

# Cyber-Resilience-Framework

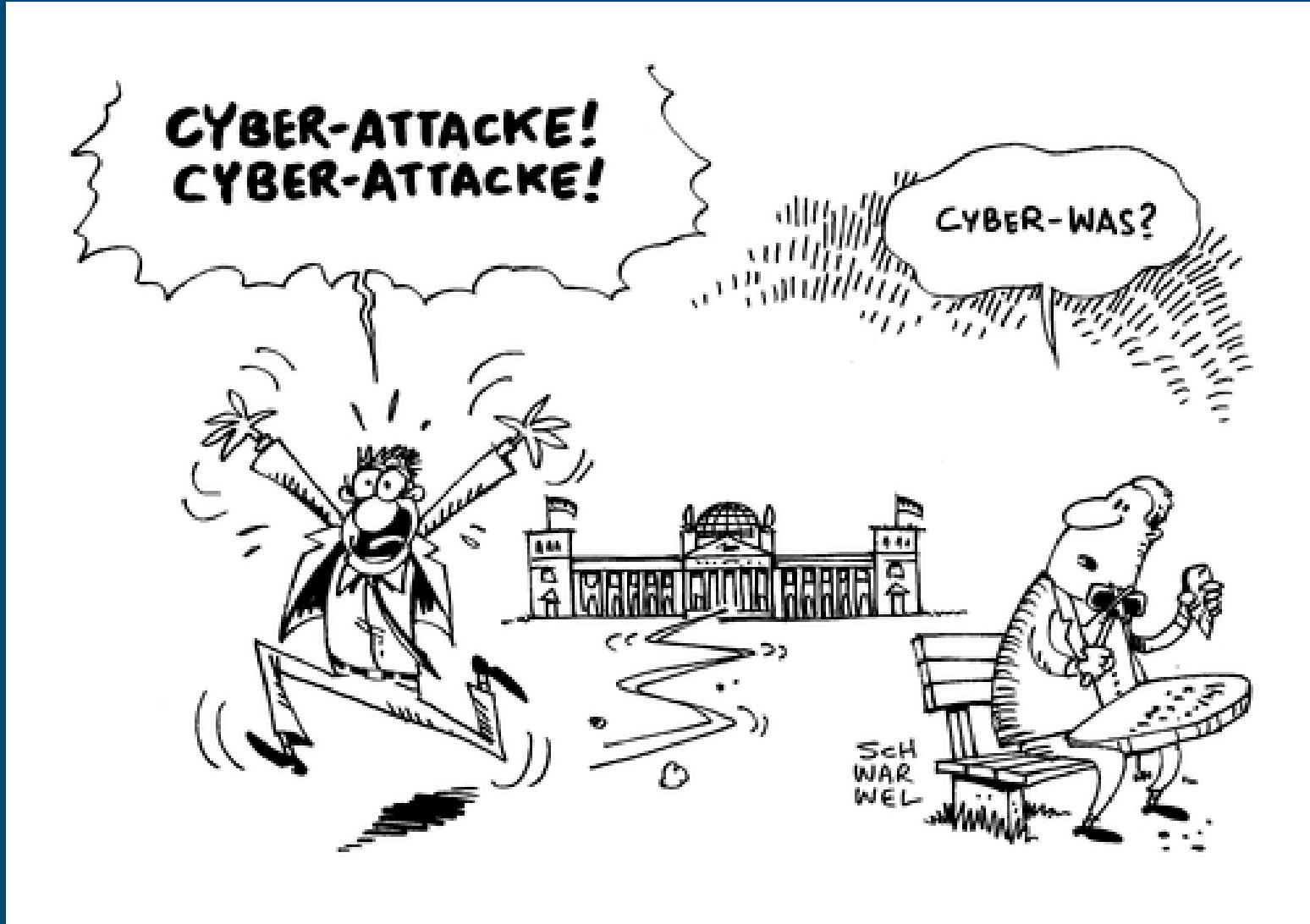
Praktische Hilfestellungen für Kommunen  
im Falle von IT-Sicherheitsvorfällen



Bundesamt  
für Sicherheit in der  
Informationstechnik

Fabienne Tegeler (BSI), 04.11.2025

Vis!t 2025, Linz



[https://de.toonpool.com/cartoons/Cyber%20Attacke%20Bundestag%20Hacker\\_249528](https://de.toonpool.com/cartoons/Cyber%20Attacke%20Bundestag%20Hacker_249528)

