Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen

Der Minister

Ministerium für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen, 40190 Düsseldorf

An den
Vorsitzenden des
Ausschusses für Digitalisierung und
Innovation des Landtags Nordrhein-Westfalen
Herrn Thorsten Schick MdL
Platz des Landtags 1
40221 Düsseldorf

LANDTAG
NORDRHEIN-WESTFALEN
17. WAHLPERIODE

VORLAGE
17/6523

A20

Aktenzeichen
01.01.06.03-000106

Telefon 0211 61772-0

Sitzung des Ausschusses für Digitalisierung und Innovation am 10. März 2022

Sehr geehrter Herr Vorsitzender,

die Fraktion der SPD hat zur o.g. Sitzung um einen schriftlichen Bericht zum Thema **„Chaos Computer Club weist auf Datenleck in Nordrhein-Westfalen hin“** gebeten.

In der Anlage übersende ich den erbetenen Bericht, mit der Bitte um Weiterleitung an die Mitglieder des Ausschusses für Digitalisierung und Innovation.

Mit freundlichen Grüßen

Prof. Dr. Andreas Pinkwart

Dienstgebäude und Lieferanschrift:
Berger Allee 25
40213 Düsseldorf

Telefon 0211 61772-0
Telefax 0211 61772-777
poststelle@mwide.nrw.de
www.wirtschaft.nrw

Öffentliche Verkehrsmittel:
Straßenbahnlinien 706, 708,
709 bis Haltestelle Poststraße

Bericht der Landesregierung
„Chaos Computer Club weist auf Datenleck in Nordrhein-Westfalen hin“

Im Rahmen einer Meldung vom 14. Februar 2022 wiesen Sicherheitsforscher vom Chaos Computer Club (CCC) auf deutschlandweit mehr als 50 unzureichend gesicherte oder fehlkonfigurierte digitale Systeme verschiedener Unternehmen und staatlicher Institutionen hin, wovon in einem Fall auch die Landesverwaltung Nordrhein-Westfalen betroffen war. Es handelt sich hierbei um ein System, das vom Landesbetrieb Information und Technik (IT.NRW) für die Landesverwaltung Nordrhein-Westfalens betrieben wird.

1. Spezifikation des betroffenen Systems und Folgen

Die o.g. Sicherheitsmeldung des CCC betrifft unmittelbar ein unzureichend konfiguriertes Referenzsystem für das Verfahren „Meldeformular zur Barrierefreiheit“. Ein Referenz- oder Testsystem ist ein System, welches weitgehend identisch zu einem produktiv genutzten System konfiguriert ist. Auf einem derartigen System können Software-Änderungen unter produktionsnahen Bedingungen erprobt werden, bevor diese im Wirkbetrieb zum Einsatz kommen. Hierbei handelt es sich um ein gängiges technisches Verfahren zur Sicherstellung von nach Möglichkeit störungsfreier Durchführung kontinuierlicher Verbesserungsmaßnahmen an Software-Umgebungen.

Auf dem von IT.NRW betriebenen betroffenen Referenzsystem war aufgrund eines Konfigurationsfehlers eine Softwarekomponente für Diagnosezwecke aus dem Internet aufrufbar, die konzeptionell nur aus dem Landesnetz erreichbar sein sollte. Diese Komponente erlaubte Einsicht in Diagnose- und Protokollierungsdaten sowie Umgebungsvariablen. Mit Hilfe

dieser Umgebungsvariablen war der Einblick in Zugangsdaten für die Verwaltung des Referenzsystems auf Ebene der Fachanwendung möglich. Von der fehlerhaften Konfiguration waren insgesamt ausschließlich Daten dieser Fachanwendung betroffen. Sonstige auf dem Server verwaltete Daten waren zu keinem Zeitpunkt gefährdet.

Die unzureichend abgesicherte Softwarekomponente für Diagnosezwecke wurde unverzüglich nach Kenntnis über die problematischen Einstellungen außer Betrieb genommen. Es gibt keine Hinweise darauf, dass zu irgendeinem Zeitpunkt der bestehenden Fehlkonfiguration von der Anwendung verwaltete Daten missbräuchlich ausgeleitet, hinzugefügt, verändert oder gelöscht worden sind.

2. Vorgehen zur Behebung der unzureichenden Konfiguration

Der Veröffentlichung der o.g. Meldung des CCC ging ein sog. *Coordinated-Disclosure*-Verfahren voraus. Im Rahmen eines solchen Verfahrens kontaktiert ein Sicherheitsforscher eine Behörde oder ein Unternehmen vorab und schnellstmöglich, um über die Vermutung einer aufgefundenen Problematik zu informieren. Hierbei wird zugesichert, dass die öffentliche Besprechung der aufgefundenen sicherheitsrelevanten Situation erst nach vollumfänglicher Korrektur der Fehlkonfiguration erfolgt.

Unmittelbar nach Meldung der Problematik durch den CCC bei der zuständigen Stelle, dem zu IT.NRW gehörigen Computer Emergency Response Team des Landes Nordrhein-Westfalen (CERT NRW), wurde die betroffene Softwarekomponente außer Betrieb genommen und mit Maßnahmen zur Behebung der Problematik begonnen. Eine begleitende parallele konstruktive und wertschätzende Kommunikation mit dem Sicherheitsforscher des CCC fand statt. Der Sicherheitsforscher wies in diesem Kontext auf die rasche Reaktion und den vorbildlichen Umgang des CERT NRW mit der aufgefundenen Problematik hin.

3. Vom Bericht des CCC umfasste nordrhein-westfälische Unternehmen

Der Landesregierung verfügt über keine Informationen hinsichtlich Gestalt und Ausmaß der Sicherheitsvorfälle bei den von der CCC-Meldung ebenfalls umfassten und in Nordrhein-Westfalen beheimateten Unternehmen. Insbesondere besteht, mit Ausnahme von Betreibern kritischer Infrastruktur, keine allgemeine Meldepflicht von informationstechnischen Sicherheitsvorfällen an das Land.