

Stadt Wien: rund 26.000 interne Dokumente aus Dokumentationsplattform abgeflossen

Stand 02.10.2026 23:06 · Sendung: - · Belegstärke: **bestätigt** · berichtet · **vermutet** · Prozent: 100 = bestätigt, 0 = sicher falsch

Einordnung

1. Nach allem, was bekannt ist, wurden Dokumente kopiert, aber nichts verschlüsselt oder physisch beschädigt; die Lücke ist laut Stadt geschlossen.
2. Der Einstieg über eine aus dem Internet erreichbare Anwendung ist in Europa der häufigste Weg für Angreifer, deshalb gehört das Wissen, was von außen erreichbar ist, und dessen gezielte Absicherung nach vorne (CC5 Risk-Based Vulnerability Management, CC2 Defensible Architecture).
3. Man muss nicht alles gleichzeitig machen: Wer sich auf die fünf SANS Critical Controls konzentriert, also Incident Response, Architektur, Sichtbarkeit, sicherer Remote Access und risikobasiertes Patchen, schafft mit KI-Unterstützung auch mit kleinem Team viel.

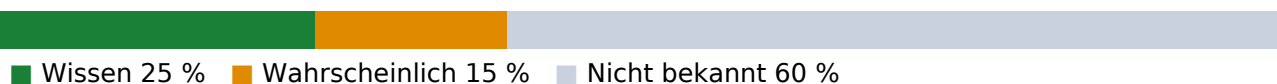
Was sich seit der Erstmeldung geändert hat

Frühere Aussage	vorher	jetzt	Status
Ein Angreifer hatte zwischen 03. und 11.09.2026 über einen Webzugang Zugriff auf Teile einer inter...	100 %	100 %	bestätigt

Neu seit dem letzten Stand

- Offizielle Pressemitteilung der Stadt Wien vom 30.09.2026 mit genauen Zahlen: 2.885 Bürgerinnen und Bürger, 2.083 Beschäftigte, 856 Auftragnehmer
- Es flossen auch technische Dokumentationen sowie Geschäfts- und Infrastrukturinformationen ab (bestätigt)
- Freiwillige NIS-Meldung am 10.09. und Information der Datenschutzbehörde am 15.09.
- Die DSN war beim Schließen der Lücke eingebunden
- Laut Mimikama bis 01.10. keine Veröffentlichung und kein Phishing mit Bezug zum Vorfall
- Das NISG 2026 gilt seit 01.10.2026; Gemeinden sind ausgenommen, die Auslegung für Wien ist offen

Wissensstand



Offiziell belegt sind Zeitraum, Umfang, Betroffenengruppen und Meldewege, weil die Stadt ungewöhnlich früh und detailliert informiert hat. Offen sind Produkt, Art der Schwachstelle, Täter und was mit den Daten passiert (widersprüchlich: A 30 % Wissen / B 25 % Wissen; der niedrigere Wert ist übernommen).

1. Was ist passiert, und warum?

WISSEN

- Ein Angreifer hatte zwischen 03. und 11.09.2026 über einen Webzugang Zugriff auf Teile einer internen Dokumentationsplattform des Magistrats. Er kopierte unter anderem Testdaten, Schulungsunterlagen, Projektdokumentationen und technische Dokumentationen (bestätigt). (100 %) [<https://presse.wien.gv.at/presse/2026/09/30/wien-datensicherheit-hat-hohen-stellenwert-sicherheitsluecke-umgehend-geschlossen>]

- CERT.at entdeckte in einem Online-Forum ein Angebot, die Schwachstelle im Webzugang zur Dokumentationsplattform zu kaufen, und informierte den Magistrat am 09.09.2026. Danach übernahmen WienCERT und die MA 01 – Wien Digital die Analyse (bestätigt). (100 %) [<https://presse.wien.gv.at/presse/2026/09/30/wien-datensicherheit-hat-hohen-stellenwert-sicherheitsluecke-umgehend-geschlossen>]

- Die Schwachstelle wurde gemeinsam mit der Direktion Staatsschutz und Nachrichtendienst (DSN) identifiziert und geschlossen (bestätigt/berichtet). (100 %)

