AUS DEM IUSTORIA-BLOG

Cyberangriff oder Datenleck im Unternehmen: Was in den ersten 72 Stunden zu tun ist

> *Verschlüsselte Server, Lösegeldforderung, geleakte Kundendaten. Was in 72 Stunden ans ÚOOÚ geht, wann in 24 Stunden an NÚKIB, was Versicherer und Partner erfahren und warum Sie nicht zahlen sollten.*

TEAM IUSTORIA

5. 11. 2026 · 12 min Lesezeit

Am Montagmorgen lassen sich die Dateien auf dem gemeinsamen Laufwerk nicht öffnen, und auf den Bildschirmen steht, die Daten seien verschlüsselt und wohin das Lösegeld zu schicken ist. Oder ein Kunde ruft an, weil jemand seine Daten aus Ihrer Datenbank im Internet anbietet. Der erste Anruf geht an den IT-Administrator, und das ist richtig. In der Kanzlei erleben wir aber, dass man an die rechtliche Seite erst nach einer Woche denkt, wenn die Server wieder laufen. Die Meldefristen sind dann bereits abgelaufen, und die Spuren, mit denen sich das Unternehmen gegenüber der Behörde, dem Versicherer oder vor Gericht hätte verteidigen können, sind mit der Neuinstallation verschwunden.

In den ersten drei Tagen geht es aber nicht nur um Technik. Entschieden wird auch, was wem zu melden ist, wer informiert werden muss, wie Beweise gesichert werden und ob gezahlt wird. Wir gehen die Fristen nach der Datenschutz-Grundverordnung (DSGVO) und nach dem neuen tschechischen Cybersicherheitsgesetz durch, sagen, was vom Versicherer und von Geschäftspartnern zu erwarten ist, und wer für die Entscheidung über ein Lösegeld einsteht.

Die ersten Stunden: Angriff stoppen, Spuren nicht löschen

Die Nationale Behörde für Cyber- und Informationssicherheit (NÚKIB) empfiehlt, Geräte nach der Entdeckung von Ransomware vom Netz zu trennen und sie nur dann auszuschalten, wenn es nicht anders geht, denn mit dem Ausschalten gehen die Spuren im Arbeitsspeicher verloren. Der Backup-Server wird als Erstes getrennt, damit der Angriff nicht auch die Sicherungen erfasst. Weiter empfiehlt NÚKIB, bitgenaue Abbilder der betroffenen Systeme anzufertigen, die Betriebsprotokolle (Logs) und Proben des Schadcodes zu sichern und außerhalb des angegriffenen Netzes zu kommunizieren, etwa per Telefon. Der Angreifer kann die Firmen-E-Mails nämlich weiter mitlesen.

Aus rechtlicher Sicht fügen wir zwei Dinge hinzu. Erstens: Führen Sie von der ersten Minute an ein Vorfallsprotokoll, also wann und von wem der Angriff entdeckt wurde, was geschah, wer was entschied und warum. Der Zeitpunkt der Entdeckung setzt die Fristen in Gang, und der Verantwortliche muss jede Verletzung des Schutzes personenbezogener Daten dokumentieren, auch wenn er sie am Ende nicht meldet (Art. 33 Abs. 5 DSGVO). Zweitens: Installieren Sie nichts neu, solange Sie keine Kopien haben. Die Spuren des Angriffs brauchen die Polizei, der Versicherer und das Amt für den Schutz personenbezogener Daten (ÚOOÚ). Vor allem aber brauchen Sie sie selbst, wenn Sie beweisen müssen, dass das Unternehmen angemessen geschützt war.

Verletzung des Schutzes personenbezogener Daten: Meldung an das ÚOOÚ binnen 72 Stunden

Eine Verletzung des Schutzes personenbezogener Daten ist neben ihrem Abfluss auch ihre unbeabsichtigte oder unrechtmäßige Vernichtung, ihr Verlust oder ihre Veränderung (Art. 4 Nr. 12 DSGVO). Ransomware, die eine Kundendatenbank oder die Lohnbuchhaltung verschlüsselt, ist daher auch dann eine solche Verletzung, wenn der Angreifer nichts mitgenommen hat. Sowohl das ÚOOÚ als auch der Europäische Datenschutzausschuss (EDSA) ordnen das als Verletzung der Verfügbarkeit ein.

