

DE

Regierungsplan zum Umgang mit Cyber- und digitalen Krisen

DEUTSCHE FASSUNG 12/09/2025

*Vom Regierungsrat am 12. September 2025 genehmigt und für verbindlich erklärt.
Im Falle von Abweichungen ist die französische Sprachversion maßgebend.*



LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG

Inhaltsverzeichnis

1.	Einleitung	3
2.	Nationaler und europäischer Rahmen	4
3.	Schlüsselbegriffe	5
3.1.	Nationale Klassifizierung von Cybersicherheitsvorfällen	5
3.2.	Klassifizierung von Cyberbedrohungen	5
4.	Formen der Zusammenarbeit	6
4.1.	Modus „Permanent“	6
4.2.	Modus „Alarm/CERC“	6
4.3.	Krisenmodus	6
5.	Krisenmanagementgremien	7
5.1.	Bewertungsstelle für Cyberbedrohung (CERC)	7
5.2.	Krisenstab (CC)	7
5.3.	Cyber-Einsatzzentrale (PCO-C)	8
5.4.	Stelle für Kommunikation und Information (CCI)	8
6.	Maßnahmen des Krisenmanagements	10
6.1.	Bewertung	10
6.2.	Verstärkte Wachsamkeit	10
6.3.	Systemaufrüstung und -schutz	10
6.4.	Wiederherstellung der Dienste	10
7.	Internationale Zusammenarbeit und Unterstützung	11
8.	Information an die Öffentlichkeit	11

1. Einleitung

Der Regierungsplan zum Umgang mit Cyber- und digitalen Krisen definiert den allgemeinen Rahmen für die Vorsorge, Koordinierung und Reaktion des luxemburgischen Staates auf Cyber- oder digitale Krisen, die den lebenswichtigen Interessen oder Grundbedürfnissen des gesamten Landes oder eines Teils davon oder seiner Bevölkerung schaden könnten, insbesondere im Falle eines größeren technischen Ausfalls oder eines groß angelegten Angriffs auf Informations- und Kommunikationstechnologiesysteme des öffentlichen und/oder privaten Sektors.

Er ist eine Aktualisierung des Cyber-Notfallplans (PIU Cyber) und baut auf diesem auf, wobei die Entwicklungen im Bereich der Cyberbedrohungen, der nationale und europäischen Rechtsrahmen sowie die neuesten Krisenmanagementpraktiken berücksichtigt werden.

Die Hauptziele des Plans sind:

- › Stärkung der Vorsorge, Prävention und des Schutzes vor Cyber- und digitalen Risiken;
- › Bestimmung der für eine wirksame nationale Koordinierung erforderlichen Leitlinien der Regierungsführung und der Krisenmanagementgremien;
- › Bestimmung allgemeiner Verfahren für die Reaktion auf Krisensituationen und deren Bewältigung sowie der jeweiligen Rollen der beteiligten Akteure;
- › Bestimmung des Rahmens für die Verbreitung von Warnmeldungen der Behörden und Informationen an die Öffentlichkeit.

Er gilt für Situationen, in denen die tatsächliche oder potenzielle Schwere eines Ereignisses dringende Entscheidungen und eine Koordinierung auf nationaler Ebene sowie gegebenenfalls eine Koordinierung mit europäischen und internationalen Krisenbewältigungsmechanismen erfordert.

Ein Cyber- oder digitaler Notfall bezeichnet ein Ereignis, das auf einen Cyber- oder Digitalsicherheitsvorfall oder eine Cyberbedrohung zurückzuführen ist, das zu einer erheblichen Störung oder zur vollständigen Nichtverfügbarkeit von Informations- und Kommunikationstechnologiesystemen führen kann und das die lebenswichtigen Interessen oder Grundbedürfnisse des gesamten oder eines Teils des Landes oder der Bevölkerung des Großherzogtums Luxemburg beeinträchtigt oder beeinträchtigen könnte.

Dieser Plan wurde vom Hochkommissariat für nationale Sicherheit (*Haut-Commissariat à la protection nationale, HCPN*) ausgearbeitet und wird von diesem verwaltet. Seine operative Umsetzung liegt in der Zuständigkeit der Regierung. Je nach Art und Tragweite der Situation arbeiten die zuständigen Ministerien, Verwaltungsbehörden und Regierungsstellen zusammen, um die festgelegten Ziele im Einklang mit den Zuständigkeiten der beteiligten Akteure zu erreichen.

