JA, DAS DATENSCHUTZ- UND SICHERHEITSRISIKO WAR SEHR HOCH. VOR ALLEM BEIM VERSAND DER IT-DIAGNOSE-DATEN AN DIE AMERIKANISCHEN HERSTELLER UND DEREN WELTWEITEN SUPPORT.

JETZT ANONYMISIEREN WIR DIE SENSIBLEN DATEN IN DUMPS, LOGS UND TRACES MIT DEM ANONYMIZATION PROCESSOR. DAMIT SIND WIR SAFE.

TEILNAHME-ZERTIFIKAT

DATENSCHUTZ IM IT-BETRIEB

§§§

Europa (DSGVO)

Schweiz (DSG)

Anonymization Processor

VERTRAUEN SIE PATENTIERTER DATA LEAKAGE TECHNOLOGIE

Original IT-Diagnose-Dokument mit sensiblen Daten

Anonymisiertes IT-Diagnose-Dokument bereinigt von sensiblen Informationen, aber technisch voll funktionsfähig

SF-SafeDump®

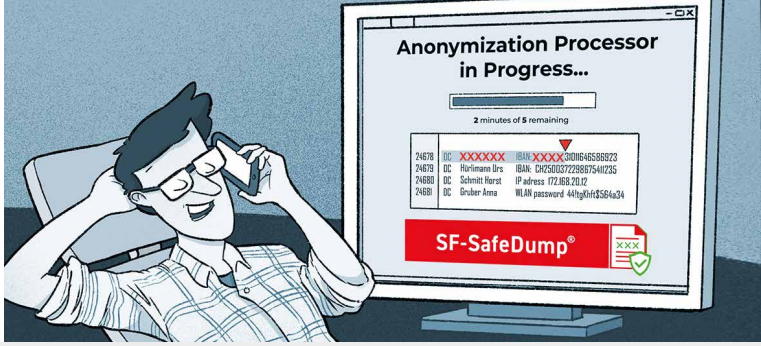
IT-REVISION

AUDIT: Datensicherheit im IT-Betrieb

- Wer hat Zugriff auf sensible Daten aus dem IT-Betrieb?
- Wie hoch ist das Datenschutz- und Sicherheits-Risiko?
- Wie werden sensible Daten in IT-Diagnose-Dateien geschützt?
- Werden Dumps, Logs und Traces anonymisiert?
- Sind Obliegenheitsverletzungen und Deckungs-einwendungen der Cyberversicherung ausgeschlossen?

Warum besteht Felix das Audit ohne Beanstandungen?

Felix verschickt seine IT-Diagnose-Daten an den Support im In- und Ausland – sicher, compliant und cyberversicherungsgerecht.



Dieses Risiko interessiert die Revision

Der IT-Betrieb schickt sensible Daten auf Weltreise – ohne „Zweck“ und „Notwendigkeit“

Sensible Personendaten, Sicherheitsinformationen und Geschäftsgeheimnisse befinden sich zum Zeitpunkt eines Computer- oder Applikations-Absturzes im Speicher und werden damit Teil von Speicherauszügen, sog. Dumps. Logs werden fortlaufend erzeugt, und Traces schneiden auf Bedarf den Netzverkehr mit. Diese IT-Diagnose-Daten bedeuten ein ernstes Datenschutz- und Sicherheitsrisiko für IT-Betrieb und Unternehmen. Es gehört in jedes IT-AUDIT.

Regelmäßig transferiert der IT-Betrieb IT-Diagnose-Daten zum Support der internationalen Hersteller – per Upload. Und mit im Gepäck: die sensiblen Daten! Die Reise geht nach Europa, USA, Indien, China und den Rest der Welt.

Dumps, Logs und Traces reisen zwar verschlüsselt, werden aber in den einzelnen Laboren und Supportzentren entschlüsselt, gespeichert und verarbeitet. So haben die Supporter und Spezialisten freien Zugang zu allen Daten - auch zu den sensiblen, die eigentlich unter strengem Daten- und Sicherheitsschutz stehen.

Vor welchem Rechtsverstoß warnt der IT-Anwalt?

