Kleine Anfrage zur schriftlichen Beantwortung
mit Antwort der Landesregierung

Anfrage der Abgeordneten Detlev Schulz-Hendel und Belit Onay (GRÜNE)

Antwort des Niedersächsischen Ministeriums für Inneres und Sport namens der Landesregierung

Wie sicher ist die IT der Ministerien und von Landeseinrichtungen?

Anfrage der Abgeordneten Detlev Schulz-Hendel und Belit Onay (GRÜNE), eingegangen am 15.03.2018 - Drs. 18/517
an die Staatskanzlei übersandt am 20.03.2018

Antwort des Niedersächsischen Ministeriums für Inneres und Sport namens der Landesregierung vom 20.04.2018,

gezeichnet

Boris Pistorius

Vorbemerkung der Abgeordneten

Das als besonders sicher geltende Netzwerk des Bundes ist Opfer eines Hackerangriffs geworden. Zeitungsberichte sprechen davon, dass sich die Hacker bis zu einem Jahr im Datennetz der Bundesverwaltung - dem Informationsverbund Berlin-Bonn (IVBB) - befunden haben. Genutzt wird der IVBB u. a. von Teilen des Bundestags, dem Bundesrat, dem Bundeskanzleramt und Bundesministerien. Im Dezember 2017 erfuhr die Bundesregierung davon, das Ausmaß des Schadens bleibt aber bisher im Dunkeln. Bereits 2015 war das Netzwerk des Bundestags von einem Hackerangriff betroffen, bisher ist immer noch nicht geklärt, was mit den damals erbeuteten 16 Gigabyte an Daten aus dem „Parlakom“-Netzwerk genau passiert ist. Vor dem Hintergrund dieser Entwicklungen richten wir die folgenden Fragen an die Landesregierung.

Vorbemerkung der Landesregierung

Mit der zunehmenden Digitalisierung der Verwaltung, Wirtschaft und Gesellschaft sind die Gefahren aus dem Cyberraum in den letzten Jahren deutlich angestiegen. Die Landesregierung verfolgt diese Entwicklung sehr aufmerksam, um das Landesdatennetz und die damit verbundenen IT-Systeme der Ministerien und weiteren Behörden im erforderlichen Maß zu schützen.

Auf technischer Seite werden die Firewallsysteme, Sicherheitsgateways, Virenscanner und weitere Systeme zur Detektion und Abwehr von Gefahren für die IT-Sicherheit durch Sicherheitslücken, Schadprogramme und sonstige Angriffe ständig weiterentwickelt und ergänzt. Diese Maßnahmen werden ständig auf ihre Wirksamkeit untersucht und entsprechend den technischen Entwicklungen angepasst. Insbesondere der Übergang vom Landesdatennetz zum Internet ist durch eine mehrstufige, aufwändige Technik abgesichert. Durch eine Benennung der konkreten Schutzmaßnahmen würde deren Wirksamkeit erheblich beeinträchtigt oder sogar vollständig aufgehoben werden, da bei Bekanntwerden potenzielle Angreifer die Möglichkeit hätten, die IT-Infrastruktur des Landes effizienter anzugreifen. Die Art und der Umsetzungsgrad der Sicherheitsmaßnahmen sowie die in Planung befindliche Sicherheitsmaßnahmen sind daher als sensible Informationen zu behandeln. Die Landesregierung bietet - soweit gewünscht - an, konkret geplante Maßnahmen in vertraulicher Sitzung des Ausschusses für Inneres und Sport darzulegen.

Auf der organisatorischen Seite ist bereits 2011 von der Landesregierung die Leitlinie zur Gewährleistung der Informationssicherheit beschlossen worden. Sie gibt als strategischer Rahmen zusammen mit acht weiter ausführenden Richtlinien vor, wie in der Landesverwaltung in Fragen der Informationssicherheit auf Basis von Risikoabschätzungen vorzugehen ist. Dieses Informationssicherheitsmanagementsystem (ISMS) der niedersächsischen Landesverwaltung entspricht den Vor-

gaben der internationalen Norm ISO 27000 für Informationssicherheit und dem IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik. Die Umsetzung und Wirksamkeit dieses Systems wird durch den Niedersächsischen IT-Planungsrat gesteuert. Er lässt sich dazu regelmäßig durch den Informationssicherheitsbeauftragten der Landesverwaltung unterrichten. Zur Umsetzung der Vorgaben des ISMS sind die Behörden der Landesverwaltung in 35 sogenannten Sicherheitsdomänen zusammengefasst. Auf dieser Ebene sind Informationssicherheitsbeauftragte eingesetzt, die in Fragen der Informationssicherheit der Behördenleitung berichten und deren Umsetzung begleiten.

