Abgeordnetenhaus BERLIN

Drucksache 19 / 11 404
Schriftliche Anfrage

19. Wahlperiode

Schriftliche Anfrage

des Abgeordneten Roman-Francesco Rogat (FDP)

vom 30. März 2022 (Eingang beim Abgeordnetenhaus am 31. März 2022)

zum Thema:

Sensibilisierung der Mitarbeiter von Berliner Verwaltung für das Thema Phishing

und **Antwort** vom 20. April 2022 (Eingang beim Abgeordnetenhaus am 21. April 2022)

Senatsverwaltung für Inneres, Digitalisierung und Sport

Herrn Abgeordneten Roman-Francesco Rogat (FDP)
über
den Präsidenten des Abgeordnetenhauses von Berlin

über Senatskanzlei - G Sen -

Antwort
auf die Schriftliche Anfrage Nr. 19/11404
vom 30.03.2022
über Sensibilisierung der Mitarbeiter von Berliner Verwaltung für das Thema Phishing
---

Im Namen des Senats von Berlin beantworte ich Ihre Schriftliche Anfrage wie folgt:

1. Welche Maßnahmen werden in den einzelnen Verwaltungen getroffen, um Mitarbeiter über das Thema Cybersicherheit im Berufsalltag aufzuklären? (Bitte tabellarisch nach Berliner Verwaltung auflisten.)

Zu 1.:
Cybersicherheit umfasst alle Aspekte der Sicherheit in der Informations- und Kommunikationstechnik und ist dabei ein Bestandteil zur Gewährleistung der Informationssicherheit in den Behörden und Einrichtungen der Berliner Verwaltung. Die grundlegenden Ziele, Anforderungen und die Strategie der Informationssicherheit werden in der Leitlinie zur Informationssicherheit der Landesverwaltung des Landes Berlin (Informationssicherheitsleitlinie – InfoSic-LL) festgelegt. Ein Grundsatz der Informationssicherheitsleitlinie ist dabei die Einbindung aller Beschäftigten im Sicherheitsmanagementprozess durch regelmäßige Schulung und Sensibilisierung hinsichtlich der Cybersicherheit.

Nach den umzusetzenden Standards des BSI liegt die Verantwortung für die Informationssicherheit der Einrichtungen bei den jeweiligen Leitungen.

Hinsichtlich der getroffenen Maßnahmen bezüglich der Aufklärung von Mitarbeitenden über das Thema Cybersicherheit im Berufsalltag, sind nachstehende Meldungen aus der Berliner Verwaltung eingegangen:

Amt für Statistik Berlin-Brandenburg	
Maßnahme Nr. 1	Anpassung Patch-Management
Maßnahme Nr. 2	regelmäßige Informationen an die Beschäftigten bezüglich der aktuellen Bedrohungslage
Maßnahme Nr. 3	regelmäßige Informationen an die Beschäftigten bezüglich der aktuellen Angriffsszenarien
Maßnahme Nr. 4	der Prozess der Vorfallsmeldung wurde einem PDCA unterzogen und erneut im Haus publiziert
Amts-, Staats-, und Generalstaatsanwaltschaft	
Maßnahme Nr. 1	IT-Sicherheit ist Bestandteil der IT-Grundschulung von neu eingestellten Mitarbeitenden
Maßnahme Nr. 2	Anlassbezogene Weiterleitung von Berlin-CERT-Mitteilungen mit ggfs. behördenspezifischen Ergänzungen
Maßnahme Nr. 3	Anlassbezogene Informationen bei Anfragen an die IT-Hotline
Berliner Feuerwehr	
Maßnahme Nr. 1	Bewusstsein schaffen: Mehrere, adressatenorientierte Informationsschreiben an die Mitarbeitenden, wo wir über die Phishing-Gefahren hinweisen. Mit Erklärungen zu den möglichen Angriffsvektoren, wie z.B. Microsoft-Produkte.
Maßnahme Nr. 2	Informationsschreiben an die Mitarbeitenden, wo sinnvolle Verhaltensmaßnahmen nochmal beschrieben werden, wie z.B.: Wie gehe ich generell mit E-Mail-Verkehr um? Wie tarnen sich E-Mails, die Phishing-Angriffe zum Zweck haben?
Maßnahme Nr. 3	Ein Artikel zum Thema: Phishing wird im internen Journal der Berliner Feuerwehr ebenfalls noch erscheinen
Maßnahme Nr. 4	E-Mails die von außen stammen, werden den Mitarbeitenden durch unsere IT, als externen E-Mail angezeigt. Dies erhöht die Wachsamkeit, ob bereits Ungereimtheiten an der E-Mail selbst auffallen.
Bezirksamt Charlottenburg-Wilmersdorf von Berlin	
Maßnahme Nr. 1	Wiederholend: MOD (Message of the Day) Nachrichten bei jedem Anmelden am PC
Maßnahme	Abgeschlossen: Dienstanweisung bezüglich Umgang mit IT