“Die genannten Datenexporte enthalten standardmäßig „Überhänge“, also „zu viele“ Daten, die gemäß der Datenschutzanforderungen wegen fehlendem „Zweck“ und „Notwendigkeit“ nicht an Dritte weitergeleitet werden dürfen. Diese in ihrer Struktur „mehrdimensionalen Überhänge“, in denen sich auch hoch-sensible Personendaten befinden, sind oftmals unverhältnismäßig und demnach rechtswidrig.“

(Horst Speichert: DSGVO-Haftungs- und Sicherheitsrisiken durch Protokoll- und Diagnosedaten im IT-Betrieb, in: Datenschutz und Datensicherheit (DuD) 47, 04/2023, S. 229)

Zum vollständigen Artikel:

https://www.enterprise-it-security.com/DuD-Artikel-Speichert-042023

Es kommt zum Abfluss datengeschützter und sicherheitskritischer Informationen

KUNDENDATEN
PERSONAL-INFORMATIONEN
FINANZDATEN
GESUNDHEITSDATEN
GESCHÄFTSGEHEIMNISSE
BEHÖRDENINFORMATIONEN
PASSWÖRTER
USER-IDS
SECURITY CONTROLS
IP-ADRESSEN
SCHLÜSSEL (KEYS)

WAS SAGEN DIE DATENSCHUTZGESETZE ZU DIESEM POTENTIELLEN STRAFTATBESTAND?

EUROPA

§§§ **DSGVO** §§§

Art. 5 Abs. 1b / Art. 6 / Art. 28
Art. 32 / Art. 44-50
Art. 58:

Unternehmens-Bußgelder bis zu 20 Mio EUR oder bis zu 4% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs

SCHWEIZ

§§§ **revDSG** §§§
(ab 1.9.2023)

Art 6, Abs. 3 / Art. 8
Art. 9 / Art. 16 / Art. 61
Art. 60-66:

Persönliche Bussen bis zu 250.000 CHF

Und, was tun Sie gegen dieses Sicherheits- und Datenschutz-Risiko?

Anonymisierung sensibler Daten im IT-Betrieb – Grundschutz für Dumps, Logs und Traces

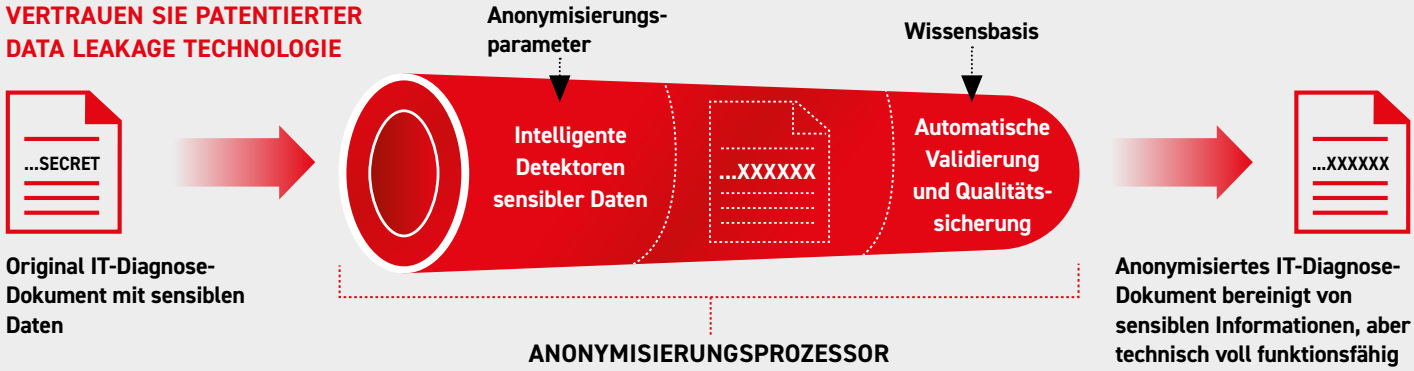
Erfahren Sie, welche sensiblen Daten im IT-Betrieb geschützt werden müssen und wie Sie dies durch Anonymisierung effizient erreichen können. Buchen Sie hier den kostenfreien Heise Webcast:

REVISIONS- UND CYBER-INSURANCE-GERECHTE LÖSUNG IM LIVE-WEBCAST AM 28.09.23, 11–12 UHR

https://www.enterprise-it-security.com/heise-webcast/security/anonymisierung/IXCT

Grundschutz für den IT-Betrieb – Automatisierte Anonymisierung und Pseudonymisierung

Anonymisierung und Pseudonymisierung sind mögliche technische Maßnahmen, um Datenschutz- und Sicherheits-Risiken zu vermeiden. SF-SafeDump ist eine auf IT-Diagnose-Daten spezialisierte Anonymisierungs- und Pseudonymisierungs-Lösung. Ihre Aufgabe ist, den technischen Wert der Diagnose-Dokumente trotz kompletter Anonymisierung zu erhalten. Sie ist patentiert und verleiht dem IT-Betrieb das richtige Schutzniveau im Umgang mit diesen technisch äußerst anspruchsvollen Datenformaten. Die Begleitdokumente von SF-SafeDump können IT-Administratoren entlasten und Datenschutz-Verantwortliche vor möglichen rechtlichen Folgen schützen.