Die am 27.09.2016 von der Landesregierung beschlossene IT-Strategie des Landes Niedersachsen „Digitale Verwaltung 2025“ stellt die Informationssicherheit als einen Schwerpunkt heraus. Neben organisatorischen Vorkehrungen zur Erhöhung der Informationssicherheit bleibt die Verbesserung der technischen Sicherheitsmaßnahmen eine Daueraufgabe. Netzinfrastrukturen sind als elektronisches Nervensystem der Öffentlichen Verwaltung die Basis für jegliche Kommunikation und Fachverfahren. Aufgrund der Vernetzung können Angriffe über einzelne Behördengrenzen hinweg auch alle anderen Behörden gefährden und im schlimmsten Fall die Handlungsfähigkeit der Verwaltung insgesamt beeinträchtigen. Der übergreifende Schutz des Landesdatennetzes und der Kommunikationsinhalte nach innen und außen genießt für die Landesregierung daher allerhöchste Priorität.

Um die Gefahren aus dem Cyberraum für die IT der Landesverwaltung langfristig und in der täglichen Konfrontation wirksam beurteilen zu können und rechtzeitig Gegenmaßnahmen einleiten zu können, betreibt die Landesregierung beim Ministerium für Inneres und Sport ein Computer Emergency Response Center, das N-CERT. Dieses aus sechs IT-Sicherheitsspezialisten bestehende Team steht in ständigem Kontakt mit dem CERT des Bundesamts für Sicherheit in der Informationstechnik, den CERTs anderer Bundesländer, aber auch bedeutender Industrie- und Telekommunikationsunternehmen sowie mit allen relevanten Landes- und Bundesbehörden. Eingehende Sicherheitshinweise werden vom N-CERT sofort bewertet und entsprechende Warnungen und Informationen den IT-Betrieben und Sicherheitsdomänen der Landesverwaltung zusammen mit einer Umsetzungsempfehlung zur Verfügung gestellt. Das schnelle Einspielen dieser Sicherheitsmaßnahmen sowie die von Herstellern zusätzlich zur Verfügung gestellten Sicherheitsupdates tragen maßgeblich dazu bei, Sicherheitslücken kurzfristig zu schließen und die Widerstandsfähigkeit der IT-Systeme der Landesverwaltung gegen Angriffe zu stärken.

Das N-CERT ist ein zentrales Element der Cybersicherheitsstrategie der Landesregierung aus dem Jahr 2012 und wurde im Oktober 2012 gegründet. Mittlerweile ist auch eine rasch steigende Zahl niedersächsischer Kommunen an das N-CERT angeschlossen, die ebenfalls vom Warn- und Informationsdienst des N-CERT profitieren. Die Cybersicherheitsstrategie betrachtet neben der Verwaltung auch die Cybergefahren für die Gesellschaft. Unsere moderne Gesellschaft ist heute ohne die über territoriale Grenzen hinweg stattfindende Vernetzung von Informations-, Steuerungs- und Versorgungssystemen nicht mehr vorstellbar. Mit den vielfältigen Chancen der Digitalisierung steigen jedoch auch die sicherheitspolitischen Herausforderungen. Nicht nur Betreiber kritischer Infrastrukturen, sondern auch die Bevölkerung sowie Akteure aus Wirtschaft, Wissenschaft, Politik und Verwaltung sind zunehmend auf verlässliche Technologien angewiesen und müssen sich vor kriminellen Handlungen im Internet schützen.