Nr. 2	
Maßnahme Nr. 3	Regelmäßig: Hinweis auf das Bits-Schulungs-Angebot zum Selbststudium
Maßnahme Nr. 4	Abgeschlossen: Mitteilung zu den internen Meldewege bei Verdacht
Maßnahme Nr. 5	in Progress: Markterkundung zur verifizierbaren und rechtsicheren Onlineschulung
Maßnahme Nr. 6	in Progress: ab 2022 jährliche Sicherheitsübungen; auch zu diesem Thema
Bezirksamt Friedrichshain-Kreuzberg von Berlin	
Maßnahme Nr. 1	Informationen und Berichterstattung zu Spam sowie Phishing-Mails im Intranet
Maßnahme Nr. 2	Regelmäßige Sensibilisierungsmails an alle Beschäftigten bei steigender Registrierung von Spam / Phishing
Maßnahme Nr. 3	Phishing bzw. Spearphishing Absendeadressen werden dem ITDZ Berlin gemeldet
Maßnahme Nr. 4	Intern für Mitarbeiter einen Meldeweg zur Prüfung verdächtiger Mails aufgebaut. IT-Stelle prüft dann verdächtige E-Mails.
Bezirksamt Lichtenberg von Berlin	
Maßnahme Nr. 1	Für alle Beschäftigten des Bezirksamtes Lichtenberg ist unbegrenzt und ohne Anmeldung das Behörden-IT-Sicherheitstraining im Intranet verfügbar (https://bits.berlin-cert.verwalt-berlin.de), mit dem die Beschäftigten für die IT-Sicherheit sensibilisiert werden. Auf diese Möglichkeit wird regelmäßig in Rund-E-Mails und im Intranet hingewiesen.
Maßnahme Nr. 2	Zum Thema „IT-Sicherheit“ können bei der Verwaltungsakademie ganzjährig Fortbildungsseminare gebucht werden.
Maßnahme Nr. 3	Nach § 23 Abs. 1 Satz 2 EGovG Bln ist auch für die Beschäftigten des Bezirksamtes Lichtenberg mindestens einmal jährlich eine verpflichtende Fortbildungsveranstaltung durchzuführen.
Maßnahme Nr. 4	Nach § 23 Abs. 1 Satz 2 EGovG Bln ist auch für alle Beschäftigten des Bezirksamtes Lichtenberg mindestens einmal jährlich eine übergreifende IT-Sicherheitsübung durchzuführen.
Bezirksamt Mitte von Berlin	
Maßnahme Nr. 1	Phishing-Simulation (2 Wellen geplant und umgesetzt. Jeweils 2 Phishing-Mails in einem Zeitraum von 2 Wochen.) Klickrate der 2. Welle noch nicht bekannt. In Welle 1 sind ~150 von

