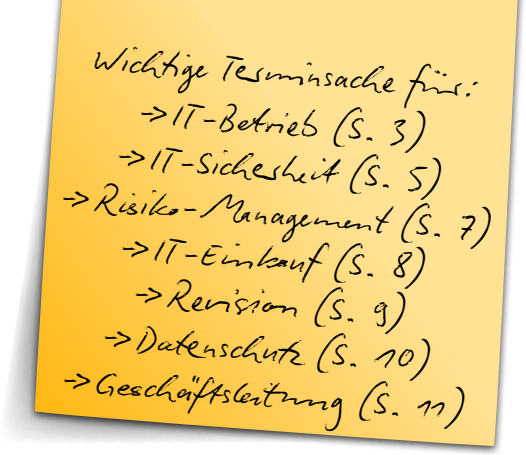
# Sicherheitsrisiko durch datenschutzwidrigen Abfluss sensibler Daten und Geschäfts-geheimnisse im IT-Betrieb




## VERLASSEN KUNDEN-, PERSONAL-, FINANZ- UND SOZIALDATEN AUCH IHRE FIRMA UNBEMERKT?

Wer denkt bei IT-Diagnose-Daten an die **ständige Gefahr des unkontrollierten Datenabflusses** und die daraus resultierenden Datenschutzverletzungen und IT-Sicherheitsrisiken? Selbst der IT-Betrieb ist sich dieser Bedrohung meist nicht bewusst.

**Dumps**, d.h. Speicherauszüge, entstehen bei allen Computer- und Applikationsabstürzen. **System-Logs** werden sogar fortlaufend erzeugt. **Netzwerk-Traces** werden gezielt erstellt. Der IT-Betrieb schickt diese Diagnose-Daten zur Fehleranalyse und -behebung an den Support ihrer Software-Anbieter und Dienstleister. Teilweise passiert dies sogar voll-automatisch, wie auch im Fall der Weiterleitung von System-Logs an das Security Monitoring (SIEM).

Diagnose-Dateien enthalten große Mengen **hochsensibler personenbezogener Daten und sicherheitsrelevanter Informationen**. Diese sind für die Problemanalyse nicht notwendig und damit **vollkommen zweckfremd**. Gemäß der Datenschutzanforderungen sollten sie auf keinen Fall Dritten zur Kenntnis gelangen. Demzufolge sollten sie vor dem Versand anonymisiert werden. Passiert dies nicht - und das ist häufig der Fall -, begeht der IT-Verantwortliche potentiell einen **Rechtsverstoß.**

## DUMP- UND LOG-FILES – TECHNISCH KOMPLEX UND LANGE ALS SICHERHEITSRISIKO IGNORIERT

Dumps und Logs dürfen demnach auf keinen Fall unbereinigt in Drittländer übermittelt werden, die im Sinne des Datenschutzes **kein gleichwertiges Schutzniveau wie Deutschland** besitzen, so etwa USA, Indien oder China. Die führenden Software-Anbieter, insbesondere deren Support- und Entwicklungszentren, sowie Labore, befinden sich allerdings genau in diesen Lokationen.

**Jedoch auch in Ländern mit gleichwertigem Schutzniveau**, wie der EU, bieten die unverhältnismäßig umfangreich und zweckfremd in Dumps und Logs versteckt enthaltenen Daten eine **datenschutzrechtliche und sicherheitskritische Angriffsfläche**. Man könnte annehmen, dass die Verschlüsselung der Daten eine compliancegerechte Lösung bieten würde. Leider nein, **denn die Diagnose-Daten müssen zur Fehleranalyse entschlüsselt werden**.

## BUSSGELDER BIS ZU 20 MIO. EURO ODER 4 % DES WELTWEITEN UNTERNEHMENSUMSATZES

Diese Strafen drohen bei Verstößen gegen die Grundsätze der Verarbeitung und unzulässigen Übermittlung von personenbezogenen Daten (Art. 83, Art. 5, 6, 7, 9 und Art. 44-49 DSGVO, §42 Abs.1 Nr. 1 BDSG). Auch können Geschädigte Schadenersatz verlangen (Art. 82 DSGVO). Genau dies kann bei unterlassener Anonymisierung von Dumps und Logs zum Versand an Dritte passieren. In einem solchen Fall **verletzt der IT-Verantwortliche seine Sorgfalts- und Fürsorgepflicht** gegenüber dem Unternehmen und haftet für den Schaden. **Das Unternehmen und der Geschäftsführer** werden im Außenverhältnis **durch Strafen belangt**. Genau dies kann die Anonymisierungslösung SF-SafeDump verhindern: Die Diagnose-Datenformate werden im Sinne von **Privacy by Design** gemäß der **Artikel 25 und 32 DSGVO lokal anonymisiert bzw. pseudonymisiert,** bei gleichzeitigem Erhalt ihrer technischen Aussagekraft.

So werden Herstellern diejenigen Daten bereitgestellt, die für die Fehler-Analyse und -Beseitigung notwendig sind. Alle schutzbedürftigen, nicht-technischen Daten werden automatisch anonymisiert. Dazu zählen **personenbezogene Daten, wie Kunden-, Finanz- und Sozialdaten, sowie unternehmensindividuelle Geschäftsgeheimnisse**. Entsprechendes gilt für sicherheitskritische Details über die Systeme und Applikationen der IT-Infrastruktur.

Empfehlenswert ist, dass die IT-Diagnose-Daten Ihr System nicht verlassen, ohne zuvor lokal anonymisiert worden zu sein. **Cloudbasierte Ansätze zur Anonymisierung würden das Risiko noch potenzieren**. Externe würden gezielt Ihre sensiblen Daten und Firmengeheimnisse analysieren, um sie den Algorithmen zuzuführen. Erfahren Sie mehr über die **Gefahr einer Cloud-Lösung** auf Seite 4.

## DATA PRIVACY FOR DIAGNOSTICS (DPFD) IM IT-BETRIEB

**DPFD ermöglicht dem IT-Betrieb punktuell die Erfüllung der Grundlagen der DSGVO** sowie die **Compliance-Anforderungen** gemäß Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI), Bundesamt für Sicherheit in der Informationstechnik (BSI), Europäischer Datenschutzbeauftragter (EDSB) sowie MITRE, NIST, ZeroTrust, SOX, EUROSOX, ISO, BASELII/III, SOLVENCYII, FERC, DOD, HIPAA und PCI.

**SF-SafeDump®**

DATA PRIVACY FOR DIAGNOSTICS

PLATTFORMÜBERGREIFENDE UND AUDITIERBARE ANONYMISIERUNG

**www.enterprise-it-security.com**

# EuGH-Entscheidung Schrems II – ergänzende technische Maßnahmen für Datenexporte in unsichere Drittländer (inkl. USA) erforderlich

IT-Diagnose-Daten werden zu den jeweiligen Software-Firmen und deren Supportzentren geschickt. Diese Hersteller befinden sich meist in **unsicheren Drittländern wie USA, China und Indien.** Die **Entscheidung des EuGH vom 16.07.2020 (Aktenzeichen C-311/18, Schrems II)** macht somit eine neue Bewertung dieses Transfers von Dumps und Logs mit den darin enthaltenen personenbezogenen Daten erforderlich.