[<https://www.heise.de/news/Stadt-Wien-entdeckt-Einbruch-in-Online-Speicher-11471899.html>]

- Phishing wird ausgeschlossen. Die IT-Verantwortlichen vermuten, dass eine spezielle Scan-KI die Lücke gefunden hat (berichtet; die KI-These ist eine Vermutung der Stadt). (100 %)

[<https://wien.orf.at/stories/3373234/>]

- CIO Klemens Himpele: „Der Angreifer hatte zu keinem Zeitpunkt Kontrolle über IT-Systeme oder Benutzerkonten der Stadt Wien.“ (bestätigt) (100 %) [<https://presse.wien.gv.at/presse/2026/09/30/wien-datensicherheit-hat-hohen-stellenwert-sicherheitsluecke-umgehend-geschlossen>]

NICHT BEKANNT

- Um welches Produkt bzw. welche Software es sich bei der Plattform handelt (Eigenentwicklung, Wiki, Dateiablage?)

- Welche Art von Schwachstelle es war (fehlerhafte Zugriffskontrolle, Konfigurationsfehler, bekannte Lücke ohne Patch oder Zero-Day)

- Wer hinter dem Angriff steckt und ob Angreifer und Anbieter im Forum dieselbe Person sind

- Ob die Schwachstelle oder die Daten verkauft bzw. weitergegeben wurden

- Welches Forum es war

- Warum der Zugriff laut Stadt bis 11.09. reichte, obwohl der Hinweis am 09.09. einging (der Ablauf der Eindämmung ist nicht veröffentlicht)

- Ob der Einsatz von KI belegt ist oder nur angenommen wird

WAHRSCHEINLICH (Einschätzung)

- Ausgenutzt wurde eine Schwachstelle in einer aus dem Internet erreichbaren Webanwendung, etwa in der Zugriffskontrolle oder Authentifizierung, und keine gestohlenen Zugangsdaten. (70 %) – Die Stadt spricht von einer Schwachstelle im Webzugang, schließt Phishing aus und sagt, Benutzerkonten seien nicht kontrolliert worden. Dass die Schwachstelle selbst verkauft wurde, spricht für einen technischen Fehler. Credential Stuffing ist aber nicht ausdrücklich ausgeschlossen (widersprüchlich: A 75 % / B 70 %).

- Täter oder Anbieter ist finanziell motiviert (Initial Access Broker oder Datenhändler) und kein staatlicher Akteur. (55 %) – Ein Verkaufsangebot in einem Forum ist typisch für den kriminellen Markt. Dass die DSN eingebunden ist, ist bei einer Gebietskörperschaft üblich und kein Hinweis auf einen staatlichen Täter. Belege gibt es in keine Richtung.

- Gefunden wurde die Lücke durch automatisiertes Scannen, möglicherweise KI-gestützt. (50 %) – So vermuten es laut ORF die IT-Verantwortlichen. Automatisiertes Massenscannen ist Alltag. Ob KI im Spiel war, lässt sich von außen nicht prüfen.

2. Was ist die Auswirkung?

WISSEN

- Kopiert wurden rund 26.000 Dokumente bzw. Seiten (ca. 9 GB). Darunter sind Magistratsinterna, technische Dokumentationen, personenbezogene Daten (teils besondere Kategorien nach DSGVO) sowie Geschäfts- und Infrastrukturinformationen (bestätigt). (100 %) [<https://presse.wien.gv.at/presse/2026/09/30/wien-datensicherheit-hat-hohen-stellenwert-sicherheitsluecke-umgehend-geschlossen>]

- Betroffen sind 5.824 Personen: 2.885 Bürgerinnen und Bürger, 2.083 Beschäftigte und 856 Auftragnehmer. Sie werden direkt informiert (bestätigt; widersprüchlich: Stadt Wien 856 / heise 865 Auftragnehmer – nur 856 ergibt die Summe 5.824). (100 %) [<https://presse.wien.gv.at/presse/2026/09/30/wien-datensicherheit-hat-hohen-stellenwert-sicherheitsluecke-umgehend-geschlossen>]

