27. Oktober 2025 | Bundesamt für Cybersicherheit BACS

Prozesse des Bundes zur koordinierten Cybervorfallbewältigung

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Bundesamt für Cybersicherheit BACS

Inhalt

1 Ausgangslage ... 3

2 Kernprozesse der koordinierten Cybervorfallbewältigung ... 3

3 Einstufung von Cybervorfällen ... 5

4 Prozesse des Bundes bei der koordinierten Vorfallbewältigung ... 6

4.1 Prozesse bei Cybervorfällen der Kategorie «gering» 6

4.2 Prozesse bei Cybervorfällen der Kategorie «moderat» 6

4.3 Prozesse bei Cybervorfällen der Kategorie «erheblich» 7

4.4 Prozesse bei Cybervorfällen der Kategorie «kritisch» 8

5 Umsetzung des Konzepts ... 8

.

1 Ausgangslage

Mit dem Bundesratsbeschluss vom 1. Mai 2024 (EXE 2024.0416) wurde das Departement für Verteidigung, Bevölkerungsschutz und Sport VBS (BACS; SEPOS) beauftragt, aufzuzeigen, wie die Koordination der Bewältigung von Cybervorfällen zwischen Bund, Kantonen und Lieferanten konkret abläuft und nach welchen Kriterien das Ausmass von Cyberangriffen beurteilt werden soll.

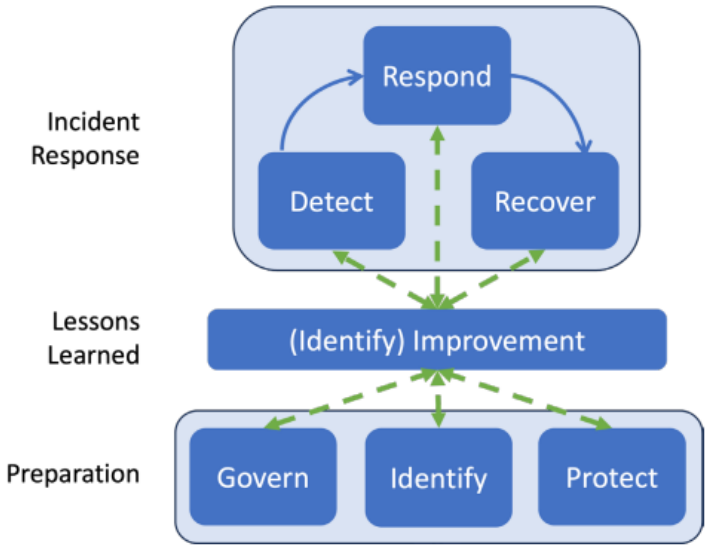
Der Auftrag ist Bestandteil der Massnahmen zum weiteren Vorgehen im Nachgang des Cyberangriffs auf die Firma Xplain AG, welcher zu einem Abfluss von sensitiven Daten von Bund und Kantonen geführt hat. Für die Bewältigung dieses Vorfalls hatte der Bundesrat einen politisch-strategischen Krisenstab «Datenabfluss» eingesetzt, welcher mit dem Beschluss vom 1. Mai 2024 aufgelöst wurde. Es wurde festgestellt, dass Unklarheit herrscht, bei welchen Cybervorfällen künftig ein politisch-strategischer Krisenstab eingesetzt werden soll und wie die Kantone und allfällige weitere Akteure eingebunden werden sollen.

Mit dem Inkrafttreten des Informationssicherheitsgesetzes (ISG; SR 128) im Jahr 2024, der Cybersicherheitsverordnung (CSV; SR 128.51) im Jahr 2025 und der Verordnung über die Krisenorganisation der Bundesverwaltung (KOBV; SR 172.010.8) im Jahr 2025 sind die gesetzlichen Grundlagen für die Koordination der Bewältigung von Cybervorfällen gegeben. Dieses Dokument zeigt auf, wie Cybervorfälle nach Schweregrad eingestuft werden und welche Koordinationsmechanismen von welcher Organisation pro Schweregrad angewendet werden. Weiter gibt das Dokument Empfehlungen ab, nach welchen Schweregraden eines Cybervorfalls ein politisch-strategischer Krisenstab eingesetzt werden sollte.