Nicht jede solche Verletzung ist aber meldepflichtig. Der EDSA nennt als Beispiel ein kleines Unternehmen, das seine Daten verschlüsselt gespeichert hatte, sie binnen weniger Stunden aus einer funktionierenden Sicherung wiederherstellte, ohne dass der Betrieb stillstand, und bei dem die Auswertung der Protokolle sicher ergab, dass der Angreifer nichts kopiert hatte; ein Risiko für die betroffenen Personen war dort unwahrscheinlich, und es genügte, den Vorfall zu dokumentieren. Bei einem Unternehmen, das seine Daten fünf Arbeitstage lang aus Papierunterlagen wiederherstellte, hält er die Meldung dagegen für notwendig. Und wo der Verantwortliche nicht sicher weiß, wie weit der Angreifer gekommen ist, soll er nach dem EDSA vom ungünstigeren Fall ausgehen.

Der Verantwortliche meldet die Verletzung dem ÚOOÚ unverzüglich und möglichst binnen 72 Stunden, nachdem sie ihm bekannt wurde. Nur wenn die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, entfällt die Meldung. Meldet er später, muss er die Verzögerung begründen (Art. 33 Abs. 1). Nach dem EDSA ist dem Verantwortlichen die Verletzung „bekannt“, sobald er hinreichende Gewissheit hat, dass es zu einem Vorfall gekommen ist und personenbezogene Daten betroffen sind. Die Frist wird in Stunden berechnet und läuft auch am Wochenende.

Warten Sie nicht, bis die IT ihre Analyse abgeschlossen hat. Kennen Sie das Ausmaß noch nicht, melden Sie, was Sie wissen, und reichen Sie den Rest schrittweise nach; die Verordnung erlaubt das ausdrücklich (Art. 33 Abs. 4 DSGVO). Eine unvollständige, aber rechtzeitige Meldung ist besser als eine vollständige mit einer Entschuldigung für die Verspätung.
Die Meldung muss die Art der Verletzung mit den Kategorien und der ungefähren Zahl der betroffenen Personen und Datensätze beschreiben, die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle nennen und die wahrscheinlichen Folgen und die ergriffenen Maßnahmen darlegen (Art. 33 Abs. 3). Das ÚOOÚ stellt dafür ein elektronisches Formular bereit. Das ausgefüllte Formular kann über die Datenbox (*datová schránka*, das staatliche elektronische Postfach für den Verkehr mit Behörden; Kennung des ÚOOÚ: qkbaa2n), per Post oder per E-Mail an posta@uoou.gov.cz übermittelt werden. Die E-Mail muss allerdings eine anerkannte elektronische Signatur (*uznávaný elektronický podpis*) tragen; sonst sieht die Behörde sie nur dann als ordnungsgemäße Meldung an, wenn Sie sie mit einem handschriftlich unterzeichneten Formular per Post oder persönlich bestätigen. Am sichersten ist die Datenbox.

Die Verantwortung trägt der Verantwortliche, also derjenige, der über die Verarbeitung entscheidet. Fand der Angriff bei einem Dienstleister statt, etwa beim Cloud-Anbieter oder beim Anbieter der Lohnabrechnungssoftware, muss er Ihnen als Auftragsverarbeiter den Vorfall unverzüglich melden (Art. 33 Abs. 2) und Sie bei der Erfüllung Ihrer Pflichten unterstützen (Art. 28 Abs. 3 Buchst. f). Die Meldung an das ÚOOÚ erstatten aber Sie. Bei Verstößen gegen diese Pflichten droht eine Geldbuße von bis zu 10 Millionen Euro oder 2 % des weltweiten Jahresumsatzes, je nachdem, welcher Betrag höher ist (Art. 83 Abs. 4).