- Meist geht es um Namen und E-Mail-Adressen, in einigen Fällen auch um Krankenstandstage oder IBAN (berichtet). (100 %) [<https://wien.orf.at/stories/3373234/>]
 - Bisher gibt es keine Hinweise auf eine Veröffentlichung und keine Erpressung (berichtet). (100 %) [<https://wien.orf.at/stories/3373234/>]
 - Mimikama hat bis 01.10. weder eine Veröffentlichung noch Phishing mit Bezug zum Vorfall festgestellt. Die Plattform warnt aber, dass ein echtes Datenleck gefälschte Nachrichten glaubwürdiger macht (berichtet). (100 %) [<https://www.mimikama.org/datenleck-stadt-wien-5824-betroffene/>]
- NICHT BEKANNT
- Welche Infrastrukturinformationen genau betroffen sind und wie sensibel sie sind (Netzpläne, Systemdokumentation, Ver- und Entsorgung?)
 - Ob die Daten schon weitergegeben oder verkauft wurden
 - Wie viele Personen zu den besonderen Kategorien nach DSGVO gehören
 - Ob Betroffenen Daten oder Dokumente später im Darknet auftauchen

WAHRSCHEINLICH (Einschätzung)

- Für die Betroffenen sind gezieltes Phishing und Betrugsversuche mit Bezug auf die Stadt Wien kurzfristig das größte Risiko. (65 %) – Namen, E-Mail-Adressen und teils IBAN reichen für glaubwürdige Spear-Phishing-Mails. Betrüger nutzen erfahrungsgemäß aus, dass gleichzeitig echte Verständigungen verschickt werden.
- Langfristig wiegen die technischen und Projektdokumentationen schwerer, weil sie späteren Angreifern als Landkarte dienen können. (55 %) – Die Stadt bestätigt technische Dokumentation sowie Geschäfts- und Infrastrukturinformationen. Wie sensibel sie sind, ist offen, und ein Teil sind Test- und Schulungsunterlagen.

3. Wie lange dauert es digital (Wiederherstellung IT)?

WISSEN

- Laut CIO Himpele hatte der Angreifer zu keinem Zeitpunkt Kontrolle über IT-Systeme oder Benutzerkonten. Die Lücke ist geschlossen (bestätigt). (100 %) [<https://presse.wien.gv.at/presse/2026/09/30/wien-datensicherheit-hat-hohen-stellenwert-sicherheitsluecke-umgehend-geschlossen>]
- Es wurde keine Ransomware festgestellt, und es wurden keine Systeme übernommen (berichtet). (100 %) [<https://inuit.at/inhalt/data-breach-bei-der-stadt-wien-26000-dokumente-%C3%BCber-sicherheitsl%C3%BCcke-kopiert>]
- Die Stadt erstattete am 10.09.2026 freiwillig eine Meldung nach dem NIS-Gesetz und informierte am 15.09.2026 die Datenschutzbehörde (bestätigt). (100 %) [<https://presse.wien.gv.at/presse/2026/09/30/wien-datensicherheit-hat-hohen-stellenwert-sicherheitsluecke-umgehend-geschlossen>]
- Die Betroffenen sollen innerhalb einer Woche ab 30.09. direkt informiert werden (bestätigt). (100 %) [<https://presse.wien.gv.at/presse/2026/09/30/wien-datensicherheit-hat-hohen-stellenwert-sicherheitsluecke-umgehend-geschlossen>]

NICHT BEKANNT

- Ob die Plattform normal weiterläuft oder vorübergehend vom Internet getrennt wurde
- Wie weit Forensik und Prüfung ähnlicher Webzugänge sind
- Ob und wann ein forensischer Abschlussbericht kommt
- Ob die Information der Betroffenen schon abgeschlossen ist

WAHRSCHEINLICH (Einschätzung)

- Ein Wiederaufbau der IT ist nicht nötig. Über Wochen fällt aber Arbeit für Forensik, Härtung und die Information der Betroffenen an. (75 %) – Es gab keine Verschlüsselung und keine Systemübernahme, und die Lücke ist laut Stadt geschlossen. Erfahrungsgemäß folgen Prüfungen weiterer von außen erreichbarer Anwendungen.

