SCHLESWIG-HOLSTEINISCHER LANDTAG **Drucksache 19/1278**
19. Wahlperiode 2019-03-04

Kleine Anfrage

des Abgeordneten Stefan Weber (SPD)

und

Antwort

der Landesregierung - Minister für Inneres, ländliche Räume und Integration

Cyberkriminalität in Schleswig-Holstein

Vorbemerkung des Fragestellers:
Die Zahl von Cyberattacken auf Unternehmen, Verwaltungen und Privatleute wächst. In einem Zeitungsartikel der Lübecker Nachrichten (25.01.19, S.5) wurde darüber berichtet, dass Firmen in Schleswig-Holstein Lösegelder an Hacker für ihre freigekauften Daten zahlen sollen, sowie dass der Verfassungsschutz mehrmals gegen Cyberkriminelle vorgegangen sein soll.

Vorbemerkung der Landesregierung:
In seiner Vorbemerkung bezieht sich der Fragesteller auf einen Artikel der Lübecker Nachrichten vom 25.01.2019 (http://www.ln-online.de/Nachrichten/Norddeutschland/Hacker-starten-immer-mehr-Cyberattacken-auf-Unternehmen-im-Norden-jetzt-kaempft-auch-der-Verfassungsschutz-gegen-die-Hacker), demzufolge der Verfassungsschutz mehrmals gegen Cyberkriminelle vorgegangen sei. Dies entspricht nicht den Tatsachen. Der Verfassungsschutz hat gegenüber der Zeitung lediglich mitgeteilt, dass er Firmen sensibilisiert habe. Dies tut er im Rahmen seines gesetzlichen Auftrages. Für ein Vorgehen gegen Cyberkriminelle

ist der Verfassungsschutz nicht zuständig und er beabsichtigt nicht, in die Kompetenzen der Polizei einzugreifen.

1. Wie viele Firmen sind in den Jahren 2017-2018 in Schleswig-Holstein Opfer von Schadsoftware (Malware) oder eines Hackerangriffes geworden? Bitte nach Kreisen und kreisfreien Städten auflisten.

Antwort:
Dem Verfassungsschutz Schleswig-Holstein sind im Jahr 2017 sechs und im Jahr 2018 zwölf mutmaßliche Angriffe auf schleswig-holsteinische Firmen im Rahmen von Cyberkampagnen bekannt geworden. Diese verteilen sich wie folgt:

2017:

Lübeck	1
Herzogtum Lauenburg	1
Ostholstein	1
Rendsburg-Eckernförde	1
Segeberg	2

2018:

Flensburg	1
Kiel	1
Lübeck	2
Dithmarschen	1
Nordfriesland	1
Ostholstein	1
Pinneberg	1
Rendsburg-Eckernförde	1
Segeberg	1
Steinburg	1
Stormarn	1

Dem Landeskriminalamt wurden im Rahmen des Sondermeldedienstes Cybercrime 161 Fälle im Jahr 2017 und 128 Fälle im Jahr 2018 gemeldet, in denen Unternehmen

als Geschädigte erfasst worden sind. Bei dem Großteil dieser 161 Fälle handelt es sich um von der Fragestellung nicht erfasste Betrugsdelikte.

Die für die Fragestellung relevanten Fälle lassen sich für 2017 wie folgt differenzieren:
28 Fälle von Ransomware
11 Fälle durch Versand von Spam-Mails mit Link zu einer Schadsoftware
7 Fälle von Account-Übernahmen
4 Fälle von DDoS-Angriffen mit Erpressung
2 Fälle von DDoS-Angriffen als bloße Computersabotage
2 Fälle von Schadsoftware für das Mining von Kryptowährungen
2 Fälle von Schadsoftware unbekannten Typs
1 Fall von Webseiten-Defacement.