Die Europäische Kommission hat im November 2025 im sogenannten digitalen Omnibus vorgeschlagen, die Frist auf 96 Stunden zu verlängern und nur noch Fälle mit hohem Risiko melden zu lassen. Zum 6. November 2026 war der Vorschlag nicht angenommen, es gelten weiterhin 72 Stunden.

Wann Sie den Personen schreiben müssen, deren Daten abgeflossen sind

Hat die Verletzung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen zur Folge, muss der Verantwortliche sie unverzüglich auch direkt benachrichtigen (Art. 34 Abs. 1 DSGVO). Typischerweise geht es um abgeflossene Passwörter, Geburtsnummern, Kontonummern, Gesundheitsdaten oder alles, was sich für Betrug missbrauchen lässt. Die Benachrichtigung ist in klarer und einfacher Sprache abzufassen und enthält eine Kontaktstelle, die wahrscheinlichen Folgen und die ergriffenen Maßnahmen (Art. 34 Abs. 2). Wir empfehlen, auch hineinzuschreiben, was die Betroffenen tun sollen: Passwörter ändern, E-Mails und Anrufen misstrauen, die sich auf Ihr Unternehmen berufen, und die Kontobewegungen im Auge behalten. Betrüger nutzen abgeflossene Daten gern für Nachrichten, die überzeugend echt wirken.

Benachrichtigen müssen Sie die Betroffenen nicht, wenn die Daten verschlüsselt und für den Angreifer unzugänglich waren, wenn Sie Maßnahmen ergriffen haben, nach denen das hohe Risiko aller Wahrscheinlichkeit nach nicht mehr besteht, oder wenn die Benachrichtigung mit einem unverhältnismäßigen Aufwand verbunden wäre. Im letzten Fall müssen Sie aber stattdessen eine öffentliche Bekanntmachung veröffentlichen (Art. 34 Abs. 3). Das ÚOOÚ kann die Benachrichtigung anordnen (Art. 34 Abs. 4).

Wer wegen eines Verstoßes gegen die Verordnung einen materiellen oder immateriellen Schaden erlitten hat, hat Anspruch auf Schadensersatz (Art. 82 Abs. 1). Der Gerichtshof der EU befasste sich im Urteil vom 14. Dezember 2023, Natsionalna agentsia za prihodite, Rechtssache C-340/21, mit einem Angriff auf die bulgarische Steuerverwaltung, nach dem die Daten von mehr als sechs Millionen Menschen im Internet auftauchten. Er entschied, dass ein Datenleck infolge eines Angriffs Dritter allein nicht bedeutet, dass die Maßnahmen des Verantwortlichen ungeeignet waren. Im Streit um Schadensersatz trägt der Verantwortliche aber die Beweislast dafür, dass sie geeignet waren, und er wird von der Haftung nicht schon dadurch befreit, dass der Angreifer das Leck verursacht hat. Schon die Befürchtung eines Missbrauchs der Daten kann zudem ein immaterieller Schaden sein, wenn sie unter den gegebenen Umständen begründet ist (Tenor, Nr. 1, 3, 5 und 6; Rn. 85). Für ein Unternehmen heißt das: Verteidigen kann es sich vor allem mit Dokumentation, also mit Sicherheitsrichtlinien, Nachweisen über Schulungen, Updates und Sicherungen und mit dem Vorfallsprotokoll.

Das neue Cybersicherheitsgesetz: Betrifft es Sie?