Selbst wenn diese Drittländer die datenverarbeitenden Services mit ihren Rechenzentren in die Europäische Union verlagern, ist nicht auszuschließen, dass die Behörden der Mutterländer und der Hauptsitze der Konzerne Zugriff auf die Daten haben. Vor allem die **USA** gelten aufgrund ihrer Vormachtstellung im IT-Bereich und den **Durchgriffsrechten von Ermittlungsbehörden** nach wie vor als Datenschutz-Risiko. Die amerikanischen Überwachungsgesetze erlauben, über die Mutterunternehmen in USA – per Weisungsrecht – auch auf die Daten dieser Tochterfirmen in Europa zuzugreifen.

## NEUE STANDARDVERTRAGSKLAUSELN FORDERN TECHNISCHEN SCHUTZ

Die **neuen Standardvertragsklauseln (Standard Contractual Clauses – SCC)**, die am 04.06.2021 von der EU-Kommission veröffentlicht wurden, verlangen, das Schutzniveau jedes Daten-Import-Landes genau zu prüfen und ggf. in Frage zu stellen: „(19) Die Übermittlung und Verarbeitung personenbezogener Daten im Rahmen von Standardvertragsklauseln sollten nicht erfolgen, wenn die Rechtsvorschriften und Gepflogenheiten des Bestimmungsdrittlandes den Datenimporteur an der Einhaltung der Klauseln hindern."

(Quelle: DURCHFÜHRUNGSBESCHLUSS (EU) .../... DER KOMMISSION vom 4.6.2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates, S. 4)

Erfüllt der Daten-Importeur nicht die gesetzlichen Datenschutz-Anforderungen der EU, so muss der Daten-Exporteur – neben zusätzlichen Vertragsregelungen - **technische Lösungen zum Schutz der Daten** einsetzen. Dies regelt **Anhang II der neuen SCCs: „TOMs – Gewährleistung der Sicherheit der Daten"**. Der Daten-Exporteur muss technisch erwirken und gewährleisten, dass schützenswerte Daten in keiner Form dem Datenimporteur zur Kenntnis gelangen und Gegenstand von Missbrauch werden könnten. Andernfalls drohen die sehr **hohen Strafen der DSGVO**.

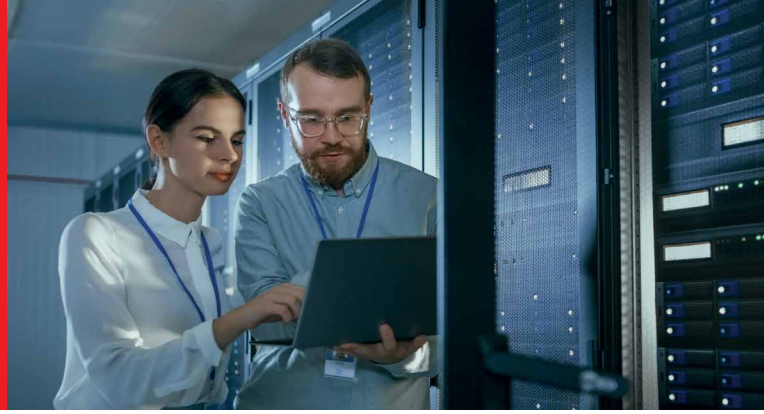
## DATENSCHUTZ MUSS TECHNISCH UMGESETZT WERDEN!

Die technischen und organisatorischen Maßnahmen (TOM) Ihrer IT-Dienstleister versprechen einen sicheren internen Umgang mit Ihren Daten und deren Schutz. Hierzu zählen auch Diagnose-Daten von Kunden. **Wie belastbar sind diese TOM-Dokumentationen und Nachweise?** Papier ist bekanntlich geduldig. Welches Restrisiko ergibt sich durch komplexe länderübergreifende Strukturen von Subunternehmern wie externen Mitarbeitern und Technologiepartnern? Auch für diese Überhänge haften Sie mit. Sie stehen potentiell in der Rückgriffshaftung.

**In der Verantwortung** für diese technischen und organisatorischen Maßnahmen stehen die **IT-Führungskräfte**. Sie müssen die Einhaltung der DSGVO konsequent unterstützen. Eine hohe Priorität gilt hierbei der Umsetzung der Grundsätze für die Verarbeitung personenbezogener Daten **(Art. 5 DSGVO): Rechtmäßigkeit, Transparenz, Zweckbindung, Datenminimierung, Speicherbegrenzung und Integrität und Vertraulichkeit**. Die Speicherung und Verarbeitung personenbezogener Daten muss also auf das für den Verwendungszweck nötige Mindestmaß begrenzt und damit frei von Überhängen sein. Sie muss verhältnismäßig sein. **Auf das hohe Volumen in IT-Diagnose-Dateien versteckter personenbezogener Daten trifft dies in keinem Fall zu. Mögliche Lösungen** sind, wie in **Artikel 25 und 32 der DSGVO benannt: Pseudonymisierung oder auch Anonymisierung.**


> "Wenn die Prüfung des Schutzmechanismus ergibt, dass er allein kein im Wesentlichen gleichwertiges Schutzniveau sicherstellen kann, müssen zusätzliche Maßnahmen ergriffen werden. Dieses hat der EuGH für Datentransfers in die USA bereits festgestellt. Zusätzliche Maßnahmen können grundsätzlich auf technischer, organisatorischer und/oder rechtlicher Ebene eingesetzt werden."
>
> Quelle: Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI), Prüfschema Drittstaatentransfers (PDF, 04.10.2021)

# IT-BETRIEB



## Verhindern Sie den – oft unbemerkten – Abfluss sensibler Daten via Dumps und Logs durch Anonymisierung

Der IT-Betrieb ist von der Gefahr des unbemerkten Datenabflusses über Dumps und Logs direkt betroffen, weil er für den Transfer und die Fehlerbehebung zuständig ist. Personen- und sicherheitsrelevante Daten verlassen das Unternehmen durch manuelle oder automatisierte Verfahren für Diagnose-Daten und gelangen so an Dritte. Dieses **Compliance- und Sicherheitsrisiko** betrifft auch Ihre Mitarbeiter externer Dienstleister im Rahmen der Arbeitnehmerüberlassung.

### IHR ANONYMISIERUNGSPROZESS SOLLTE LOKAL, AUDITIERBAR UND QUALITÄTSGESICHERT SEIN

Achten Sie streng darauf, dass sämtliche IT-Diagnose-Dokumentenformate einer Anonymisierung unterzogen werden, nicht nur Dumps, sondern auch Logs, Json-Files u.v.m. Für eine auditierbare Qualitätssicherung ist ein wiederholter Scan erforderlich. Es sollten entlastende Begleitdokumente erstellt werden. **Viele Hersteller-Tools oder Cloud-Lösungen scheiden dadurch aus** und stellen selbst ein Risiko für Ihre Entlastung dar (siehe S. 4).

**Verhindern Sie dieses Sicherheits- und Datenschutz-Risiko!**

### SF-SAFEDUMP UNTERSTÜTZT DEN IT-BETRIEB

SF-SafeDump kennt und anonymisiert das für Ihr Business relevante Typen-Spektrum sensibler Daten. Es kann darüber hinaus individuell ergänzt und erweitert werden. Der risikobehaftete Abfluss dieser Daten via IT-Diagnose-Dokumente wird somit verhindert. Es wird vollständig automatisiert betrieben und bietet so eine zuverlässige Anwendungsfunktionalität. Die spezielle Technologie von SF-SafeDump kommt während der **Anonymisierung ohne Zugriff auf Produktionsdatenbanken** aus und schafft somit nicht selbst weitere Datenschutzrisiken. Auch kann jeder IT-Betriebsmitarbeiter risikofrei und selbständig seine eigenen Diagnose-Dokumente lokal anonymisieren. SF-SafeDump läuft hoch performant auf dem Laptop.

