LANDTAG NORDRHEIN-WESTFALEN
16. Wahlperiode

Drucksache **16/7759**

19.01.2015

Antwort

der Landesregierung

auf die Kleine Anfrage 2970 vom 9. Dezember 2014
des Abgeordneten Daniel Schwerd PIRATEN
Drucksache 16/7548

"Regin": Spionagewerkzeuge des NSA in freier Wildbahn. Was unternimmt die Landesregierung?

Der Minister für Inneres und Kommunales hat die Kleine Anfrage 2970 mit Schreiben vom 16. Januar 2015 namens der Landesregierung im Einvernehmen mit der Ministerpräsidentin und allen übrigen Mitgliedern der Landesregierung beantwortet.

Vorbemerkung der Kleinen Anfrage

> *Der Glaube an einen übernatürlichen Ursprung des Bösen ist nicht notwendig; die Menschen sind von sich aus zu jeder Gemeinheit fähig.* (Joseph Conrad)

Die IT-Sicherheitsunternehmen Symantec und Kaspersky Labs berichteten am 24. November 2014 von einer neuartigen Spionagesoftware, der sie den Namen „Regin“ gaben. Damit wurden seit 2008 Unternehmen, Forschung, Behörden und auch Privatpersonen ausgespäht. Regionale Schwerpunkte waren Russland und Saudi-Arabien mit je einem Viertel der Infektionen, aber auch Westeuropa, darunter Deutschland.

Etwa die Hälfte der Infektionen betraf Einzelpersonen und kleine Unternehmen, ein Viertel Unternehmen der Telekommunikationsbranche, weitere Schwerpunkte waren Energieunternehmen, Fluglinien, Gastgewerbe und Forschungseinrichtungen. Auch die EU-Kommission, sowie die Internationale Atomenergiebehörde IAEA waren Opfer der Malware.

Die Software wird als ausgesprochen komplex bezeichnet, die Software ist mehrstufig, modular und mehrfach verschlüsselt aufgebaut. Nur die erste Stufe der Infektion kann überhaupt entdeckt werden. Selbst nach der Entdeckung der Spionagesoftware ist es schwer festzustellen, was die Software auf dem befallenen Rechner tatsächlich im Einzelnen tut. Selbst Symantec sagt, der Leitungsumfang der Malware sei noch längst nicht vollständig

Datum des Originals: 16.01.2015/Ausgegeben: 22.01.2015

bekannt. Der modulare Aufbau erlaubt es, die Angriffssoftware auf das Ziel maßzuschneidern, abgefangene Daten werden verschlüsselt gespeichert und verschlüsselt kommuniziert.

Als Ersteller kommt nach Einschätzung der Sicherheitsunternehmen nur eine staatliche Stelle in Frage. Unterlagen, die der Enthüllungsplattform The Intercept vorliegen, verweisen auf den NSA und GCHQ als Urheber. Der Gründer der niederländischen IT-Sicherheitsfirma Fox IT vermutet, hinter dem Trojaner stecken die Spionageprogramme „Straitbizarre“ und „Unitedrake“ der NSA-Abteilung ANT.

Der starke Schwerpunkt auf kleine Unternehmen sowie Energie und Forschung legt den Schluss nahe, dass Wirtschaftsspionage ein Einsatzschwerpunkt der Software ist.

1. Welche Infektionen mit „Regin“ sind in Landesregierung, Ministerien, Landesbehörden und landeseigenen Betrieben NRWs aufgetreten? Nennen Sie jeden einzelnen Fall mit betroffener Stelle, Auswirkungen und Zeitpunkt der Feststellung.

Der Landesregierung liegen keine Erkenntnisse darüber vor, dass eine Infektion mit der Schad- bzw. Spionagesoftware „Regin“ innerhalb der Landesverwaltung stattgefunden hat.

2. Wie viele Infektionen von Kommunen, kommunalen Betrieben, Organisationen, Privatwirtschaft und Privatpersonen in NRW mit „Regin“ sind der Landesregierung oder ihren zuständigen Stellen bekannt? Nennen Sie die Zahl der Infektion aufgeschlüsselt nach dem jeweiligen Wirtschaftsbereich.

Der Landesregierung liegen keine eigenen Erkenntnisse über mögliche Infektionen mit der Schadsoftware „Regin“ in Stellen außerhalb der Landesverwaltung vor.