# Agenda

- Dialog für Cybersicherheit
- Workstream „Cyber-Resilience-Framework. In IT-Krisen schneller agieren. (RESI)“
- Was steckt im Framework?
- Struktur und Anwendung
- Das Szenario – Eine Blaupause für den Ernstfall
- Ergebnisse
- Ausblick

# Dialog für Cybersicherheit



Digitalisierung



Vernetzung



Innovationen

BSI

Multistakeholder-  
Dialog

Staat



Wissenschaft



Wirtschaft



Kultur und Medien



Zivilgesellschaft



Cybersicherheit – alle Perspektiven einbeziehen

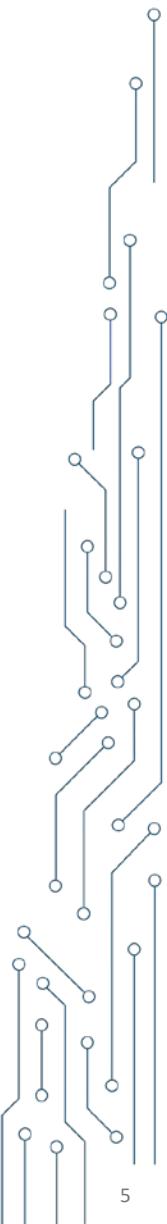
<https://www.dialog-cybersicherheit.de>

# Workstream „Cyber-Resilience-Framework. In IT-Krisen schneller agieren. (RESI)“

**Vision:** Stärkung von Kommunen, damit diese im Falle eines Cyberangriffs schneller und effektiv reagieren können

**Ziel:** Entwicklung eines Resilienz-Frameworks für effizientere Reaktionsprozesse von Kommunen und somit Minimierung der Schäden für Bürger:innen

- Aufbau auf bereits vorhandenen Hilfsmittel, Konzepte und Prozesse
- Schließung von Lücken durch die Entwicklung zielgerichteter Hilfsmittel
- Entwicklung eines fiktiven kommunalen Ransomware-Szenarios als Blaupause



# Was steckt im Framework?

## Ausgangslage

- IT-Krisen zeigen: **Zusammenarbeit zwischen Verwaltungsebenen ist schwierig**
- Unterschiedliche Prozesse, Methoden, Erwartungen
- Kommunen: hohe Krisenkompetenz aber IT-Krisen oft Neuland
- Föderale Strukturen erschweren schnelle Koordination
- Ziel: **Handlungsfähigkeit & Vertrauen sichern** trotz Chaosphase