2 Kernprozesse der koordinierten Cybervorfallbewältigung

Cybervorfälle sind in Artikel 5 des ISG definiert als «Ereignis bei der Nutzung von Informatikmitteln, das dazu führt, dass die Vertraulichkeit, Verfügbarkeit oder Integrität von Informationen oder die Nachvollziehbarkeit ihrer Bearbeitung beeinträchtigt ist». Ein Cyberangriff liegt dann vor, wenn ein Cybervorfall absichtlich ausgelöst wurde. Dazu gehören das unbefugte Eindringen in Computersysteme durch den Einsatz von Schadsoftware oder durch das Ausnützen von Schwachstellen, aber auch Angriffe auf die Verfügbarkeit von Dienstleistungen durch Überlastungsangriffe.

Tritt ein Cybervorfall ein, werden Gegenmassnahmen notwendig. Diese werden allgemein als Vorfallbewältigung (oder englisch «Incident Response») bezeichnet. Das National Institute of Standards and Technology (NIST) hat die für die Vorfallbewältigung grundlegenden Prozesse in seinem «Incident Response Life Cycle Model» zusammengefasst (siehe Grafik 1).



Grafik 1: *Kernprozess Vorfallbewältigung (A.Nelson and al. (2025), NIST Special Publication 800).*

Die Kernprozesse für die operative Bewältigung von Cybervorfällen basieren auf der Erkennung von Cybervorfällen («Detect»), auf der Reaktion («Respond») und auf der Wiederherstellung («Recover»). In der Erkennungsphase werden mögliche Cybervorfälle möglichst frühzeitig entdeckt und es wird analysiert, welchen Ursprung der Vorfall hat, welche Akteure aus welchen Motiven den Cybervorfall verursacht haben und welche technischen Eigenschaften der Vorfall (z. B. die verwendete Schadsoftware) aufweist. Im zweiten Schritt (Reaktion) werden Gegenmassnahmen ergriffen, um den Cybervorfall zu stoppen oder zumindest sein Schadensausmass zu minimieren. In der Wiederherstellungsphase geht es schliesslich darum, eingetretenen Schaden zu beheben sowie betroffene Daten und Systeme wieder in funktionsfähigen Zustand zu versetzen.

Diese Prozesse werden bei jeder Vorfallbewältigung durchgeführt, wobei das Ausmass ihrer Umsetzung stark von der Art des Vorfalls und seinen Auswirkungen abhängt. Meist können diese Schritte aber direkt vom zuständigen Sicherheitsteam in kurzer Zeit umgesetzt werden, welche dann auch die weiteren Prozesse zur Verbesserung des Schutzes der Organisation vor künftigen Vorfällen («Lessons Learned» und «Preparation») initiieren.

Mit der zunehmenden digitalen Vernetzung geschieht es aber immer häufiger, dass Cybervorfälle über die Grenzen einer Organisation hinausgehen. Cybervorfälle können beispielsweise Systeme betreffen, welche von Dritten betrieben werden oder bei welchen Schnittstellen und Abhängigkeiten zu Dritten bestehen. Zudem wirken sich durch Cybervorfälle verursachte Funktionsstörungen oft rasch auf Dritte aus. Letztendlich ist es auch häufig der Fall, dass Unternehmen den Betrieb ihrer Sicherheitsteams an sogenannte «Managed Security Service Providers» auslagern. Die Zuständigkeit liegt dadurch bei mindestens zwei Akteuren. Diese müssen sich untereinander koordinieren oder koordiniert werden. Je nach Betroffenheit und Auswirkungen übernimmt diese Aufgabe die Organisation, bei der der Cybervorfall eingetreten ist, eine Organisation, auf die sich der Vorfall auswirkt, ein Cybersicherheitsunternehmen im Auftrag einer der vorgenannten Organisationen oder eine zuständige Stelle des Bundes gemäss Kapitel 4.