Neben den Investitionen in IT-Sicherheit kommt daher auch der Bekämpfung der Cyberkriminalität eine wichtige Rolle zu. In der strategischen Ausrichtung der niedersächsischen Landespolizei 2020 sind die personellen, organisatorischen und technologischen Voraussetzungen zur Bekämpfung der Cybercrime wesentliche Kernelemente. Vor diesem Hintergrund wurden 2016 in der niedersächsischen Polizei im Rahmen einer Pilotierung insgesamt zwölf sogenannte Taskforces Cybercrime/Digitale Spuren (TF CC/DS) in den Polizeidirektionen neu eingerichtet. Für diese Einheiten und das Landeskriminalamt Niedersachsen wurden bis 2017 mehr als 35 neue Beschäftigungsmöglichkeiten für IT-Spezialisten mit Studienabschlüssen in der Informatik oder vergleichbar geschaffen. Für diese Arbeitsbereiche wurden damit einhergehend Verbesserungen der technischen Ausstattungen sowohl in forensischen als auch in den ermittelnden Bereichen vorgenommen. Im Zusammenwirken mit der Hochschule Emden/Leer wurde zudem die Weiterbildung innerhalb der Polizei gestärkt.

Im Landeskriminalamt Niedersachsen ist die bereits am 31.01.2011 eingerichtete Zentrale Ansprechstelle Cybercrime (ZAC) mit der zum 01.04.2016 erfolgten Integration in das Sachgebiet „Koordinierungs- und Interventionsstelle bei Cyberangriffen“ (KIST) weiter gestärkt worden. Darüber hinaus ist das Landeskriminalamt Niedersachsen seit 2014 Mitglied einer Sicherheitskooperation mit dem BITKOM e. V. und weiteren Landeskriminalämtern. Die Landesregierung legt mit ihrer Strategie gegen Cybercrime insgesamt großen Wert auf ein nachhaltiges Verhindern rechtsfreier Räume in der digitalen Welt.

1. Welche zusätzlichen Maßnahmen, neben den bisherigen Schutzmaßnahmen, plant die Landesregierung?

Über die in den Vorbemerkungen der Landesregierung genannten Maßnahmen hinaus wird derzeit der Entwurf für ein Niedersächsisches Gesetz zur Förderung und zum Schutz der digitalen Verwaltung (Niedersächsisches IT-Sicherheits- und E-Government-Gesetz - NITSGovG) erstellt,. Dieser Gesetzentwurf umfasst u. a. die Rechtsgrundlagen für den Einsatz weiterer technologischer Maßnahmen, die den Schutz des Landesdatennetzes und der angeschlossenen Systeme erhöhen. Diese Regelungen sind erforderlich, um aktuellen und zukünftigen Angriffstechnologien noch effizienter entgegentreten zu können.

2. Wie viele Haushaltsmittel werden in die IT-Sicherheit der Ministerien im Jahr 2018 investiert?

Das Spektrum von Maßnahmen zur IT-Sicherheit ist weit gefächert und beschränkt sich keineswegs auf die allgemein bekannten Schutzvorkehrungen wie Anti-Viren-Software oder Firewall-Systeme. Beispielsweise tragen physische Sicherheitsmaßnahmen gegen unberechtigten Zutritt von Gebäuden und Räumen, Infrastrukturservices, Netzwerkmanagementsysteme, Schutzmaßnahmen bei den Netzübergängen, gehärtete Serverkonfigurationen, Maßnahmen zum Endgeräteschutz, die Beschaffung aktueller Netzwerktechnologie und die Erneuerung von Betriebssystemen und Anwendungssoftware erheblich auch zur IT-Sicherheit bei. Ergänzt werden diese Beiträge durch organisatorische Maßnahmen in der Landesverwaltung, welche beispielsweise auf der Leitlinie zur Gewährleistung der Informationssicherheit beruhen. Sensibilisierungsmaßnahmen für die Beschäftigten der Landesverwaltung zum sicheren Umgang mit Informationstechnik runden das Maßnahmenspektrum ab. Die Aufwände für die IT-Sicherheit werden daher nicht im Einzelnen erfasst, sondern sind i. d. R. Bestandteil der jeweiligen einzelnen Vorhaben und Maßnahmen.

Im Übrigen wird auf die Vorbemerkung der Landesregierung verwiesen.

3. Plant die Landesregierung, weitere Mittel in die IT-Sicherheit der einzelnen Ministerien zu investieren (bitte Auflistung nach Ministerien)?