Monitoring und Begleitdokumente um das Entstehen und Verarbeiten von IT-Diagnose-Daten liefern einen entlastenden Compliance-**Nachweis gegenüber Revision und Datenschutz**.

### ZUM SCHUTZ VON SICHERHEIT UND DATEN IST DAS MITTEL DER WAHL DIE TOOLBASIERTE, AUTOMATISIERTE, LOKALE ANONYMISIERUNG

- **Es reicht nicht, Diagnose-Daten für den Transfer einfach nur zu verschlüsseln.** Denn für die Analyse müssen sie entschlüsselt werden. Durch Anonymisierung kann man die darin enthaltenen sensiblen Daten vor Fremdzugriff schützen und im Sinne von Artikel 5,6,7,9 und 44-49 DSGVO handeln.
- Die **automatisierte, lokale Anonymisierung der IT-Diagnose-Daten** vermindert das Data-Leakage-Problem. Sie muss systematisch und verlässlich angewandt werden. Manuelle Verfahren bei Gigabyte großen Dumps sind reine Illusion. Auch Forensik-Tools helfen nicht wirklich weiter, weil sie keine Anonymisierung vornehmen.
- Es reicht nicht aus, nur über ein – theoretisch nutzbares – Tool zu verfügen. Für einen **Entlastungsnachweis** muss es selbst risikofrei sein (siehe S. 4), tatsächlich eingesetzt werden, wirksam sein und dies via Qualitätssicherung und Begleitdokumente nachweisen.
- Die vollständige und **fehlerfreie Anonymisierung** von IT-Diagnose-Dokumenten ist eine **äußerst komplexe Herausforderung und algorithmisch sehr aufwändig**. IT-Diagnose-Dokumente sind bereits durch kleinste Veränderungen ihres technischen Wertes beraubt. Die Datenstrukturen und -kodierungen von Dumps und Logs sind jeweils systemspezifisch, komplex und extrem vielfältig. Eine grobe Anonymisierung würde für Ungenauigkeiten oder gar korrupte Dateien sorgen. Debug- und Analyse-Tools des Herstellers müssen jedoch den anonymisierten Dump trotz Anonymisierung fehlerfrei verarbeiten können.

# IHR ANONYMISIERUNGSPROZESS DARF SELBST KEIN DATENSCHUTZRISIKO SEIN!

## KEIN TOOL MIT PRODUKTIONSDATENBANK-ZUGRIFF!

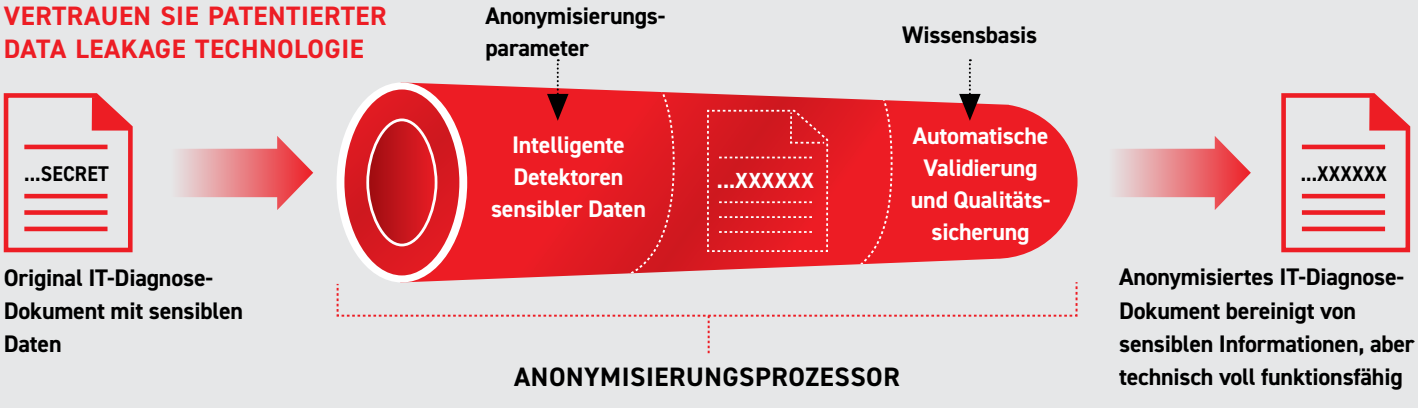
Eine sehr **wichtige Anforderung** an die implementierte Anonymisierungslösung ist folgende: Sie muss eigenständig alle relevanten Datentypen finden und darf nicht selbst ein Datenschutzrisiko darstellen. Die technischen Anonymisierungsprozesse sollten zum Beispiel **nicht vom direkten Zugriffsrecht auf die Kundendatenbank abhängig sein**. Dies wäre der Fall, wenn die Suche in den Diagnose-Dokumenten nach unternehmensspezifischen Kundendaten, wie etwa Vor- und Nachnamen, direkte Zugriffe auf Produktionsdatenbanken während der Anonymisierung erforderte. So hätten der technische Prozess und die damit involvierten Mitarbeiter Zugriff auf diese sensiblen Daten selbst. Dies wäre per se ein Risiko oder eine Datenschutzverletzung.

## CLOUD-BASIERTE ANONYMISIERUNG VON IT-DIAGNOSE-DATEN ERSCHEINT KOMFORTABEL, VERSCHÄRFT ABER DIE RISIKOLAGE VON UNTERNEHMEN UND WIRTSCHAFT!

- **Eine Cloud-Lösung ändert nichts an der Datenschutzwidrigkeit.** Die personenbezogenen und sensiblen Daten würden weiterhin zweckfremd und unverhältnismäßig Ihr Unternehmen verlassen. Besonders deutlich wird dies im Fall, dass **Cloud-Anonymisierungs-Anbieter und Diagnose-Daten-empfangender Software-Hersteller identisch sind**, d.h. dem gleichen Unternehmen angehören.
- **Das Datenschutz-Risiko würde durch eine Cloud-Lösung in keiner Form beseitigt.** Sie hätten eine Vereinbarung zur **Auftragsverarbeitung** mit dem Cloud-Anonymisierer, wie mit dem Hersteller. Sie müssten die sensiblen Daten und Geschäftsgeheimnisse im Detail vertraglich festhalten und begründen, warum Sie diese bewusst zweckfremd nach außen geben.
- Auch wenn eine **Cloud-Lösung** praktikabel und einfach erscheinen mag, so würde sie **umfangreiche Vorarbeiten** notwendig machen. Technisch kann eine standardisierte Lösung aus der Cloud nicht ohne Mehraufwand, also „out of the box", in der notwendigen Qualität funktionieren. Denn wie sollen die Cloud-Anbieter ohne Vorwissen und Anpassung alle Ihre individuellen Datentypen und Geschäftsgeheimnisse erkennen, analysieren und anonymisieren können? Auch sogenannte künstliche Intelligenz hilft hier nicht. Diese müsste ebenfalls erst mühsam antrainiert werden.
- **Die fatale Folge einer in die Cloud ausgelagerten Anonymisierung** wäre, dass sich Externe in verschiedenen Verarbeitungsstufen und Lokationen intensiv mit Ihren sensiblen Daten und Firmengeheimnissen beschäftigen müssten. Denn Sie würden die Daten systematisieren, um sie eigenen Algorithmen zuführen zu können. Der neue Fokus speziell auf die sensiblen Daten von Firmen und somit ganzer Wirtschaftsräume würde eine ungleich höhere Datenschutz-Gefahr bedeuten als der bisher erfolgte freie Versand von Dumps und Logs. Dieser lief praktisch unbemerkt unter dem Radar. Mit den Cloud-Aktivitäten würde er noch mehr ins Bewusstsein rücken und könnte sogar Anknüpfungspunkt für staatliche, geheimdienstliche oder wirtschaftspolitische Interessen werden.
- Aktuelle Trends, wie **Zero Trust**, untersagen deshalb pauschales Vertrauen. Dazu gehört definitiv auch ein gutgläubiger, unkontrollierter Upload der eigenen Firmengeheimnisse in eine Cloud-Lösung.

