LANDTAG MECKLENBURG-VORPOMMERN **Drucksache 7/756**
7. Wahlperiode **27.07.2017**

KLEINE ANFRAGE

der Abgeordneten Thomas de Jesus Fernandes und Nikolaus Kramer, Fraktion der AfD

Cyberkriminalität in Mecklenburg-Vorpommern

und

ANTWORT

der Landesregierung

Die EU-Kommission will die Cyberkriminalität bis 2020 mit insgesamt 450 Millionen Euro an Forschungsausgaben bekämpfen. Einer Studie aus 2016 zufolge haben 75 Prozent der Unternehmen keinen Notfallplan für Hackerangriffe (Quelle: http://www.computerwelt.at/news/technologiestrategie/security/detail/artikel/111472-75-prozent-der-unternehmen-ohne-notfallplan-fuer-hackerangriffe/).

1. Wie schützen die Landesregierung und die ihr unterstellten Ministerien und Behörden sich gegen Hackerangriffe?

Die steigende Verflechtung der Informationstechnologie (IT) mit den Geschäftsprozessen in der öffentlichen Verwaltung sowie die zunehmende Nutzung von Ebenen-übergreifenden IT-Verfahren machen es erforderlich, die Thematik Informationssicherheit verbunden unter anderem mit der gemeinsamen Abwehr von IT-Angriffen (durch Hacker) ganzheitlich zu betrachten. Aus diesem Grund hat die Landesregierung im Jahr 2014 die „Leitlinie zur Gewährleistung der Informationssicherheit in der Landesverwaltung von Mecklenburg-Vorpommern“ (IS-Leitlinie M-V) und das „Konzept zum Aufbau und Betrieb eines Informationssicherheitsmanagements in der Landesverwaltung von Mecklenburg-Vorpommern“ (ISM-Konzept M-V) verabschiedet.

Neben dem in der IS-Leitlinie M-V verankerten Mindestsicherheitsstandard „BSI IT-Grundschutz“ wurde ausgehend vom ISM-Konzept in der Landesverwaltung eine (ressortübergreifende) Informationssicherheitsorganisation aufgebaut. Auf der operativen Ebene unterstützt das Computer Emergency Response Team (CERT M-V) durch seine reaktiven, proaktiven und nachhaltigen Basisdienste die IT-Sicherheitsbeauftragen in den Ministerien und in den nachgeordneten Behörden.

Der Minister für Inneres und Europa hat namens der Landesregierung die Kleine Anfrage mit Schreiben vom 26. Juli 2017 beantwortet.

So werden beispielsweise durch den proaktiven Warn- und Informationsdienst sowie durch die Mitgliedschaft des CERTs M-V im VerwaltungsCERT-Verbund die IT-Sicherheitsbeauftragten und die IT-Dienstleister kontinuierlich über aktuelle IT-Angriffe oder über Sicherheitslücken in Hard- und Softwareprodukten informiert. Zu Themen der Informationssicherheit, über Schulungs- oder Sensibilisierungsveranstaltungen im Land informiert das CERT M-V tagesaktuell über ein Portalsystem.

Mit der Etablierung eines ressortübergreifenden, softwarebasierten ISM-Werkzeugs für die Erstellung, Aktualisierung und Fortschreibung von IT-Sicherheitskonzepten auf Basis von „BSI IT-Grundschutz“ wird das Informationssicherheitsmanagementsystem der Landesverwaltung ziel- und zweckgerichtet unterstützt und weiterentwickelt.

Flankierend zu diesen organisatorischen Maßnahmen sind sowohl zentral bei der DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH als auch dezentral in den jeweiligen Behörden mehrere IT-Systeme und Softwareprodukte, wie zum Beispiel Anti-Virensoftware, mit verschiedenartig wirkenden Schutzfunktionen im Einsatz.

2. Gab es hier in der Vergangenheit bereits Vorfälle?

   Wenn ja,
   a) wann und auf welche Art und Weise?
   b) welcher Schaden ist hierbei entstanden (bitte aufschlüsseln nach Schadensart und finanziellem Schaden)?

Die Fragen 2, 2a) und 2b) werden zusammenhängend beantwortet.

Die am Perimeter des Netzübergangs vom Landesdatennetz zum Internet eingesetzten IT-Systeme mit ihren Schutzfunktionen registrieren täglich eine Vielzahl von Angriffsversuchen.