Seit dem 1. November 2025 gilt das Gesetz Nr. 264/2025 Slg. über die Cybersicherheit, das die europäische NIS-2-Richtlinie in tschechisches Recht umsetzt. Es erfasst Erbringer regulierter Dienste in 15 Sektoren, von Energie, verarbeitendem Gewerbe und Lebensmitteln über Verkehr, Wasser- und Abfallwirtschaft und Gesundheitswesen bis zu digitalen Diensten (§ 4 Abs. 1). In der Regel geht es um mittlere und große Unternehmen; ein kleines Unternehmen nur dann, wenn es für den Staat von besonderer Bedeutung ist, und manche Dienste registriert die Behörde unabhängig von der Größe (§ 5). Die konkreten Dienste legt die Verordnung Nr. 408/2025 Slg. über regulierte Dienste fest. Warten Sie nicht auf eine Aufforderung der Behörde: Den Dienst muss der Erbringer NÚKIB selbst melden, und zwar spätestens 60 Tage nach dem Tag, an dem er die Voraussetzungen erfüllt hat (§ 6 Abs. 1). Bei der Unternehmensgröße zählen auch die Gesellschaften der Gruppe mit, sodass das Gesetz auch eine kleine Tochtergesellschaft eines großen Konzerns erfassen kann; außer Betracht bleiben nur Gruppengesell-

schaften, deren technische Ressourcen vollständig von denen getrennt sind, mit denen das Unternehmen den regulierten Dienst erbringt (§ 7 Buchst. c). Ein Unternehmen, das kürzlich gewachsen ist, eine neue Tätigkeit aufgenommen hat oder einer Gruppe beigetreten ist, sollte das sofort prüfen.

Ein Erbringer im Regime höherer Pflichten (*režim vyšších povinností*) meldet Vorfälle an NÚKIB, ein Erbringer im Regime niedrigerer Pflichten (*režim nižších povinností*) an das Nationale CERT, und zwar nur solche mit erheblichen Auswirkungen auf den Dienst (§ 15 Abs. 1 bis 3). Die Fristen sind kürzer als nach der DSGVO: Die Erstmeldung erfolgt spätestens 24 Stunden nach Feststellung des Vorfalls (§ 16 Abs. 1). Binnen 72 Stunden folgt dann eine Meldung mit einer ersten Bewertung und binnen 30 Tagen danach ein Abschlussbericht. Das gilt im Regime niedrigerer Pflichten für jeden gemeldeten Vorfall mit erheblichen Auswirkungen auf den Dienst, im Regime höherer Pflichten dann, wenn NÚKIB mitteilt, dass der Vorfall erhebliche Auswirkungen auf den Cyberraum des Staates hat (§ 16 Abs. 2 und 3). Gemeldet wird über das NÚKIB-Portal (§ 16 Abs. 4). Mit den Meldungen muss der Erbringer spätestens ein Jahr nach Zustellung der Registrierungsentscheidung beginnen (§ 15 Abs. 4). Wer sie unterlässt, riskiert eine Geldbuße von bis zu 250 Millionen CZK oder 2 % des weltweiten Umsatzes im Regime höherer Pflichten und bis zu 175 Millionen CZK oder 1,4 % im Regime niedrigerer Pflichten, je nachdem, welcher Betrag höher ist (§ 59 Abs. 4).

Die Meldung an NÚKIB und die Meldung an das ÚOOÚ sind zwei getrennte Pflichten, und die eine ersetzt die andere nicht. Die Behörden tauschen lediglich Informationen aus, damit derselbe Pflichtverstoß nicht doppelt geahndet wird (§ 64 Abs. 5). Und ein Unternehmen, das nicht unter das Gesetz fällt, kann NÚKIB einen Vorfall freiwillig melden (§ 15 Abs. 5); das Gesetz sieht vor, dass sich die Behörde oder das Nationale CERT auch zu einer solchen Meldung äußern und methodisch helfen (§ 17 Abs. 5).

Polizei, Versicherer und Geschäftspartner

Der Angriff ist in der Regel eine Straftat des unbefugten Zugriffs auf ein Computersystem und des Eingriffs in dieses (§ 230 des tschechischen Strafgesetzbuchs), die Lösegeldforderung zudem Erpressung (§ 175). Die Polizei einzuschalten, empfiehlt auch NÚKIB. Die Strafanzeige belegt außerdem, dass das Unternehmen Opfer war, und Versicherer wie Partner werden danach fragen.

