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
17/4780

A20

Aktenzeichen
01.01.06.03-000106
(bei Antwort bitte angeben)

Telefon 0211 61772-0

Sitzung des Ausschusses für Digitalisierung und Innovation am 14. Januar 2021

Sehr geehrter Herr Vorsitzender,

in der o.g. Sitzung hatte ich zugesagt, zu dem Thema **„Informationssicherheit in der Landesverwaltung NRW – Sicherheit der IT-Systeme“** einen umfassenden allgemeinen Bericht zu erstatten.

In der Anlage übersende den 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
„Informationssicherheit in der Landesverwaltung NRW – Sicherheit der IT-Systeme“

1. Vorbemerkung

In der 50. Sitzung des Ausschusses für Digitalisierung und Innovation vom 14.01.2021 bot Herr Minister Professor Pinkwart aufgrund von allgemeinen Fragen zum Stand der Informationssicherheit in der Landesverwaltung einen zusammenfassenden Bericht an. Dieses Angebot wird mit Vorlage dieses Beitrags erfüllt.
Nach Einschätzung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und des landeseigenen Computer Emergency Response Teams (CERT NRW) ist die Gefährdungslage als „Hoch“ einzuschätzen. Das bedeutet, dass jederzeit mit wirkungsvollen Cyberangriffen auf die staatlichen Institutionen und Einrichtungen des Landes zu rechnen ist.
Angreifer handeln aus unterschiedlichen Motiven. Jedoch besteht für die Abwehr von Gefährdungen ein großer Unterschied darin, mit welchem Hintergrund Angreifer die Landesverwaltung NRW ins Visier nehmen. Exemplarisch seien folgende Beispiel angeführt:

- Staatliche Akteure beabsichtigen dauerhaft unentdeckt zu bleiben, Informationen zu sammeln und diese auszuschleusen sowie im Konfliktfall endgültig und unwiderruflich die Kontrolle über informationstechnische Systeme zu erlangen bzw. diese zu zerstören.
- Kriminelle Organisationen beabsichtigen nur so lange unerkannt zu bleiben, bis sie sich eine Position erarbeitet haben, ihr Erpressungspotenzial ausspielen zu können.

- Aktivisten sind im Regelfall daran interessiert, ihre Botschaften zu verbreiten und politische Ansehensverluste herbeizuführen.
- Jugendliche oder andere Interessengruppen testen ihre Fähigkeiten aus einem Forschungs- oder Spieltrieb heraus, häufig zunächst mit nicht selbstprogrammierten, aber potenten Werkzeugen.

Staatliche Akteure stellen im Regelfall so mächtige Angreifer dar, dass ihre Aktionen häufig nur aufgrund von Erkenntnissen des Verfassungs- oder Staatsschutzes entdeckt werden. Für alle anderen Beispielsfälle besteht zumindest die Chance, gegen die Landesverwaltung gerichtete Aktionen mit eigenen Mitteln zu erkennen. Meist gelingt eine Verhinderung oder eine Abschwächung (Mitigation) des Angriffs. Für den Fall des Versagens aller Maßnahmen sind Notfallkonzepte erforderlich, die die zügige Wiederherstellung des ungestörten Betriebszustands ermöglichen.
Neben technischen Abwehr- und Härtungsmaßnahmen zählen die Vorfallserkennung (Detektion) und Reaktion sowie Datensicherungen (Backups) für einen Wiederaufbau informationstechnischer Systeme (Disaster Recovery) zu der Liste der erforderlichen Maßnahmen.
Absicherungen, die sich technisch nicht realisieren lassen, müssen organisatorisch aufgefangen werden. Durch die Sensibilisierung der Beschäftigten kann z.B. das Angriffsziel Mensch (Social Engineering) geschützt werden.
Jeder, auch erfolglose, Angriff schult den Angreifer in seinem Vorgehen. Daher ist es sinnvoll, sowohl über die eigenen Erfolgsfaktoren der Abwehr Stillschweigen zu wahren, als auch den nächsten Schritt der Evolution einer Angriffsmethode zu antizipieren. Jedwede Informationen helfen Angreifern. Daher wird der Berichtspflicht unter Verzicht auf die detaillierte Beschreibung technischer Umsetzungen und Gegenmaßnahmen nachgekommen.