2. Nationaler und europäischer Rahmen

Der Plan ist Teil des nationalen Krisenmanagementsystems, das vom Hochkommissariat für nationale Sicherheit (HCPN) koordiniert wird, und steht im Einklang mit den europäischen Rahmenwerken für Cybersicherheit und Krisenmanagement, insbesondere:

- › Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, bekannt als NIS-2-Richtlinie;
- › Die Empfehlung des Rates vom 6. Juni 2025 zu einem EU-Konzept für das Krisenmanagement im Bereich der Cybersicherheit („Cyber Blueprint“);
- › Europäische Mechanismen für die Zusammenarbeit und Koordinierung in Krisenfällen, wie die integrierte EU-Regelung für die politische Reaktion auf Krisen (IPCR) und das Europäische Netzwerk der Verbindungsorganisationen für Cyberkrisen (EU-CyCLONe) für die operative Ebene.

Diese Positionierung gewährleistet die Kohärenz zwischen der Reaktion Luxemburgs und den europäischen Ansätzen, insbesondere wenn Cyberkrisen über die nationalen Grenzen hinausgehen.

3. Schlüsselbegriffe

3.1. Nationale Klassifizierung von Cybersicherheitsvorfällen

Um eine schnelle, angemessene und koordinierte Reaktion zu gewährleisten, unterscheidet der nationale Rahmen zwischen:

- › **Grenzüberschreitender Cybersicherheitsvorfall großen Ausmaßes:** Sicherheitsvorfall, der eine Störung verursacht, deren Ausmaß die Reaktionsfähigkeit Luxemburgs übersteigt, oder der beträchtliche Auswirkungen auf mindestens einen anderen Mitglied- oder einen Drittstaat hat;
- › **Nationaler Cybersicherheitsvorfall großen Ausmaßes:** Sicherheitsvorfall, der eine Störung verursacht, die eine Gefahr für die lebenswichtigen Interessen oder die Grundbedürfnisse des gesamten Landes oder eines Teils davon oder der Bevölkerung darstellt und dringende Entscheidungen und Koordinierungsmaßnahmen erfordert;
- › **Erheblicher Sicherheitsvorfall:** ein Sicherheitsvorfall, der
 - schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann;
 - andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann;
- › **Sicherheitsvorfall:** ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigt.

Diese Klassifizierung wird verwendet, um das Ausmaß des Vorfalls zu bewerten und die Art der Zusammenarbeit und den Grad der Mobilisierung der beteiligten Akteure anzupassen.

3.2. Klassifizierung von Cyberbedrohungen

Der Plan unterscheidet zwischen mehreren Stufen von Cyberbedrohungen, basierend auf ihren potenziellen Auswirkungen, ihrem Umfang und der Art der anvisierten Ziele, um geeignete und vorbeugende Wachsamkeits- und Kooperationsmaßnahmen festzulegen.

4. Formen der Zusammenarbeit

Der Regierungsplan zum Umgang mit Cyber- und digitalen Krisen basiert auf drei sich ergänzenden Formen der Zusammenarbeit.

4.1. Modus „Permanent“

Außerhalb von Krisensituationen wird der Plan im permanenten Modus umgesetzt. Dieser Modus dient der Vorbereitung und umfasst:

- › die kontinuierliche Überwachung der Cyberbedrohungslage und der systemischen Risiken;
- › die Anpassung und Aktualisierung von Krisenplänen und -verfahren;
- › die regelmäßige Durchführung von Übungen und Tests.

4.2. Modus „Alarm/CERC“

Wenn ein Ereignis ein erhebliches Schadensrisiko darstellt, ohne jedoch eine tatsächliche Krise auszulösen, erfolgt die Koordination im Modus „Alarm/CERC“. Dieser Modus zielt darauf ab, eine erhöhte Wachsamkeit zu gewährleisten, einen schnellen und gezielten Informationsaustausch zwischen den relevanten Akteuren zu ermöglichen und frühzeitige Maßnahmen zur Schadensbegrenzung zu ergreifen, um eine Eskalation zu einer Krisensituation zu verhindern.

4.3. Krisenmodus

Wenn ein Cyber- oder Digitalsicherheitsvorfall lebenswichtige Interessen oder Grundbedürfnisse bedroht, wird der „Krisenmodus“ aktiviert, um ein koordiniertes und effizientes nationales Management zu gewährleisten.

Dieser Modus ermöglicht die Aktivierung geplanter Reaktionsmechanismen, die Strukturierung des für das Verständnis und die Überwachung des Ereignisses erforderlichen Informationsaustauschs und die Koordinierung von Cyber-Reaktionsmaßnahmen mit anderen Krisenmanagement-Plänen, sei es auf sektoraler, nationaler oder internationaler Ebene.

