LANDTAG NORDRHEIN-WESTFALEN
16. Wahlperiode

Drucksache **16/10826**

20.01.2016

Antwort

der Landesregierung

auf die Kleine Anfrage 4141 vom 14. Dezember 2015
des Abgeordneten Frank Herrmann PIRATEN
Drucksache 16/10480

Sicherheitsbewusstsein in der Landesverwaltung

Der Minister für Inneres und Kommunales hat die Kleine Anfrage 4141 mit Schreiben vom 19. Januar 2016 namens der Landesregierung im Einvernehmen mit der Ministerpräsidentin sowie allen übrigen Mitgliedern der Landesregierung beantwortet.

Vorbemerkung der Kleinen Anfrage

Die Berliner Polizei will ihre Beamten für das Thema der IT-Sicherheit sensibilisieren und hat dazu Phishing-Emails an ihre Beamten gesendet und geprüft, ob Polizisten dort ihre Zugangsdaten und Passwörter preisgeben. Nach Informationen des Tagesspiegels soll dabei die Hälfte der Beamten auf diesen Test hereingefallen sein.[1]

Vorbemerkung der Landesregierung:

Die Landesregierung hat die Einführung eines Informationssicherheitsmanagementsystems ISMS beschlossen. Dafür stellt sie ab dem kommenden Haushaltjahr 60 zusätzliche Stellen und jährliche Sachmittel in Höhe von 8.3 Mio. Euro zur Verfügung. Die bereits vorhandenen Maßnahmen zur Informationssicherheit sollen dadurch noch weiter verbessert werden.
Dazu zählen auch erweiterte Sensibilisierungskampagnen, die ergänzend zu den seit Jahren praktizierten Maßnahmen durchgeführt werden.

[1] http://www.tagesspiegel.de/berlin/telefonstreich-bei-der-berliner-polizei-attacke-noch-nicht-aufgeklaert/12659326.html

Datum des Originals: 19.01.2016/Ausgegeben: 25.01.2016

Die im Rahmen einer Kleinen Anfrage vorgegebenen Fristen lassen eine umfassende Beteiligung der nachgeordneten Bereiche in den Ressorts nicht zu. Daher wird im Wesentlichen auf die Situation in den Ministerien und oberer Landesbehörden sowie IT.NRW Bezug genommen.

1. Gab es in Nordrhein-Westfalen vergleichbare Tests mit dem der Berliner Polizei? (bitte aufschlüsseln nach öffentlicher Stelle und wesentlichen Ergebnissen)

Nein.

2. Auf welche Art und Weise führt das Land Nordrhein-Westfalen Schulungsmaßnahmen durch, um Mitarbeiter für das Thema Datensicherheit zu sensibilisieren? (bitte nach Maßnahmen und Schulungsinhalten aufgliedern)

Durch Informationsangebote im Intranet, Warnhinweise per E-Mail, Schulungsvideos, gedruckte Flyer und Poster werden allgemeine Verhaltensweisen und spezielle, aktuelle Gefährdungslagen vermittelt. Dabei sind zentrale Angebote des CERT NRW und auch lokale Angebote verfügbar. Die Ressorts haben einheitliche Sicherheitshinweise für die Beschäftigten der Landesverwaltung erarbeitet.

Darüber hinaus gibt es zum einen dezentrale IT-Sicherheitsschulungen und zum anderen vertiefende Lehrgänge im IT-Fortbildungsprogramm des Innenministers. Diese befassen sich mit dem BSI-Grundschutz, dem Erstellen sicherer Webanwendungen, Network Security Monitoring, Threat Modeling (Security by Design) und Live-Hacking Demonstrationen. Diese werden regelmäßig modernisiert und erweitert.

Zusätzlich werden Fortbildungsangebote anderer Anbieter genutzt. Der von der Bundesakademie für öffentliche Verwaltung BAköV angebotene „Lehrgang für Informationssicherheitsbeauftrage in der Verwaltung“ zählt dazu genau wie bedarfsgerechte Lehrgänge kommerzieller Anbieter zu speziellen technischen Fragestellungen. Für IT-Fachpersonal wurden auch Herstellerlehrgänge zu Fragen der IT-Sicherheit der verwendeten Produkte belegt.

3. Wie viele Mitarbeiter wurden in diesem Jahr für die Themen der IT- und Datensicherheit sensibilisiert und geschult? (bitte nach Organisationseinheiten aufschlüsseln)

Alle Mitarbeiterinnen und Mitarbeiter sind durch die oben genannten Maßnahmen für die Themen der IT- und Datensicherheit sensibilisiert.
Darüber hinaus wurden allein auf Ebene der Ministerien und oberen Landesbehörden sowie IT.NRW mehr als 800 Beschäftigte in Schulungen und Informationsveranstaltungen speziell unterwiesen. Die Angebote werden in den folgenden Jahren fortgesetzt und intensiviert.

Da diese Veranstaltungen meist ressortübergreifend durchgeführt werden, ist eine weitere Aufschlüsselung kurzfristig nicht möglich.

4. Wie stellt die Landesregierung sicher, dass alle Personen, die mit schützenswerten Daten arbeiten, auf Sicherheitsrisiken und übliche Angriffsszenarien hingewiesen werden?

In Arbeitsbereichen mit schützenswerten Daten sind technische und organisatorische Maßnahmen eingeführt.
Neben der Strukturierung von Zugriffsrechten und separaten Netzstrukturen sind auch spezielle Arbeitsanweisungen bis hin zu Sicherheitsüberprüfungen mit jährlich zu wiederholenden Unterweisungen eingeführt.

5. Welches Bild zeichnen in diesem Jahr durchgeführte Sicherheitstests von der IT- und Datensicherheit in der Landesverwaltung?

Durch die konsequente Anwendung der eigenen IT-Konzepte, den Einsatz des CERT NRW sowie die den Betrieb von zentralen Schutzmaßnahmen ist eine Grundsicherheit etabliert, die sich in den vergangenen Jahren sehr bewährt hat.

Trotzdem werden die Strukturen und Abläufe immer wieder kritisch hinterfragt und regelmäßig z.B. Penetrationstests an zentralen und dezentralen Verfahren durchgeführt; die Erkenntnisse daraus werden in unverzügliche Maßnahmen zur Verbesserung der Informationssicherheit überführt.

Die Landesregierung sieht sich in Fragen der Informationssicherheit bereits gut aufgestellt. Informationssicherheit ist kein Projekt, sondern ein andauernder Prozess. Die technische Entwicklung erzeugt immer wieder neue Sicherheitslücken. In diesem Bewusstsein hat die Landesregierung auch für den Schadensfall Maßnahmen im Sinne eines Risikomanagements getroffen, das die Auswirkung von eintretenden Schadensfällen abmildert oder ganz unterdrückt.