Die für die Fragestellung relevanten Fälle lassen sich für 2018 wie folgt differenzieren:
20 Fälle von Ransomware
7 Fälle von Account-Übernahmen
3 Fälle von Webseiten-Defacement
4 Fälle von um Telefonanlagen-Hacking
1 Fall von einem DDoS-Angriff
8 Fälle von Datenerpressung nach Hacking
1 Fall von unberechtigten Systemzugriffen

Da die Falldaten nicht statistisch aufbereitet vorliegen, kann die gewünschte Aufschlüsselung nach Kreisen und Kreisfreien Städten lediglich für die unmittelbar beim Landeskriminalamt bearbeiteten Fälle erfolgen. Für eine vollständige Aufschlüsselung aller Fälle wäre eine Einzelauswertung in Form einer Einsichtnahme und vollständigen Durchsicht eines jeden betroffenen Ermittlungsvorgangs erforderlich.

Bei den im Landeskriminalamt bearbeiteten Fällen stellt sich die Verteilung differenziert nach Modus Operandi und Firmensitz wie folgt dar:

	Delikt	Modus Operandi	Firmensitz
2017	Ausspähen von Daten	Firmennetzwerk gehackt, Beziehungstat, TV: entlassener Systemadministrator	Kiel
	Erpressung, Computersabotage	Ransomware, Systeme verschlüsseln, Lösegeld für Entschlüsselung fordern	Kreis Segeberg
	Ausspähen von Daten	Firmennetzwerk gehackt, Beziehungstat, TV: entlassener Systemadministrator	Kiel
	Erpressung, Computersabotage	Ransomware, Systeme verschlüsseln, Lösegeld für Entschlüsselung fordern	Kreis Segeberg
	Datenveränderung Ausspähen von Daten	Firmenserver wird für Bitcoinmining unter Einbringung entsprechender Malware missbraucht	Lübeck
	Computersabotage	DDoS-Angriff auf Webserver	Lübeck
2018	Ausspähen von Daten	unberechtigter Zugriff auf Email-Postfach einer Firma; Löschung von Emails, Einrichtung von Email-Regeln; Beziehungstat, TV: entlassener Systemadministrator	Kiel
	Erpressung, Computersabotage	Ransomware, Systeme verschlüsseln, Lösegeld für Entschlüsselung fordern, Lösegeld gezahlt	Kreis Schleswig-Flensburg
	Computersabotage	DDoS-Angriff auf Rechenzentrum	Kreis Rendsburg-Eckernförde
	Ausspähen von Daten	Hacking eines Webshops, Veränderung der Zahlungsinformationen	Kiel
	Computerbetrug		
	Ausspähen von Daten	Telefonanlagen-Hacking	Kiel
	Computerbetrug		
	Erpressung, Computersabotage	Ransomware, Systeme verschlüsseln, Lösegeld für Entschlüsselung fordern	Kreis Pinneberg
	Ausspähen von Daten, Computerbetrug	SIP-Fraud, VoIP-Kennungen missbrauchen	Kiel
	Erpressung, Computersabotage	Ransomware, Systeme verschlüsseln, Lösegeld für Entschlüsselung fordern	Kiel
	Ausspähen von Daten, Computerbetrug	SIP-Fraud, VoIP-Kennungen missbrauchen	Kiel
	Erpressung, Computersabotage	Ransomware, Systeme verschlüsseln, Lösegeld für Entschlüsselung fordern	Kreis Pinneberg
	Ausspähen von Daten, Computerbetrug	SIP-Fraud, VoIP-Kennungen missbrauchen	Flensburg
	Erpressung, Computersabotage	Ransomware, Systeme verschlüsseln, Lösegeld für Entschlüsselung fordern, Lösegeld gezahlt	Kreis Segeberg
	Ausspähen von Daten, Computerbetrug	SIP-Fraud, VoIP-Kennungen missbrauchen	Flensburg
	Ausspähen von Daten, Computerbetrug	SIP-Fraud, VoIP-Kennungen missbrauchen	Flensburg
	Erpressung, Computersabotage	Ransomware, Systeme verschlüsseln, Lösegeld für Entschlüsselung fordern	Itzehoe
	Erpressung, Computersabotage	Ransomware, Systeme verschlüsseln, Lösegeld für Entschlüsselung fordern	Kreis Rendsburg-Eckernförde
	Erpressung, Ausspähen von Daten	Datenerpressung nach „Datendiebstahl“ durch sog. SQL-Injections, bundesweites Sammelverfahren mit (derzeit) 31 Einzeltaten, davon 6 Taten in S.-H.	Kiel, Flensburg, Kreis Dithmarschen, Kreis Stormarn, Kreis Rendsburg-Eckernförde, Kreis Schleswig Flensburg
	Erpressung, Computersabotage	Ransomware, Systeme verschlüsseln, Lösegeld für Entschlüsselung fordern	Kreis Pinneberg, Radiologie Elmshorn
	Erpressung, Computersabotage	Ransomware, Systeme verschlüsseln, Lösegeld für Entschlüsselung fordern, Lösegeld gezahlt	Kreis Segeberg
	Erpressung, Computersabotage	Ransomware, Systeme verschlüsseln, Lösegeld für Entschlüsselung fordern	Kreis Pinneberg, Stadtwerke Barmstedt