	3000 Beschäftigten reingefallen. Wiederholung wird nicht angestrebt. Grund ist Maßnahme Nr. 4
Maßnahme Nr. 2	Newsletter des InfSiBe im Intranet alle 2 Wochen mit Infos aus dem BSI Newsletter und Berlin-CERT
Maßnahme Nr. 3	Information der Beschäftigten über das BITS (bereitgestellt vom ITDZ Berlin)
Maßnahme Nr. 4	Aktuell ist eine Studie mit der Ruhr-Universität Bochum in Planung, um den aktuellen Stand der Wissenschaft zu nutzen, um eine nachhaltige Verhaltensänderung bei den Beschäftigten zu erreichen.
Maßnahme Nr. 5	In Notfällen kann eine Meldung an alle Beschäftigten herausgegeben werden, die zum Zeitpunkt der Meldung angemeldet sind. Das Fenster bewegt sich dabei bis zur Kenntnisnahme immer wieder in den Vordergrund.
Bezirksamt Steglitz-Zehlendorf von Berlin	
Maßnahme Nr. 1	Einweisung aller Beschäftigten in den sicheren Umgang mit der eingesetzten IKT. Das betrifft insbesondere Komponenten, die ausdrücklich der Umsetzung von datenschutzrechtlichen oder Sicherheitsanforderungen dienen.
Maßnahme Nr. 2	Schulungen für IT-Verfahren schließen relevante Sicherheitsmaßnahmen ein.
Maßnahme Nr. 3	Angebot der Verwaltungsakademie Berlin an Fortbildungsveranstaltungen zur Sensibilisierung für Informationssicherheit.
Maßnahme Nr. 4	Bei besonderen Gefährdungen und bei Häufungen z.B. von nicht ausgefilterten SPAM-Mails, Social Engineering-Versuchen oder von Credential-Leaks (im außerdienstlichen Bereich) werden zielgruppenorientiert alle Beschäftigten konkret über die Gefährdungen informiert und hinsichtlich Sicherheitsmaßnahmen sensibilisiert und informiert. Je nach Situation schließt das Themenbereiche ein wie beispielsweise Absicherung von Computer, Smartphone und Accounts, Sicherheit der elektronischen Kommunikation, mobile Internetzugänge in Fremdnetzen, Datenschutz und Vertraulichkeit im Internet und Sozialen Medien, Online-Banking, Erkennen von und Umgang mit potentiell schädigenden E-Mails, Phishing und Webseiten, Sicherheits- und Datenschutzfragen bei mobiler Arbeit, Verhalten bei Störungen oder Integritätsverlust oder Meldewege. Entsprechende Verhaltenshinweise beziehen sich in solchen Fällen auch auf die Nutzung von IKT im privaten Bereich.

Maßnahme Nr. 5	Bereitstellung von zielgruppenspezifischem Informationsmaterial zu Themen der Informationssicherheit.
Maßnahme Nr. 6	Abstimmung mit dem Personalservice und dem Datenschutzbeauftragten zu Informations-, Weiterbildungs- und Handlungsdefiziten und erforderlichen Maßnahmen.
Die Regierende Bürgermeisterin von Berlin Senatskanzlei	
Maßnahme Nr. 1	Die Sensibilisierung findet jährlich verpflichtend und in persönlicher Anwesenheit statt.
Maßnahme Nr. 2	Beim Onboarding erfolgt eine Einweisung zu den IT-Grundlagen inkl. Cybersicherheit.
Maßnahme Nr. 3	Es erfolgen regelmäßige Informationen über das Beschäftigenportal und Sensibilisierungsmails.
Maßnahme Nr. 4	Durchführung von speziellen Veranstaltungen, z. B. "Achtung die Hacker kommen"
Maßnahme Nr. 5	Hinweis und Verlinkung auf das Trainings- und Informationssystem BITS des ITDZ Berlin.
ITDZ Berlin	
Maßnahme Nr. 1	Regelmäßige Veröffentlichung im ITDZnet (Intranet des ITDZ Berlin) zu Mindeststandards für IT-Anwender mit aktualisierten praktischen Hinweisen zur IT-Sicherheit
Maßnahme Nr. 2	Situationsbedingte Information zu aktuellen Bedrohungslagen über Mail und ITDZnet
Maßnahme Nr. 3	Regelmäßige Schulung und Weiterbildung der Informationssicherheitsbeauftragten (TSOs) der einzelnen Abteilungen
Maßnahme Nr. 4	Durchführung eines mehrstufigen ISMS-Sensibilisierungsprogramms zur Informationssicherheit
Maßnahme Nr. 5	Durchführung zielgerichteter Schulungen in den Fachabteilungen zur Cyberabwehr
Maßnahme Nr. 6	Ganzjährige kontinuierlich fortlaufende Durchführung von ISMS-Audits mit KVP-Zeit-/ Maßnahmenplan
Maßnahme Nr. 7	Regelmäßige ISMS-Teamkonferenzen mit Informationssicherheitsbeauftragten der einzelnen Abteilungen. Sensibilisierung zur Informationssicherheit in den Abteilungskonferenzen durch die Abteilungs-TSOs
Maßnahme Nr. 8	Controlling der Maßnahmen durch Management-Attention im monatlichen Security Cockpit
Landesamt für Bürger- und Ordnungsangelegenheiten (LABO)	