3. Welche Gefahren bestehen nach Ansicht der Landesregierung für Landesregierung, Ministerien, Landesbehörden sowie landeseigenen Betrieben durch „Regin“? Nennen Sie jedes Risiko, welches für jede der Infrastrukturen besteht.

Aufgrund bisher bekannter Informationen hat die Schadsoftware „Regin“ insbesondere folgende Angriffsziele:

- Ausspähen von Benutzereingaben
- Abfangen und Ausspähen von Zugangsdaten
- Ausspähen von Netzwerkverkehr
- Ausspähen von Daten über Prozesse und Hauptspeicher der kompromittierten Computer

Das Ausmaß der Gefährdung wäre entscheidend davon abhängig, wie schnell die Schadsoftware durch das Sicherheitssystem erkannt und bekämpft werden kann. Für die Landesverwaltung verweise ich hierzu auf die Antwort zur Frage 4.

4. Welche Maßnahmen hat die Landesregierung ergriffen, um Infektionen mit „Regin“ in Behörden, Ministerien, staatlichen Stellen sowie landeseigenen Betrieben zu erkennen bzw. abzuwehren? Nennen Sie jede einzelne Maßnahme mit Umsetzungszeitraum.

Die Landesregierung hat als zentrale Anlaufstelle für präventive und reaktive Maßnahmen in Bezug auf sicherheits- und verfügbarkeitsrelevante Vorfälle in IT-Systemen das „Computer Emergency Response Team“ (CERT) bei IT.NRW eingerichtet. Es arbeitet im Rahmen der Sicherheitsinfrastruktur mit den Behörden und Einrichtungen des Landes zusammen und ist in das Netz der CERTs von Bund und Ländern eingebunden. Durch eine enge, bundesweite Zusammenarbeit bei der Angriffserkennung, der Feststellung von Schwachstellen, u.a. durch Pene-trationstests und der konkreten Bekämpfung von Infektionen mit Schadsoftware wird den steigenden Gefährdungen im Bereich der IT-Sicherheit Rechnung getragen werden.
Darüber hinaus werden folgende Maßnahmen standardmäßig durchgeführt, um Hackerangriffe sowie Infektionen mit Schadsoftware abzuwehren bzw. zu erkennen:

- zentraler wie auch dezentraler Einsatz von Antivirusprodukten unterschiedlicher Hersteller
- schnellstmögliche Absicherung bekannter Schwachstellen
- Einschränkung von Nutzerrechten
- restriktive Firewallregeln auf Endgeräten und an Netzübergängen
- mehrstufige Firewalls zwischen Landesverwaltungsnetz und Internet
- Einsatz von Intrusion Detection & Prevention Systemen
- Warnung der Endanwender vor neuen Phishing-Wellen mit Schadsoftware

Darüber hinaus werden die genannten Schutzvorkehrungen im Verdachtsfall durch anlassbezogene Maßnahmen zur Schadensbegrenzung und -bekämpfung ergänzt. Trotz dieser umfassenden Schutzmaßnahmen kann es insbesondere gegen neue und hochkomplexe Schad- und Spionagesoftware keinen hundertprozentigen Schutz geben.

5. Welche Maßnahmen hat die Landesregierung ergriffen, um - ggf. durch das Landesamt für Verfassungsschutz - Kommunen, kommunalen Betriebe, Organisationen, Privatwirtschaft und Privatpersonen in NRW bei der Erkennung und Abwehr von Infektionen mit „Regin“ zu unterstützen bzw. proaktiv dagegen zu schützen? Nennen Sie jede einzelne Maßnahme mit Umsetzungszeitraum

Die Verantwortung für die Umsetzung geeigneter Sicherheitsmaßnahmen beim Einsatz der Informationstechnik liegt bei den jeweiligen privaten Organisationen bzw. den Kommunen. Dem Kommunalbereich hat der IT-Planungsrat zur Harmonisierung der Sicherheitsniveaus in der öffentlichen Verwaltung die Umsetzung der Sicherheitsleitlinie und der darin beschriebenen Sicherheitsmaßnahmen empfohlen. Das Land unterstützt die Wirtschaft durch Sensibilisierungsmaßnahmen zur IT-Sicherheit sowie den Kommunalbereich bei der Umsetzung der Sicherheitsleitlinie.