WHITEPAPER

Sicherheitsrisiko durch datenschutzwidrigen Abfluss sensibler Daten und Geschäftsgeheimnisse im IT-Betrieb

Wichtige Terminsache fürs:
->IT-Sicherheit (S. 3)
->IT-Betrieb (S. 6)
->Risiko-Management (S. 8)
->Revision (S. 9)
->Datenschutz (S. 10)
->Geschäftsleitung (S. 11)

Der chinesische Hack des Microsoft Master Keys aus einem Crash-Dump hat alle alarmiert

VERLASSEN SICHERHEITS-, PERSONEN-, FINANZ- UND SOZIALDATEN AUCH IHRE FIRMA UNBEMERKT?

Wer denkt bei IT-Diagnose-Daten an die **ständige Gefahr des unkontrollierten Datenabflusses** und die daraus resultierenden Sicherheitsrisiken und Datenschutzverletzungen? Selbst der IT-Betrieb ist sich dieser Bedrohung meist nicht bewusst. Bei Microsoft sorgte der Angriff von Storm-0558 durch einen gestohlenen Schlüssel, extrahiert aus einem Crash-Dump, für ein gravierendes Sicherheitsproblem (siehe Seite 3).

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.**

DATENABFLUSS ÜBER DUMP- UND LOG-FILES – 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 die Schweiz** 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**.

SICHERHEIT FÜR SENSIBLE DATEN DURCH ANONYMISIERUNG

IT-Leiter und Sicherheitsbeauftragte verantworten neben der IT-Sicherheit auch den Schutz der Unternehmensdaten. Ihnen verschafft die Anonymisierungslösung SF-SafeDump eine auditierbare Entlastung im Hinblick auf das neue Datenschutzgesetz und die Security-Compliance. Sie anonymisiert alle Datenformate im Sinne des Artikels 6 Abs. 4 revDSG bei gleichzeitigem Erhalt ihrer technischen Aussagekraft.

So werden Herstellern nur diejenigen Daten bereitgestellt, die für die Fehler-Analyse und -Beseitigung notwendig sind. Alle schutzbedürftigen, nicht-technischen Daten werden automatisch anonymisiert. Dazu zählen **Personendaten, 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 Haus 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 7.

CYBER-RISK- UND DATENSCHUTZ-VERSICHERUNG – SCHUTZ NICHT VERLIEREN!

Dumps, Logs und Traces bieten vielfältige Möglichkeiten für Angriffe auf IT-Sicherheit und Datenschutz. Diese können zu Obliegenheitsverletzungen und Deckungseinwendungen der Cyberversicherung führen. Anonymisierung von IT-Diagnose-Daten reduziert das Risiko von Cybercrime und Verlust des Versicherungsschutzes.

Die Schweiz macht ihre sensiblen Daten sicher - Ab 01.09.2023 verschärftes Datenschutzgesetz

LEITER IT UND SICHERHEITS-VERANTWORTLICHE IN PERSÖNLICHER VERANTWORTUNG

Die Revision des Schweizer Datenschutzgesetzes (revDSG) führt zu Verschärfungen der Pflichten und Risiken im Umgang mit Personendaten. Das revidierte Gesetz orientiert sich an der DSGVO und ist am 01.09.2023 in Kraft getreten. Betroffen sind Unternehmen mit Sitz in der Schweiz sowie im Ausland, wenn sich deren Personendaten-Bearbeitung in der Schweiz auswirkt.

Auch in der **Cyberrisikenverordnung der Bundesverwaltung (CYRV)** ist unrechtmässiges Daten-Handling als **Cybervorfall** geregelt: „unbeabsichtigtes oder von Unbefugten beabsichtigtes Ereignis, das dazu führt, dass die Vertraulichkeit, Integrität, Verfügbarkeit oder Nachvollziehbarkeit von Daten beeinträchtigt ist oder es zu Funktionsstörungen kommen kann" (Art. 3 CYRV). Da mit Diagnose-Dokumenten auch sicherheitskritische Details über die IT-Systeme das Unternehmen verlassen, sind Dumps und Logs auch ein Cyber-Risk-Thema. Das verbietet eine Cloud-Lösung.

Die **persönliche Haftung der Verantwortlichen** führt zu einer hohen Aufmerksamkeit für das Thema. Im 8. Kapitel „Strafbestimmungen", Artikel 60 bis 66 des Bundesgesetzes über den Datenschutz, werden **Bussen bis zu 250 000 Franken** für eine Gesetzesübertretung veranschlagt.

Es handelt sich um strafrechtlich verhängte, persönliche Bussen für die verantwortlichen Mitarbeitenden. Sie dürfen weder vom Unternehmen noch von einer Versicherung beglichen werden.

Die Informatik sollte die **Gewährleistung der Datensicherheit**, wie sie in **Art. 8, Absatz 1 revDSG** gesetzlich gefordert werden, unterstützen: „Der Verantwortliche und der Auftragsbearbeiter gewährleisten durch geeignete technische und organisatorische Massnahmen eine dem Risiko angemessene Datensicherheit."

Eine hohe Priorität gilt der Umsetzung folgender **Datenschutzgrundsätze: Recht- und Verhältnismässigkeit sowie Zweckgebundenheit.** Die Speicherung und Bearbeitung von Personendaten muss also auf das für den Verwendungszweck nötige Mindestmass begrenzt und damit frei von Überhängen sein. Sie muss verhältnismässig sein. Auf Personendaten in Diagnose-Dateien trifft dies in keinem Fall zu. Mögliche Lösungen sind, laut Artikel 6 Abs. 4 revDSG, **Anonymisierung oder Vernichtung von Daten.**

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 Mitarbeitenden und Technologiepartnern? Auch für diese Überhänge haften Sie mit. Sie stehen potentiell in der Rückgriffshaftung.