5. Krisenmanagementgremien

5.1. Bewertungsstelle für Cyberbedrohung (CERC)

Die Bewertungsstelle für Cyberbedrohung (*Cellule d'Évaluation du Risque Cyber, CERC*) ist für die Analyse, Bewertung und Nachverfolgung von Cybersicherheitsvorfällen und Cyberbedrohungen zuständig. Sie sorgt für eine verstärkte Wachsamkeit, bewertet die Schwere und die potenziellen Auswirkungen von Ereignissen und gibt bei Bedarf Empfehlungen ab oder vereinbart Maßnahmen, insbesondere im Hinblick auf einen Übergang in den Krisenmodus.

5.2. Krisenstab (CC)

Im Krisenmodus wird die Führung des Krisenmanagements an die Art und das Ausmaß des Ereignisses angepasst. Der Krisenstab (*Cellule de Crise, CC*) wird vom Premierminister im Falle einer drohenden oder tatsächlichen Krise aktiviert. Er initiiert, koordiniert und beaufsichtigt die Ausführung aller Maßnahmen, die zur Bewältigung der Krise und ihrer Auswirkungen sowie zur Wiederherstellung des Normalzustandes dienen. Er bereitet die notwendigen Entscheidungen vor, die der Regierung zur Genehmigung vorgelegt werden. Im Falle eines operativen Einsatzes vor Ort erweitert sich seine Aufgabe auf die Koordinierung und Kontrolle der Ausführung dieses Einsatzes.

Der Krisenstab setzt sich mindestens aus folgenden Akteuren zusammen:

1. dem Hochkommissar für nationale Sicherheit;
2. dem Generalsekretär der Regierung;
3. dem Generaldirektor der großherzoglichen Polizei;
4. dem Generalstabschef der luxemburgischen Armee;
5. dem Direktor des Staatlichen Nachrichtendienstes (*Service de renseignement de l'État*);
6. dem Direktor des Zentrums für Informationstechnologien des Staates (*Centre des technologies de l'information de l'État*);
7. dem Direktor der ministeriellen Abteilung für Medien, Konnektivität und digitale Politik (*Service des medias, de la connectivité et de la politique numérique*);
8. dem Direktor der Luxemburgischen Regulierungsbehörde (*Institut luxembourgeois de régulation*);
9. einem Vertreter des Wirtschaftsministeriums;
10. einem Vertreter des Ministeriums für Digitalisierung.

Der Krisenstab ist während der gesamten Dauer der Krise bis zur Wiederherstellung des Normalzustandes tätig.

Entsprechend der Umstände und der zu behandelnden Angelegenheiten kann der Krisenstab um Vertreter anderer öffentlicher Einrichtungen erweitert werden, beispielsweise der Finanzaufsichtsbehörde (*Commission de Surveillance du Secteur Financier, CSSF*), der Luxemburger Behörde für Normung, Akkreditierung, Sicherheit und Qualität von Produkten und Dienstleistungen (*Institut luxembourgeois de la normalisation, de l'accréditation, de la sécurité et qualité des produits et services*), der Zivilluftfahrtbehörde (*Direction de l'aviation civile*), der im Falle einer sektorübergreifenden Cyberkrise betroffenen Ministerien und Gemeinden sowie Vertretern der Betreiber/Eigentümer kritischer Infrastrukturen.

Die Mitglieder, welche nicht am Krisenstab teilnehmen können, müssen sich vertreten lassen.

Der Krisenstab verfolgt den Entwicklungsverlauf auf der Grundlage von Informationen, die von der Cyber-Einsatzzentrale (PCO-C) zusammengestellt werden.

5.3. Cyber-Einsatzzentrale (PCO-C)

Der Krisenstab kann die Cyber-Einsatzzentrale (*Cellule Opérationnelle Cyber, PCO-C*) mit der Ausführung, Umsetzung und Beaufsichtigung der vereinbarten Maßnahmen und Handlungen beauftragen. Im Krisenmodus übernimmt die Cyber-Einsatzzentrale die Rolle der Bewertungsstelle für Cyberbedrohung (CERC) und ist zusätzlich mit der Koordinierung, sowie der operativen Umsetzung der vereinbarten Maßnahmen beauftragt. Sie fungiert als Bindeglied zwischen der strategischen und der technischen Ebene.

5.4. Stelle für Kommunikation und Information (CCI)

Die Stelle für Kommunikation und Information (*Cellule Communication et Information, CCI*) ist für die Kommunikation und Information gegenüber den Medien und Bürgern zuständig. Sie ist für die öffentliche und institutionelle Kommunikation verantwortlich und sorgt für eine klare, kohärente und koordinierte Information gegenüber den Bürgern, den Medien und allen Beteiligten.