Maßnahme Nr. 1	Das Behörden-IT-Sicherheitstraining (BITS) wurde als E-Learning-Werkzeug allen LABO-Beschäftigten im Januar 2022 zur Verfügung gestellt. Die Beschäftigten wurden von der Direktorin aufgefordert, alle neun Lektionen von BITS, d.h. die Lektionen "E-Mail", "Viren", "Passwörter", "Surfen im Internet", "Vertrauliche Daten", "Social Media", "Cloud", "Mobile Geräte" und "Mein Arbeitsplatz" durchzuarbeiten.
Maßnahme Nr. 2	Meldungen zur Informationssicherheit werden regelmäßig im Beschäftigtenportal durch die Informationssicherheitsbeauftragte publiziert. In den letzten Monaten erfolgte dies zu den Themen: "Achtung! Massive Phishing-Welle mit Links zu OneDrive", "Achtung! Phishing-E-Mails mit potenziell gefährlichen HTML-Anhängen", "Umgang mit verdächtigen E-Mails im LABO", "Potenzieller Missbrauch der Domain labo-berlin.de" und "Keine IT-Internetserviceseiten sondern Software aus dem LABO-IT-Portfolio nutzen".
Maßnahme Nr. 3	Regelmäßig (alle 8 Wochen) finden Besprechungen des 2021 wieder aktivierten Informationssicherheitsmanagement-Teams des LABO zum Thema Informationssicherheit aller Abteilungen statt. Die Team setzt sich zu jeweils einem Mitglied jeder Abteilung und dessen Vertreter, dem Datenschutzbeauftragten und der Informationssicherheitsbeauftragten des LABO zusammen.
Maßnahme Nr. 4	Die Informationssicherheitsbeauftragte des LABO sensibilisiert kurzfristig nach einem Sicherheitsvorfall den entsprechenden LABO-Beschäftigten zum Thema Informationssicherheit.
Maßnahme Nr. 5	Berlin-CERT Meldungen leitet die Informationssicherheitsbeauftragte an alle Fachverfahrensverantwortlichen und an alle Fachverfahrensfunktionspostfächer weiter. Die LABO-Fachverfahrensverantwortlichen wurden von der IT-Sicherheitsbeauftragten gebeten, die passenden Meldungen von Berlin-CERT zu abonnieren, sofern nicht bereits geschehen. Der Vorteil besteht darin, dass die zu abonnierenden Meldungen konfigurierbar sind und so inhaltlich passend sowie ohne Zeitverlust erhalten werden können.
Landesamt für Einwanderung	
Maßnahme Nr. 1	E-Mail an alle Mitarbeitenden bei konkreten Warnungen des BSI
Maßnahme Nr. 2	Regelmäßig angebotene Schulungen