2. Historische Einordnung

Die Bedeutung der Informationssicherheit wird in der Landesverwaltung von Nordrhein-Westfalen seit jeher als zugehörig zur Entwicklung der Informationstechnik begriffen und entsprechend behandelt. In der gegenwärtigen Transformationsphase der Gesellschaft aufgrund der fortschreitenden Digitalisierung aller Lebensbereiche, sind leistungsfähige Maßnahmen der Informationssicherheit eine unverzichtbare Grundvoraussetzung aller digitalen Angebote der Landesverwaltung.
Die Informationssicherheit in der Landesverwaltung ist daher eine gut in der Verwaltung verwurzelte Selbstverständlichkeit geworden. Folgende Meilensteine der Entwicklung sollen einen Eindruck über die Kontinuität und den bedarfsgerechten Ausbau geben:

- Umsetzung des BSI IT-Grundschutzes in der Landesverwaltung seit 1998
- Aufbau des CERT NRW mit Einrichtungsbeschluss im Jahr 2003
- Mitgliedschaft in der AG Informationssicherheit (IT-Planungsrat) seit 2013
- Gründungsmitglied des Verwaltungs-CERT-Verbunds (VCV) im Jahr 2013
- Beschluss der Leitlinie zur Informationssicherheit der Landesverwaltung Nordrhein-Westfalen (Informationssicherheitsleitlinie NRW) durch die Landesregierung im Jahr 2015
- Regelung der herausgehobenen Rolle des Beauftragten der Landesregierung Nordrhein-Westfalen für Informationstechnik (CIO) für die Koordinierung der Informationssicherheit in der Landesverwaltung nach § 22 Abs. 3 Nr. 5 EGovG NRW im Jahr 2016

- Vollständige Mitgliedschaft des Landes Nordrhein-Westfalen in der Allianz für Cybersicherheit seit dem Jahr 2018

3. Aufbau eines ressortübergreifenden Informationssicherheitsmanagementsystems

Mit der zunehmenden Vernetzung aller Lebensbereiche hat die Landesregierung im Jahr 2015 einen weiteren Schritt zur Qualitätssteigerung vollzogen. Auf Basis der Landesverfassung ist zwar das Ressortprinzip verbindlich, allerdings ordnet sich diese Verantwortung in ein System der Koordinierung der informationstechnischen Sicherheit durch den Beauftragten der Landesregierung für Informationstechnik (CIO) ein. Durch ein gemeinsames, abgestimmtes Vorgehen wird seither die Zusammenarbeit und der Austausch zwischen den Ressorts genutzt, um verbindliche Mindeststandards umzusetzen. Dies dient dem wirtschaftlichen Ressourceneinsatz durch Kooperation und gemeinsam genutzten Lösungen.
Da das Informationssicherheitsmanagement eine Verantwortung der obersten Leitungsebene ist, wurde 2015 die Informationssicherheitsleitlinie NRW durch das Kabinett als Verwaltungsvorschrift beschlossen.
Auf dieser Basis wurden zur Unterstützung und Beratung des Beauftragten der Landesregierung für Informationstechnik (CIO) sowie der Ressortleitungen die Rollen des Informationssicherheitsbeauftragten der Landesverwaltung (Chief Information Security Officer – NRW CISO) und der Informationssicherheitsbeauftragten der Ressorts (Ressort-CISOs) geschaffen. Damit ist die notwendige Unterstützung und Beratung der Leitungsebene sichergestellt, um dieser Verantwortung in einem hochtechnisierten und komplexen Umfeld gerecht werden zu können.
Der Informationssicherheitsbeauftragte der Landesverwaltung (NRW CISO) hat nach der Informationssicherheitsleitlinie NRW unter anderem die Aufgabe, die Wirksamkeit der Umsetzung von vereinbarten Maßnahmen zu prüfen.

Das Vorgehensmodell, das in Nordrhein-Westfalen verpflichtend zur Anwendung kommt, ist der IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Somit hat sich die Landesregierung dazu bekannt, die Informationssicherheit in der Landesverwaltung in einem kontinuierlichen Verbesserungsprozess weiterzuentwickeln. Dazu wird dauerhaft die Finanzierung von Stellen und investiven Mitteln für die Ressorts bereitgestellt.

4. Das Landesverwaltungsnetz

Der zentrale technische Baustein, der sowohl die Zusammenarbeit der Ressorts mit Zugriff auf einheitliche Verfahren ermöglicht, als auch einen regulierten und zentral zu schützenden Bereich darstellt, ist das Landesverwaltungsnetz (LVN).