4. Ist in der Anlage etwas kaputt, das lange dauert?

WISSEN

- Betroffen war eine Dokumentationsplattform. Laut Stadt ermöglichte die Lücke nur Zugriff auf bestimmte Inhalte dieser Plattform und nicht auf IT-Systeme oder Konten (bestätigt). (100 %) [<https://presse.wien.gv.at/presse/2026/09/30/wien-datensicherheit-hat-hohen-stellenwert-sicherheitsluecke-umgehend-geschlossen>]

ps://presse.wien.gv.at/presse/2026/09/30/wien-datensicherheit-hat-hohen-stellenwert-sicherheitsluecke-umgehend-geschlossen]

- Auch heise berichtet, dass nur auf bestimmte Inhalte zugegriffen wurde (berichtet). (100 %)

[<https://www.heise.de/news/Stadt-Wien-entdeckt-Einbruch-in-Online-Speicher-11471899.html>]

- Laut ORF gab es keinen direkten Zugriff auf die städtische IT-Infrastruktur (berichtet). (100 %)

[<https://wien.orf.at/stories/3373234/>]

NICHT BEKANNT

- Ob die abgefloßenen Infrastrukturinformationen Angaben zu Leittechnik, Fernwirktechnik, OT oder Netzplänen städtischer Betriebe enthalten
- Ob Auftragnehmer der Infrastruktur unter den 856 betroffenen Auftragnehmern sind

WAHRSCHEINLICH (Einschätzung)

- Physische Anlagen oder OT sind nicht beeinträchtigt. (85 %) – Es gab einen Lesezugriff auf eine Dokumentationsplattform ohne Systemkontrolle, und es wurden keine Störungen gemeldet.
- Die Gefahr ist vor allem indirekt: Abgeflossene technische Doku kann spätere gezielte Angriffe erleichtern. (45 %) – Technische Doku und Infrastrukturinformationen sind bestätigt. Ob sie für Angriffe brauchbar sind, ist offen.

5. Wie viele solcher Ziele gibt es?

WISSEN

- Laut IBM X-Force Threat Intelligence Index 2026 war die Ausnutzung öffentlich erreichbarer Anwendungen in Europa mit 40 % die häufigste Initial-Access-Methode. Die 44 % beschreiben einen weltweiten Anstieg solcher Angriffe und keinen Anteil (berichtet/Herstellerstudie). (100 %)
[<https://newsroom.ibm.com/2026-02-25-ibm-2026-x-force-threat-index-ai-driven-attacks-are-escalating-as-basic-security-gaps-leave-enterprises-exposed>]
- Laut IBM X-Force 2026 ließen sich 56 % der 2025 veröffentlichten Schwachstellen ohne Authentifizierung ausnutzen (berichtet/Herstellerstudie). (100 %) [<https://industrialcyber.co/reports/ibm-x-force-reports-44-surge-in-exploitation-of-public-facing-applications-as-supply-chain-and-identity-attacks-intensify/>]
- Weitere IBM-Quelle zu den X-Force-2026-Zahlen für Europa (Herstellerstudie). (100 %)
[<https://ncee.newsroom.ibm.com/XForce2026en>]
- CISA, FBI und MS-ISAC warnten 2023 bei der Confluence-Lücke CVE-2023-22515 (Zero-Day, Broken Access Control) vor breiter, anhaltender Ausnutzung. Dokumentationsplattformen sind also ein bekanntes Ziel (bestätigt; dass Wien Confluence nutzt, ist NICHT belegt). (100 %)
[<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-289a>]
- Shodan (aggregiert): OT-Protokolle öffentlich erreichbar in Österreich: 4553 gesamt (HMI/VNC 1078, DNP3 959, IEC-104 448, Niagara Fox 435) (100 %)

NICHT BEKANNT

- Wie viele Verwaltungen in Österreich bzw. DACH Wikis, Doku- oder Kollaborationsplattformen mit Webzugang betreiben (keine belastbare öffentliche Zahl)
- Ob dieselbe Schwachstelle auch anderswo existiert

WAHRSCHEINLICH (Einschätzung)

- Wikis, Dateiablagen, Ticket- und Testsysteme mit Webzugang gibt es in praktisch jeder größeren Verwaltung und in vielen Versorgungsunternehmen, und automatisierte, auch KI-gestützte Scans finden sie schnell. (70 %) – Das ist Branchenerfahrung und deckt sich mit den IBM-Zahlen zu öffentlich erreichbaren Anwendungen als häufigstem Einstieg. Eine konkrete Zahl für DACH fehlt (widersprüchlich: A 70 % / B 80 %; wegen fehlender Zahl ist der niedrigere Wert übernommen).

