Ministerium der Justiz
des Landes Nordrhein-Westfalen
Der Minister

Ministerium der Justiz Nordrhein-Westfalen, 40190 Düsseldorf

Präsident des Landtags Nordrhein-Westfalen
Herrn André Kuper MdL
Platz des Landtags 1
40221 Düsseldorf

für die Mitglieder
des Rechtsausschusses

LANDTAG
NORDRHEIN-WESTFALEN
18. WAHLPERIODE

VORLAGE
18/2728

A14

24.06.2024

Aktenzeichen
1500-IT.90/IT-Sicherheit-allgemein
bei Antwort bitte angeben

Bearbeiter: Herr Dr. Czaplik
Telefon: 0211 8792-278

43. Sitzung des Rechtsausschusses des Landtags am 26. Juni 2024
Bericht zu TOP „Bericht der Landesregierung zur digitalen Infrastruktur und IT-Sicherheit in der nordrhein-westfälischen Justiz“

Anlage
1 Bericht

Sehr geehrter Herr Landtagspräsident,

zur Information der Mitglieder des Rechtsausschusses übersende ich als Anlage einen öffentlichen Bericht zu dem o. g. Tagesordnungspunkt.

Mit freundlichen Grüßen

Dr. Benjamin Limbach

Dienstgebäude und
Lieferanschrift:
Martin-Luther-Platz 40
40212 Düsseldorf
Telefon: 0211 8792-0
Telefax: 0211 8792-456
poststelle@jm.nrw.de
www.justiz.nrw

Ministerium der Justiz
des Landes Nordrhein-Westfalen

43. Sitzung des Rechtsausschusses
des Landtags Nordrhein-Westfalen
am 26. Juni 2024

Schriftlicher Bericht zu TOP
„Bericht der Landesregierung zur digitalen Infrastruktur und IT-Sicherheit in der nordrhein-westfälischen Justiz“

1. **Wie entwickelte sich die Anzahl der IT-Mitarbeiter beim Zentralen IT-Dienstleister der Justiz des Landes NRW (ITD) seit dem 01.07.2022?**

Die besetzten Stellenanteile zu den jeweiligen Stichtagen ergeben sich aus folgender Tabelle:

	zugewiesene Stellen(-anteile)	besetzte Stellenanteile
30.06.2022	552,98	451,93
31.12.2022	552,98	464,38
30.06.2023	552,98	472,97
31.12.2023	552,98	465,51
15.06.2024	554,98	473,95

Zu anderen Stichtagen ist keine Ermittlung der Stellenbesetzungen möglich.

2. **Wie viele Stellen sind beim Zentralen IT-Dienstleister der Justiz des Landes NRW (ITD) derzeit vakant?**

Zum Stichtag 15.06.2024 sind insgesamt 81,03 Stellen unbesetzt.

3. **Wie ist die Überwachung und Reaktion auf Sicherheitsvorfälle beim IT-Dienstleister organisiert? (Bitte bei der Beantwortung der Frage auf die Anzahl der Mitarbeiter im IT-Sicherheitsteam und deren berufliche Qualifikation eingehen)**

Die Überwachung und Reaktion auf Sicherheitsvorfälle ist beim ITD prozessual und standardisiert in entsprechenden Richtlinien geregelt, die sich in das System der landesweiten bzw. justizweiten Richtlinien einfügt. Diese Regelungen und deren Umsetzung waren in den vergangenen drei Jahren des Zertifizierungsprozesses immer wieder ein zentraler Prüfpunkt im Rahmen der Audits und wurde von den Auditoren durchgängig als positiv herausgehoben.

Die geregelten Prozesse definieren im Besonderen

1. die umgehende Identifikation möglicher Sicherheitsvorfälle (unterschiedlichster Art),
2. deren unverzügliche Weiterleitung an die für die Behandlung des Vorfalls zuständige Stelle,
3. deren Erstbewertung zur Festlegung möglicher weiterer Eskalationsstufen,
4. die Verantwortung zur Behandlung des Vorfalls und Vermeidung/Minimierung eines möglichen Schadenseintritts und
5. die Meldung an maßgebliche „interessierte Parteien".