Die externe Kommunikation wird von der Abteilung für Krisenkommunikation des HCPN (*Département Communication de crise*) organisiert und horizontal koordiniert, insbesondere um Fehlinformationen vorzubeugen und die Kohärenz der verbreiteten Nachrichten zu gewährleisten.

Die Stelle für Kommunikation und Information (CCI) wird grundsätzlich zeitgleich mit dem Krisenstab einberufen. Was die darin vertretenen Stellen betrifft, so spiegelt die

Zusammensetzung der CCI so weit wie möglich die Zusammensetzung des Krisenstabs wider. Die CCI informiert die Öffentlichkeit regelmäßig über den Vorfall und seinen Verlauf sowie über die von den nationalen Behörden ergriffenen Maßnahmen.

Offizielle Informationen werden über die institutionellen Kanäle der Regierung verbreitet, insbesondere über das Portal www.infocrise.lu. Je nach Art, Schwere und Dringlichkeit der Situation kann die Regierung den Einsatz des nationalen Warn- und Informationssystems LU-Alert beschließen, welches eine schnelle und zielgerichtete Verbreitung wichtiger Informationen ermöglicht. Aktuelle Warnmeldungen werden über die Website www.lu-alert.lu, die **mobile Anwendung „LU-Alert“** und gegebenenfalls über geolokalisierte SMS- und Cell-Broadcast-Nachrichten übermittelt.

6. Maßnahmen des Krisenmanagements

Der Plan bestimmt Maßnahmen im Krisenmanagement, die eine angemessene und flexible Reaktion auf Cyber- oder digitale Ereignisse ermöglichen, mit dem Ziel, die lebenswichtigen Interessen des Landes, seiner Bürger und kritischer Wirtschaftssektoren zu schützen.

6.1. Bewertung

Die Bewertung ist der erste Schritt im Krisenmanagementzyklus. Sie dient dazu, die Dringlichkeit des Ereignisses, sein Ausmaß und seine tatsächlichen oder potenziellen Auswirkungen auf die lebenswichtigen Interessen oder Grundbedürfnisse des gesamten Landes oder eines Teils davon oder seiner Bevölkerung zu beurteilen.

6.2. Verstärkte Wachsamkeit

Die verstärkte Wachsamkeit umfasst Maßnahmen, die bei einer Situation mit erhöhtem Risiko ergriffen werden, insbesondere die Analyse der verfügbaren Informationen und die kontinuierliche Bewertung des Situationsverlaufs.

6.3. Systemaufrüstung und -schutz

Diese Maßnahme zielt darauf ab, das Risiko der Ausnutzung technischer Schwachstellen zu begrenzen, und kann auf Empfehlung der PCO-C und nach Entscheidung des Krisenstabs zur Umsetzung geeigneter Schutz- oder Begrenzungsmaßnahmen führen.

6.4. Wiederherstellung der Dienste

Die Wiederherstellung der Dienste ermöglicht die schrittweise Wiederaufnahme der betroffenen Aktivitäten gemäß festgelegten Prioritäten, bis eine normale und stabile Situation wiederhergestellt ist.

7. Internationale Zusammenarbeit und Unterstützung

Da eine Cyberkrise internationale Ausmaße annehmen kann, ist die Zusammenarbeit mit ausländischen Partnern von entscheidender Bedeutung. Internationale Unterstützung kann insbesondere im Rahmen von Kooperationsvereinbarungen mit ausländischen Incident-Response-Teams sowie innerhalb europäischer und internationaler Organisationen und Kooperationsnetzwerken angefordert werden.

8. Information an die Öffentlichkeit

Die Benachrichtigung der Öffentlichkeit ist ein zentraler Bestandteil des Krisenmanagements. Die Regierung informiert regelmäßig und koordiniert über die Entwicklung der Lage, mögliche Auswirkungen und die zu befolgenden Anweisungen.

Offizielle Informationen werden über die institutionellen Kanäle der Regierung verbreitet, darunter das Portal „www.infocrise.lu“. Je nach Art, Schwere und Dringlichkeit der Situation kann die Regierung das nationale Warn- und Informationssystem LU-Alert nutzen, welches eine schnelle und zielgerichtete Verbreitung wichtiger Informationen ermöglicht.

Ergänzend dazu können alle anderen als geeignet erachteten Kommunikationskanäle genutzt werden, um eine breite, schnelle und zugängliche Übermittlung der Nachrichten an möglichst viele Bürger zu gewährleisten.