Deckt eine Versicherung den Schaden, zeigen Sie dem Versicherer das Ereignis unverzüglich an, geben Sie wahrheitsgemäß Auskunft, legen Sie die Belege vor und gehen Sie so vor, wie es im Vertrag vereinbart ist (§ 2796 Abs. 1 des tschechischen Bürgerlichen Gesetzbuchs). Der letzte Teil wird leicht übersehen. Bevor Sie einen Forensik-Dienstleister beauftragen oder mit dem Angreifer irgendetwas aushandeln, lesen Sie die Versicherungsbedingungen; was dort über das Vorgehen nach dem Ereignis steht, bindet auch Sie. Wie lange der Versicherer prüfen darf und wann Sie einen Vorschuss verlangen können, beschreibt unser Ratgeber zur Schadensprüfung und zum Vorschuss (auf Tschechisch).

Geschäftspartner spielen in zweierlei Hinsicht eine Rolle. Liefern Sie wegen des Angriffs nicht rechtzeitig, haften Sie für den Schaden, und befreien kann Sie nur ein außergewöhnliches, unvorhersehbares und unüberwindbares Hindernis (§ 2913 Abs. 2 des Bürgerlichen Gesetzbuchs). Darauf, dass ein Gericht einen Cyberangriff als ein solches Hindernis anerkennt, würden wir heute nicht setzen: Angriffe sind alltäglich, und dass ein Unternehmen

sich gegen sie schützt, wird erwartet. Prüfen Sie deshalb Ihre Verträge darauf, was sie über höhere Gewalt, die Meldung von Vorfällen und Fristen sagen. Wie eine gute Klausel über höhere Gewalt aussehen sollte, beschreiben wir im Artikel Fünf Vertragsklauseln, die Ihnen Millionen sparen können (und die niemand liest). Eigene Meldefristen enthalten oft Auftragsverarbeitungsverträge und Verträge, die ein Erbringer eines regulierten Dienstes mit seinen Lieferanten schließt; für Letztere schreibt das Cybersicherheitsgesetz Sicherheitsanforderungen ausdrücklich vor (§ 13 Abs. 5). Partnern, deren Daten oder Systeme betroffen sein könnten, schreiben Sie rechtzeitig und sachlich, was geschehen ist und was sie tun sollen. Vermutungen über den Schuldigen und Überlegungen, was man hätte besser machen können, gehören nicht in ein solches Schreiben.

Lösegeld: eine Entscheidung, für die die Geschäftsleitung haftet

NÚKIB empfiehlt, unter keinen Umständen Lösegeld zu zahlen. Die Zahlung ermutigt den Angreifer zu weiteren Angriffen, nichts garantiert, dass er die Daten entschlüsselt oder löscht, die Entschlüsselung entfernt den Schadcode nicht, und rechtlich kann die Zahlung die Sorgfalt eines ordentlichen Geschäftsleiters (*péče řádného hospodáře*) verletzen. Der letzte Grund betrifft den Geschäftsführer oder das Vorstandsmitglied persönlich. Er muss sein Amt mit der notwendigen Loyalität sowie mit den erforderlichen Kenntnissen und der erforderlichen Sorgfalt ausüben (§ 159 Abs. 1 des Bürgerlichen Gesetzbuchs) und im Streitfall selbst beweisen, dass er so gehandelt hat (§ 52 Abs. 2 des tschechischen Gesetzes über Handelskorporationen). Ihn schützt die Business Judgment Rule: Wer in gutem Glauben vernünftigerweise annehmen durfte, informiert und im vertretbaren Interesse der Gesellschaft zu handeln, hat sorgfältig gehandelt (§ 51 Abs. 1).

Erwägt die Geschäftsleitung eine Zahlung, etwa weil das Unternehmen ohne die Daten nicht überleben würde, braucht die Entscheidung Grundlagen: eine Einschätzung, ob und wie schnell sich der Betrieb aus den Sicherungen wiederherstellen lässt, eine Bezifferung der Schäden, die Stellungnahme des Versicherers und ein Protokoll darüber, warum sie so entschieden hat, wie sie entschieden hat. Mehr zur Haftung des Geschäftsführers finden Sie in unserem Ratgeber dazu, wofür ein Geschäftsführer haftet (auf Tschechisch).