Polizei Berlin	
Maßnahme Nr. 1	E-Mail an alle vom Informationssicherheitsbeauftragen (V) zur Sensibilisierung
Maßnahme Nr. 2	Jährlich mehrmals (in der Regel 6) stattfindende Sensibilisierungsveranstaltungen "Die Hacker kommen"
Maßnahme Nr. 3	Persönliche Sensibilisierungsgespräche der dezentralen Informationssicherheitsverantwortlichen in den Ämtern und Direktionen
Maßnahme Nr. 4	Sensibilisierungskampagne CYBÄR
Senatsverwaltung für Bildung, Jugend und Familie	
Maßnahme Nr. 1	alle Beschäftigten: Intranet-Meldungen zu diversen Themen: - Phishing-E-Mails (SPAM E-Mails mit Schadsoftware, schadhafte Links in E-Mails, Verschlüsselungstrojaner) - allgemeine Cybersicherheitshinweise - Hinweise zu veröffentlichten Sicherheitsrichtlinien und weiteren Dokumenten
Maßnahme Nr. 2	alle Beschäftigten: Sicherheitskampagne posterbasiert
Maßnahme Nr. 3	alle Beschäftigten: Aufklärung und Sicherheitshinweise zur Nutzung bei Herausgabe von Hardware (Laptop, Tablet, Smartphone)
Maßnahme Nr. 4	alle Beschäftigten: Verabschiedung und Bekanntgabe von sicherheitsbezogenen Dienstanweisungen
Maßnahme Nr. 5	alle Beschäftigten: - Infoblatt Informationssicherheit für neue Mitarbeiterinnen und Mitarbeiter (in der Begrüßungsmappe zum Dienstantritt) - Infoblätter zu weiteren sicherheitsrelevanten Themen (bspw. Keepass, Passwortsicherheit, verdächtige E-Mails)
Maßnahme Nr. 6	Führungskräfte (ihrerseits Weitergabe an Mitarbeiter im Verantwortungsbereich): im Rahmen von internen Gremiensitzungen: - Sicherheitsrisiken und mögliche Maßnahmen - Beispiele von Sicherheitsvorfällen - Sicherheitsmaßnahmen in Stabsabteilungen - Weitergabe von Daten - Sichere E-Mail
Senatsverwaltung für Finanzen Berlin und Berliner Finanzämter	

Maßnahme Nr. 1	Information und Aufklärung der Vertretenden im Informationssicherheitsgremium der SenFin (regelmäßig, monatlich)
Maßnahme Nr. 2	Information und Aufklärung der Mitarbeitenden im internen Beschäftigtenportal (anlassbezogen) sowie per Schnellmitteilung
Maßnahme Nr. 3	Bereitstellung von Information der Mitarbeitenden im internen Beschäftigtenportal (dauerhaft)
Maßnahme Nr. 4	Durchführung von Informationsveranstaltungen z.B. „Die Hacker kommen“
Maßnahme Nr. 5	Durchführung eines internen Phishingtest
Senatsverwaltung für Inneres, Digitalisierung und Sport	
Maßnahme Nr. 1	Regelmäßige Info-Mails (zu Themen wie Phishing, Ukraine-Krise, Emotet, mobiles Arbeiten, etc.)
Maßnahme Nr. 2	Zusätzliches Schulungsangebot wie "die Hacker kommen", Adventskalender, etc. zur freiwilligen Teilnahme
Maßnahme Nr. 3	Erstellung einer hausweiten Schulung für das Jahr 2022 (EGovG-Bln)
Maßnahme Nr. 4	Aushänge (Plakate im DG)
Senatsverwaltung für Justiz, Vielfalt und Antidiskriminierung sowie Berliner Justizvollzugsanstalten und Soziale Dienste der Justiz	
Maßnahme Nr. 1	Die Behörden im Geschäftsbereich der Senatsverwaltung für Justiz, Vielfalt und Antidiskriminierung werden durch vielfältige Maßnahmen für Bedrohungen im Bereich der Informationssicherheit sensibilisiert. Neben regelmäßigen Hinweisen in den im Intranet veröffentlichten Artikeln werden Informationsschreiben sowohl zu allgemeinen als auch zu anlassbezogen konkreten Bedrohungslagen mit Handlungsempfehlungen versendet. Zudem werden Mitarbeitenden im Geschäftsbereich niedrigschwellige Schulungen, beispielsweise über das Behörden-IT-Sicherheitstraining des ITDZ Berlin (BITS), angeboten.
Maßnahme Nr. 2	Die Senatsverwaltung für Justiz, Vielfalt und Antidiskriminierung hat hierüber hinaus die Bereitstellung von Onlineschulungen unter anderem im Bereich der Informationssicherheit veranlasst. Die Teilnahme der Mitarbeitenden insbesondere an sogenannten Awareness-Kursen wird derzeit geplant und organisiert.