Im Ministerium für Wirtschaft, Arbeit und Tourismus ist es im Jahr 2009 zu einem Vorfall mit dem Conficker-Virus gekommen. Durch den Virusbefall wurde das Netzwerk des Ministeriums für einen Tag blockiert. Schäden finanzieller Art traten nicht auf.

Im Jahr 2016 war ein primärer Angriffsvektor von Hackern oder von Cyberkriminellen der Versand von gefälschten und mit Schadsoftware behafteten E-Mails. In diesem Kontext gab es vereinzelt Infektionen, die vorsorglich eine Neuinstallation der betroffenen Rechnersysteme notwendig machten. Weitreichende Schäden, insbesondere durch Ransomware (Verschlüsselungstrojaner) konnten durch Datenrücksicherungen vermieden werden.

Durch einen IT-Sicherheitsvorfall im Jahr 2016 (erfolgreicher Befall mit Ransomware) ist zusätzliche Unterstützungsleistung durch die DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH notwendig gewesen. Dadurch ist ein finanzieller Schaden in Höhe von 2.811,38 Euro entstanden.

Innerhalb der Landesverwaltung werden IT-Sicherheitsvorfälle durch das CERT M-V statistisch erfasst, analysiert und ausgewertet; eine summarische Kostenaufstellung für interne und/oder externe Aufwände in Verbindung mit IT-Sicherheitsvorfällen existiert nicht.

3. Gibt es rückläufige Informationen von Unternehmen in Mecklenburg-Vorpommern, die von Cyberangriffen betroffen waren?
Wenn ja, welchen Inhalt haben diese Informationen?

Die Strafanzeigen einzelner Firmen bezogen sich im Wesentlichen auf folgende Begehungsweisen:

a) Firmen erhielten E-Mails mit Anhängen, die den Eindruck vermittelten, dass diese von einem Geschäftspartner stammen (Rechnungen von angeblichen Geschäftspartnern und Telekommunikationsunternehmen).

b) Den Firmen wurden angebliche Bewerbungsunterlagen als Anhang einer E-Mail zugestellt. Die Empfänger sollten veranlasst werden, die Anhänge zu öffnen. Dieses wiederum führte in einigen Fällen dazu, dass der betroffene Computer und über Netzwerke verbundene PC mit einer Schadsoftware verschlüsselt wurden und ein Zugriff dann nicht mehr gegeben war. Den geschädigten Firmen wurde gegen Zahlung einer Gebühr, im Regelfall über die virtuelle Währung Bitcoins, eine Entschlüsselung zugesichert.

c) Komplex CEO-Fraud - hierbei werden E-Mails an die Buchhaltung der jeweiligen Firma versandt. Als Absender der E-Mail war der Firmeninhaber beziehungsweise ein Mitglied der Geschäftsführung aufgeführt. In den E-Mails wurde gefordert, kurzfristige Überweisungen von hohen Geldbeträgen auf ausländische Konten vorzunehmen. Gleichzeitig wurde der Druck auf dem Empfänger der E-Mail aufgebaut, den angeforderten Betrag umgehend und ohne Prüfung zu überweisen.

d) Missbräuchliche Nutzung von Routern, die in Solarparks installiert wurden. Durch fehlerhafte Router-Konfigurationen war es möglich, kostenpflichtige Auslandsverbindungen herzustellen und auszuführen.

Rückläufige Informationen von Unternehmen in Mecklenburg-Vorpommern, die von Cyberangriffen betroffen waren, werden nicht gesondert erfasst und sind nicht auswertbar. Insofern können keine weitergehenden Angaben zu dieser Frage gemacht werden.

4. Wie und mit welchen Maßnahmen sensibilisiert beziehungsweise unterstützt das Land Mecklenburg-Vorpommern Unternehmen beim Thema Cyberkriminalität?

Durch die Präventionsbeamten der Landespolizei Mecklenburg-Vorpommern wurden 2016 insgesamt 358 Maßnahmen[1] (Präventionsveranstaltungen aber auch Einzelberatungen) zum Thema Cybercrime im Land Mecklenburg-Vorpommern durchgeführt.
Darüber hinaus unterstützt das Landeskriminalamt Präventionsveranstaltungen von Firmen, Verbänden, Kammern und weitere, u. a. im Rahmen der durch das Landeskriminalamt initiierten Sicherheitspartnerschaft Mecklenburg-Vorpommern mit Vorträgen und Teilnahmen.