Zwei Dinge gelten immer. Das Geld darf nicht an Personen und Gruppen auf der Sanktionsliste der EU gehen; für Cyberangriffe hat die Union ein eigenes Sanktionsregime (Art. 3 Abs. 2 der Verordnung (EU) 2019/796 des Rates), und ein Verstoß gegen internationale Sanktionen in größerem Umfang ist eine Straftat (§ 410 des Strafgesetzbuchs). Der Angreifer stellt sich freilich nicht vor. Bevor die Geschäftsleitung zahlt, soll deshalb zuerst ein Forensik-Dienstleister bestimmen, um welche Gruppe es sich handelt, das Ergebnis wird mit den Sanktionslisten abgeglichen und gehört in das Protokoll über die Entscheidung. Und die Zahlung ändert nichts an den Meldepflichten: Die Verletzung ist bereits eingetreten, und das Versprechen des Angreifers, die Daten gelöscht zu haben, kann niemand überprüfen.

Schreiben Sie heute auf eine Seite, wer bei einem Angriff entscheidet, die Telefonnummern von Geschäftsleitung, IT-Administrator, Versicherer und Anwalt sowie das Vorgehen bei der Meldung an das ÚOOÚ. Bewahren Sie sie außerhalb der Firmensysteme auf, zum Beispiel ausgedruckt.
Prüfen Sie, ob Ihr Dienst in der Verordnung Nr. 408/2025 Slg. aufgeführt ist. Wer die Voraussetzungen des Cybersicherheitsgesetzes erfüllt, muss sich binnen 60 Tagen selbst bei NÚKIB melden.

Prüfen Sie in den Verträgen mit IT- und Cloud-Dienstleistern, binnen wie vieler Stunden sie Ihnen einen Vorfall melden müssen und welche Unterlagen sie Ihnen schicken. Ohne sie können Sie die Meldung an das ÚOOÚ nicht erstellen.

Überblick

Frage	Antwort	Vorschrift
Ist die Verschlüsselung von Daten durch Ransomware eine Verletzung des Schutzes personenbezogener Daten?	Ja, es geht um einen Verlust der Verfügbarkeit; zu melden, es sei denn, ein Risiko für die Betroffenen ist unwahrscheinlich	Art. 4 Nr. 12, Art. 33 Abs. 1 DSGVO
Frist für die Meldung an das ÚOOÚ	Unverzüglich, möglichst binnen 72 Stunden ab Kenntnis; später nur mit Begründung	Art. 33 Abs. 1 DSGVO
Wann die Betroffenen zu benachrichtigen sind	Bei voraussichtlich hohem Risiko, unverzüglich	Art. 34 DSGVO
Geldbuße bei Verstoß gegen die Meldepflichten	Bis zu 10 Millionen Euro oder 2 % des weltweiten Umsatzes	Art. 83 Abs. 4 DSGVO
Meldung nach dem Cybersicherheitsgesetz	Erstmeldung binnen 24 Stunden; bei einem Vorfall mit erheblichen Auswirkungen Meldung binnen 72 Stunden und Abschlussbericht binnen 30 Tagen nach der Meldung	§ 16 des Gesetzes Nr. 264/2025 Slg.
Meldung eines regulierten Dienstes an NÚKIB	Binnen 60 Tagen nach Erfüllung der Voraussetzungen	§ 6 Abs. 1 des Gesetzes Nr. 264/2025 Slg.
Anzeige an den Versicherer	Unverzüglich und nach dem im Vertrag vereinbarten Verfahren	§ 2796 Abs. 1 des Bürgerlichen Gesetzbuchs
Lösegeld	NÚKIB rät ab; Zahlungen an Personen auf der Sanktionsliste sind verboten	Art. 3 Abs. 2 der Verordnung (EU) 2019/796

Haben Sie gerade mit einem Angriff oder einem Datenleck zu tun? Wir helfen zu entscheiden, was wem zu melden ist, bereiten die Meldung an das ÚOOÚ, die Benachrichtigung der Betroffenen und die Schreiben an Versicherer und Partner vor und geben der Geschäftsleitung Grundlagen für Entscheidungen, die später überprüft werden. Datenschutz und Cybersicherheit betreuen wir im Rahmen unserer Leistungen im Bereich IT-Compliance. Schreiben Sie uns.