Upload ohne Reue – SF-SafeDump Anonymization Processor

Der Anonymisierungsprozessor packt das Problem „an der Wurzel" und neutralisiert die identifizierbaren, sensiblen Daten vor ihrem Versand. Personenbezogene Daten werden so nicht mehr (re-) identifizierbar und Sicherheitsdetails nicht mehr offengelegt. Der alltägliche Upload von IT-Diagnose-Daten wird mit SF-SafeDump datenschutz-compliant und sicher. Der gesamte Prozess ist automatisiert, Batch-fähig und qualitätsgesichert. SF-SafeDump ist eine Windows-Applikation und unterstützt IT-Diagnose-Daten aller wichtigen IT-Plattformen.

Und übrigens – Outsourcing und Cloud sind kein Freibrief

Ihre IT-Dienstleister handeln in Ihrem Namen und müssen das Datenschutz- und Sicherheitsrisiko genauso hoch einschätzen wie Sie. Sie sind dafür verantwortlich, dass Ihre Provider die IT-Diagnose-Daten Ihrer Server und Applikationen vor dem Upload anonymisieren und pseudonymisieren.

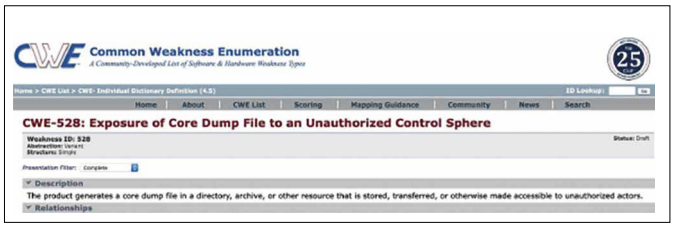
Wie verhindern Sie Konflikte mit Ihrer IT- und D&O-Versicherung?

Cyber-Versicherungsschutz nicht verlieren!

Vermeiden Sie Obliegenheitsverletzungen und Deckungseinwendungen Ihrer Cyberversicherung wegen vorvertraglicher Anzeigepflichtverletzung (§§ 19 ff. VVG) oder Gefahrerhöhung (§§ 23 VVG).

IT-Diagnose-Daten sind ein Cyber Security Risiko

NIST und PCI identifizieren Dumps und Logs als gravierende Sicherheitslücke. Diese enthalten potentiell Blaupausen für Ransom-Angriffe, wenn Ihre Encryption-Schlüssel direkt einsehbar bzw. extrahierbar sind. So gefährden sie auch Sicherheits-Architekturen wie Zero Trust, CARTA oder CSF.
Dumps und Logs gehören zu den Top 25 Sicherheitsrisiken gemäß CWE von MITRE.



Sicherheitsgesetze und -strategien in D-A-CH – Achtung sensible Daten

KRITISCHE INFRASTRUKTUREN	
KRITIS in Deutschland	IT-Sicherheitsgesetz 2.0 – IT-SiG 2.0 2021/2023
KII in Österreich	Government Computer Emergency Response Team (Bundeskanzleramt)
KI in der Schweiz	Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS)

BEHÖRDEN UND PUBLIC-IT	
Deutschland	BSI-Gesetz (BSIG)
Österreich	Österreichisches Informations-sicherheitshandbuch 4.3.3
Schweiz	Regierungs- und Verwaltungs-organisationsgesetz (RVOG)

Wünschen Sie weitere Informationen?

Erhalten Sie kostenfrei per Direkt Download

INFO-VIDEO – kurz erklärt
Anonymisierung sensibler Daten in IT-Diagnose-Dateien - Stoppt das Datenschutz-Risiko im IT-Betrieb
https://www.enterprise-it-security.com/info-video-de

WHITEPAPER
12-seitige Informationsbroschüre „Sicherheitsrisiko durch datenschutzwidrigen Abfluss sensibler Daten und Geschäftsgeheimnisse im IT-Betrieb" als PDF
für die Schweiz
www.enterprise-it-security.com/Whitepaper-CHDD3.pdf

COPYRIGHT UND WARENZEICHEN INFOS
www.enterprise-it-security.com/warenzeichen-copyright-de

für Deutschland, Österreich und EU
www.enterprise-it-security.com/Sicherheitsrisiko-Whitepaper-DE-V3.pdf

Schicken Sie Ihre Dumps, Logs und Traces risikofrei auf die Reise

SF-SafeDump®

DATA PRIVACY FOR DIAGNOSTICS
MIT PATENTIERTER ANONYMISIERUNG

GESELLSCHAFT FÜR INFORMATIK MITGLIED

swissICT Member

ENTERPRISE-IT-SECURITY.COM
Dr. Stephen Fedtke System Software
Seestrasse 3a · CH-6300 Zug · Schweiz
Telefon: +41 (0)41 710 7444
+800-37333853 (weltweit kostenfrei)

www.enterprise-it-security.com

Anonymisierung für Sicherheit und Datenschutz im IT-Betrieb