# Was steckt im Framework?

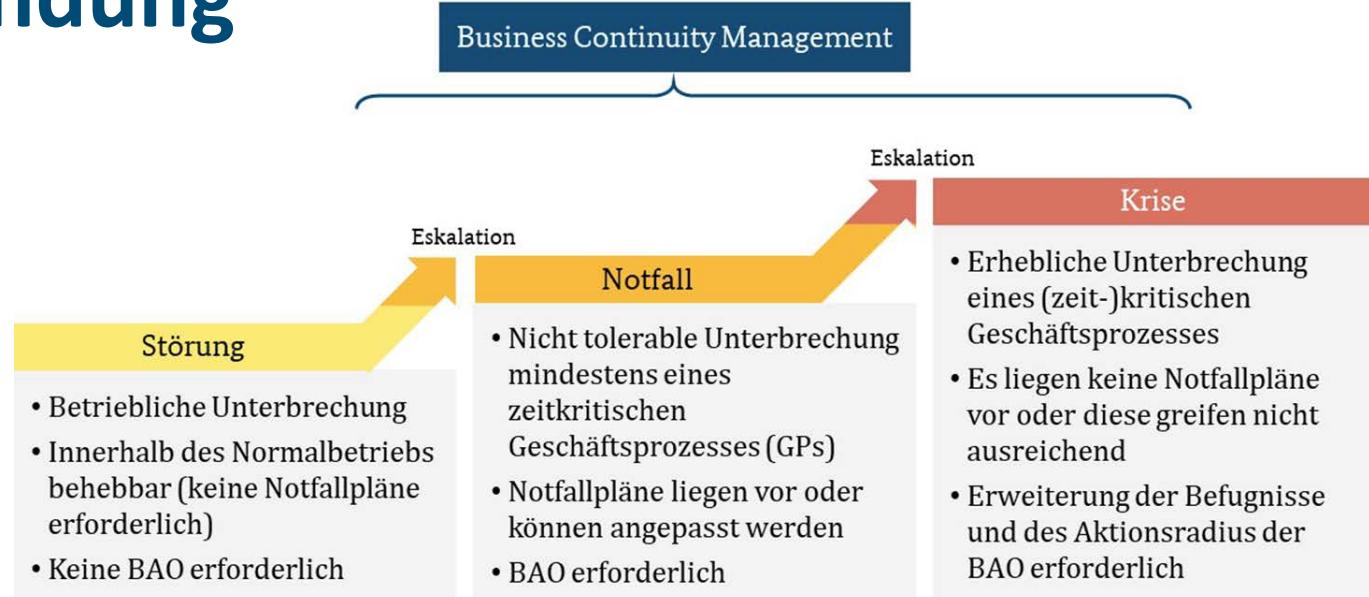
## Ziel und Ansatz des Frameworks

- RESI = **strukturelles und konzeptionelles Framework**, das Kommunen bei der **Organisation, Analyse und Bewertung** ihres IT-Krisenmanagements unterstützt
- **Schafft Ordnung & Orientierung** in der Krisenphase
- Bietet: vorgefertigte Komponenten, standardisierte Abläufe, Werkzeuge
- Ziel: **geordnetes Handeln** statt ad-hoc-Reaktionen
- Fokus: **Nutzung & Bündelung bestehender Hilfsmittel**
- Grundlage: BSI-Standard 200-4 (Business Continuity Management)

# Struktur und Anwendung

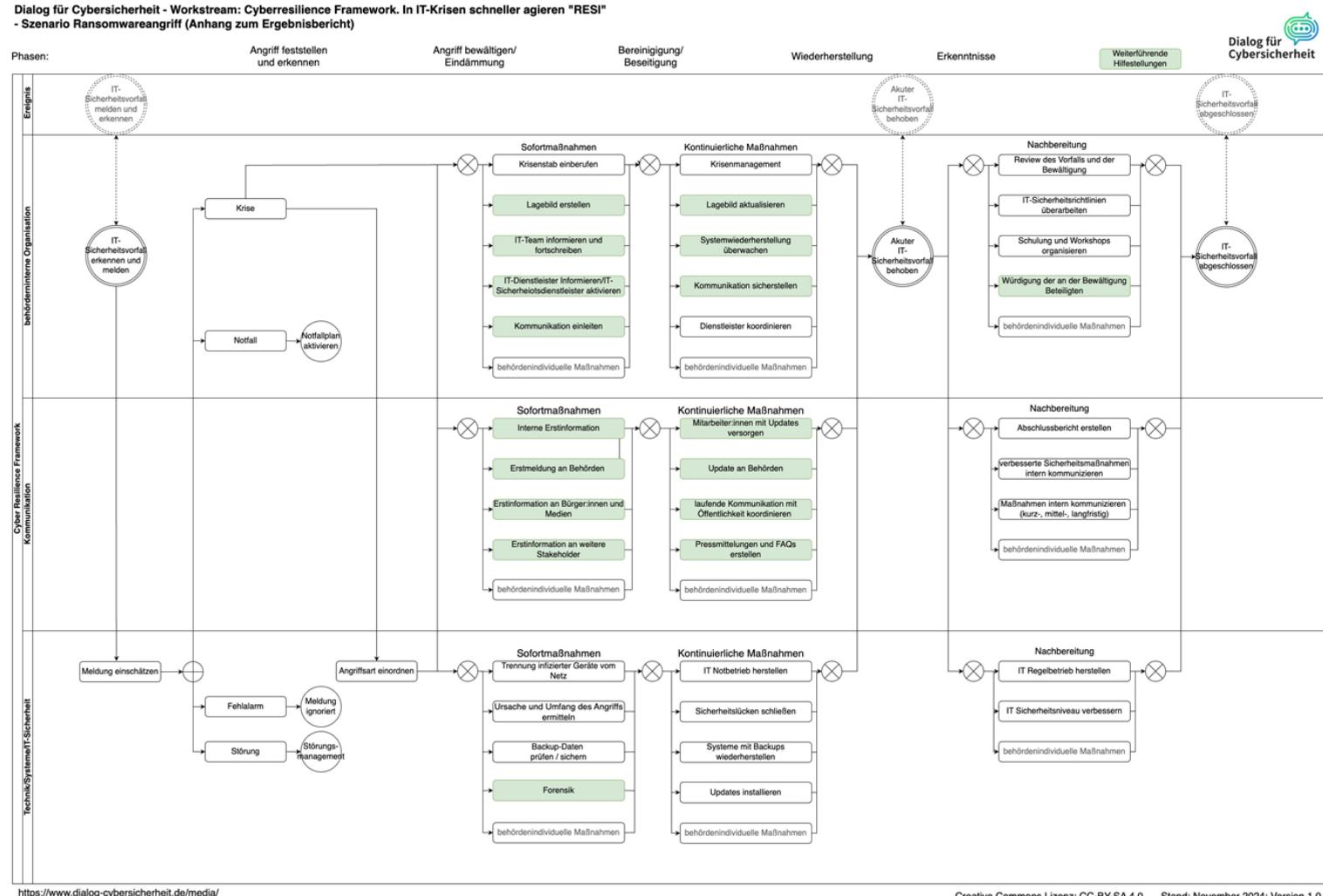
## Abgrenzung:

- Störung
- Notfall
- Krise



- Klare Rollen, Kommunikationswege, Entscheidungsprozesse
- Gute Vorbereitung verkürzt Reaktionszeit & minimiert Schaden
- Einheitliche Struktur für Kommunen, Behörden & Dienstleister
- Orientierung auch bei Stress, Unsicherheit & Zeitdruck

# Das Szenario – Eine Blaupause für den Ernstfall

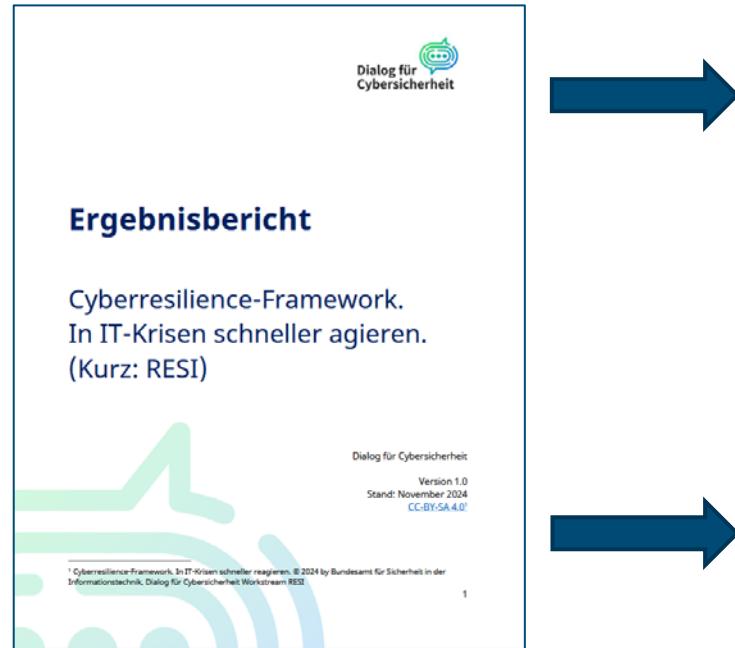


### 3 Handlungsstränge:

- behördeninterne Organisation
  - Kommunikation
  - Technik/Systeme/IT-Sicherheit

# Ergebnisse des Workstreams RESI

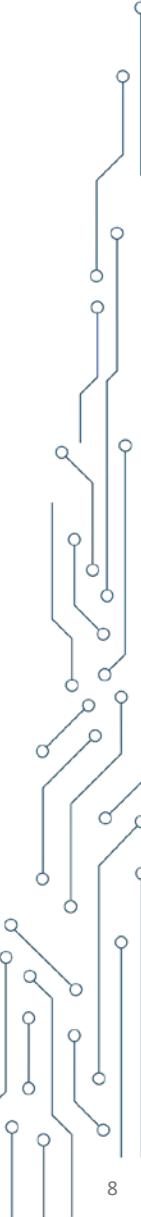
## Zwei zentrale Handreichungen



- Ablaufdiagramm eines Angriffs mit Phasen & Handlungspfaden
  - Verlinkung zu bestehenden & neuen Hilfsmitteln  
  - Vorlagen, Checklisten, Kontaktlisten
  - Unterstützung für interne & externe Kommunikation