Wenn mehrere Akteure direkt in die Vorfallbewältigung involviert sind, ist eine sorgfältige gegenseitige Abstimmung – eine koordinierte Cybervorfallbewältigung – von zentraler Bedeutung. Diese koordinierte Cybervorfallbewältigung funktioniert nur dann, wenn möglichst rasch klar wird, welche Prozesse wie und durch wen umgesetzt werden. Eine nachvollziehbare und transparente Einstufung von Cybervorfällen ist deshalb essenziell für eine effiziente Vorfallbewältigung.

Dies gilt umso stärker für eine Vorfallbewältigung, bei welcher die Bundesverwaltung aufgrund von betroffenen öffentlichen Interessen einbezogen wird. Gestützt auf Artikel 73a ISG führt das Bundesamt für Cybersicherheit (BACS) technische Analysen zur Bewertung und Abwehr von Cybervorfällen und Cyberbedrohungen durch und unterstützt kritische Infrastrukturen bei deren Bewältigung. Das BACS übernimmt damit in solchen Fällen eine Schlüsselrolle bei der koordinierten Vorfallbewältigung. Der Gesetzgeber hat diese Rolle aber gleichzeitig eingeschränkt. Das BACS unterstützt subsidiär und übernimmt keine Aufgaben, welche in angemessener Zeit von privaten Anbietern durchgeführt werden können (Art. 74 Abs. 3 ISG). Für das Zusammenspiel zwischen den Akteuren aus Privatwirtschaft, Kantonen und Bund in der koordinierten Cybervorfallbewältigung ist es daher entscheidend, klar zu definieren, welche Rolle der Bund bei welcher Art von Vorfällen übernimmt.

3 Einstufung von Cybervorfällen

Die nachvollziehbare und transparente Einstufung von Cybervorfällen dient der zielgerichteten Rollenverteilung während eines Vorfalls. Zugleich ist wichtig zu betonen, dass die Einstufungen von Cybervorfällen niemals allgemeingültig sein können und sich oft im Verlauf der Vorfallbewältigung ändern. Jede Organisation bewertet den Vorfall aus ihrer subjektiven Perspektive, und es kommt oft vor, dass die anfängliche Einstufung im Laufe der Entwicklung dynamisch angepasst werden muss. Diese Subjektivität und Dynamik stellen eine Herausforderung für die koordinierte Vorfallbewältigung dar, der mit sorgfältiger und kontinuierlicher Kommunikation zwischen allen beteiligten Akteuren begegnet werden muss. Die Einstufung selbst ist hingegen nicht komplex. Sie basiert auf den beiden folgenden, sich gegenseitig beeinflussenden Faktoren:

- Betroffenheit: Welche Systeme und Organisationen sind vom Cybervorfall direkt oder indirekt betroffen?
- Auswirkungen: Welche Auswirkungen sind durch den Cybervorfall bereits eingetreten und mit welchen weiteren Auswirkungen ist zu rechnen?

Für eine einzelne Organisation sind diese zwei Dimensionen im Normalfall rasch beurteilbar. Viele Sicherheitsteams wenden intuitiv Kriterien zur Beurteilung dieser zwei Dimensionen an und entscheiden in kurzer Zeit, mit welchen Strukturen sie den Vorfall bewältigen.

Bei der koordinierten Vorfallbewältigung mit mehreren betroffenen Organisationen ist es wichtig, dass alle beteiligten Akteure verstehen, wie der Vorfall von ihren Partnern eingestuft wird. Selbst wenn ein Vorfall in einer einzelnen Organisation viele Systeme betrifft und Auswirkungen auf andere Organisationen hat, kann die Einstufung durch die beteiligten Organisationen unterschiedlich ausfallen. Eine Verschlüsselung von Systemen durch einen Ransomware-Angriff ist für eine einzelne Organisation beispielsweise oft ein Vorfall, der unmittelbare Handlungen erfordert, während er für Dritte (insbesondere auch für den Bund bezüglich Wahrung des öffentlichen Interesses) nur selten unmittelbare Handlungen nötig macht.