2. Wie viele Fälle aus den Jahren 2017-2018 sind der Landesregierung bekannt, in denen durch Schadsoftware oder Hackerangriffe der Betriebsablauf von Firmen beeinträchtigt wurde? Bitte die jeweilige Beeinträchtigung beschreiben.

Antwort:
Bei den dem Verfassungsschutz Schleswig-Holstein bekannt gewordenen Angriffen ist es nach Informationen des Verfassungsschutzes nicht zu Beeinträchtigungen gekommen.

Nach Erkenntnissen des Landeskriminalamtes reicht die Palette der Betroffenheit von einem geringen zeitlichen Aufwand in der „Verwaltung“ beim Erkennen einer Schadsoftware-E-Mail bis hin zu einem kompletten, tagelangen Stillstand des Betriebes.
Anhand der beim Landeskriminalamt geführten Verfahren können die (maßgeblichen) Beeinträchtigungen wie folgt konkretisiert werden:

	Delikt	**Modus Operandi**	**Firmensitz**	**Beeinträchtigung**
2017	Erpressung, Computersabotage	Ransomware, Systeme verschlüsseln, Lösegeld für Entschlüsselung fordern	Kreis Segeberg	Systemausfall, Aufwand durch Zurückspielen der Daten über Backups
	Erpressung, Computersabotage	Ransomware, Systeme verschlüsseln, Lösegeld für Entschlüsselung fordern	Kreis Segeberg	Systemausfall über mehrere Tage; verschlüsselte Daten konnten nicht wieder hergestellt werden; schwerwiegende, existenzbedrohende Beeinträchtigung
	Datenveränderung	Firmenserver wird für Bitcoinmining unter Einbringung entsprechender Malware missbraucht	Lübeck	Leistungsminderung des Servers
	Ausspähen von Daten			
	Computersabotage	DDoS-Angriff auf Webserver	Lübeck	Webserver / Internetpräsens mehrere Stunden nicht erreichbar

