszentren in Liestal und Muttenz, Cybersecurity in Baselbieter Unternehmen, usw.) durchgeführt.

Auch die Fachstelle Cybercrime der Staatsanwaltschaft ist seit dem 1. April 2020 operativ tätig. Im Zeitraum vom 1. April 2020 bis 31.12.2021 sind insgesamt 252 Anzeigen eingegangen und in Bearbeitung.

2. Welche Arten von Cyberangriffen wurden registriert?

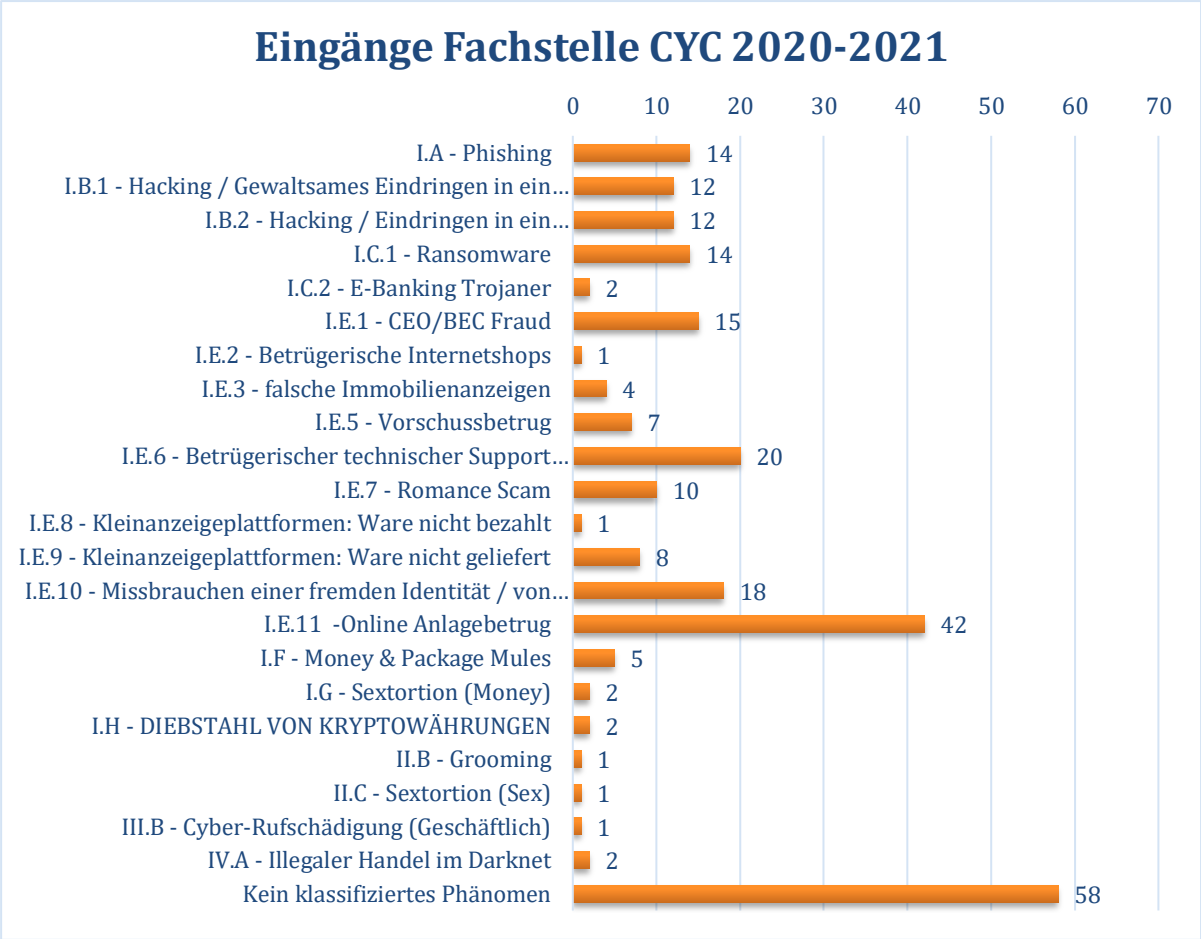
Der Begriff "Cyberangriff" ist ein nicht juristisch definierter Begriff. Gemäss Nationaler Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022 umfasst der Begriff Cyberangriff folgende fünf Kategorien:

1. Cyberkriminalität,
2. Cyberspionage,
3. Cybersabotage und –Terrorismus,
4. Desinformation und Propaganda sowie
5. Cyber in Konflikten.