Im Rahmen laufender Vorhaben zur Erneuerung zentraler und dezentraler Hard- und Softwarekomponenten wird ein besonderes Augenmerk auf eine angemessene IT-Sicherheit gelegt. Die Projekte werden auf der Basis von Risikoanalysen bewertet und aktuelle und neuartige Angriffsmethoden berücksichtigt, insbesondere auch bekannte Angriffe gegen die IT der Bundesregierung und der Verwaltungen von Bund und Ländern. Eine exakte Aufteilung der eingesetzten Haushaltsmittel in den fachlichen Nutzen und die IT-Sicherheit ist - wie in der Antwort zu Frage 2 dargelegt - nicht möglich, da neue Nutzungsmöglichkeiten regelmäßig mit zusätzlichen Sicherheitsmerkmalen einhergehen.

Zu Informationen über die Einführung dedizierter Sicherheitstechnologien und -maßnahmen bietet die Landesregierung an, konkrete Informationen in vertraulicher Sitzung des Ausschusses für Inneres und Sport darzulegen, siehe Vorbemerkung der Landesregierung.

4. Welche technischen Maßnahmen und Softwareumstellungen plant die Landesregierung, um die IT-Sicherheit der Ministerien sicherzustellen?

Die Landesregierung bietet an, konkrete Informationen in vertraulicher Sitzung des Ausschusses für Inneres und Sport darzulegen, siehe Vorbemerkung der Landesregierung.

5. Hat es in der Vergangenheit auch Hackerangriffe in Niedersachsen auf die Landesministerien oder Landeseinrichtungen gegeben? Falls ja, mit welchem Hintergrund?

Die niedersächsische Landesverwaltung ist vergleichbar mit anderen öffentlichen und privaten Organisationen ständigen Hackerangriffen in unterschiedlicher Intensität ausgesetzt. Die Angriffe folgen häufig bekannten Mustern und haben beispielsweise zum Ziel, über Ransomware Lösegeld zu erpressen, an vertrauliche Informationen zu gelangen oder die Internetpräsenz von Landeseinrichtungen durch Denial-of-Service-Angriffe zu stören. Die Landesregierung bietet an, konkrete Informationen in vertraulicher Sitzung des Ausschusses für Inneres und Sport darzulegen, siehe Vorbemerkung der Landesregierung.

6. Falls ja, wie ist die Aufklärungsrate der Hackerangriffe?

Die Landesregierung bietet an, konkrete Informationen in vertraulicher Sitzung des Ausschusses für Inneres und Sport darzulegen, siehe Vorbemerkung der Landesregierung.

7. Wie steht die Landesregierung zu Open-Source-Programmen als Standard für die öffentliche Verwaltung?

Open-Source-Programme können die Erreichung der IT-strategischen Ziele der Landesregierung unterstützen. Der Einsatz von Open Source Software (OSS) wird daher im Rahmen von Auswahlverfahren regelmäßig geprüft. Entscheidend für die Software-Auswahl in der Landesverwaltung ist, dass die geforderten Fähigkeiten im Gesamtsystemzusammenhang erreicht werden können. Hierzu sind eine Reihe weiterer Kriterien wie Funktionalität, Interoperabilität, Sicherheit, Realisierungs-, Pflege- und Ausbildungsaufwand, Verfügbarkeit von Fachanwendungen und Bedienbarkeit zu prüfen. Bei der weiteren Auswahl der geeigneten Software-Angebote erhält dann das wirtschaftlichste den Zuschlag.

Eine wichtige Rolle spielt OSS vor allem in den Rechenzentren der Landesverwaltung, insbesondere beim Einsatz von Linux- oder Apache-Servern, Systemmanagementsoftware und SQL-Datenbanken. So waren bei dem Landesdienstleister IT.Niedersachsen (IT.N) im Bereich der Serverbetriebssysteme im Jahr 2017 auf physikalischen Servern und Clustern 86 OSS-(LINUX)-Installationen gegenüber 24 proprietären UNIX-Installationen sowie 45 Windows-Installationen im Einsatz. Bei den virtuellen Servern waren es 258 OSS-(LINUX)-Installationen gegenüber 16 proprietären UNIX-Installationen sowie 126 Windows-Installationen. Im Bereich der Webserver ist das Verhältnis mit 35 (OSS)-Apache-Installationen gegenüber zehn proprietären UNIX-Webservern und 18 Microsoft Internet Information Servern ähnlich. Weitere größere Einsatzfelder für OSS-Systeme sind der Bereich der Redaktionssysteme sowie der Applikationsserver.