Maßnahme Nr. 3	Schließlich hat die Senatsverwaltung für Justiz, Vielfalt und Antidiskriminierung zunächst für die Behörden des Berliner Justizvollzuges und für die Sozialen Dienste der Justiz im Jahr 2021 zusätzlich eine Anti-Phishing-Kampagne mittels präparierter Nachrichten mit anschließender Auswertung und Schwerpunkt-Sensibilisierung bezüglich realer Bedrohungsszenarien durchgeführt.
Senatsverwaltung für Kultur und Europa (politisch administrativer Bereich)	
Maßnahme Nr. 1	Kenntnisnahme der IT-Sicherheitsrichtlinien bei Dienstantritt
Maßnahme Nr. 2	Problembezogene Schulung durch Rundmail und ggf. persönliche Beratung nach Hinweisen des ITDZ Berlin
Maßnahme Nr. 3	Problembezogene Schulung durch Rundmail und ggf. persönliche Beratung nach eigenen Hinweisen auf IT-sicherheitsrelevante Vorfälle
Maßnahme Nr. 4	Unregelmäßige Security-Awareness Schulungen der gesamten Belegschaft (z.Zt. Durch die Pandemie unterbrochen)
Senatsverwaltung für Kultur und Europa (Landesarchiv)	
Maßnahme Nr. 1	Ersteinweisung bei Dienstantritt
Maßnahme Nr. 2	Regelmäßige Schulung (einmal jährlich) durch IT-Sicherheitsbeauftragte
Maßnahme Nr. 3	Problembezogene Schulung durch Rundmail und ggf. persönliche Beratung nach Hinweisen des ITDZ Berlin
Maßnahme Nr. 4	Problembezogene Schulung durch Rundmail und ggf. persönliche Beratung nach eigenen Hinweisen auf IT-sicherheitsrelevante Vorfälle
Maßnahme Nr. 5	Regelmäßige Schulung des in der IT eingesetzten Personals
Maßnahme Nr. 6	Regelmäßige Schulung der IT-Sicherheitsbeauftragten
Senatsverwaltung für Stadtentwicklung, Bauen und Wohnen sowie Senatsverwaltung für Umwelt, Mobilität, Verkehr und Klimaschutz	
Maßnahme Nr. 1	Information und Sensibilisierung der Beschäftigten per E-Mail und Login-Benachrichtigungsfenster, laufend
Maßnahme Nr. 2	Anpassung von IT-bezogenen Schulungsinhalten an geänderte Bedrohungslagen, laufend
Maßnahme Nr. 3	Aufbau einer Awareness-Plattform als Teil des Schulungskonzeptes, ggf. gezielte Ansprachen nach Kontaktaufnahme zum Helpdesk

Senatsverwaltung für Wirtschaft, Energie und Betriebe	
Maßnahme Nr. 1	allgemeine Informationen/Warnungen bei gehäuftem Auftreten ähnlicher Ereignisse; meist als 'Aktuelle Meldung' im Intranet; Beschreibung der Ereignisse (z.B. Phishing E-Mail); Hinweise auf besondere Merkmale (Absender, URLs, Sprache) zur Erkennung und zum Umgang;
Maßnahme Nr. 2	persönliche Beratung bei einzelnen, zweifelhaften Ereignissen; Erläuterung am konkreten Beispiel
Maßnahme Nr. 3	allgemeine Informationen/Warnungen als Reaktion auf externe Meldungen zu potentiellen Bedrohungen; meist als 'Aktuelle Meldung' im Intranet; Beschreibung der Bedrohung und Umgangsregeln;
Maßnahme Nr. 4	falls passend, Hinweise auf Quellen zur persönlichen Information; z.B. BITS; c't Security Checklisten; BSI für Bürger;
Maßnahme Nr. 5	In der Vergangenheit gab es Informationsveranstaltungen zum Thema. (z.B. vom ZAC des LKA durchgeführt)
Sozialgericht Berlin	
Maßnahme Nr. 1	Regelmäßige Informationsveranstaltungen zur IT-Sicherheit (Gefahren und Möglichkeiten der Abwehr)
Maßnahme Nr. 2	Behörden-IT-Sicherheitstraining (BITS) - ein webbasiertes Training (WBT) - im Intranet des Sozialgerichts Berlin veröffentlicht
Maßnahme Nr. 3	Wissenstransfer und Sensibilisierung durch anlassbezogene E-Mails zu aktuellen Gefahrenlagen, angereichert mit komprimierten Hintergrundinformationen
Maßnahme Nr. 4	Regelmäßiges Update der Führungskräfte zum Lagebild der IT-Sicherheit am SG Berlin (Gefahren, Maßnahmen, Hinweise, ...)