6. Kann das wieder passieren?

WISSEN

- Laut Stadt wurde die konkrete Lücke geschlossen (bestätigt). (100 %) [<https://presse.wien.gv.at/presse/2026/09/30/wien-datensicherheit-hat-hohen-stellenwert-sicherheitsluecke-umgehend-geschlossen>]

- Die Opposition hat verlangt, die Sicherheitsmaßnahmen zu evaluieren und wo nötig zu verstärken (berichtet). (100 %)

[<https://www.heise.de/news/Stadt-Wien-entdeckt-Einbruch-in-Online-Speicher-11471899.html>]

- Das NISG 2026 gilt seit 01.10.2026 und erfasst die öffentliche Verwaltung auf Bundes- und Landesebene (Ämter der Landesregierungen). Gemeinden sind nach § 24 Abs. 3 ausgenommen (bestätigt/Gesetz; wie das bei Wien als Land und Gemeinde zugleich ausgelegt wird, ist offen). (100 %) [<https://www.usp.gv.at/aktuelles/newsliste/NIS-2.html>]

- Betroffene Einrichtungen müssen sich bis 31.12.2026 registrieren (berichtet). (100 %)

[<https://www.cybervize.de/de/wissen/nisg-at/ueberblick-anwendungsbeginn-uebergangslage>]

NICHT BEKANNT

- Ob andere Systeme der Stadt dieselbe Schwachstelle oder Konfiguration haben
- Welche technischen und organisatorischen Konsequenzen die Stadt über das Schließen der Lücke hinaus zieht
- Ob die Datenschutzbehörde ein Verfahren führt

WAHRSCHEINLICH (Einschätzung)

- Ähnliche Vorfälle bei Verwaltungen im DACH-Raum sind in den nächsten Monaten wahrscheinlich, weil automatisiertes und KI-gestütztes Scannen die Zeit vom Fehler bis zur Ausnutzung verkürzt. (75 %) – Darauf deuten der Trend in X-Force 2026, die Vermutung der Stadt selbst und frühere Fälle in Verwaltungen hin (widersprüchlich: A 75 % / B 80 %; der niedrigere Wert ist übernommen).

Lage

Zwischen 03. und 11.09.2026 hatte ein Angreifer über einen Webzugang Zugriff auf Teile einer internen Dokumentationsplattform des Wiener Magistrats. Er kopierte rund 26.000 Dokumente bzw. Seiten (ca. 9 GB), darunter personenbezogene Daten von 5.824 Personen sowie technische Dokumentation, Geschäfts- und Infrastrukturinformationen. Aufgefallen ist der Vorfall, weil CERT.at in einem Online-Forum ein Verkaufsangebot für die Schwachstelle entdeckte und den Magistrat am 09.09. informierte. Laut Stadt gab es keine Kontrolle über IT-Systeme oder Benutzerkonten, keine Erpressung und bisher keine Veröffentlichung. Plattform, Täter und Art der Lücke sind öffentlich nicht bekannt.

Angriff	Unbefugter Zugriff über einen Webzugang auf Teile einer internen Dokumentationsplattform des Magistrats und Kopie von rund 26.000 Dokumenten bzw. Seiten (ca. 9 GB). Keine Verschlüsselung, keine Systemübernahme, keine Erpressung bekannt.
Wann / Status	03.–11.09.2026; Hinweis von CERT.at am 09.09.2026; öffentlich gemacht am 30.09.2026 · eingedämmt
Täter	unbekannt; die Schwachstelle wurde in einem Online-Forum zum Kauf angeboten – unbekannt
Betreiber / Branche	Stadt Wien / Magistrat der Stadt Wien (IT: MA 01 – Wien Digital, WienCERT) · Kommune / öffentliche Verwaltung (Land und Gemeinde)
Anlage / Alter	Interne Dokumentationsplattform mit Webzugang (IT, keine OT) · unbekannt
Region	Wien, Österreich
Auswirkungen	Keine Auswirkungen auf Versorgung oder städtische Dienste bekannt; nichts verschlüsselt, keine Systemübernahme. Betroffen sind 5.824 Personen (2.885 Bürgerinnen und Bürger, 2.083 Beschäftigte, 856 Auftragnehmer), meist mit Namen und E-Mail-Adresse, teils mit Krankenstandtagen oder IBAN. Kurzfristiges Risiko ist Phishing und Betrug mit Bezug auf die Stadt. Offen ist, wie sensibel die abgeflommenen Infrastrukturinformationen sind.