Anonymisierung via **Cloud-Service** klingt verlockend, ist aber nicht nachhaltig problemlösend, sondern **eher gefährlich**. Auch wir haben die Option „SF-SafeDump in der Cloud" intensiv geprüft und nach gemeinsamer Risiko- und Bedarfs-Analyse mit großen IT-Betreibern aus gutem Grund verworfen. **Eine automatisierte, auditierbare und lokale Anonymisierung** in Eigenregie ist wirklich zielführend.

## VERTRAUEN SIE PATENTIERTER DATA LEAKAGE TECHNOLOGIE



# Sicherheitsrelevante Informationen in IT-Diagnose-Daten machen Sie verwundbar

Diagnose-Daten wie Dumps und Logs enthalten als Momentaufnahme des Systems neben personenbezogenen Daten **auch security-relevante Informationen**. Diese können von Dritten missbraucht werden, um gegen Ihr Team mit optimalem Angriffsvektor anzutreten.

## ANALYSIEREN SIE DIE SECURITY-GEFAHREN DURCH DUMPS UND LOGS

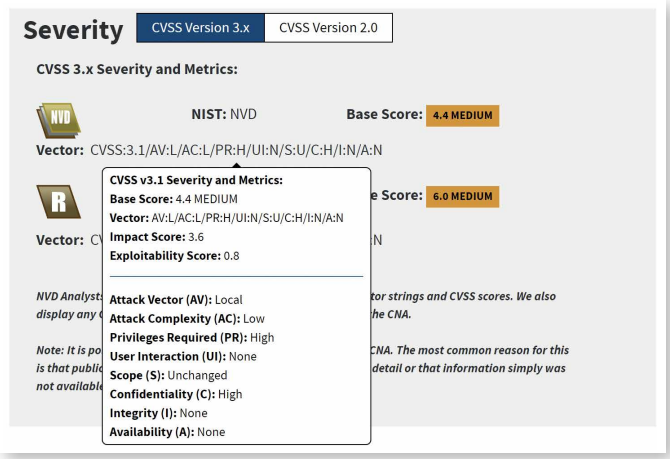
- Etablieren Sie einen regelmäßigen gemeinsamen Dialog mit dem IT-Betrieb, dem Datenschutz und der Revision.
- Legen Sie gemeinsam fest, welche Informationen über die IT-Infrastruktur und deren Konfiguration für Außenstehende nicht einsehbar sein dürfen. Dies reicht von IP-Adressen, über Details eingesetzter Sicherheitsprodukte bis hin zu spezifischen Registry-Einträgen. Die meisten Details werden insbesondere über System-Dumps potentiell offengelegt.
- Entwickeln Sie im Team die Regeln, wie der Zugriffsschutz auf IT-Diagnose-Dateien definiert sein muss. Insbesondere auf einem Produktionssystem darf nur ein ausgewählter Personenkreis Zugang zu diesen Dateien erhalten.
- Überraschen Sie im nächsten Audit die interne Revision und die externen Wirtschaftsprüfer. Manifestieren Sie proaktiv das Risiko um Diagnose-Dokumente und dessen Eliminierung in Ihren Policies und Compliance-Guidelines.

## SF-SAFEDUMP UNTERSTÜTZT DIE IT-SICHERHEIT

SF-SafeDump konzentriert sich beim Anonymisieren diagnostischer Dokumente nicht nur auf personenbezogene Daten, sondern auch auf sicherheitstechnische Details. SF-SafeDump **unterstützt Ihre Compliance** gegenüber MITRE, PCI NIST, Bundesamt für Sicherheit in der Informationstechnik (BSI), Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI), Europäischer Datenschutzbeauftragter (EDSB) sowie SOX, EUROSOX, ISO, BASELII/III, SOLVENCYII, FERC, DOD und HIPAA. **Unternehmensspezifische Software oder System-Komponenten können individuell in die Anonymisierung eingeschlossen werden.** Wenn Sie auf Sicherheits-Architekturen wie zum Beispiel **Zero Trust, CARTA oder CSF** setzen, ist die Dump- und Log-Anonymisierung die naheliegendste, elementare Voraussetzung für die Absicherung gegen das Risiko „Hersteller".

So enthalten **Dumps potentiell auch die Blaupause für Ransom-Angriffe,** wenn Ihre Encryption-Schlüssel direkt dort einsehbar bzw. extrahierbar sind. Dies bestätigen auch NIST, PCI und MITRE.

## NIST UND PCI IDENTIFIZIEREN DUMPS UND LOGS ALS GRAVIERENDE SICHERHEITSLÜCKE

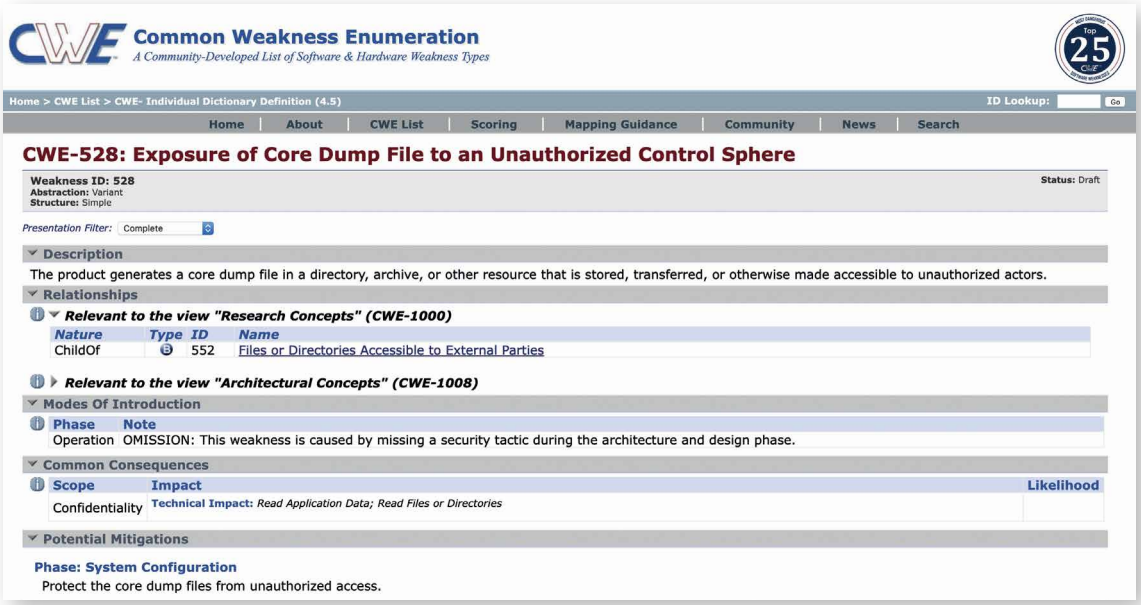



nvd.nist.gov/vuln/detail/CVE-2021-23211

**„PCI CONTROL OBJECTIVES 3.6**
**The software does not disclose sensitive data through unintended channels – GUIDANCE:**
Proactive measures to ensure that sensitive data is not inadvertently "leaked" should be implemented by the software vendor or within the software. Disclosure of sensitive data to unauthorized parties often occurs via unknown or unintended outputs or channels. For example: sensitive data could be unintentionally disclosed through error- or exception-handling routines, logging or debugging channels, third-party services and/or components, or through the use of shared resources such as memory, disk, files, keyboards, displays, and functions. Protective mechanisms, whether process or programmatic in nature, should be implemented to ensure that sensitive data is not accidentally disclosed through such means."