Bei den PC-Betriebssystemen hat sich der Einsatz von OSS als Betriebssystem nicht durchgesetzt. Hier bewegt sich der Marktanteil von Linux in Deutschland bei ca. 1 bis 3 %. Im Bereich der allgemeinen Landesverwaltung sowie der Justiz werden bis auf wenige Ausnahmen ausschließlich Windows-Betriebssysteme eingesetzt. In den meisten Ministerien sowie einer Reihe von Behörden wird der von IT.N zentral betriebene „Niedersachsen-Client“ mit dem Betriebssystem Windows 8.1 auf über 8 000 Arbeitsplätzen eingesetzt. Gleichwohl wird mit dem „Niedersachsen-Client“ in der Praxis der verstärkte Einsatz von OSS auf den IT-Arbeitsplätzen unterstützt. Grafische Anwendungen, Browser oder Programme zur Datenkompression sind als Standardsoftware installiert oder werden als standardisierte Zusatzsoftware angeboten.

Für die Polizei kam die im Jahr 2012 eingesetzte Projektgruppe zur Erarbeitung einer IKT-Strategie - ebenso wie zuvor der Landesrechnungshof und ein Gutachten aus dem Jahr 2009 - zu dem Er-

gebnis, dass der Betrieb und die Pflege von zwei unterschiedlichen Betriebssystemen (LINUX und Windows) für die Arbeitsplatz-PCs der Polizei einen vermeidbar hohen personellen und finanziellen Aufwand erfordern. Es wurde empfohlen zu prüfen, ob unter strategischen, technischen und wirtschaftlichen Gesichtspunkten eine standardisierte und zentralisierte Mehr-Plattform-Lösung fortgeführt oder auf eine Ein-Plattform-Lösung umgestellt werden sollte. In einer Wirtschaftlichkeitsuntersuchung im Jahr 2014 wurden die beiden Szenarien vergleichend gegenüberstellt. Daraus ergab sich, dass der Betrieb nur einer Microsoft-Plattform durch den zentralen Landesdienstleister IT.N die wirtschaftlichste Lösung darstellt. Infolgedessen wurde durch den niedersächsischen Innenminister entschieden, in einem mehrjährigen Projekt die vorhandene polizeiliche IKT-Infrastruktur auf eine einheitliche, zentralisiert bei IT.N zu betreibende Betriebssystemebene umzustellen. Das Betriebssystem auf den „Polizei-Clients“ ist Windows 10. Das Umsetzungsprojekt ist inzwischen weit fortgeschritten.

Die Steuerverwaltung betreibt ihre IT-Arbeitsplätze zurzeit noch weitestgehend unter dem Client-Betriebssystem openSuse. Hinzu kommt eine Reihe von Infrastrukturdiensten, die zum Betrieb dieser IT-Arbeitsplätze erforderlich sind. Der Koalitionsvereinbarung zwischen der SPD und der CDU sieht hierzu vor, „den bisher Linux-basierten Verfahrensbetrieb aufzugeben mit dem Ziel, auf diesem Weg die länderübergreifende Zusammenarbeit zu erleichtern und den Aufwand in Programmierung und Verfahrensbetreuung zu reduzieren.“ Eine Voruntersuchung der erforderlichen Maßnahmen nebst einer Aufwandsanalyse zur Umsetzung ist inzwischen begonnen worden.

8. Plant die Landesregierung eine Ausweitung spezieller Schulungen der Mitarbeiterinnen und Mitarbeiter der Landesministerien z. B. bezüglich des Umgangs mit E-Mail-Anhängen und Links in fremden E-Mails?

Im Ministerium für Inneres und Sport wurde bereits 2014 die Kampagne „AUFGEPASST“ für mehr Informationssicherheit in der niedersächsischen Landesverwaltung entwickelt. Diese Kampagne steht allen Landesbehörden und Kommunen in Niedersachsen zur Verfügung und soll durch spannende Live-Hacking-Veranstaltungen, bedarfsgerechte Hintergrundinformationen und Werbematerial die Mitarbeiterinnen und Mitarbeiter in den Behörden für Informationssicherheit sensibilisieren und Handlungssicherheit, beispielsweise beim Umgang mit E-Mails, vermitteln. Die Live-Hacking-Veranstaltungsreihe konnte seit 2013 über 3 100 Beschäftige der Landes- und Kommunalverwaltungen erreichen. In 2017 wurden sieben dieser Veranstaltungen durchgeführt, für 2018 ist eine noch höhere Zahl geplant. Dabei steht nicht nur die reine Zahl an Teilnehmerinnen und Teilnehmern im Vordergrund, sondern auch eine von diesen ausgehende Multiplikatorenwirkung, die über den reinen Besuch der Veranstaltung hinausgeht.