Checklist Lagefassung		Wingit Cybersecurity
Anzahl der zu beantwortenden Fragen für Lagefassung beauftragten und eingesetzten werden. Sie kann „einer Feste“ in der Anzahlheit der Befragte und anderen Registrierungsumfangsgrößen werden.		
TeilFrage	Frage	Ergebnis
<b>TEIL ANGRIFF</b>		
Was ist der Angriff? Was ist es für ein Angriff?		
Wer wurde der Angriff benannt?		
Was ist die Angriffsmotivierung?		
Sind Menschen im Gefahr? (z.B. durch Eindringen technischer Funktionen, Verlust von Daten, Verlust von Dienstleistungen, Verlust von Kompetenzen, Zündungstechnologie, etc.)		
<b>AUFGABENFRISTEN (FEST / INFINI)</b>		
Ist der Angriffsteil organisatorisch und zeitlich fest? Ist er mit allen relevanten Personen besprochen?		
In welchem Ausmaß ist die Arbeitszeitplanung der Beteiligten eingeschränkt?		
Was ist die Angriffsmotivierung? (z.B. durch Eindringen technischer Funktionen, Verlust von Daten, Verlust von Dienstleistungen, Verlust von Kompetenzen, Zündungstechnologie, etc.)		
Ist die Arbeitszeitplanung der Beteiligten möglich? (Wenige Reaktionen bei Angriffsteil, kein Angriffsteil, kein Angriffsteil, kein Angriffsteil)		
Bei wem ist die Arbeitszeitplanung eingeschränkt?		
<b>AUFGABENFRISTEN (FEST / INFINI)</b>		
Wer ist der Angriffsteil, der die technisch, verfügbare IT (Server, Telefon, Matherasse, Webiste, etc.)?		
Werste Angriffsteil ist angewiesen, Angriffsteil zu koordinieren und durchzuführen?		
Welche Wissen müssen Angriffsteil haben? Welche Angriffsteil setzt Fragen auf die Befragten?		
Wie lange sind die Daten für Angriffsteil vorschriftlich verfügbare?		
Wer ist der Angriffsteil, der die technisch, verfügbare IT (Server, Telefon, Matherasse, Webiste, etc.)?		
Stehen Angriffsteile am unteren Ende einer hierarchischen Zugriffsumgebung (Emergency Response Team) oder durch Beschränktes Steuerungsfähigkeit, kann Angriffsteil keine Reaktionen, keine Sitzungsverfügbarkeit, keine Sitzungsverfügbarkeit verschaffen oder nutzen?		
<b>DATENSICHERHEIT</b>		
Zur Datensicherheit? Wenn ja, welche Angriffsteil?		
Legt eine Sicherheitsprüfung/Gesichtserkennung vor?		
Legt eine Datensicherheitsteilung vor, bei der auch Befragte Personen Angriffsteil sind?		
Was müssen potentiell betroffene Personen wissen, um sich jetzt von dem Auslösern zu befreien? Wie kann es auslösen?		

Notfall-Kontaktliste: Wichtige Ansprechpartner im Krisenfall					
Notfall-Kontaktliste: Wichtige Ansprechpartner im Krisenfall					
Ansprechpartner	Name	Telefon direkt	Mobile direkt	E-Mail direkt	gpt. Telefon (privat)
Krisenstab					
Verwaltungsrat (HNB, Bürgermeister)					
Recht & Compliance					
Geberthilf und Galerienkunst					
IT-Abschaffung-Dienstleister					
Kommunikation/Pressestelle					
Arbeitsicherheit					
Wissen: Mitglieder des Krisenstabes					
<b>Befehlshaber und Verwaltung</b>					

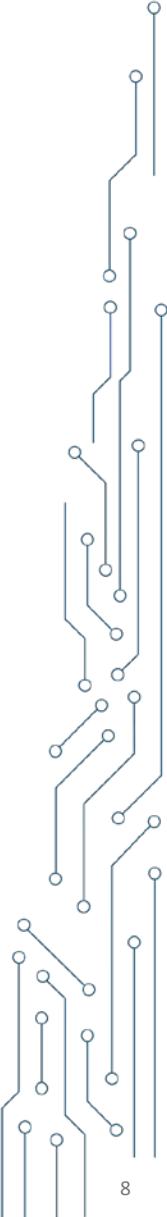


# Ausblick

- Die Arbeitsgruppe **RESI** arbeitet ehrenamtlich weiter
- Das **Ablaufszenario** wurde in ein Prozessmodell nach **BPMN** überführt
- **Start mit Szenario-Entwicklung DDoS**
- Aktualisierung des Ergebnisberichtes RESI
- Einarbeitungen von Rückmeldungen – **GERN MITMACHEN**
- Stehen gern als Ansprechpartner zur Verfügung
- E-Mail: [resi@dialog-cybersicherheit.de](mailto:resi@dialog-cybersicherheit.de)



Laden Sie den RESI  
Ergebnisbericht hier  
herunter



# Vielen Dank für Ihre Aufmerksamkeit!

Fabienne Tegeler

Fachbereichsleitung „Verbindungswesen und Recht“

**Fabienne.Tegeler@bsi.bund.de**

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Godesberger Allee 87

53175 Bonn

[www.bsi.bund.de](http://www.bsi.bund.de)



Bundesamt  
für Sicherheit in der  
Informationstechnik



Bild: © AdobeStock/Nirut