(Excerpt from the Payment Card Industry (PCI) Software Security Framework, Secure Software Requirements and Assessment Procedures, Version 1.1, April 2021, p. 28, courtesy of PCI Security Standards Council, LLC. © 2021 PCI Security Standards Council, LLC. All Rights Reserved.)

# Dumps und Logs gehören zu den Top 25 Sicherheitsrisiken gemäß CWE von MITRE



CWE Common Weakness Enumeration
A Community-Developed List of Software & Hardware Weakness Types

Home > CWE List > CWE- Individual Dictionary Definition (4.5) ID Lookup: Go

Home | About | CWE List | Scoring | Mapping Guidance | Community | News | Search

**CWE-528: Exposure of Core Dump File to an Unauthorized Control Sphere**

Weakness ID: 528
Abstraction: Variant
Structure: Simple
Status: Draft

Presentation Filter: Complete

**Description**

The product generates a core dump file in a directory, archive, or other resource that is stored, transferred, or otherwise made accessible to unauthorized actors.

**Relationships**

*Relevant to the view "Research Concepts" (CWE-1000)*

| Nature | Type | ID | Name |
|---|---|---|---|
| ChildOf | B | 552 | Files or Directories Accessible to External Parties |

*Relevant to the view "Architectural Concepts" (CWE-1008)*

**Modes Of Introduction**

| Phase | Note |
|---|---|
| Operation | OMISSION: This weakness is caused by missing a security tactic during the architecture and design phase. |

**Common Consequences**

| Scope | Impact | Likelihood |
|---|---|---|
| Confidentiality | Technical Impact: Read Application Data; Read Files or Directories | |

**Potential Mitigations**

Phase: System Configuration
Protect the core dump files from unauthorized access.

Das Risiko von Dumps und Logs erreicht durchweg hohe Scores gemäß CVSS und CWSS.

cwe.mitre.org/data/definitions/528.html

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

| BETREIBER KRITISCHER 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 | |
|---|---|
| Deutschland | BSI-Gesetz (BSIG) |
| Österreich | Österreichisches Informations-sicherheitshandbuch 4.3.3 |
| Schweiz | Regierungs- und Verwaltungs-organisationsgesetz (RVOG) |

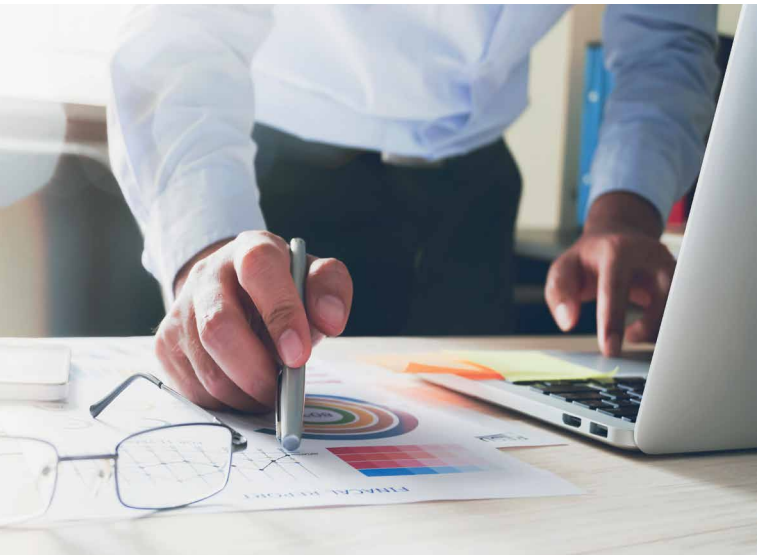
# RISIKO-MANAGEMENT

## Evaluieren Sie das Unternehmens- und Sicherheits-Risiko unterlassener Anonymisierung von Dumps und Logs

Manche IT-Risiken im Unternehmen sind auf den ersten Blick nicht ersichtlich. Die komplexen IT-Systeme bieten zahlreiche, nur schwer erkennbare Angriffspunkte und somit Risiken für Ihr Unternehmen. Wer hätte vermutet, dass in Diagnose-Dateien und System-Logs potentiell sehr große Mengen hochsensibler Personen- und Sicherheitsdaten verborgen sind? **Geraten diese un-anonymisiert an Dritte, stellen sie ein Datenschutz-, Sicherheits- und somit potentielles Unternehmensrisiko dar.**

### FORDERN SIE VON DEN VERANTWORTLICHEN KONKRETE RISIKOREDUZIERENDE MASSNAHMEN

- Bewerten Sie die Detailrisiken der Diagnose-Dokumente und Protokolldaten. Kommunizieren Sie diese an die betroffenen Unternehmensbereiche. Machen Sie konkrete Vorgaben für den Zugriffsschutz auf Diagnose-Dokumente.
- Sorgen Sie für Awareness im IT-Betrieb und in der IT-Security. Die Argumentation ist mit den bekannten Problemstellungen der Data-Leakage und Testdaten-Anonymisierung vergleichbar.
- Fordern Sie via automatisierter, lokaler Anonymisierung eine Vermeidung des Risikos im Fall der externen oder internen Weiterleitung. Überprüfen Sie die Anonymisierungsprozesse auf Risiken (siehe S. 4)!



### OUTSOURCING IST KEIN FREIBRIEF – IHRE DIENSTLEISTER HABEN DAS GLEICHE SICHERHEITS-RISIKO MIT DUMPS UND LOGS

> „Wo man Server nicht selbst, sondern von Service- oder Hosting-Providern betreiben lässt, gilt es, die hier skizzierten Risiken bezüglich der eigenen Daten proaktiv zu adressieren und für eine entsprechende Pflicht zur Anonymisierung von Dumps und Logs in dessen Tätigkeitsbereich zu sorgen."
>
> Quelle: kes Die Zeitschrift für Informations-Sicherheit 3, 2014, S. 28

Nutzen Sie Cloud-basierte oder outgesourcte IT-Dienstleistungen? Dann fordern Sie vom jeweiligen Anbieter die Anonymisierung seiner IT-Diagnose-Daten, wenn es Ihre Systeme oder Anwendungen betrifft. Andernfalls würde er sensible Daten Ihres Unternehmens an nachgelagerte Dienstleister schutzlos weiterleiten. Bewerten Sie zusammen mit dem Datenschutz-Verantwortlichen das **Restrisiko und die Belastbarkeit der mit Herstellern und Service-Partnern geschlossenen Vereinbarungen zur Auftragsverarbeitung und der technisch organisatorischen Maßnahmen (TOM).** Wie belastbar sind diese wirklich?

### SF-SAFEDUMP UNTERSTÜTZT DAS RISIKO-MANAGEMENT

Der 360-Grad-Ansatz von SF-SafeDump für die Risikoreduzierung im Umgang mit Diagnose- und Protokolldaten gibt Ihnen einen detaillierten Einblick in die eigene Systematisierung der Risikobereiche.