2. Welche Instanz ist für die Planung der Phishing-Sensibilisierung innerhalb der Senatsverwaltung der Justiz verantwortlich?

Zu 2.:
Für die Planung entsprechender Sensibilisierungsmaßnahmen liegt die Verantwortung grundsätzlich bei den jeweiligen Informationssicherheitsbeauftragten (InfSiBes). Für die im Jahr 2021 in den Behörden des Berliner Justizvollzuges und bei den Sozialen Diensten der Justiz durchgeführte Anti-Phishing-Kampagne wurden ergänzend die Fachaufsicht in der Senatsverwaltung (Abteilung III) und die Gesamtbeschäftigtenvertretungen an der Planung, Durchführung und Auswertung einbezogen.

3. Wie ist diese Phishing-Sensibilisierung in der Senatsverwaltung der Justiz gestaltet?

Zu 3.:
Hinsichtlich der Anti-Phishing-Kampagne bei den Behörden des Berliner Justizvollzuges und bei den Sozialen Diensten der Justiz wurden die Mitarbeitenden im Vorfeld mit erheblichem zeitlichem Abstand über die geplante Versendung einer fingierten Phishing-Mail inklusive eines groben Zeitraumes in Kenntnis gesetzt. Der Versand der Nachricht und die anschließende Auswertung erfolgten durch einen spezialisierten Dienstleister. Bei Anklicken des eingebundenen Links innerhalb der Aktionszeit wurde den Nutzenden sofort eine Information angezeigt. Ferner wurden die Aktion nach zweitägiger Laufzeit gemeinsam mit dem Dienstleister ausgewertet und ein Informationsschreiben mit einer auf der versendeten Nachricht basierenden Einordnung der Merkmale von Phishing-Mails an die Mitarbeitenden versendet. Eine Feedback-Bewertung durch die Mitarbeitenden der teilnehmenden Behörden hat eine grundsätzlich positive Resonanz ergeben. Bemängelt wurde indes insbesondere, dass die Kampagne vom Jahr 2020 auf das Folgejahr verschoben wurde. Hierfür ursächlich war, dass nach erfolgter Bestätigung der technischen Durchführbarkeit der Kampagne Umsetzungsbedenken seitens des ITDZ-Berlin mitgeteilt wurden, welche Umplanungen und eine alternative Umsetzung erforderlich machten.

4. Wie viele Mitarbeiter nahmen an dieser Maßnahme teil?

Zu 4.:
Im Rahmen der Anti-Phishing-Kampagne bei den Behörden des Berliner Justizvollzuges und bei den Sozialen Diensten der Justiz wurden die fingierte Phishing-Mail sowie das nachfolgende Informations- und Auswertungsschreiben an alle in der Domain hinterlegten E-Mailadressen mit Ausnahme von Funktions- und Gruppenadressen versendet. Hiernach handelt es sich um ca. 3.600 Mitarbeitende.

5. Wurde eine Evaluation durchgeführt? Wenn ja,
   a. wie viele Angestellte folgten der Phishing-Mail?
   b. wie wird vor diesem Hintergrund das Sicherheitsrisiko der Berliner Verwaltung für Justiz durch Phishing eingeschätzt?
   c. welche Maßnahmen werden von der Senatsverwaltung der Justiz ergriffen, um dieses Sicherheitsrisiko zu minimieren?
   d. ist eine Wiederholung der Phishing-Sensibilisierung innerhalb der Senatsverwaltung der Justiz geplant?

