Beispiel einer Vorfallsmeldung

Beispielsachverhalt: Nach erfolgreichem Phishing-Angriff wurde der Account missbraucht, um SPAM an Dritte zu versenden. Das KIM hat daraufhin den Account gesperrt.

An welcher Stelle in der Universität ist der Vorfall passiert?	Lehrstuhl Glücksforschung.
Was ist vorgefallen? (primäre Auswirkungen)	• Offenlegung / unbefugte Kenntnisnahme von schützenswerten Daten • nicht autorisierte Verwendung von IT-Ressourcen
Sind personenbezogene Daten von dem Vorfall betroffen?	Ja
Welche Kategorien von personenbezogenen Daten sind betroffen?	E-Mail-Kommunikation (Posteingang und -ausgang), darunter auch privater Natur sowie Listen von Teilnehmern der Glücksforschungskonferenzen 2018 und 2019 (Name, Einrichtung, Anmeldedatum, E-Mail-Adresse).
Welche Kategorien von Personen sind betroffen?	Studierende, Mitarbeiter, Externe.
Die Daten wie vieler Personen sind betroffen?	Sehr hohe Anzahl an E-Mail-Korrespondenten; 110 Konferenzteilnehmer im Jahr 2018, bisher 64 für 2019.
Welche Folgen der Verletzung des Schutzes der personenbezogener Daten halten Sie für wahrscheinlich?	Keine Angabe möglich.
Sind sonstige, schützenswerte Daten von dem Vorfall betroffen?	Ja
Welche Kategorien von sonstigen schützenswerten Daten sind in welchem Umfang betroffen?	Entwürfe der Förderungsanträge für das Forschungsprojekt "HappyLife".
Welche Folgen halten Sie für wahrscheinlich?	Keine ernsthaften Folgen für die weitere Forschung erwartet.
Sind negative Auswirkungen auf Arbeitsabläufe / Fachaufgaben eingetreten oder zu erwarten?	Ja
Erläuterungen (Auswirkungen auf Arbeitsabläufe / Fachaufgaben)	Durch Sperrung des Kontos war vorübergehend von diesem kein Zugriff auf die Universitätsdienste möglich.
Sind in Bezug auf das Ansehen der Universität in der Öffentlichkeit negative Auswirkungen zu erwarten?	Ja

Erläuterungen (Reputationsschäden)	Nur, wenn diese Daten abgegriffen wurden und dies bekannt wird.
Erläuterungen (Vorfall und Auswirkungen)	Ein Angreifer hat meine Uni-Konto-Zugangsdaten erlangt und mit diesen über den E-Mail-Server der Universität Spam-E-Mails an Dritte verschickt. Es gibt keinen Anhaltspunkt, dass diese Zugangsdaten für einen anderen Zweck missbraucht wurden (Einsicht in das Postfach oder Kopie desselben, Zugriff auf den persönlichen Nextcloud-Datenspeicher etc.), dies kann aber derzeit nicht ausgeschlossen werden.
Wann ist der Vorfall eingetreten?	Zwischen 01.04.2019 und 02.04.2019.
Was waren (vermutete) Ursachen und/oder begünstigende Umstände?	• Fahrlässigkeit / Sorgfaltspflichtverletzung (z.B. versehentliches Löschen, Anstecken eines gefundenen USB-Sticks) • Identitätsmissbrauch, Social Engineering (z.B. Phishing, E-Mail-Absenderfälschung)
Erläuterungen (Ursachen und Einflüsse)	Die Zugangsdaten wurden vermutlich über ein Phishing-Angriff abgegriffen.
Wie haben Sie Kenntnis von dem Vorfall erlangt?	Hinweis von Dritten
Erläuterungen (Kenntnisnahme)	Das KIM hat den Account gesperrt, sodass die Zugangsdaten nicht mehr funktionierten.
Wann haben Sie Kenntnis von dem Vorfall erlangt?	02.04.2019, ca. 16:00.
Welche Gegenmaßnahmen wurden bereits eingeleitet, um die Schadensauswirkungen zu begrenzen bzw. zu beheben?	Zugangspasswort wurde zurückgesetzt. Alle Nutzereinstellungen in SOGo wurden überprüft.
Sind die Schadensauswirkungen damit so weit wie möglich eingegrenzt oder vollständig behoben?	Ja
Welche Gegenmaßnahmen wurden bereits eingeleitet, damit sich der Vorfall nicht wiederholt (Ursachenbekämpfung)?	Ich habe mich über aktuelle Phishing-Methoden informiert und werde dies regelmäßig erneut tun.
Sind die identifizierten Ursachen damit vollständig behoben?	Ja
Name der meldenden Person	Max Mustermann
Ggf. Funktion der meldenden Person bei der verantwortlichen Stelle	Wissenschaftlicher Mitarbeiter
E-Mail-Adresse der meldenden Person	max.mustermann@uni-konstanz.de