Die Begleitdokumente eines Beispiel-Anonymisierungsvorgangs liefern Ihnen bereits wichtige Erkenntnisse für Ihre konkrete Risikoeinschätzung.

# IT-EINKAUF

## Vereinfachen Sie Ihren Einkaufsprozess durch verlässliche Data Compliance

IT-Einkäufer wählen Dienstleister und Software-Anbieter nach fachlichen und ökonomischen Kriterien aus. Angesichts der wachsenden Sicherheitsbedrohungen und gesetzlichen Auflagen spielen **Vertrauen und Compliance auch beim IT-Einkauf eine immer größere Rolle**. Immerhin erhalten externe Partner auf vielfältige Weise Zugang zum „Herzstück" Ihres Unternehmens.

IT-Diagnose-Daten wie Dumps und Logs, die der IT-Betrieb regelmäßig an die IT-Dienstleister schickt, sind wie ein „aufgeschlagenes Buch". Ungeschützt bieten sie unerlaubte Einblicke in Ihre Firmeninterna. Durch automatisierte, lokale Anonymisierung können Sie die **personenbezogenen Daten und security-relevanten Informationen vor dem Zugriff Dritter schützen** und gleichzeitig die notwendigen Schutzmaßnahmen moderater ansetzen.

Anonymisierte IT-Diagnose-Daten **unterstützen Ihre Einkaufsprozesse** positiv. Da Sie Ihre Daten selbst schützen, steht Ihnen ein **größerer Kreis von potentiellen Anbietern** zur Verfügung. Sie sind nicht mehr ausschließlich auf deren Vertrauensversprechen und Belastbarkeit angewiesen.

### KONZENTRIEREN SIE SICH WIEDER AUF DAS WESENTLICHE UND DIE ÖKONOMISCHE SEITE DES BESCHAFFUNGSPROZESSES:

- Oft liegt die Notwendigkeit komplexer technisch organisatorischer Maßnahmen (TOM) für die Vereinbarungen zur Auftragsverarbeitung mit Software-Herstellern allein im Austausch von Diagnose-Daten begründet. Gibt es hier **keine Risiken mehr, vereinfacht dies die Vertragsverhandlungen** nachhaltig. So können Sie nun auch mit kleinen, innovativen und agilen Hersteller-Unternehmen kooperieren. Diese bieten auch oft unter wirtschaftlichen Gesichtspunkten Vorteile.

### SF-SAFEDUMP UNTERSTÜTZT DEN IT-EINKAUF

SF-SafeDump erlaubt einen risikoreduzierten Austausch von Diagnose-Daten mit Software-Herstellern. Anforderungen und Aufwände zur **Erfüllung von TOM und Auftragsverarbeitung** können im beiderseitigen Interesse fokussiert, vertrauensvoll und kostenoptimal angesetzt werden. Das Restrisiko einer fehlenden Belastbarkeit ist nachhaltig vermindert. Auch erfüllen Sie die Anforderungen an die ergänzenden technischen Maßnahmen gemäß EuGH-Entscheidung Schrems II und Anhang II der neuen Standardvertragsklauseln zu „TOMs – Gewährleistung der Sicherheit der Daten".

- Verpflichten Sie Cloud- und Outsourcing-Dienstleister zur Anonymisierung von IT-Diagnose-Daten im Fall Ihrer Systeme und Daten. Umschiffen Sie auch hier alle komplizierten vertraglichen Details zu diesem Thema dank automatisierter, lokaler Anonymisierung.
- Des weiteren besteht die Option, dass Sie für Ihren Dienstleister die Anonymisierung vornehmen. Dieser darf Ihre sensiblen Daten nicht selbst Dritten überlassen, sondern erhält von Ihnen die bereinigten Diagnose-Dokumente für den eigentlichen Versand.

# REVISION

## Prüfen Sie ab sofort den Sicherheits- und DSGVO-konformen Umgang mit IT-Diagnose- und Protokoll-Daten

Als **Revisor und Wirtschaftsprüfer** sollten Sie einen **neuen prüfungsrelevanten Bereich „Diagnose-Dokumente“** definieren. Hierfür gilt es, neue Compliance-Prozesse vom IT-Betrieb einzufordern. Sie dienen dem Schutz der personenbezogenen Daten und sicherheitsrelevanten Informationen vor unerlaubter Weitergabe, Einsicht und Verarbeitung. Denn, werden sie an Dritte weitergeleitet, verursachen sie zweierlei: Zum einen bedeuten sie eine **Datenschutzverletzung** und somit einen Haftungsfall für die Verantwortlichen. Zum zweiten bewirken sie eine **Sicherheitsverletzung**, weil **offengelegte sicherheitsrelevante Informationen, wie IP Adressen, User IDs, Passwörter und Keys**, eine gefährliche Angriffsfläche darstellen. Die Risiken sind vielfältig und können das Unternehmensergebnis sowie den Jahresabschluss negativ beeinflussen.

> “Die Regel sollte eine Pflicht zur konsequenten Dump- und Log-Anonymisierung sein – hauseigene Richtlinien sind entsprechend zu erweitern. Dies gilt allem voran für System-Dumps – eine nicht-anonymisierte Weitergabe wäre hier regelrecht verantwortungslos.“

Quelle: kes Die Zeitschrift für Informations-Sicherheit 3, 2014, S. 28

### SF-SAFEDUMP UNTERSTÜTZT DIE REVISION

Für die auditierbare Nachvollziehbarkeit bietet SF-SafeDump ein Allphasen-Monitoring von der Entstehung bis zur finalen Handhabung von IT-Diagnose-Dokumenten.

SF-SafeDump ermöglicht die Nachweisbarkeit und Qualitätssicherung bezogen auf die Anonymisierung der sensiblen Daten durch leistungsstarke, automatisierte Instrumente.

### REVISIONSPRÜFUNG

**DIESE FRAGESTELLUNGEN UND UNTERSUCHUNGEN SOLLTEN TEIL IHRER PRÜF-ROUTINEN SEIN**

- Existiert ein Monitoring um den Bereich diagnostischer Dokumente im produktiven IT-Umfeld?
- Wird beides überwacht? Das Entstehen sensibler IT-Diagnose-Dokumente als auch ihr interner und externer Austausch?
- Welche Datentypen wurden als sensibel klassifiziert? Werden diese anonymisiert oder zumindest pseudonymisiert?
- Werden die sensiblen Diagnose-Dokumente rechtskonform, d.h. lokal anonymisiert und verschlüsselt an Software-Hersteller und Provider geschickt? Gibt es hierfür einen konkreten Nachweis?
- Wurde per Risikoanalyse entschieden, ob interne Entwickler Zugriff auf Dumps und Logs aus dem Produktionsumfeld erhalten? Wie strikt sind die Zugriffsschutzregeln im Test- bzw. Entwicklungsumfeld und in der Produktion?
- Überprüfen Sie im Rahmen entsprechender Revisionsprozesse stichprobenweise, ob alle Diagnose-Dokumente DSGVO-konform und gemäß der firmeneigenen Regeln behandelt worden sind?
- Verdeutlichen Sie Ihren Kollegen die Wichtigkeit dieses Themas? Verifizieren Sie den Nachweis, dass die Anonymisierung der Protokoll- und Diagnose-Daten qualitätsgesichert – und nicht nur „symbolisch“ – vollzogen wird? Überprüfen Sie den effektiven Einsatz entsprechender Werkzeuge und Prozesse. Lassen Sie sich entsprechende Begleitdokumente als Beleg ihrer Ausführung zeigen.
- Ist der Anonymisierungsprozess selbst risikofrei? (siehe S. 4)

# DATENSCHUTZ

## Berücksichtigen Sie auch die verdeckten Datenschutz- und Sicherheits-Risiken der IT-Systeme: Dumps und Logs

Als Datenschutzverantwortlicher sollten Sie alle potentiellen Datenschutzfallen im Unternehmen kennen, gleichgültig wie technisch versteckt oder komplex diese sind. IT-Diagnose-Dokumente stellen in diesem Sinne sogar eine **äußerst „tiefe" Datenschutzfalle** dar. Daher sind auch alle Diagnose-Daten erzeugenden Systeme innerhalb der IT-Infrastruktur von großer Bedeutung für den Datenschutz.