Fazit

Die rechtlichen Fristen nach einem Cyberangriff laufen unabhängig davon, wann die Systeme wieder anlaufen: 72 Stunden für das ÚOOÚ, bei regulierten Diensten 24 Stunden für NÚKIB oder das Nationale CERT und unverzüglich für den Versicherer. Ein Unternehmen, das in den ersten Stunden die Spuren sichert, ein Vorfallsprotokoll führt und rechtzeitig meldet, auch mit unvollständigen Informationen, hat später gegenüber der Behörde, dem Versicherer und vor Gericht etwas in der Hand.

Ein Unternehmen, das schon vorher weiß, ob es unter das Cybersicherheitsgesetz fällt und was ihm die Dienstleister in den Verträgen zusagen, muss das nicht erst während des Angriffs klären.

Quellen

- Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates, Datenschutz-Grundverordnung, Art. 4 Nr. 12, Art. 28 Abs. 3 Buchst. f, Art. 33, Art. 34, Art. 82 und Art. 83 Abs. 4.
- Gesetz Nr. 264/2025 Slg. über die Cybersicherheit, §§ 4 bis 8, § 13, § 15, § 16, § 17, § 59 und § 64 (Fassung ab 1. November 2025).
- Verordnung Nr. 408/2025 Slg. über regulierte Dienste.
- Gesetz Nr. 89/2012 Slg., Bürgerliches Gesetzbuch, § 159, § 2796 und § 2913.
- Gesetz Nr. 90/2012 Slg. über Handelskorporationen, § 51 und § 52.
- Gesetz Nr. 40/2009 Slg., Strafgesetzbuch, § 175, § 230 und § 410.
- Verordnung (EU) 2019/796 des Rates über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedstaaten bedrohen, Art. 3.
- Urteil des Gerichtshofs der EU vom 14. Dezember 2023, Natsionalna agentsia za prihodite, Rechtssache C-340/21.
- Europäischer Datenschutzausschuss, Leitlinien 9/2022 für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der DSGVO, Version 2.0, und Leitlinien 01/2021 zu Beispielen für die Meldung von Verletzungen des Schutzes personenbezogener Daten, Version 2.0, Fälle Nr. 01 und 02.
- NÚKIB, Ransomware: Empfehlungen zur Eindämmung, Prävention und Reaktion, Version 1.2 vom 22. Mai 2023, Abschnitt 4.
- Amt für den Schutz personenbezogener Daten, Verletzung des Schutzes personenbezogener Daten (uoou.gov.cz).

Dieser Artikel dient der allgemeinen Information und ist keine Rechtsberatung. Er beruht auf der Rechtslage zum Tag der Veröffentlichung; ob und wem ein konkreter Vorfall zu melden ist, hängt davon ab, welche Daten und Dienste er betroffen hat und ob das Unternehmen unter das Cybersicherheitsgesetz fällt.

Cyberangriff oder Datenleck im Unternehmen: Was in den ersten 72 Stunden zu tun ist

Team IUSTORIA · Veröffentlicht 5. 11. 2026

https://www.iustoria.cz/de/blog/cyberangriff-oder-datenleck-im-unternehmen-die-ersten-72-stunden/

Der Text ist urheberrechtlich geschützt. Die unveränderte Weitergabe des gesamten Dokuments ist willkommen; die Übernahme von Teilen in andere Texte nur mit Quellenangabe. © IUSTORIA, advokátní kancelář, s.r.o.