Behörden	CERT.at (Hinweis), WienCERT und MA 01 – Wien Digital (Analyse, Incident Response), Direktion Staatsschutz und Nachrichtendienst DSN (Identifikation und Schließen der Lücke), freiwillige Meldung nach NIS-Gesetz (10.09.), Datenschutzbehörde (informiert am 15.09.).
Regulatorik	Am 10.09.2026 erfolgte eine freiwillige Meldung nach dem NIS-Gesetz. Das NISG 2026 (Umsetzung NIS2) gilt seit 01.10.2026 und erfasst die öffentliche Verwaltung auf Bundes- und Landesebene. Gemeinden sind nach § 24 Abs. 3 ausgenommen; wie das bei Wien als Land und Gemeinde zugleich ausgelegt wird, ist offen. Registrierung bis 31.12.2026. Datenschutz: DSGVO-Meldung an die Datenschutzbehörde und Benachrichtigung der Betroffenen laufen.

Angriffsvektor

Bekannt: Schwachstelle im Webzugang zur Dokumentationsplattform; Phishing ausgeschlossen; keine Kontrolle über Systeme oder Konten. Die Art der Lücke ist nicht öffentlich.

- Hypothese: Fehler in Zugriffskontrolle oder Authentifizierung einer aus dem Internet erreichbaren Webanwendung, dadurch Lesezugriff auf Inhalte ohne gültiges Konto (hoch): Passt zu „Schwachstelle im Webzugang“, zu „keine Kontrolle über Benutzerkonten“ und zum Verkauf der Schwachstelle als solcher. Laut IBM X-Force 2026 ist die Ausnutzung öffentlich erreichbarer Anwendungen in Europa der häufigste Einstieg.
- Hypothese: bekannte, noch nicht gepatchte Schwachstelle in einer Standard-Wiki- oder Dokumentationssoftware (mittel): Dokumentationsplattformen waren schon Ziel breiter Ausnutzung (CISA-Advisory zu CVE-2023-22515). Welches Produkt Wien einsetzt, ist nicht belegt.
- Hypothese: Fehlkonfiguration, etwa ein unbeabsichtigt öffentlich erreichbarer Bereich oder eine Test-Umgebung (mittel): Unter den Inhalten sind Testdaten und Schulungsunterlagen. Konfigurationsfehler bei Webzugängen sind häufig und werden von automatisierten Scans schnell gefunden.
- Hypothese: Credential Stuffing mit anderswo erbeuteten Zugangsdaten (gering): Nicht ausdrücklich ausgeschlossen, aber die Stadt spricht von einer Schwachstelle und sagt, Benutzerkonten seien nicht kontrolliert worden.

Zeitleiste

03.09.2026 Beginn des unbefugten Zugriffs über den Webzugang – **bestätigt** [<https://presse.wien.gv.at/presse/2026/09/30/wien-datensicherheit-hat-hohen-stellenwert-sicherheitsluecke-umgehend-geschlossen>]

09.09.2026 CERT.at informiert den Magistrat über ein Verkaufsangebot für die Schwachstelle in einem Online-Forum; WienCERT und MA 01 beginnen die Analyse – **bestätigt** [<https://presse.wien.gv.at/presse/2026/09/30/wien-datensicherheit-hat-hohen-stellenwert-sicherheitsluecke-umgehend-geschlossen>]

10.09.2026 Freiwillige Meldung nach dem NIS-Gesetz – **bestätigt** [<https://presse.wien.gv.at/presse/2026/09/30/wien-datensicherheit-hat-hohen-stellenwert-sicherheitsluecke-umgehend-geschlossen>]