### WO FINDEN UNBEMERKT WEITERGABEN SENSIBLER DATEN STATT?

Sicher ist Ihnen bekannt, dass Dumps und Logs potentiell sehr große Mengen an Personen- und Sicherheitsdaten enthalten und Ihr IT-Betrieb diese an die Hersteller zur Diagnose übermittelt. Können Sie dafür garantieren, dass die mit den Herstellern gerne großzügig getroffenen Vereinbarungen über Auftragsverarbeitungen juristisch „bulletproof" sind? Oder besteht dennoch ein **Restrisiko von Unwirksamkeit des Datenschutzes?**

In Fachkreisen besteht Zweifel an der Zulässigkeit praktizierter „Großzügigkeiten". Diese entstehen zum einen durch ein Zuviel in Bezug auf die große Menge zweckfremder Daten in Diagnose-Dokumenten. Zum zweiten entstehen diese **„Überhänge"** durch ein Zuviel in Bezug auf das sensible Spektrum der Daten. Außerdem resultieren Überhänge aus einem Zuviel in Bezug auf die Länge der Kette von Zwischenverarbeitungs- und Weiterreichinstanzen, bis Dumps und Logs das Labor des Herstellers erreichen. Das Restrisiko und eine dafür mögliche **Rückgriffshaftung** steigt mit jeder weiteren involvierten Partei. Risiken können gemäß Art. 25 und 32 DSGVO **durch Anonymisierung oder Pseudonymisierung** der personenbezogenen Daten eingeschränkt werden.

### PLANEN SIE DATENSCHUTZGERECHTE UND TECHNISCH WIRKSAME DATA-GOVERNANCE-KONZEPTE MIT INTERDISZIPLINÄREN TEAMS

- Definieren Sie gemeinsam mit den Daten-Eigentümern im Unternehmen, welche Daten über den Weg der IT-Diagnose-Dokumente keinesfalls das Unternehmen verlassen dürfen.
- Entscheiden Sie, für welche Daten eine Anonymisierung unabdingbar und für welche Daten eine Pseudonymisierung akzeptabel ist.
- **Überprüfen Sie den Anonymisierungsprozess auf Risiken** und auditierbare Anwendung (siehe S. 4).
- Erweitern Sie die Awareness und wägen Sie gemeinsam ab, inwieweit nicht nur extern, sondern auch inhouse eine Bereitstellung von Dumps und Logs aus der Produktion für die eigenen Entwickler zu untersagen ist. **Sollten produktive Diagnose-Daten für die interne, technische Problemanalyse ebenso anonymisiert werden wie für externe Dritte?** Orientieren Sie sich hierbei gerne an den Policies zur Testdaten-Generierung, ein sehr ähnlich gelagertes Problem. Entscheidend ist auch die Frage, wie hoch der Anteil externer Partner und Mitarbeiter ist.
- Prüfen Sie auch in Verträgen mit **Cloud-basierten oder outgesourcten IT-Dienstleistungen**, ob eine gleichwertige Anonymisierung von IT-Diagnose-Daten gewährleistet ist. Denn **in den Dumps und Logs der Dienstleister sind viele sensible Daten Ihres Unternehmens enthalten**, und über die Weiterleitung entscheidet ausschließlich der Dienstleister.
- Vereinbaren Sie mit der **Revision** einen belastbaren und damit formell entlastenden Prüfplan auf Basis regelmäßiger stichprobenbasierter Kontrollen im Umfeld „Diagnose-Dokumente".

### SF-SAFEDUMP UNTERSTÜTZT DEN DATENSCHUTZ

SF-SafeDump unterstützt plattformübergreifend IT-Diagnose-Daten und führt mit lokaler Anonymisierung zur **Entlastung gemäß Artikel 5,6,7,9 und 44-49 DSGVO sowie §42 Abs.1 Nr. 1 BDSG und EuGH-Entscheidung Schrems II.**

SF-SafeDump wird „out of the box" mit einem nachhaltig breiten und detaillierten Spektrum detektierbarer Datentypen ausgeliefert. Es erlaubt ferner, unternehmensspezifische Datentypen für die Analyse zu definieren und individuell über zuverlässige Anonymisierung und Pseudonymisierung zu entscheiden.

SF-SafeDump bietet für Compliance und Qualität neben der Anonymisierung auch ein aktivierbares Monitoring um IT-Diagnose-Dokumente. Automatisch erstellte Begleitdokumente geben klaren auditierbaren Entlastungsnachweis für alle Parteien.

# GESCHÄFTSLEITUNG

## Schließen Sie diese offene Datenschutz-Flanke, um die Sicherheitsbedrohung Ihres Unternehmens durch IT-Diagnose-Daten zu vermeiden.

Das **Risiko** der routinemäßigen **Übermittlung** nicht-anonymisierter Dumps und Logs ist in den meisten Unternehmen nicht bekannt. Eventuell **ahnt der IT-Betrieb die Gefahr,** sucht aber noch nach Lösungen.

Jedes Unternehmen mit eigenem IT-Betrieb hat mit sehr hoher Wahrscheinlichkeit mit IT-Diagnose-Daten zu tun. Es ist folgerichtig, dass diese Protokoll-Daten mit Herstellern, Service-Partnern und deren Subunternehmen ausgetauscht werden müssen. Eine durchschnittlich große IT **überträgt pro Jahr mindestens 100 Dumps aus produktiven Umgebungen** an externe Partner. Es gibt hierfür keine alternative Lösung.

### VORSICHT IST ABER AUCH FÜR INTERNE IT-SERVICES UND IHRE MITARBEITER GEBOTEN

Es sollte ausgeschlossen werden, dass Softwareentwickler und Applikationsverantwortliche bei Banken, Versicherungen oder Sozialdatenverarbeitern über Dumps und Logs aus Produktionsumgebungen Zugang zu streng geheimen und schutzbedürftigen Daten erhalten. **Bankgeheimnisse oder Sozial- und Gesundheitsdaten** via IT-Diagnose-Dateien unkontrolliert einsehbar zu machen, wären Beispiele für grobe Fahrlässigkeit.

Es ist sehr wichtig, diese Datenschutz- und Sicherheits-Lücke intern ins Bewusstsein zu rücken und Awareness für die Risiken um IT-Diagnose-Dokumente zu schaffen. Entsprechende Vorfälle würden der Reputation Ihres Unternehmens enorm schaden!

Bedenken Sie auch, dass Ihre **Mitarbeiter** gleichfalls ein Recht auf Datenschutz haben. Machen Sie sich weder extern noch intern angreifbar!