	Delikt	Modus Operandi	Firmensitz	Beeinträchtigung
2018	Erpressung, Computersabotage	Ransomware, Systeme verschlüsseln, Lösegeld für Entschlüsselung fordern, Lösegeld gezahlt	Kreis Schleswig-Flensburg	Systemausfall, Aufwand durch Zurückspielen der Daten über Backups
	Computersabotage	DDoS-Angriff auf Rechenzentrum	Kreis Rendsburg-Eckernförde	31 komplette Systemausfälle von 4 – 97 Minuten verteilt auf 12 Tage, 2.800 Arbeitsplätze betroffen
	Erpressung, Computersabotage	Ransomware, Systeme verschlüsseln, Lösegeld für Entschlüsselung fordern	Kreis Pinneberg	Systemausfall, Aufwand durch Zurückspielen der Daten über Backups
	Erpressung, Computersabotage	Ransomware, Systeme verschlüsseln, Lösegeld für Entschlüsselung fordern	Kiel	Systemausfall, Aufwand durch Zurückspielen der Daten über Backups
	Erpressung, Computersabotage	Ransomware, Systeme verschlüsseln, Lösegeld für Entschlüsselung fordern	Kreis Pinneberg	Systemausfall, Aufwand durch Zurückspielen der Daten über Backups
	Erpressung, Computersabotage	Ransomware, Systeme verschlüsseln, Lösegeld für Entschlüsselung fordern, Lösegeld gezahlt	Kreis Segeberg	Systemausfall, Aufwand durch Zurückspielen der Daten über Backups
	Erpressung, Computersabotage	Ransomware, Systeme verschlüsseln, Lösegeld für Entschlüsselung fordern	Itzehoe	Systemausfall, Aufwand durch Zurückspielen der Daten über Backups
	Erpressung, Computersabotage	Ransomware, Systeme verschlüsseln, Lösegeld für Entschlüsselung fordern	Kreis Rendsburg-Eckernförde	Systemausfall, Aufwand durch Zurückspielen der Daten über Backups
	Erpressung, Computersabotage	Ransomware, Systeme verschlüsseln, Lösegeld für Entschlüsselung fordern	Kreis Pinneberg	Systemausfall, Aufwand durch Zurückspielen der Daten über Backups, Radiologie einer Klinik betroffen, entsprechende medizinische Untersuchungen konnten über 2 Tage nicht erfolgen
	Erpressung, Computersabotage	Ransomware, Systeme verschlüsseln, Lösegeld für Entschlüsselung fordern, Lösegeld gezahlt	Kreis Segeberg	mindestens 1 Woche durch kompletten Ausfall aller Systeme betroffen, mehrere Wochen zur Entschlüsselung der Daten notwendig, währenddessen nur eingeschränkte Nutzbarkeit der IT, schwerwiegende, existenzbedrohende Beeinträchtigung
	Erpressung, Computersabotage	Ransomware, Systeme verschlüsseln, Lösegeld für Entschlüsselung fordern	Kreis Pinneberg	Systemausfall, Aufwand durch Zurückspielen der Daten über Backups

3. Trifft der Bericht der LN vom 25.01.2019 S.5 zu, dass es selbst Spezialisten von BKA, LKA und einer Versicherung nicht gelungen sein soll, eine Attacke von nordkoreanischer Hacker-Software zu stoppen? Ist dieser Fall der Landesregierung bekannt und falls ja, sind der Landesregierung bekannt aus welchen Ländern die meisten Cyberattacken stammen? Wenn Ja bitte auflisten.

Antwort:
Mutmaßlich dürfte hier ein Fall von November 2018 aus dem Kreis Segeberg gemeint sein, der bei dem für Cybercrime zuständigen Dezernat des Landeskriminalamtes bearbeitet wird.
Strafverfolgungsbehörden erhalten erst nach Vollendung eines Angriffs Kenntnis, insofern kann der Angriff nicht mehr gestoppt werden. Hier hätte, wenn überhaupt, nur die Firma selbst durch sofortiges Erkennen der Ransomware und Treffen von

unverzüglichen Maßnahmen die Fortsetzung der Verschlüsselung verhindern können. Viel wichtiger sind in diesem Kontext aber präventive IT-Sicherheitsmaßnahmen in den Unternehmen, um entsprechende Szenarien von vornherein zu unterbinden.
Das Landeskriminalamt verfügt über keine verifizierten Erkenntnisse, dass es sich in diesem Fall um eine „nordkoreanische“ Hacker-Software gehandelt hat, zumal primär ein Ransomware-Angriff vorlag.
Eine Statistik über den staatlichen Ursprung von Cyberangriffen bzw. zu einer entsprechenden globalen Verteilung liegt dem Landeskriminalamt nicht vor.