2015
- Vortrag auf der 50. Sitzung der Sicherheitspartnerschaft Mecklenburg-Vorpommern zum Thema „Bitcoins - Herausforderungen für Wirtschaft und Strafverfolgung“
- Vortrag auf der 26. GastRo (Fachmesse für Hotellerie, Gastronomie und Gemeinschaftsverpflegung) in Rostock zum Thema „Cybercrime - Sicherheit im Internet“
- Vorträge auf einer Veranstaltung der Industrie- und Handelskammer zu Rostock zum Thema „Alles Cyber, oder was? So schützen Sie Ihr Unternehmen“
- Teilnahme am 15. Hanse Sail Business Forum zur Thematik „Digitalisierung – Chancen und Herausforderungen für die Unternehmen in Mecklenburg-Vorpommern“
- IT-Sicherheitstag der DVZ Datenverarbeitungszentrum Mecklenburg-Vorpommern GmbH
- XIX. Mandantenseminar Rechtsanwaltssozietät WIGU zum Thema "Sicherheit im Internet - Verhaltensprävention für das sichere Bewegen im Internet"
- Operation Blackfin: Das Landeskriminalamt Mecklenburg-Vorpommern beteiligte sich mit zwei Präventionsmaßnahmen an der Operation Blackfin. Bei der durch die National Cybercrime Agency (GB) in Zusammenarbeit mit Europol/EC3 initiierten „Blackfin Campaign“/„OP Blackfin“ handelt es sich um eine Präventions- beziehungsweise um eine Sensibilisierungskampagne, welche unter anderem das Ziel beinhaltet, die Bevölkerung hinsichtlich der Gefahren im Internet und der Phänomene der Cybercrime aufzuklären und zu sensibilisieren. Die europaweite Maßnahme fand in der Woche vom 09.11. bis 14.11.2015 statt. In Mecklenburg-Vorpommern wurden die Veranstaltungen am 10.11.2015 auf dem DEHOGA MV Branchentag sowie ein Vortrag in diesem Kontext auf dem 3. Präventionstag des Landkreises Mecklenburger Seenplatte am 12.11.2015 durchgeführt.

2016
- Vortrag auf den „Rügener Krankenhaustagen“ des Verbandes der Krankenhausdirektoren Deutschlands e. V. (VKD)
- IT-Sicherheitstag der DVZ M-V GmbH (Veranstaltung für Behörden des Landes),
- Fortbildungsveranstaltung der Rechtsanwaltskammer (RAK),
- Sicherheitsrelevante Informationen, auch aus anderen Bundesländern, zum Beispiel zu Erpressungen (Ransomware), CEO Fraud, Phishing-Angriffen und dergleichen werden an die Partner der Sicherheitspartnerschaft Mecklenburg-Vorpommern weitergeleitet.

Bei Notwendigkeit erfolgen kurzfristig Präventionshinweise über verschiedene Medien.

[1] Präventionsjahresbericht Mecklenburg-Vorpommern 2016

5. Wie viele Beamte in welchen Abteilungen der Landespolizei und in den Staatsanwaltschaften befassen sich ausschließlich mit dem Themenkomplex Cyberkriminalität?

In der Landespolizei befassen sich insgesamt 56 Beamtinnen und Beamte ausschließlich mit dem Themenkomplex Cyberkriminalität (Landeskriminalamt 26 Personen, Kriminalpolizeiinspektionen 21 Personen, Kriminalkommissariate 9 Personen).

Hinsichtlich der Staatsanwaltschaften wird auf die Antwort der Landesregierung auf die Kleine Anfrage des Abgeordneten Sandro Hersel, Fraktion der AfD, vom 29.05.2017, „Bekämpfung der Informations- und Kommunikationskriminalität“, Drucksache 7/634, Bezug genommen.

