Fragenkatalog Data Security

Created by Savini Marco, last modified on Mar 04, 2024

DSEC-1: Kategorisierung von Daten, Classification des données

Beschreibung

Datenstämme sind wie folgt kategorisiert:

- öffentlich
- intern
- vertraulich

Abhängig von der Kategorisierung gelten andere Prozesse.

Description

Les jeux de données sont classifiés :

- accessible à tout le monde
- interne
- confidentiel

En fonction de la classification, différents processus s'appliquent.

Frage

Wie werden Datenstämme in der Organisationseinheit kategorisiert.

Antwort	Punkte
Die Datenstämme sind nicht kategorisiert, weder innerhalb der Organisationseinheit noch stadtweit.	0
Es gibt eine organisationseinheit-interne Kategorisierung von Daten und die wichtigsten Datenstämme sind entsprechend klassifiziert. Die Klassifizierung selbst hat aber keinen oder wenig Einfluss auf den Alltag.	1
Es gibt eine stadtweite Kategorisierung von Datenstämmen und die wichtigsten Datensätze sind kategorisiert. Die Kategorisierung hat einen Einfluss auf die Datenflüsse und Zugriffsberechtigungen. Die Einflüsse sind nicht dokumentiert.	2
Alle Datenstämme sind kategorisiert. Die Regeln zur Handhabung von Datenstämmen der Kategorie vertraulich sind dokumentiert und werden angewandt.	3
Es gibt stadtweite Regeln zur Handhabung von Datenstämmen aller Kategorien, auch öffentlich und intern.	4
Die stadtweiten Regeln zur Handhabung von kategorisiert Datenstämmen wird regelmässig den Mitarbeiter kommuniziert. Z.B. in Form von obligatorischen eLearning Kursen.	5

Question

Comment les jeux de données sont-ils classifiés dans l'unité organisationnelle ?

Réponse	Points
Il n'y a pas de classification, ni interne ni à l'échelle de la ville.	0

Réponse	Points
Il existe une classification interne à l'unité organisationnelle des données et les principaux jeux de données sont classifiés en conséquence. Cependant, la classification elle-même a peu ou pas d'impact sur le quotidien.	1
Il existe une classification des jeux de données à l'échelle de la ville et les principaux ensembles de données sont classifiés. La classification influence les flux de données et les autorisations d'accès. Les impacts ne sont pas documentés.	2
La classification à l'échelle de la ville est appliquée à tous les jeux de données. Les règles de gestion des classifications critiques sont documentées et mises en œuvre.	3
Il existe des règles à l'échelle de la ville pour la gestion des jeux de données classifiés.	4
Les règles à l'échelle de la ville pour la gestion des jeux de données classifiés sont régulièrement communiquées aux employés, par exemple sous forme de cours d'eLearning obligatoires.	5

DSEC-2: Dokumentation von Herausgaben sensitiver Datenstämme, Documentation de la divulgation de jeux de données sensibles

Beschreibung

Auch sensitive Datenstämme können unter bestimmten Umständen (z.B. Einwohnerdaten zur Forschungszwecken) herausgegeben werden. Diese Flüsse müssen einem Prozess folgen und sind zu dokumentieren. Dabei fallen Prozessdaten an, wie z.B.

Feld	Typ	Beispiel
Konktaktaufnahme Datum	Datum	23/02/2021
Kontaktaufnahme Person	Text	Martolo, Sonia
Kontaktaufnahme Institution	Text	Universität Bern, Zahnmedizin
Zweck	Text	Studie “Oral health, oral health related quality of life and nutritional aspects in retired-age population in the canton of Bern”
Freigabe durch	Text	Hans Meier
Personenidentifizierende Daten	Ja/Nein	Ja
CISO informiert	Ja/Nein	Ja
Anzahl Datensätze	Zahl	10850
Status Anfrage	In Bearbeitung, Freigegeben, Abgelehnt	Freigegeben
Auslieferung Datum	Datum	13/11/2021
Quellsystem	Text	Innosolv

Spezielle Bemerkungen	Text	-

Description

Même les jeux de données sensibles peuvent être divulgués sous certaines conditions (par exemple, les données des résidents à des fins de recherche). Ces flux doivent suivre un processus et être documentés. Ce processus génère des données de processus, telles que :

Champ	Type	Exemple
Date de contact	Date	23/02/2021
Personne de contact	Texte	Martolo, Sonia
Institution de contact	Texte	Université de Berne, Dentisterie
Objectif	Texte	Étude "Santé bucco-dentaire, qualité de vie liée à la santé bucco-dentaire et aspects nutritionnels chez les personnes retraitées dans le canton de Berne"
Autorisation par	Texte	Hans Meier
Données identifiant les personnes	Oui/Non	Oui
CISO informé	Oui/Non	Oui
Nombre de dossiers	Nombre	10850
Statut de la demande	En traitement, Approuvé, Refusé	Approuvé
Date de livraison	Date	13/11/2021
Système source	Texte	Innosolv
Remarques spéciales	Texte	-

Frage

Wie wird die Herausgabe sensitiver Datenstämme gehandhabt?

Diese Frage kann auch mit "nicht anwendbar" beantwortet werden. Das muss bei der Gewichtung berücksichtigt werden.