Zur Überwachung und Reaktion dienen konkret u. a. folgende Werkzeuge:

1. Zentrale Malware-Systeme, automatisierte Behandlungsmechanismen und Prozesse bei Malware-Funden,
2. Firewall-Instanzen inklusive Intrusion Detection Systems (IDS),
3. Security Information and Event Management-System (SIEM),
4. Ticket-System zur unverzüglichen Aufnahme und Weiterleitung sowie Dokumentation von Vorfällen,
5. klar definierte Meldewege und Eskalationsprozesse (bis hin zur Notfallbewältigung) sowie
6. kurze Kommunikationswege zwischen operativer IT-Sicherheit und strategischer Informationssicherheit bzw. Notfallmanagement.

Die Überwachung und Reaktion wird – neben den für die operative Administration (Systeme, Netze, Firewalls etc.) zuständigen Beschäftigten –

1. durch drei Mitarbeiterinnen und Mitarbeiter in der Stabsstelle Sicherheit bei ITD 6 - Zentraler IT-Betrieb und Betriebsvorbereitung - und
2. sieben Mitarbeiterinnen und Mitarbeiter (6,5 AKA) in der strategischen Informationssicherheit in ITD 7 - IT-Sicherheit und Datenschutz - (wobei absehbar ein personeller Zuwachs um 1,0 AKA durch die Nachbesetzung einer Stelle des richterlichen Dienstes zu erwarten ist)

durchgeführt bzw. gesteuert.

Die Beschäftigten der operativen Bereiche verfügen über eine aufgabenbezogene, laufbahnadäquate Qualifikation und werden sowohl fachbezogen wie auch im Thema Informationssicherheit fortgebildet.

Die Beschäftigten im Bereich der Informationssicherheit (Stabsstelle ITD 6, ITD 7) verfügen unter anderem über folgende Qualifikationen:

1. (teilweise, mit Ausnahme der richterlichen Mitarbeiterinnen und Mitarbeiter) Bachelor-/Master-Qualifikation in IT-nahen Themengebieten oder vergleichbare Qualifikation
2. (größtenteils) Zertifizierte ISO-Officer nach ISO 27001 und/oder TÜV-geprüfter Informationssicherheitsbeauftragter nach BSI
3. Fortbildungen in den Bereichen Incident-Management, BSI-IT-Grundschutz, Notfallmanagement etc.
4. Kontinuierliche Fortbildungen in relevanten Themenbereichen

4. **Mit welchen präventiven Maßnahmen erhöht die Landesregierung die IT-Sicherheit in der nordrhein-westfälischen Justiz? (Bitte bei der Beantwortung der Frage auf den Einsatz fortschrittlicher Sicherheitslösungen wie z.B. Firewalls, Anti-Malware-Software und Intrusion Detection Systems (IDS) und Verschlüsselungstechnologien eingehen)**

Für das Rechenzentrum sind beispielhaft folgende (infrastrukturelle) Maßnahmen getroffen:

1. Präventiver Schutz durch zentrale Datenhaltung im Rechenzentrum der Justiz („Zentralisierung", zentraler Citrix-Arbeitsplatz, Speicherung der Daten im geschützten Rechenzentrum (RZ))
2. Rechenzentrumsinfrastruktur mit
    a. umfassenden Redundanzen der IT-Systeme (Storage (RAID), Firewalls, Netzkomponenten, Leitungen, Spiegel-RZ, georedundanter Standort des RZ),
    b. Unterbrechungsfreie Stromversorgung (USV),
    c. Netzersatzanlage (NEA),
    d. Brandmeldeanlage (BMA),
    e. Einbruchmeldeanlage (EMA),
    f. Videoüberwachung des RZ,
    g. gesicherte Zutrittssystem (Vereinzelung), geregelter und restriktiver Zutrittsprozess etc.

Netzseitig sind umfangreiche Maßnahmen getroffen. Hierzu zählen z. B.

1. zentrale Firewallsysteme, IDS,
2. Schutz durch das LVN (Firewall-Gateways, Mail-Gateways, zentrale Malware-Mechanismen, Sperrlisten „bösartiger" Webseiten),
3. Zentrale Anti-Malware-Systeme,
4. SIEM zur proaktiven Erkennung möglicher Angriffe und Vorfälle,
5. Firewalls in den Justiz-Standorten.

Die Kommunikation zwischen den lokalen Endgeräten und den zentralen „Citrix-Arbeitsplätzen" erfolgt verschlüsselt.