6. Welche rechtlichen Möglichkeiten der Strafverfolgung gibt es bei Angriffen aus dem Ausland?

Die rechtlichen Möglichkeiten der im Ausland zu führenden Ermittlungen richten sich regelmäßig nach den von der Bundesrepublik Deutschland mit einzelnen Staaten oder mit einzelnen Staatengemeinschaften abgeschlossenen Rechtshilfeabkommen, die unterschiedliche Voraussetzungen an Rechtshilfeersuchen stellen. Grundlegendes Merkmal der Rechtshilfeabkommen ist, die Souveränität des ausländischen Staates zu wahren, was dazu führt, dass hoheitliche Ermittlungshandlungen in dem Staat nur nach vorheriger Genehmigung der dort zuständigen Stellen und im Regelfall auch nur durch die dortigen Ermittlungskräfte durchgeführt werden können. Zudem sind im Ausland geführte Ermittlungen regelmäßig nur dann zulässig, wenn die verfolgte Tat auch in dem ausländischen Staat gesetzlich unter Strafe gestellt ist.

Weitergehende grenzüberschreitende Ermittlungsmöglichkeiten bestehen im Rahmen der Europäischen Union. Dort sind spezifische Instrumente zur grenzüberschreitenden Ermittlung der Informations- und Kommunikationskriminalität geschaffen worden. Auf justizieller Seite stellt die Einheit für die justizielle Zusammenarbeit der Europäischen Union (Eurojust) das Europäische Justizielle Netzwerk (EJN) zur Verfügung, welches eine beschleunigte Rechtshilfe ermöglicht. Zudem bietet Eurojust die Vermittlung von Joint Investigation Teams (JIT) an, in welchen die Genehmigung von Ermittlungsmaßnahmen beziehungsweise die Beantragung einer richterlichen Anordnung der Maßnahme für ein bestimmtes grenzüberschreitendes Ermittlungsverfahren auf die Ebene der in den beteiligten Staaten zuständigen Sachbearbeiter delegiert werden kann.

Für nähere Informationen zu den rechtlichen Möglichkeiten von Rechtshilfemaßnahmen bei der Verfolgung der Informations- und Kommunikationskriminalität in Europa wird auf das öffentlich zugängliche Angebot von Eurojust, Europol und des Council of Europe Bezug genommen. Die letztgenannte Organisation verantwortet die Cybercrime-Convention (CCC oder auch Budapest-Convention) als weiteres, spezifisch für die Verfolgung der Informations- und Kommunikationskriminalität geschaffenes europäisches Rechtshilfeinstrument.

Weitere Erläuterungen sind über das folgende öffentliche Angebot der benannten Organisationen abrufbar:

http://www.eurojust.europa.eu/Practitioners/Pages/European-Judicial-Network-.aspx
http://www.eurojust.europa.eu/Practitioners/JITs/Pages/legal-framework.aspx
https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
https://www.coe.int/en/web/cybercrime/the-budapest-convention

7. Wie viele Fälle von Cyberkriminalität wurden in Mecklenburg-Vorpommern seit 2011 registriert und wie viele Fälle wurden bereits aufgeklärt (bitte aufschlüsseln nach Herkunftsland der Attacke und dem jeweiligen Kalenderjahr)?

Die Polizeiliche Kriminalstatistik (PKS) enthält nur Fälle mit Tatort in Deutschland. Daher liegen zu Attacken aus anderen Herkunftsländern keine aufbereiteten Daten vor. Laut PKS entwickelten sich die Fallzahlen seit 2011 wie folgt:

Summenschlüssel Computerkriminalität			**Straftaten mit Tatmittel Internet**		
	Fälle gesamt	**aufgeklärte Fälle**		**Fälle gesamt**	**aufgeklärte Fälle**
2011	1.431	769	2011	5.304	4.267
2012	1.668	541	2012	4.968	3.234
2013	2.479	636	2013	7.025	4.091
2014	1.470	812	2014	4.530	3.643
2015	1.565	713	2015	4.318	2.959
2016	2.397	1.437	2016	5.306	3.868

Durch Änderungen des Summenschlüssels Computerkriminalität im Jahr 2016 (zusätzliche Aufnahme von Straftaten gemäß § 263a des Strafgesetzbuches) und die bundesweite Vereinheitlichung der Erfassungspraxis bei Straftaten mit unbekanntem Tatort ab 2014 ist eine Vergleichbarkeit der Jahreszahlen zum Teil eingeschränkt beziehungsweise nicht gegeben. So wurden ab 2014 Internetstraftaten mit unbekanntem Tatort nicht mehr in der PKS erfasst.