Zu 5a.:
In Abstimmung mit den zuständigen Beschäftigtenvertretungen wurde bei der Auswertung der Kampagne für die Behörden des Berliner Justizvollzuges und

für die Sozialen Dienste der Justiz auf die Erhebung insbesondere der einzelnen IP-Adressen sowie der Behördenzugehörigkeit verzichtet. Hintergrund war, dass der Fokus der Maßnahme auf der Sensibilisierung der Mitarbeitenden lag. Eine konkrete Zahl kann entsprechend nicht mitgeteilt werden.

Zu 5b. und 5c.:
Phishing gehört statistisch zu den beliebtesten Angriffsvektoren im Kontext der IT-gestützten Informationsverarbeitung, weshalb es bewusst als Szenario für eine Schwerpunktaktion ausgewählt wurde. Die Sensibilisierung der Mitarbeitenden ist deshalb eine von mehreren Maßnahmen zur Gefahrenreduzierung. So werden als schadhaft identifiziert oder gemeldete E-Mails beispielsweise bereits automatisiert von eingesetzten Filtersystemen erkannt und abgewiesen. Wenngleich grundsätzlich ein stetiger Anstieg der gefundenen Elemente beispielsweise den statistischen Gesamtmeldungen des Berlin-CERTs zu entnehmen ist, werden die Filtereinstellungen neben weiteren kurzfristigen Umsetzungen der durch die CERT-Verbünde empfohlenen dezentralen Einzelanpassungen stetig aktualisiert, so dass das Gesamtrisiko entsprechend signifikant reduziert ist.

Zu 5d.:
Planung und Durchführung entsprechender Kampagnen haben sich als aufwendig erwiesen, wenngleich die positiven Erfahrungen mit der dargestellten Anti-Phishing Kampagne Anlass für eine Wiederholung geben. Dementsprechend ist eine abermalige Durchführung erst für das Jahr 2023 und verbunden mit der Erwartung angedacht, dann ggf. einen durch das ITDZ-Berlin bereitgestellten Service nutzen zu können.

6. Gibt es Bestrebungen diese Phishing-Sensibilisierung auf andere Verwaltungen auszuweiten? Wenn ja,
   a. welche?
   b. in welchem Stadion sind diese Planungen?
   c. wird es eine offizielle Berichtserstattung geben?

Zu 6.:
Die Durchführung entsprechender Anti-Phishing-Kampagnen im Geschäftsbereich der Justiz wird grundsätzlich für sinnvoll erachtet. Konkrete Planungen sind mit Blick auf die vorgenannte Erwartung eines zentral angebotenen Services, wirksamer technischer Anti-Phishing-Maßnahmen und anderer Awareness-Maßnahmen (vgl. Antwort zu Frage 1) zunächst zurückgestellt.

Zu 6a.:
Die Etablierung einer landesweiten Informationssicherheitssensibilisierung für die Berliner Verwaltung als Maßnahme in Umsetzung der IKT-Sicherheitsarchitektur wird auch Angebote zur Sensibilisierung mittels Phishing beinhalten.

Zu 6b.:
Die Etablierung einer landesweiten Informationssicherheitssensibilisierung für die Berliner Verwaltung als Maßnahme in Umsetzung der IKT-Sicherheitsarchitektur wird auf der Grundlage eines Landes-Konzeptes erfolgen. Die Erstellung dieses Konzepts ist in 2022 geplant. Das schließt die Abstimmung mit den beteiligten Rolleninhabern zur Aus- und Fortbildung von Landespersonal ein. Eine Umsetzung wird nach erfolgreicher Beteiligung der Beschäftigtenvertretungen im Wege einer Ausschreibung der im Konzept enthalten Dienstleistungen erfolgen.
Zu 6c.:
Ja, ein quantitatives Reporting wird im Rahmen der Abrechnung zu dem beabsichtigen IKT-Basisdienst erfolgen. Angaben zur Nutzung werden nach Etablierung der Dienstleistung im jährlichen Informationssicherheitsbericht aufgenommen.

Berlin, den 20. April 2022

In Vertretung

Dr. Ralf Kleindiek
Senatsverwaltung für Inneres, Digitalisierung und Sport