Der Betrieb des Landesverwaltungsnetzes (LVN) ist als hoheitliche Aufgabe dem Landesbetrieb IT.NRW sowie den Sondernetzbetreibern (Landesamt für Zentrale Polizeiliche Dienste, Rechenzentrum der Finanzverwaltung) übertragen. In einer gemeinsamen Ausschreibung beschaffen diese Netzbetreiber der Landesverwaltung regelmäßig Datenübertragungskapazitäten, auf die dann in einem isolierten Netz eigene Betriebsleistungen aufgebracht werden. Der Vorteil liegt in einem abgegrenzten technischen Rahmen, der unbeeinflusst von äußeren Einflüssen auch in Krisensituationen eine stabile und leistungsfähige Verwaltungsplattform bietet. Das Vorgehen hat sich in mehr als zwei Jahrzehnten als äußerst zuverlässig und flexibel skalierbar erwiesen. Durch dieses geschlossene Ökosystem ist ein Eindringen in die Verwaltungsstrukturen extrem erschwert.

Durch diese technische Abgrenzung können auch einheitliche Mindeststandards definiert und umgesetzt werden. Diese sind von allen Behörden

und Einrichtungen als Anschlussbedingungen einzuhalten und eigenverantwortlich durch gleichwertige Maßnahmen für die nach dem Ressortprinzip selbstbetriebenen Infrastrukturen zu ergänzen.

5. Netzübergänge

Der Betrieb von gesicherten Übergängen aus dem Landesverwaltungsnetz (LVN) zum Internet und zu Netzen Dritter ist ausschließlich den Netzbetreibern des Landes gestattet. Diese müssen an den Netzübergängen Sicherheitstechnik einsetzen, die nach den Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) oder vergleichbaren und anerkannten europäischen Standards zertifiziert ist. Damit ist sichergestellt, dass ausschließlich ausgebildetes Fachpersonal diese neuralgischen Punkte zuverlässig betreibt und die Technologie beherrscht.
Kommunikation wird grundsätzlich einseitig aus dem Landesverwaltungsnetz (LVN) in Richtung fremder Netze aufgebaut, sodass unerwünschte Kommunikation von fremden Netzen in Richtung des Landesverwaltungsnetzes (LVN) pauschal abgewiesen werden kann.
Für gewünschte Verbindungen in Richtung der Landesverwaltung bestehen streng regulierte Ausnahmen. Dafür stehen besonders gesicherte und einheitlich betriebene Verfahren zur Verfügung, beispielsweise für die Telearbeit oder die Fernwartung.
Für den gesicherten, mobilen Zugriff auf Ressourcen im Landesverwaltungsnetz (LVN) stehen geeignete Lösungen für Smartphones und Tablets der Beschäftigten zur Verfügung.
Dem Zugang von E-Mails in das Landesverwaltungsnetz (LVN) ist über ein vielstufiges System eine Erkennung von unerwünschter Kommunikation (SPAM) und Schadsoftware durch Scans vorgeschaltet. Hiermit können bis zu 70 % der eingehenden Nachrichten rechtskonform abgelehnt werden, die sich als unerwünscht oder schädlich einordnen lassen. Die

Ablehnung ist mit einem Hinweis an den Absender für den Fall eines Irrtums versehen. Die Fehlerquote ist zu vernachlässigen. Das schützt die Beschäftigten der Landesverwaltung mit hoher Zuverlässigkeit vor SPAM und Schadsoftware und entlastet gleichzeitig.

Die Kommunikation mit anderen Verwaltungsstrukturen erfolgt z.B. nach dem Gesetz über die Verbindung der informationstechnischen Netze des Bundes und der Länder (IT-NetzG) über das sogenannte Verbindungsnetz. Hier ist eine jederzeitige, krisensichere und abgesicherte Verwaltungskommunikation mit Bund, Ländern und Kommunen möglich. Gemäß den Anschlussbedingungen ist für das Verbindungsnetz ebenfalls eine BSI-Zertifizierung erforderlich.

Der Zugriff auf Netze Dritter wird den Beschäftigten der Landesverwaltung über lokale Proxyserver (Dienstevermittler) in den Behörden angeboten. Diese lokalen Dienstevermittler greifen dann bei den Netzbetreibern der Landesverwaltung über weitere zentrale Proxyserver zu. Dadurch bestehen Schutzmöglichkeiten an mehreren Punkten für alle browserbasierten Anwendungen.

Trotz aller zentralen Maßnahmen gelangt Schadsoftware in das Landesverwaltungsnetz (LVN). Über mit Schadcode versehene und unerkannte E-Mails und durch die Übertragung von Schadcode über verschlüsselte Kanäle, die aus dem Landesverwaltungsnetz (LVN) nach außen initialisiert wurden, ist dies etwa möglich. In einem solchen Fall werden lokale Maßnahmen in den Behörden aktiv, um eine Infektion zu stoppen und Schäden zu verhindern oder jedenfalls zu begrenzen. Die Sensibilisierung der Beschäftigten über die bestehenden Restrisiken und das korrekte Verhalten im Schadensfall über die Kampagne „Na sicher! NRW“ rundet die vorgesehenen Maßnahmen ab.