Im polizeilichen Umfeld ist die Cyberkriminalität in verschiedene Tatvorgehen gegliedert. Für die Jahre 2020 und 2021 wurden die nachfolgenden Cybercrime-Straftaten registriert:

Tatvorgehen	2020	2021
Total	**557**	**826**
Cyber-Wirtschaftskriminalität	**489**	**769**
Phishing	18	33
Hacking: Gewaltsames Eindringen in ein Datenverarbeitungssystem	12	17
Hacking: Eindringen in ein Datenverarbeitungssystem mit fremden Zugangsdaten	24	18
Malware – Ransomware	10	16
Malware – E-Banking Trojaner	0	0
Malware – Spyware	0	1
Malware – Rogueware/Scareware	0	3
Malware – Botnet	0	1
DDoS	0	0
Cyberbetrug	409	645
davon: CEO/BEC Betrug	–	*5*
davon: Betrügerische Internetshops	–	*17*
davon: Falsche Immobilienanzeigen	–	*5*
davon: Vorschussbetrug	–	*23*
davon: Betrügerischer technischer Support	–	*31*
davon: Romance Scam	–	*23*
davon: Kleinanzeigeplattformen – Ware nicht bezahlt	–	*15*
davon: Kleinanzeigeplattformen – Ware nicht geliefert	–	*195*
davon: Missbrauch von Online-Zahlungssyst./Wertkarten oder einer fremden Identität, um einen Betrug zu begehen	–	*284*
davon: Online Anlagebetrug	–	*34*
davon: Anderer Internetbetrug	–	*13*
Money/Package Mules	7	6
Sextortion (money)	9	26
Diebstahl von Kryptowährungen	0	3
Cyber-Sexualdelikte	**45**	**46**
Verbotene Pornografie	42	37
Grooming	1	0
Sextortion (sex)	2	9
Live Streaming	0	0
Cyber-Rufschädigung und unlauteres Verhalten	**23**	**11**
Cybersquatting	2	0
Cyber-Rufschädigung (geschäftlich)	1	0
Cyberbullying/Cybermobbing	20	11
Darknet	**0**	**0**
Illegaler Handel im Darknet	0	0
Andere	**0**	**0**
Data leaking	0	0

Die bei der Fachstelle Cybercrime der Staatsanwaltschaft in den Jahren 2020/2021 eingegangenen Strafverfahren lassen sich in folgende Tatvorgehen gliedern:



Anzumerken ist, dass Delikte zum Nachteil von Privatpersonen, die mit Hilfe des Internets begangen werden (z.B. Drohungen, sexuelle Belästigungen etc., einfache Onlinebetrüge) und die keine besonderen IT-Kenntnisse zur Ermittlung der Täterschaft bedingen, bei der Staatsanwaltschaft in der Hauptabteilung Allgemeine Delikte untersucht werden.

3. Wie viele der registrierten Fälle betreffen Privatpersonen und wie viele KMU?

Es wird bei der Polizei nur die Unterteilung in natürliche und juristische Personen erhoben. Dabei zeigt sich folgendes Bild:

	2020		2021	
Geschädigte natürliche Personen	323	87.1%	405	80.0%
Geschädigte juristische Personen	48	12.9%	101	20.0%
Total	371	100%	506	100%

Anzumerken ist, dass die Gesamtanzahl geschädigter natürlicher und geschädigter juristischer Personen nicht mit der Gesamtanzahl der Cybercrime-Straftaten übereinstimmt, da beispielsweise die gleiche Person mehrmals geschädigt sein kann.

Bei der Staatsanwaltschaft Basel-Landschaft wird ebenfalls nur die Unterscheidung von juristischen und natürlichen Personen getroffen, eine separate Erhebung von «KMU» erfolgt nicht. Zur Anzahl Anzeigen von natürlichen und juristischen Personen liegen folgende Zahlen vor:

- I.C.1 – Ransomware: von den 14 Angriffen betreffen 12 juristische Personen, 2 öffentlich-rechtliche Körperschaften (Gemeinden) sowie 2 natürliche Personen.

Auf Grund der Phänomendefinition des fedpol sind bei nachfolgenden Phänomenen ausschliesslich juristische Personen – und damit keine natürlichen Personen – betroffen:

- I.E.1 – CEO/BEC Fraud: 15
- III.B – Cyber-Rufschädigung (Geschäftlich): 1

Auf Grund der Phänomendefinition des fedpol sind bei nachfolgenden Phänomenen ausschliesslich natürliche Personen – und damit keine KMU – betroffen:

- I.E.7 – Romance Scam: 10

Sexualdelikte:

- I.G –Sextortion (Money): 2
- II.B – Grooming: 1
- II.C – Sextortion (Sex): 1

Die übrigen Phänomene betreffen derzeit mehrheitlich natürliche Personen.

4. Welche Branchen sind wie stark betroffen?

Diese Frage kann von der Polizei Basel-Landschaft und der Staatsanwaltschaft Basel-Landschaft nicht beantwortet werden, da dazu keine Daten erhoben werden.