Dem schleswig-holsteinischen Verfassungsschutz ist der in dem Zeitungsartikel genannte Angriff nicht bekannt.
Die meisten ausländischen Angriffe mit Spionage-/Sabotagehintergrund stammen aus der Russischen Föderation, der Volksrepublik China sowie der Islamischen Republik Iran (Quelle: Verfassungsschutzbericht 2017 des Bundes, S. 269 ff.).

4. Wie viele Fälle von Lösegeldzahlungen an Hacker zwecks Freikauf gesperrter Firmendaten sind der Landesregierung insgesamt bekannt?

Antwort:
Die Anzahl der insgesamt geleisteten Lösegeldzahlungen ist der Landesregierung nicht bekannt. In den bei dem für Cybercrime zuständigen Dezernat des Landeskriminalamtes bearbeiteten Strafverfahren ist in drei Fällen eine Lösegeldzahlung erfolgt, lediglich in einem Fall war anschließend eine Entschlüsselung möglich bzw. erfolgreich. In diesem Phänomenbereich ist von einem hohen Dunkelfeld auszugehen.

5. Sind der Landesregierung Vorkommnisse bekannt, durch welche Krankenhäuser, Anlagen der öffentliche Wasser- oder Energieversorgung oder öffentlichen Zwecken dienenden Telekommunikationsanlagen in Schleswig-Holstein durch Schadsoftware oder Hackerangriffe im Betriebsablauf beeinträchtigt wurden? Bitte nach Kreisen, kreisfreien Städten, Betreibern und jeweiliger Beeinträchtigung auflisten.

Antwort:
Die der Frage zugrunde liegenden Geschäftsbereiche sind nicht automatisch Betreiber kritischer Infrastrukturen gemäß KRITIS-VO, was zu einer grundsätzlichen Zuständigkeit im LKA führen würde. In anderen Fällen besteht keine Meldepflicht gegenüber der Polizei.

Das für Cybercrime zuständige Dezernat des Landeskriminalamtes hat folgende Fälle bearbeitet, die der Fragestellung entsprechen. Dabei handelte es sich in keinem Fall bei den betroffenen Firmen um ein KRITIS-Unternehmen im Sinne der KRITIS-VO.

Tatzeit	**Delikt**	**Modus Operandi**	**Firmensitz**	**Beeinträchtigung**
17.02.2016	Erpressung, Computersabotage	Ransomware, Systeme verschlüsseln, Lösegeld für Entschlüsselung	Kreis Stormarn, Krankenhaus	Systemausfall, Aufwand durch Zurückspielen der Daten über Backups, uneingeschränkte Arbeitsfähigkeit erst nach 6 Tagen wieder erlangt, Betrieb der Klinik nicht gefährdet, keine Patientengefährdung
12.07.2016	Computersabotage	Löschen von IT-Systemen und Patientendaten	Kreis Segeberg, Krankenhaus	2 Monate lang erhebliche Störungen in der IT-Infrastruktur der Firma, wiederholt unterschiedlichste Systemausfälle durch Sabotagehandlungen eines **Innentäters**, Patientengefährdung und Existenzbedrohung der Klinik lag zweifelsfrei vor
20.10.2018	Erpressung, Computersabotage	Ransomware, Systeme verschlüsseln, Lösegeld für Entschlüsselung	Kreis Pinneberg, Krankenhaus	nur Radiologie innerhalb der Klinik betroffen, Systemausfall, Aufwand durch Zurückspielen der Daten über Backups, entsprechende medizinische Untersuchungen konnten über 2 Tage nicht erfolgen, keine Patientengefährdung
30.12.2018	Erpressung, Computersabotage	Ransomware, Systeme verschlüsseln, Lösegeld für Entschlüsselung fordern	Kreis Pinneberg, öffentliche Wasser- oder Energieversorgung	(kurzfristiger) Systemausfall nur im IT-Bereich, Energiesektor selbst war nicht betroffen, Aufwand durch Zurückspielen der Daten über Backups