Der Niedersächsische IT-Planungsrat hat in seiner 21. Sitzung am 04.03.2015 die Ressorts aufgefordert, in den Behörden ihres Geschäftsbereichs Sensibilisierungsmaßnahmen zur Verbesserung der Informationssicherheit in der Landesverwaltung auf regelmäßiger Basis durchzuführen.

Um dezentrale Fortbildungen zu ermöglichen, wird beim Studieninstitut des Landes Niedersachsen seit 2016 eine mittlerweile fünfteilige Seminarreihe über 13 Tage angeboten, die sich an Führungskräfte, Informationssicherheitsbeauftragte, IT-Verantwortliche und Datenschutzbeauftragte richtet. Sie soll mit den zentral bereitgestellten Kampagnenmitteln für eine Ausweitung der Sensibilisierung und Schulung der Anwenderinnen und Anwender auch für den Umgang mit betrügerischen E-Mails und schadhaften Links sorgen.

Im Alltag werden die Sicherheitswarnungen des N-CERT, z. B. zu schädlichen E-Mails, durch die Informationssicherheitsbeauftragen adressatengerecht für die Anwenderinnen und Anwender aufbereitet. Hierdurch erfolgt eine ständige Sensibilisierung.

9. Wie will die Landesregierung generell niedersächsische Unternehmen vor Cyberkriminalität schützen?

Das Ministerium für Inneres und Sport bietet den niedersächsischen Unternehmen, aber auch den Bürgerinnen und Bürgern sowie der Verwaltung eine Reihe von Informations- und Kontaktmöglichkeiten bei Fragen zu Cyberangriffen.

Das Landeskriminalamt Niedersachsen bietet mit der „Zentralen Ansprechstelle Cybercrime“ (ZAC) (https://zac-niedersachsen.de/) einen Ansprechpartner insbesondere für kleine und mittelständische niedersächsische Unternehmen. Wesentliche Aufgabe der ZAC ist die Beratung von Unternehmen, aber auch öffentlichen Behörden und Einrichtungen. Dies umfasst eine Erstberatung im Schadensfall sowie die Vermittlung fachkundiger Polizeibeamtinnen und -beamter aus den örtlich zuständigen Dienststellen für die Anzeigenaufnahme. Parallel erfolgt eine zielgerichtete Beratung, um im Fall einer akuten Angriffssituation erste geeignete Maßnahmen ergreifen zu können. Die ZAC arbeitet an der Schnittstelle zwischen der strafrechtlichen Aufarbeitung eines Cybervorfalls und dem präventiven Beratungsbedarf vor und nach einem Cyberangriff. Dies wird insbesondere von den Unternehmen positiv bewertet. Dadurch soll das Vertrauen von Unternehmen in die Polizei gestärkt werden, was zu einer steigenden Bereitschaft führen soll, Sachverhalte anzuzeigen. Im Jahr 2017 hat es ca. 200 Kontaktaufnahmen durch niedersächsische Unternehmen mit der ZAC gegeben.

Unterstützt wird die ZAC auch durch die bei den lokalen Polizeibehörden eingerichteten Pilotorganisationen der Taskforces Cybercrime/Digitale Spuren (TF CC/DS), zu deren Aufgaben ebenfalls eine Beratung und Mitwirkung bei der Prävention gehört.

Das Landeskriminalamt Niedersachsen hat darüber hinaus die bundesweit anerkannte Webseite „Ratgeber Internetkriminalität“ eingerichtet, erreichbar unter dem Link https://www.polizei-praevention.de/home.html. Dort werden für eine breite Öffentlichkeit u. a. aktuelle Meldungen zu Bedrohungen aus dem Internet, aber auch Themen zur Prävention präsentiert. Über diese ist die ZAC zu kontaktieren.