Antwort	Punkte
Nicht anwendbar, die Organisationseinheit hat keine sensitiven Daten oder gibt diese nie heraus, auch nicht an andere Verwaltungsebenen (z.B. Kanton).	
Die Herausgabe sensitiver Informationen wird nicht dokumentiert.	0
Die Herausgabe folgt einem internen Prozess und ist in Form von Email Verkehr dokumentiert.	1
Bei der Herausgabe wird der CISO mindestens zur Information involviert.	2
Der Prozess bei der Herausgabe von internen oder vertraulichen Daten ist stadtweit vereinheitlicht und die Dokumentation elektronisch verfügbar.	3

Antwort	Punkte
Die Dokumentation wird mit Prozessdaten manuell ergänzt, z.B. in Form eines Excel Sheets. Die Prozesse werden vom CISO regelmässig geprüft und überwacht.	4
Der Prozess ist vollständig digitalisiert und alle Prozessdaten sind jederzeit ersichtlich.	5

Question

Comment est gérée la divulgation de jeux de données sensibles ?

Cette question peut également être répondue par "non applicable". Cela doit être pris en compte dans l'évaluation.

Réponse	Points
Non applicable, l'unité organisationnelle ne possède pas de données sensibles ou ne les divulgue jamais, même pas à d'autres niveaux d'administration (par exemple, le canton).	
La divulgation d'informations sensibles n'est pas documentée.	0
La divulgation suit un processus interne et est documentée sous forme de correspondance par email.	1
Lors de la divulgation, le CISO est impliqué au moins pour information.	2
Le processus de divulgation de données internes ou confidentielles est uniformisé à l'échelle de la ville et la documentation est disponible électroniquement.	3
La documentation est manuellement complétée avec des données de processus, par exemple sous forme d'un fichier Excel. Les processus sont régulièrement vérifiés et surveillés par le CISO.	4
Le processus est entièrement numérisé et toutes les données de processus sont visibles à tout moment.	5

DSEC-3: Zugriff, Accès

Beschreibung

Die Zugriffskontrolle auf die Daten ist klar, verständlich und nachvollziehbar. Die Prozesse berücksichtigen die klassischen Fälle wie Mitarbeiterwechsel, so dass niemand Zugriff auf Daten erhält, der es nicht sollte. Die Zugriffe sind besonders wichtig bei Daten, die als vertraulich klassifiziert sind. Doch auch bei den anderen Klassifizierungen oder wenn keine Klassifizierung existiert sind mindestens die schreibenden Zugriffe auf Daten klar (es ist hingegen z.B. nicht relevant, wer lesend auf öffentliche Daten zugreifen kann).

Description

Le contrôle d'accès aux données est clair, compréhensible et traçable. Les processus prennent en compte les cas classiques tels que le changement d'employés, de sorte que personne n'obtient l'accès aux données s'il ne le devrait pas. Les accès sont particulièrement importants pour les données classifiées comme confidentielles. Cependant, même pour les autres classifications ou en l'absence de classification, au minimum les accès en écriture aux données sont clairement définis (il n'est par exemple pas pertinent de savoir qui peut accéder en lecture aux données publiques).

Frage

Wie werden die Datenzugriffe auf die Datenstämme gehandhabt.

Antwort	Punkte
Es gibt keine Übersicht der Zugriffsberechtigungen auf die Datenstämme und es ist auch nicht in sinnvollen Mass möglich diese Zugriffe zu eruieren.	0
Es gibt keine Übersicht der Zugriffsberechtigungen, aber ad hoc kann bestimmt werden, ob eine bestimmte Person A Zugriff auf eine Ressource X hat.	1
Es gibt keine Übersicht der Zugriffsberechtigungen, aber ad hoc kann bestimmt werden, welche Personen welchen Zugriff auf die Ressource X haben.	2
Es gibt eine Übersicht über die Zugriffsberechtigungen, wer welchen Zugriff auf welche Ressource hat. Diese Übersicht wird regelmässig generiert und überprüft. Die Zugriffe werden über Rollen, nie über Personen gesteuert.	3
Es sind alle Prozesse dokumentiert, bei welchen sich die Zugriffsberechtigungen ändern müssen. Die Verwaltung der Prozesse wird mit einem spezialisierten Werkzeug, i.d.R. einem IAM, generiert.	4
Die Zugriffsberechtigungen werden automatisch aus digitalisierten Prozessen heraus generiert und aktualisiert. Anomalien bei den Zugriffen werden automatisch erkannt und eskaliert.	5

Question

Comment sont gérés les accès aux jeux de données ?

Réponse	Points
Il n'existe aucune vue d'ensemble des autorisations d'accès aux jeux de données et il n'est pas raisonnablement possible de déterminer ces accès.	0
Il n'y a pas de vue d'ensemble des autorisations d'accès, mais il est possible de déterminer ad hoc si une certaine personne A a accès à une ressource X.	1
Il n'y a pas de vue d'ensemble des autorisations d'accès, mais il est possible de déterminer ad hoc quelles personnes ont quel accès à la ressource X.	2
Il existe une vue d'ensemble des autorisations d'accès, indiquant qui a quel accès à quelle ressource. Cette vue d'ensemble est régulièrement générée et vérifiée. Les accès sont contrôlés via des rôles, jamais directement via des personnes.	3
Tous les processus sont documentés, où les autorisations d'accès doivent être modifiées. La gestion des processus est générée avec un outil spécialisé, généralement un IAM (Identity and Access Management).	4
Les autorisations d'accès sont générées et mises à jour automatiquement à partir de processus numérisés. Les anomalies dans les accès sont automatiquement détectées et escaladées.	5

dmma data_security classification public internal sensitive translated