Für den Bund gilt es, die Betroffenheit und die Auswirkungen jeweils aus einer gesamtgesellschaftlichen Perspektive zu beurteilen. Das BACS stuft Vorfälle danach ein, ob in der Schweiz viele Organisationen betroffen sind und ob ein Vorfall Auswirkungen auf das Funktionieren der Wirtschaft oder auf das Wohlergehen der Bevölkerung hat. Es orientiert sich in seiner koordinierenden Rolle für die Cybervorfallbewältigung an einem vierstufigen Modell, welches zwischen geringen, moderaten, erheblichen und kritischen Cybervorfällen unterscheidet. Dieses Modell soll gewährleisten, dass die koordinierte Vorfallbewältigung nach der immer gleichen Praxis umgesetzt wird und die rechtlichen Bedingungen jederzeit eingehalten werden.

Schwere-grad	Betroffenheit	Auswirkungen
Gering	Einzelpersonen oder Organisationen, die nicht zu den kritischen Infrastrukturen zählen	Der Cybervorfall löst keine Beeinträchtigungen von Funktionen aus oder diese haben nur geringe Auswirkungen auf das Funktionieren der Wirtschaft oder das Wohlergehen der Bevölkerung.
Moderat	Eine kritische Infrastruktur	Beim Cybervorfall handelt es sich um einen meldepflichtigen Cyberangriff nach Art. 74*d*.
Erheblich	Mehrere kritische Infrastrukturen	
Kritisch	Erhebliche Anzahl von Unternehmen / Kritische Teilsektoren	Schwerwiegende Auswirkungen auf das Funktionieren der Wirtschaft oder das Wohlergehen der Bevölkerung.

Tabelle 1: *Übersicht Einstufung von Cybervorfällen.*

4 Prozesse des Bundes bei der koordinierten Vorfallbewältigung

Basierend auf der Einstufung des Cybervorfalls erfolgt die Wahl eines passenden Prozesses zur koordinierten Vorfallbewältigung. In diesem Kapitel wird dargestellt, welche Prozesse bei welcher Kategorie durch das BACS in seiner koordinierenden Rolle für die Vorfallbewältigung angewendet werden. Wichtig ist erneut festzuhalten, dass sich die Einstufung eines Vorfalles dynamisch ändern kann und somit auch die Prozesse entsprechend angepasst werden.

4.1 Prozesse bei Cybervorfällen der Kategorie «gering»

Cybervorfälle der Kategorie «gering» können dem BACS freiwillig gemeldet werden (Art. 73b Abs.1 ISG). Das BACS nimmt die Meldung entgegen und gibt auf Antrag eine Empfehlung zum weiteren Vorgehen ab, sofern dafür keine weiteren Analysen und Abklärungen erforderlich sind (Art. 73b Abs.12 ISG). Die Verantwortung für die Vorfallbewältigung liegt in solchen Fällen bei der betroffenen Organisation oder Person. Der Bund übernimmt keine koordinierende Rolle.