11.09.2026 Ende des Zugriffszeitraums; Lücke gemeinsam mit der DSN geschlossen – **bestätigt** [<https://presse.wien.gv.at/presse/2026/09/30/wien-datensicherheit-hat-hohen-stellenwert-sicherheitsluecke-umgehend-geschlossen>]

15.09.2026 Information der Datenschutzbehörde – **bestätigt** [<https://presse.wien.gv.at/presse/2026/09/30/wien-datensicherheit-hat-hohen-stellenwert-sicherheitsluecke-umgehend-geschlossen>]

30.09.2026 Stadt Wien macht den Vorfall öffentlich; ORF und heise berichten; Betroffene werden innerhalb einer Woche informiert – **bestätigt** [<https://wien.orf.at/stories/3373234/>]

01.10.2026 NISG 2026 tritt in Kraft; Mimikama stellt bis dahin weder Veröffentlichung noch Phishing mit Bezug zum Vorfall fest – **berichtet** [<https://www.mimikama.org/datenleck-stadt-wien-5824-betroffene/>]

Vergleichsfälle

- Confluence-Zero-Day CVE-2023-22515 (gemeinsames Advisory von CISA, FBI und MS-ISAC) (2023): Dokumentationsplattformen mit Webzugang sind ein bekanntes und breit angegriffenes Ziel. Sie gehören beim Patchen nach vorne (kein Bezug zum Wiener Produkt belegt).

[<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-289a>]

- Land Kärnten (2022): Als Vergleich für Verwaltungen im DACH-Raum genannt (nur in B erwähnt, ohne Quelle).
- Südwestfalen-IT (2023): Als Vergleich für kommunale IT genannt (nur in B erwähnt, ohne Quelle).

Begriffe einfach erklärt

OT: Operational Technology – die Technik, die Anlagen wie Wasserwerke, Kraftwerke oder Verkehrsampeln steuert, im Gegensatz zur Büro-IT.

Schwachstelle: Ein Fehler in Software oder Konfiguration, über den Unbefugte Zugriff bekommen können.

Webzugang: Eine Anwendung, die über den Browser aus dem Internet erreichbar ist.

CERT.at: Das nationale Computer-Notfallteam Österreichs, das Sicherheitswarnungen sammelt und Betroffene informiert.

Initial Access Broker: Kriminelle, die Zugänge oder Schwachstellen zu fremden Systemen finden und an andere Täter verkaufen.

Phishing: Gefälschte Mails oder Nachrichten, die Menschen zur Preisgabe von Daten oder zu Zahlungen verleiten sollen.

NIS2 / NISG 2026: EU-Richtlinie und österreichisches Gesetz, das wichtigen Einrichtungen Pflichten zur Cybersicherheit und zur Meldung von Vorfällen auferlegt.

Incident Response: Der geplante Ablauf, wie eine Organisation einen Sicherheitsvorfall erkennt, eindämmt und aufarbeitet.

Früherer Stand: Erstmeldung (02.10.2026 22:46)

Wissen 25 % · wahrscheinlich 10 % · nicht bekannt 65 %

Laut Stadt Wien hatte ein Angreifer vom 03. bis 11.09.2026 über einen Webzugang Zugriff auf Teile einer internen Dokumentationsplattform des Magistrats und kopierte rund 26.000 Dokumente (ca. 9 GB) mit Daten von 5.824 Personen sowie Geschäfts- und Infrastrukturinformationen. Aufgefallen ist der Fall, weil CERT.at in einem Online-Forum ein Verkaufsangebot zu dieser Schwachstelle entdeckte und die Stadt am 09.09. informierte. Laut Stadt gab es keine Kontrolle über IT-Systeme oder Benutzerkonten, die Lücke ist geschlossen, und bisher gibt es weder eine Veröffentlichung noch eine Erpressung.

Öffentliche Einschätzung von OT-Cyber auf Basis öffentlicher Quellen. Prozent = Einschätzung: 100 % bestätigt, 0 % sicher falsch. Fachliche Einschätzung, keine Schuldzuweisung.