In Zusammenarbeit mit der Zentralstelle Prävention des Landeskriminalamtes Niedersachsen wird zudem die E-Mail-Adresse trojaner@zik-nds.de betrieben. Bei entsprechendem Verdacht wird eine Schadsoftwareanalyse angeboten, um u. a. frühzeitig auf der Webseite „Ratgeber Internetkriminalität“ vor neuer Schadsoftware oder erkannten Infektionswegen warnen zu können.

Durch Beratungen bzw. Vorträge bei Unternehmensverbänden (z. B. IHK und VDMA) werden zeitgleich zahlreiche mittelständische Unternehmen erreicht, um auf Gefahren, die Art und Weise der Ausführung von Angriffen, aber auch auf Schutzmaßnahmen hinzuweisen. Im Jahr 2017 wurden insgesamt 54 Vortragsveranstaltungen durchgeführt. Die ZAC ist zudem ständiger Vertreter im Arbeitskreis Cybersicherheit der IHK Hannover. Über eine bundesweite Vernetzung der ZAC-Dienststellen ist ein regelmäßiger Informationsaustausch gewährleistet.

Die Präventionsarbeit des Fachbereichs Wirtschaftsschutz im niedersächsischen Verfassungsschutz zur Abwehr von Angriffen fremder Staaten und ihrer Nachrichtendienste im Bereich der Cyberspionage umfasst die Beratung zu denselben Angriffswerkzeugen und Arten, wie sie auch im cyberkriminellen Bereich zum Einsatz kommen, und sind somit integraler Bestandteil des Unternehmensschutzes.

10. Wie will die Landesregierung die Bürgerinnen und Bürger Niedersachsens, aber auch Unternehmen vor Spionage von ausländischen Geheimdiensten oder Hackern schützen?

Für die Bürgerinnen und Bürger bieten beispielsweise die niedersächsischen Polizeibehörden im Deliktsumfeld der Internetkriminalität Beratungs- und Informationsangebote an. Dazu zählen u. a. der Ratgeber Internetkriminalität, eine „Cyber-Licence“ zur Erhöhung der Medienkompetenz im Zusammenwirken mit den kommunalen Schulträgern und weitere Informationsveranstaltungen. Die in den Vorbemerkungen der Landesregierung genannte Zentrale Ansprechstelle Cybercrime (ZAC) steht auch den Mitarbeiterinnen und Mitarbeitern von Firmen zur Verfügung.

Der niedersächsische Verfassungsschutz hat im September 2000 den Fachbereich Wirtschaftsschutz eingerichtet. Aufgabe des Wirtschaftsschutzes ist es u. a., niedersächsische Wirtschaftsunternehmen, insbesondere durch Aufklärung und Abwehr von Wirtschaftsspionage, vor Know-how-Verlust zu schützen.

Die Tätigkeiten des Arbeitsbereichs Wirtschaftsschutz im niedersächsischen Verfassungsschutz haben das Ziel, mit den innovativen und technologieorientierten Unternehmen in Niedersachsen ein

vertrauensvolles Verhältnis zu pflegen und zwischen Wirtschaft und Verfassungsschutz einen Dialog zu führen. Dieser gegenseitige Informationsaustausch soll bewirken, dass

– in der Wirtschaft eine Sensibilität für Gefährdungen durch Wirtschaftsspionage besteht,

– die Wirtschaft den Verfassungsschutz als kompetenten Ansprechpartner für Sicherheitsfragen und -vorfälle ansieht,

– sich durch ein erhöhtes Hinweisaufkommen die Erkenntnislage des Verfassungsschutzes verbessert,

– Sicherheitsmaßnahmen in den Unternehmen initiiert werden und

– durch Prävention Schäden durch Wirtschaftsspionage reduziert werden.

Der Wirtschaftsschutz hat sich in der niedersächsischen Wirtschaft gut etabliert und sich inzwischen zu einem stark nachgefragten Partner für die Wirtschaft entwickelt. Das Angebot umfasst Beratungen zu den Themen Wirtschaftsspionage, Cybersicherheit, Know-how-Schutz, Sicherheit in der Informations- und Kommunikationstechnologie, Geheimschutz in der Wirtschaft, Sicherheit auf Geschäftsreisen im Ausland, Innentäterproblematik und Social Engineering.

Zurzeit sind ca. 1 000 Unternehmen feste Kunden des Wirtschaftsschutzes. Im Jahr 2017 wurden 150 Vorträge und 80 individuelle Firmenberatungen durchgeführt.

(Verteilt am 25.04.2018)