6. Elektronisches Verwaltungshandeln

Verwaltungsverfahren werden in der Regel durch die IT-Dienstleister/Netzbetreiber der Landesverwaltung in professionellen Rechenzentren betrieben. Dort sind physische Sicherungen für den Zutritt, Sabotageschutz, unterbrechungsfreie Stromversorgung, Klimatisierung, (Gas-)-Löschanlagen, (Geo)-Redundanzen, Sicherungskonzepte usw. etabliert. Insbesondere zentrale Basiskomponenten, die im Auftrag des Beauftragten der Landesregierung für Informationstechnik (CIO) oder des Ministeriums für Wirtschaft, Innovation, Digitalisierung und Energie für alle Ressorts bereitgestellt werden, werden nach den Prinzipien des IT-Grundschutzes des Bundesamtes für Sicherheit in der Informationstechnik (BSI) in einem kontinuierlichen Verbesserungsprozess abgesichert.

IT.NRW betreibt als Dienstleister des Landes eine Betriebsinfrastruktur, die seit 2018 BSI-zertifiziert ist und in diesem Jahr rezertifiziert werden wird. Wird diese Infrastruktur als Plattform für das Verwaltungshandeln der Ressorts genutzt, steht das etablierte Niveau der Informationssicherheit soweit zur Verfügung, dass nur eine Systemhärtung auf Ebene der Anwendung ergänzt werden muss.

Für alle E-Government-Verfahren des Beauftragten der Landesregierung für Informationstechnik (CIO) oder des Ministeriums für Wirtschaft, Innovation, Digitalisierung und Energie ist seit Inkrafttreten der Informationssicherheitsleitlinie NRW ein Penetrationstest vor Inbetriebnahme obligatorisch. Ein Penetrationstest ist ein simulierter Hackerangriff auf ein produktionsnahes Testsystem durch fachlich versierte Spezialisten. Diese wenden aus dem Blickwinkel von Hackern vergleichbare Angriffsmethoden an und bestimmen die Widerstandskraft des Systems. Nach objektiven Bewertungskriterien (CVSS: Common Vulnerability Scoring System) werden die so aufgedeckten Sicherheitslücken bewertet und es wird ein Fehlerbehandlungsplan erarbeitet, um sie vor Inbetriebnahme zu schließen.

Für Bestandsverfahren der Landesverwaltung führt das CERT NRW regelmäßige, automatisierte Schwachstellenscans durch. Erneute Penetrationstests sind erst bei wesentlichen Änderungen der Infrastruktur oder Architektur erforderlich.

7. Computer Emergency Response Team NRW

Das CERT NRW ist ressortübergreifend für die gesamte Landesverwaltung zuständig und wird fachlich durch den Informationssicherheitsbeauftragten der Landesverwaltung (NRW CISO) im Auftrag des Beauftragten der Landesregierung für Informationstechnik (CIO) gesteuert.
Das Grundprinzip des Handels des CERT NRW wird mit „Assume Compromise“ charakterisiert: Es wird davon ausgegangen, dass Angreifer einen Weg in das Landesverwaltungsnetz (LVN) finden. Daher genügt es also nicht, das Eindringen möglichst schwer zu machen. Es muss auch aktiv nach eventuell gelungenen Angriffen gesucht werden. Entscheidend ist, Cyber-Attacken schnell zu entdecken und auf diese nach vorbereiteten Abläufen zu reagieren.
Als Kopfstelle für Warn- und Informationsmeldungen in der Landesverwaltung und in den angeschlossenen CERT-Verbünden müssen Informationen über Bedrohungen schnell fließen. Durch die Vernetzung mit anderen CERTs und den Austausch von Informationen erweitert sich der Horizont für das Lagebild entscheidend. Das CERT NRW erstellt auch eigene Warnmeldungen und bereitet aus externen Quellen eingehende Warnungen für die Landesverwaltung auf. Für die Prüfung der Betroffenheit und Umsetzung der Maßnahmen sind dann die verfahrensverantwortlichen Personen in den Ressorts zuständig.
In der Landesverwaltung besteht eine Meldepflicht für alle Beschäftigten, Sicherheitsvorfälle unverzüglich zu melden. Gemäß einer Richtlinie sind die Meldewege dazu definiert. Sobald das CERT NRW beteiligt wird, kann