**Fordern Sie die verantwortlichen Unternehmensbereiche, Revision, Risiko-Management, IT-Betrieb, IT-Sicherheit, IT-Einkauf und Datenschutz dazu auf, zu kooperieren.**

### SICHERHEITSRISIKO DURCH VERSAND NICHT ANONYMISIERTER IT-DIAGNOSE- UND PROTOKOLL-DATEN

Die Wahrscheinlichkeit, dass **Ihr IT-Betrieb im Bereich der Diagnose-Daten nicht 100%ig data-compliant agiert**, ist sehr hoch. Es handelt sich nicht nur um eine Datenschutz-, sondern auch um eine gravierende Sicherheitslücke. Die in den Dumps und Logs offengelegten Informationen über Ihre Server, Anwendungen und Systeme können als Blueprint für einen Angriff dienen. Die Weitergabe von Dumps und Logs stellt ein **ernstes Sicherheitsrisiko** dar!

### BEDEUTUNG FÜR KRITISCHE INFRASTRUKTUREN (KRITIS)

**Betreiber Kritischer Infrastrukturen (KRITIS)** sollten die Gefahren der IT-technischen Angreifbarkeit durch verbotenes Durchsuchen von Dumps und Logs nach Sicherheitsdetails sehr ernst nehmen. Zweifelsohne stehen die Bereiche Finanzen, Behörden, Gesundheit, Energie, Entsorgung, Nahrung, Öffentliche Sicherheit, Verkehr, Information und Kommunikation im besonderen Fokus der Aggressoren. Das deutsche IT-Sicherheitsgesetz IT-SiG 2.0 von 2021/2023 verpflichtet KRITIS-Betreiber zu technischen und organisatorischen Maßnahmen für die Sicherung ihrer IT-Systeme.

### SF-SAFEDUMP UNTERSTÜTZT DIE GESCHÄFTSLEITUNG

SF-SafeDump bietet die auditierbare, hersteller- und produktübergreifende, lokale Anonymisierung von Protokoll- und Diagnose-Daten. Der Arbeitsaufwand ist dank maximaler Automation im IT-Alltag für alle Beteiligten minimal.

SF-SafeDump erbringt für Ihr Unternehmen die formellen Entlastungsnachweise, beinhaltet die notwendigen Compliance-Monitoring-Funktionen und birgt keine versteckten Risiken, wie z.B. eine Cloud-Lösung, etc. (siehe S. 4).

# Ihr Schutz gegen unerlaubten Datenabfluss, DSGVO- und Sicherheits-Verletzung

## DIE AUDITIERBARE ANONYMISIERUNG VON IT-DIAGNOSE-DATEN BIETET IHNEN:

- ✓ IT-Sicherheit und Datenschutz für Diagnose-Daten, wie durch **DSGVO und Schrems II** gefordert
- ✓ **Lokale Anonymisierung** sensibler, personenbezogener Daten in Dumps und Logs
- ✓ Verhinderung von Data Leakage durch **Eliminierung des Datenlecks** IT-Diagnose-Datei
- ✓ **Vermeidung von DSGVO- und BDSG-Verletzungen und Bußgelder** durch unerlaubte Übermittlung sensibler Daten
- ✓ **Korrekte Auftragsverarbeitungen mit den Herstellern** durch Verhinderung von Datenabflüssen und Erfüllung der Anforderungen gemäß EuGH-Entscheidung Schrems II
- ✓ **Problemfreies Dump- und Log-File-Handling mit den IT-Dienstleistern.** Die Diagnose-Daten können wie gewohnt komprimiert, verschlüsselt, übertragen, verwaltet und analysiert werden.
- ✓ Anonymisierung von **IT-Diagnose-Datenformate**, wie u.a. Dump-, Log-, Trace-, XML- und JSON-Dateien, einschließlich Diagnose-Container- und Event-Log-Dateien
- ✓ **Herstellerunabhängiges und plattformübergreifendes Verfahren:** Unterstützung aller gängigen IT-Plattformen und deren Derivate, wie Windows, Unix, Linux (in Planung), Sun Solaris, z/OS, z/Linux, AIX, u.v.m., inklusive Container-Varianten – vom Laptop bis zum Server
- ✓ Anonymisierung auch von **sicherheitsrelevanten Informationen und Geschäftsgeheimnissen** in IT-Diagnose-Dateien
- ✓ Eine Lösung, die auch **Ihre IT-Dienstleister** für den sicheren Versand Ihrer IT-Diagnose-Daten nutzen sollten.
- ✓ Beitrag zur **Erfüllung der Obliegenheiten und Auflagen ihrer IT-Versicherung.** Vermeidung von Fahrlässigkeit oder Vorsatz im Hinblick auf Versicherungsschutz und Versicherungsleistung der Cyber-Versicherung.
- ✓ Datensicherheit auch beim **Inhouse-Zugriff** auf IT-Diagnose-Daten, wenn Entwickler Dumps und Logs der Produktionssysteme analysieren müssen.
- ✓ Unterstützung bei der Erfüllung der **Security- und Compliance-Verpflichtungen aus MITRE, PCI, NIST**, Bundesamt für Sicherheit in der Informationstechnik (BSI), Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI), Europäischer Datenschutzbeauftragter (EDSB) sowie SOX, EUROSOX, ISO, BASELII/III, SOLVENCYII, FERC, DOD und HIPAA
- ✓ Lösung für die Erfüllung des **Gesetzesparagraphen BSIG §5 des deutschen BSI-Gesetzes,** das den behördeninternen Umgang mit IT-Diagnose-Daten definiert. Automatisierte Pseudonymisierung ist hier das Mittel der Wahl für den Schutz personenbezogener Daten in Protokolldaten.
- ✓ Einhaltung des **deutschen IT-Sicherheitsgesetzes IT-SiG 2.0 von 2021/2023, das KRITIS-Betreiber** zu technischen und organisatorischen Maßnahmen für die Sicherung ihrer IT-Systeme verpflichtet.
- ✓ Einhaltung des **deutschen IT-Sicherheitsgesetzes IT-SiG 2.0 von 2021/2023, das KRITIS-Betreiber** zu technischen und organisatorischen Maßnahmen für die Sicherung ihrer IT-Systeme **verpflichtet**.
- ✓ Beitrag zur Umsetzung von **Sicherheitsarchitekturen** basierend auf Modellen wie **Zero Trust** von Forrester, CARTA (Continuous Adaptive Risk and Trust Assessment) und SASE von Gartner und CSF (Cybersecurity Framework) von NIST. So auch SD-WAN, SWG, CASB, ZTNA, FWaaS, MFA, IAM, PAM u.v.m.
- ✓ **Auditierbare Data-Compliance** durch Abdeckung des gesamten Life-Cycles des Diagnose-Dokuments: Monitoring - Anonymisierung - intensive Qualitätssicherung - Begleitdokumente. Kein Eigen-Risiko der Lösung (siehe S. 4).
- ✓ **Abteilungsübergreifende Compliance-Absicherung** und damit Entlastung für Geschäftsleitung, Revision, Risiko-Management, IT-Betrieb, IT-Sicherheit, IT-Einkauf und Datenschutz

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

**BUCHEN SIE UNVERBINDLICH EINE ONLINE-PRÄSENTATION**
www.enterprise-it-security.com/sf-safedump-praesentation-ch

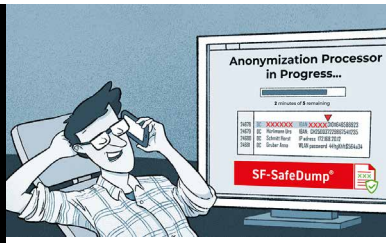
**SF-SafeDump®**

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)**
**info@enterprise-it-security.com**
**www.enterprise-it-security.com**




Anonymisierung für Sicherheit und Datenschutz im IT-Betrieb