5. Wie hat sich die Corona-Pandemie auf die Cyberaktivität im Kanton Basel-Landschaft ausgewirkt?

Die Cyber-Fallzahlen gemäss der Polizeilichen Kriminalstatistik (PKS) sind von 557 Fällen im Jahr 2020 auf 826 im Jahr 2021 angestiegen. Das entspricht einem Anstieg von über 48%. Inwiefern ein Zusammenhang zur Pandemie besteht, lässt sich allerdings nicht abschliessend feststellen. Fest steht aber, dass die Corona-Pandemie ein starker Treiber der Digitalisierung war, was sich vermutlich auch auf die Fallzahlen niedergeschlagen hat.

6. Hatte Homeoffice einen Einfluss auf die Cybercrime-Aktivität und wenn ja, wie äusserte sich dieser?

Diese Frage kann von der Polizei Basel-Landschaft und der Staatsanwaltschaft Basel-Landschaft nicht beantwortet werden, da dazu keine Daten vorliegen.

7. *Wurde die kantonale Verwaltung Opfer von Cyberangriffen und wie schützt sich diese generell gegen Cyberangriffe?*

Von Cybercrime-Straftaten wie DDoS (Distributed Denial of Service) oder Phishing ist auch die kantonale Verwaltung nicht verschont. Die Schutzmassnahmen haben bislang gegriffen und die Auswirkungen reduziert. Die Informationssicherheit wurde nicht beeinträchtigt. Punktuell gab es aber Leistungseinbussen.

Die Verwaltung BL betreibt ein Informationssicherheitsmanagementsystem (ISMS) zum Schutz der anvertrauten Daten und Informationsbearbeitungen vor Cyberangriffen und anderen Sicherheitsvorfällen. Im Rahmen des ISMS bestehen technische und organisatorische Massnahmen, wie auch Massnahmen zur Sensibilisierung der Anwender. Vorfälle werden analysiert und wo nötig Massnahmen im Sinne einer kontinuierlichen Verbesserung angepasst. Die Weiterentwicklung der Informationssicherheit folgt einer mehrjährigen Roadmap. Darin sind zusätzliche Massnahmen geplant, um sich der laufend verändernden Bedrohungslage anzupassen.

8. *Kann die Seite «Kompetenzzentrum Cybercrime» auf der Website des Kantons Basel-Landschaft ansprechender und nutzerfreundlicher gestaltet werden (Beispiel Kanton Zürich https://www.zh.ch/de/sicherheit-justiz/delikte-praevention/gefahren-im-internet.html#25031585) und ist geplant, dort einen jährlichen Bericht über die Aktivitäten des Zentrums zu veröffentlichen?*

Erste Abklärungen aufgrund der Interpellationsfrage haben ergeben, dass es gut möglich sein sollte, die Seite «Kompetenzzentrum Cybercrime» ansprechender und nutzerfreundlicher zu gestalten. Dieser Input wird insofern gerne aufgenommen.

Die Tätigkeiten beziehungsweise Erkenntnisse und Angaben über die Cyberkriminalität finden Eingang in die jährlich publizierte Kriminalstatistik des Kantons Basel-Landschaft sowie in den jährlich publizierten Jahresbericht der Staatsanwaltschaft des Kantons Basel-Landschaft. Ein separater Bericht ist nicht vorgesehen.

9. *Wurden aufgrund des Ukraine-Konflikts vermehrt Cyberattacken auf Firmen im Kanton registriert (bspw. in der Energiebranche)?*

Stand 1. Mai 2022 wurden dem Kompetenzzentrum Cybercrime keine solchen Attacken gemeldet. Weiter besteht Stand heute keine Meldepflicht für die Meldung von Cyberattacken, auch nicht für Betreiber von kritischen Infrastrukturen.

Auch bei der Staatsanwaltschaft wurde in dieser Periode – ab 24. Februar 2022 bis 10. Mai 2022 – noch keine Cyberattacke gemeldet; ob ein Angriff tatsächlich stattgefunden hat, ist mangels Meldepflicht der betroffenen Betreiber kritischer Infrastrukturen derzeit für die Strafverfolgungsbehörden nicht überprüfbar. Es besteht allerdings ein Entwurf der Änderung der Verordnung vom 9. März 2007 über Fernmeldedienste (FDV), worin die Einführung einer Meldepflicht vorgesehen ist.

Allgemein ist festzuhalten, dass das Motiv einer Täterschaft im Cyberbereich nur schwer zu eruieren ist. Daher ist oft keine Aussage möglich, ob die Tat mit krimineller oder politischer Motivation begangen wurde und ob eine kriminelle Gruppierung, eine staatlich geduldete, evtl. gar geförderte kriminelle Organisation oder ein Staat selbst hinter einem Angriff steckt.

Liestal, 14. Juni 2022

Im Namen des Regierungsrats

Der Präsident:

Thomas Weber

Die Landschreiberin:

Elisabeth Heer Dietrich