es mit Fehleranalysen unterstützen, Gegenmaßnahmen empfehlen und bis zum späteren Wiederanlauf eines betroffenen Systems begleiten.
Um die fachliche Expertise ständig zu erweitern und Trends zu erkennen, sind im CERT NRW auch aktive Recherchen in Quellen verschiedenster Art erforderlich. Das Networking in Cybersicherheitszirkeln, Hospitationen mit anderen CERTs und die Mitwirkung an externen Projekten steigert das Fachwissen und festigt die vertrauensvolle Zusammenarbeit. Das CERT NRW bietet allen Behörden und Einrichtungen Beratung, Schulung, Penetrationstests, Schwachstellenscans sowie forensische und Bedrohungsanalysen an.
Die Dienstleistungen des CERT NRW werden planmäßig noch in diesem Jahr im 24/7 Modus angeboten. Gegenwärtig sind Angebote an die NRW-Kommunen gerichtet, schrittweise von den CERT NRW-Dienstleistungen zu profitieren.

8. Erfahrungen

Das Zusammenspiel von Erfahrungen aus Jahrzehnten eines sicheren IT-Betriebs in landeseigenen Infrastrukturen, organisatorischer Verantwortungszuweisung, verbindlichen Mindeststandards sowie technisch und wirtschaftlich sinnvollen Maßnahmen zur Absicherung ist das Grundgerüst, auf dem die Informationssicherheit zum Schutz der Landesverwaltung erfolgreich wirken kann.
Motivierte und fachlich hervorragende Teams waren Voraussetzung, diesen Zustand zu erreichen und sind es weiterhin, um diesen Zustand zu erhalten. Das ist im Hinblick auf den Wettbewerb um die klügsten Köpfe am Arbeitsmarkt die größte Herausforderung. Der kriminellen Energie von Angreifern muss man die Macht vernetzter Intelligenz und den Spieltrieb der eigenen Experten entgegenstellen. Jede Technologie ist letztlich trotz

aller Schutzmaßnahmen überwindbar. Es handelt sich im Grunde um einen Kampf des Intellektes zweier Fraktionen in einem technischen Umfeld.

Die nichttechnischen Angriffsszenarien sind von gleichwertiger Bedeutung. Angreifer attackieren das schwächste Glied in der Kette zur effektiven Durchsetzung ihrer Ziele; das ist meistens der Mensch. Ein psychologisch geschulter Angreifer kann ohne technisches Hintergrundwissen über das Personal das Eindringen in eine IT-Infrastruktur bewerkstelligen. Daher ist die konstante Sensibilisierung der Beschäftigten über solche Methoden wichtig, damit keine Ermüdung oder innere Ablehnung einer angemessenen Vorsicht auftritt.

Informationssicherheit ist eine dauerhaft und kontinuierlich zu betreibende Aufgabe, die mit den notwendigen Ressourcen versehen leistbar ist, bei der ein Erfolg aber nicht vollständig garantiert werden kann.

9. Aus aktuellem Anlass: „Mehrere Schwachstellen in Microsoft Exchange Server“

Am Mittwochmorgen, den 03.03.2021, konnten erste Warnungen recherchiert werden. Am Mittag warnte das Bundesamt für Sicherheit in der Informationstechnik (BSI) vor einer kritischen Schwachstelle in Microsoft Exchange (höchstmögliche „Warnstufe 4 / Rot“: Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrechterhalten werden.) Darin wird vor einem Angriff mutmaßlich staatlicher Akteure gewarnt. Ziel des Angriffs seien amerikanische Forschungseinrichtungen mit Pandemie-Fokus, Hochschulen, Anwaltsfirmen, Organisationen aus dem Rüstungssektor, Think Tanks und NGOs. Microsoft vermutet hinter den Vorfällen eine staatliche Hackergruppe aus China, die HAFNIUM genannt wird.

Das landeseigene Computer Emergency Response Team (CERT NRW) hat die Warnungen ausgewertet und an die zuständigen Fachbereiche zur zügigen Umsetzung der Empfehlungen gesteuert. IT.NRW hat für sich und seine Kunden diese Maßnahmen direkt umgesetzt.

Innerhalb der nächsten Tage folgten weitere differenzierte Informationen, die ebenfalls sofort bewertet wurden. Dadurch ließ sich für die Landesverwaltung aber keine weitere Risikoerhöhung ableiten. Nach dem aktuellen Ermittlungsstand (08.03.2021, 12 Uhr) auf Basis der gegenwärtigen Erkenntnisse sind die Systeme der Landesverwaltung nicht kompromittiert worden.