Internet- und Intranet-Angebote der Justiz (https) sowie interne Kommunikationsverbindungen zwischen Systemen (z. B. Server-zu-Server-Kommunikation) erfolgen durchgängig verschlüsselt.

Zudem wird in der ISMS Richtlinie „Klassifizierung" geregelt, dass je nach Vertraulichkeit der Informationen diese ggf. zu verschlüsseln sind. Zu diesem Zweck

werden DOI-CA-Zertifikate und „GnuPG for WinDesktop“ zur Verschlüsselung von E-Mails inkl. deren Anlagen eingesetzt.

Ferner ist zu beachten, dass das aktuelle (relevante) Geschehen kontinuierlich beobachtet wird. Dies geschieht unter anderem durch Abonnement und unverzüglich Auswertung insbesondere des BSI-Tageslageberichts, von WID- und von CERT-Meldungen. Schließlich findet jährlich eine Risikoanalyse statt. Hierzu wurde im Audit-Bericht aus dem Mai 2024 von externen Auditoren positiv festgehalten, dass das Risikomanagement sehr gut prozessual definiert sei und gut umgesetzt werde.

5. In welchen Abständen werden die IT-Sicherheitsrichtlinien in der nordrheinwestfälischen Justiz überprüft?

Die Sicherheitsrichtlinien und weitere gelenkte Dokumente zur Informationssicherheit werden zyklisch spätestens alle zwei Jahre sowie anlassbezogen auf ihre Aktualität evaluiert, bei Bedarf aktualisiert und allen Beschäftigten erneut bekannt gegeben.

Zudem werden die ISMS-Richtlinien des ITD im Rahmen des Zertifizierungsprozesses in halbjährlichen Audits auf ihre Vollständigkeit, Aktualität und Einhaltung durch externe Auditoren überprüft.

6. Wie werden Mitarbeiter für den sicheren Umgang mit IT-Ressourcen und Daten sensibilisiert?

Die Beschäftigten der Justiz werden sowohl anlassbezogen durch entsprechende Awareness-E-Mails bei akut auftretenden Vorfällen (z. B. bei Kompromittierung von potentiellen Kommunikationspartnern oder bei Malware-Kampagnen) als auch kontinuierlich auf unterschiedlichen Kanälen (gedruckte und Online-Flyer, Online-Schulungsangebote, Informationssicherheitstage, Vortragsveranstaltungen, Live-Hackings) sensibilisiert.

Die Beschäftigten des ITD werden noch einmal eigens kontinuierlich geschult und sensibilisiert. Hierzu existiert ein Schulungskonzept inkl. eines ständig aktualisierten Schulungsplanes. Letzterer beinhaltet u. a.

1. zyklische Sensibilisierungs-E-Mails und Hinweise auf themenspezifische Internet-/Intranet-Angebote (z. B. „Deutschland sicher im Netz“)
2. strukturierte Ersteinweisung in Informationssicherheit und Datenschutz im Rahmen des Onboarding-Prozesses
3. verpflichtende Web-based-Trainings (WBTs) für bestimmte (administrative) Rollen
4. regelmäßige Schulungsangebote zum Thema „Informationssicherheit und Datenschutz“
5. regelmäßige simulierte Phishing-Kampagnen.

7. **Zu „Mein Justizpostfach“: Liegen der Landesregierung Erkenntnisse über das Nutzungsverhalten der Bürger in Nordrhein-Westfalen vor?**

Hier liegen keine Erkenntnisse bezogen auf NRW vor. Nach Angaben der BLK-AG IT Standards (EGVP-Projektbüro) existieren bundesweit 8.386 Postfächer. Angaben bezogen auf ein Bundesland können derzeit nicht geliefert werden.

8. **Zu „Mein Justizpostfach“: Liegen der Landesregierung Erkenntnisse zum Anteil elektronischer Einreichungen insbesondere von Sachverständigen und Berufsbetreuern vor?**

Hierzu liegen keine Erkenntnisse vor, da diese Daten nicht gesondert erfasst werden.

9. **Zu „Mein Justizpostfach“: Führte die Einführung dieser Kommunikationsmöglichkeit bereits zu der von den Gerichten erhofften Reduzierung des „Scanaufwands“ in der Justiz?**

Hierzu liegen keine Erkenntnisse vor, da diese Daten nicht gesondert erfasst werden.