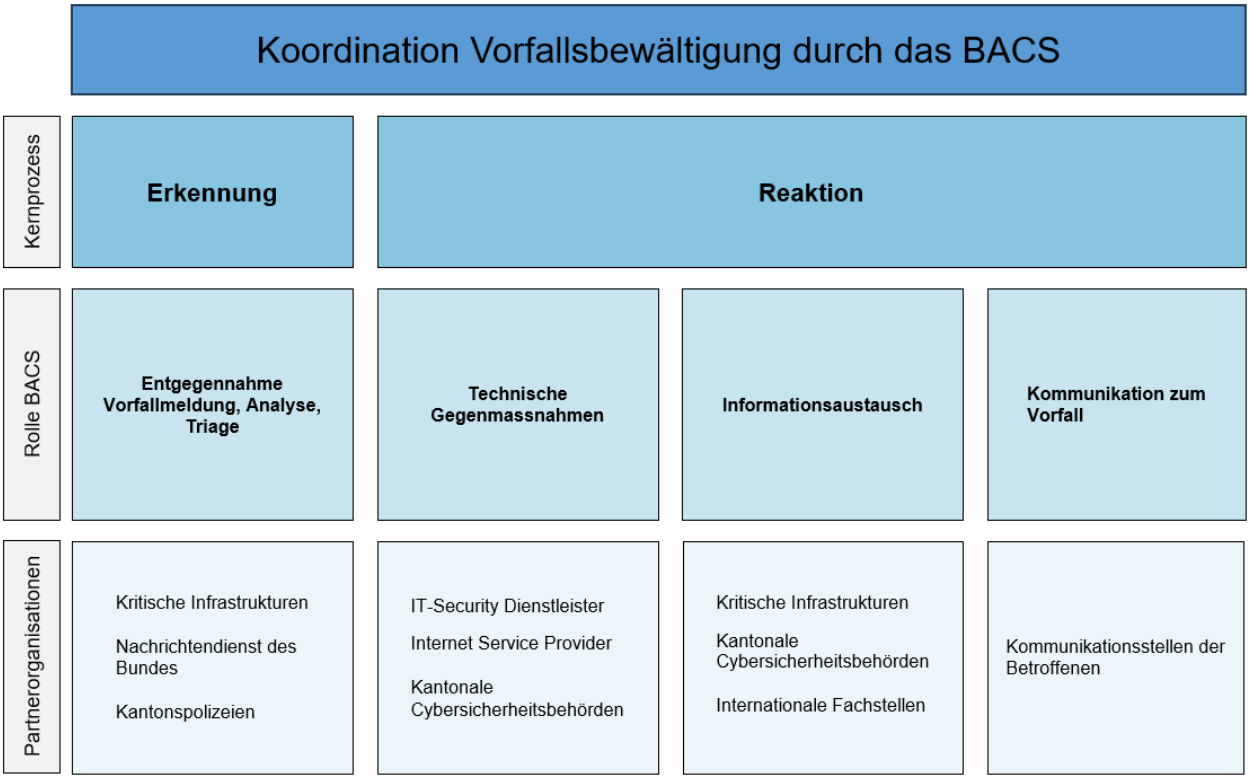
4.2 Prozesse bei Cybervorfällen der Kategorie «moderat»

Cyberangriffe auf Betreiberinnen kritischer Infrastrukturen sind seit dem 1. April 2025 gemäss Art. 74a ISG meldepflichtig. Der Bund – konkret das BACS – ist im Gegenzug dazu verpflichtet, die Betroffenen bei der Vorfallbewältigung zu unterstützen, sofern die Beschaffung von Unterstützung auf dem Markt nicht rechtzeitig möglich ist (Art. 74a Abs. 3 ISG). Das BACS betreibt zu diesem Zweck das Government Computer Emergency Response Team (GovCERT), welches die erste Hilfe zur Vorfallbewältigung direkt mit den betroffenen Unternehmen koordiniert. Bei Cybervorfällen in der Bundesverwaltung kann das BACS gestützt auf Artikel 12 Absatz 3 der Informationssicherheitsverordnung (ISV; SR 128.1) zudem über seine generell subsidiäre Rolle hinaus die betroffenen Verwaltungseinheiten bei Bedarf direkt unterstützen und beraten.

Stellt sich heraus, dass mehrere Organisationen der Schweiz gleichzeitig von einem Cybervorfall betroffen sind oder die Bewältigung nicht mit bekannten Methoden innert nützlicher Frist möglich ist, fokussiert sich das BACS auf die Sicherstellung des Informationsflusses zwischen allen beteiligten Organisationen. Hierfür nutzt es die Informationsplattform Cyber Security Hub (CSH), auf der es Warnungen, Einschätzungen und Empfehlungen veröffentlicht, den Betroffenen eine Plattform zum gegenseitigen Austausch bietet und so zur koordinierten Vorfallbewältigung beiträgt.

4.3 Prozesse bei Cybervorfällen der Kategorie «erheblich»

Ab der Stufe «erheblich» übernimmt das BACS in erster Instanz eine zentralere Rolle bei der Koordination der Vorfallbewältigung. Betrifft der Cybervorfall die Bundesverwaltung ist das Staatssekretariat für Sicherheitspolitik (SEPOS) federführend für die Vorfallbewältigung. Es kann die Federführung für die Bewältigung des Vorfalls an das BACS übertragen (Art. 12 Abs. 7 ISV). Betrifft der Vorfall mehrere Betreiberinnen kritischer Infrastrukturen, oder hat er erhebliche Auswirkungen (z. B. Funktionsstörungen) oder dauert an, ohne dass erfolgreiche Gegenmassnahmen ergriffen werden können, so ist die fachliche Unterstützung und Koordination durch das BACS wichtig. Die konkrete Umsetzung dieser koordinativen und unterstützenden Arbeiten und der Einbezug von Partnerorganisationen sind schematisch in Grafik 2 abgebildet. Darin ist ersichtlich, dass sich die Unterstützung des BACS auf die Kernprozesse der Erkennung und der Reaktion beschränkt. Die Wiederherstellung der Funktionsfähigkeit der Systeme («Recovery») bleibt vollumfänglich in der Verantwortung der betroffenen Organisationen.



Grafik 2: *Koordination Vorfallbewältigung durch das BACS.*

4.4 Prozesse bei Cybervorfällen der Kategorie «kritisch»

Bei Vorfällen der Stufe «kritisch» handelt es sich um Cybervorfälle, welche entweder schon zu einer Krise geführt haben oder das Potenzial haben, eine Krise auszulösen. Da solche Cybervorfälle eine unmittelbare und schwere Gefahr für Staat, Gesellschaft und Wirtschaft darstellen, setzt der Bundesrat für die Bewältigung des Vorfalls und die Minderung der Auswirkungen einen Krisenstab ein. Die Einsetzung und Koordination eines Krisenstabes wird durch die Verordnung vom 20. Dezember 2024 über die Krisenorganisation der Bundesverwaltung (KOBV) geregelt. Die Ausgestaltung, insbesondere auch die Frage, welches Departement die Federführung übernimmt, hängt davon ab, welche kritischen Sektoren vom Cybervorfall betroffen sind. Wenn es zu schwerwiegenden Ausfällen bei kritischen Sektoren kommt, steht die Bewältigung dieser Situation im Fokus. Für die Bewältigung des Cybervorfalls können grundsätzlich die gleichen Prozesse wie bei Cybervorfällen der Kategorie «erheblich» genutzt werden. Der politisch-strategische Krisenstab kann aber nötigenfalls zusätzlich mittels politisch-strategischer Vorgaben die operative Krisen- bzw. Vorfallbewältigung steuern (Art. 5 Abs. 3 Bst. b KOBV).

5 Umsetzung des Konzepts

Das in diesem Konzept beschriebene Vorgehen des BACS bei der koordinierten Vorfallbewältigung basiert auf den bestehenden rechtlichen Grundlagen. Diese wurden in den letzten Monaten mit der Verabschiedung der KOBV und der Inkraftsetzung der Änderung des ISG vom 29. September 2023 zur Einführung einer Meldepflicht für Cyberangriffe bei kritischen Infrastrukturen per 1. April 2025 mit entscheidenden Elementen ergänzt.

Da die Prozesse der koordinierten Vorfallbewältigung bereits gelebte Praxis sind, besteht kein unmittelbarer Handlungsbedarf zur Stärkung der Umsetzung z. B. durch die Schaffung neuer gesetzlicher Grundlagen. Es ist allerdings wichtig, dass die Einstufung der Cybervorfälle und die entsprechenden Vorfallbewältigungsprozesse klarer kommuniziert werden. Die koordinierte Vorfallbewältigung funktioniert nur, wenn allen Partnern von Anfang an die Zuständigkeiten und die erwartbare Unterstützung klar sind.

Das BACS wird die Prozesse der koordinierten Vorfallbewältigung und die Einstufung der Cybervorfälle deshalb weiterhin eng mit den Kantonen und den Betreiberinnen kritischer Infrastrukturen abstimmen und seine Aufgaben und Zuständigkeiten transparent kommunizieren.