> **Sanktionen:** Natürliche Personen können bei vorsätzlicher Verletzung der Informations- und Auskunftspflichten sowie der Sorgfaltspflichten neu mit Busse bis CHF 250'000 bestraft werden. Ausreichend ist der Eventualvorsatz, weshalb die Strafbarkeit bereits gegeben ist, wenn eine tatsächlich eingetretene Verletzung in Kauf genommen wurde. Dies führt dazu, dass – im Gegensatz zur DSGVO bei der lediglich Unternehmen oder Organisationen im Fokus stehen – nach dem revidierten DSG Verantwortliche im Unternehmen wie CEOs, CIOs oder andere Funktionen direkt sanktioniert werden können. Die Zuständigkeit liegt dabei bei den kantonalen Staatsanwaltschaften."
>
> Quelle: Reto Fanger, Rechtsanwalt und Gründer Advokatur Fanger: Das ist neu am revidierten Schweizer Datenschutzgesetz, in: netzwoche.ch, 17.12.2020 - 08:00 Uhr

SECURITY BREACH BEI MICROSOFT
USA – MAI 2023

Aus Crash-Dump Master-Key von Microsoft gestohlen – Chinesische Hacker Zugriff auf US-Behörden-Emails

IT-DIAGNOSE-DATEN SIND EIN GEFÄHRLICHES IT-SICHERHEITS-RISIKO!

Sicherheitskritische Informationen über die eigenen IT-Systeme wie zum Beispiel Keys, Passwörter oder Zertifikate gelangen bei einem Crash in den Dump. Werden diese sensiblen Daten nicht anonymisiert, sind sie eine wertvolle Beute für Hacker und für alle, die Zugang zu den IT-Diagnose-Daten haben. Sie können für einen gezielten Angriff genutzt werden, wie etwa bei Microsoft im Mai 2023 geschehen. Chinesische Hacker des Storm-0558 haben einen Microsoft Master Key aus einem Crash Dump entwendet. Damit konnten sie u.a. Outlook-Konten hacken und US-Behörden ausspionieren.

So analysierte Microsoft die Cyber-Attacke in seinem Blog am 06.09.2023:

RESULTS OF MAJOR TECHNICAL INVESTIGATIONS FOR STORM-0558 KEY ACQUISITION

MSRC / By MSRC / September 06, 2023 / 3 min read Microsoft On July 11, 2023

https://msrc.microsoft.com/blog/2023/09/results-of-major-technical-investigations-for-storm-0558-key-acquisition/

„Our investigation found that a consumer signing system crash in April of 2021 resulted in a snapshot of the crashed process ("crash dump"). The crash dumps, which redact sensitive information, should not include the signing key. In this case, a race condition allowed the key to be present in the crash dump (this issue has been corrected). The key material's presence in the crash dump was not detected by our systems (this issue has been corrected).

We found that this crash dump, believed at the time not to contain key material, was subsequently moved from the isolated production network into our debugging environment on the internet connected corporate network. This is consistent with our standard debugging processes. Our credential scanning methods did not detect its presence (this issue has been corrected)."

netzwoche news berichtet über den Schlüssel-Diebstahl am 11.09.2023 – 10:00 Uhr: "Masterkey" für Microsoft Cloud

UPDATE: GESTOHLENER MICROSOFT-KEY STAMMT AUS WINDOWS-CRASH-DUMP

Eine Hackergruppe aus China hat mutmasslich während einem Monat auf diverse E-Mail-Konten der US-amerikanischen Bundesverwaltung zugreifen können. Der gestohlene "Masterkey" stammt wohl aus einem Crash-Dump.

https://www.netzwoche.ch/news/2023-07-25/update-gestohlener-microsoft-key-ist-maechtiger-als-angenommen

IT-SICHERHEIT

Sicherheitskritische Informationen in IT-Diagnose-Daten machen Sie verwundbar

IT-Diagnose-Daten wie Dumps, Logs und Traces enthalten als Momentaufnahme des Systems neben Personendaten **auch hochgradig 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

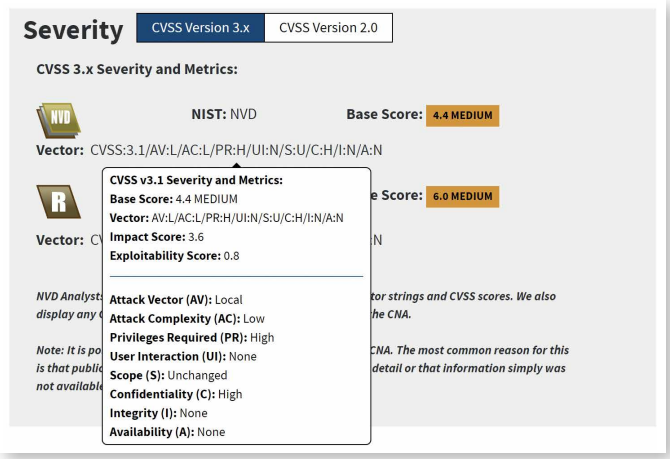
- Etablieren Sie einen regelmässigen gemeinsamen Dialog mit dem IT-Betrieb, dem Datenschutz und der Revision.
- Legen Sie gemeinsam fest, welche Informationen über die IT-Infrastruktur und deren Konfiguration für Aussenstehende nicht einsehbar sein dürfen. Dies reicht von IP-Adressen, über Details eingesetzter 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 Personendaten, sondern auch auf sicherheitstechnische Details. SF-SafeDump **unterstützt Ihre Compliance** gegenüber MITRE, PCI NIST, dem Bundesamt für Informatik und Telekommunikation BIT, dem Nationalen Zentrum für Cybersicherheit (NCSC) 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

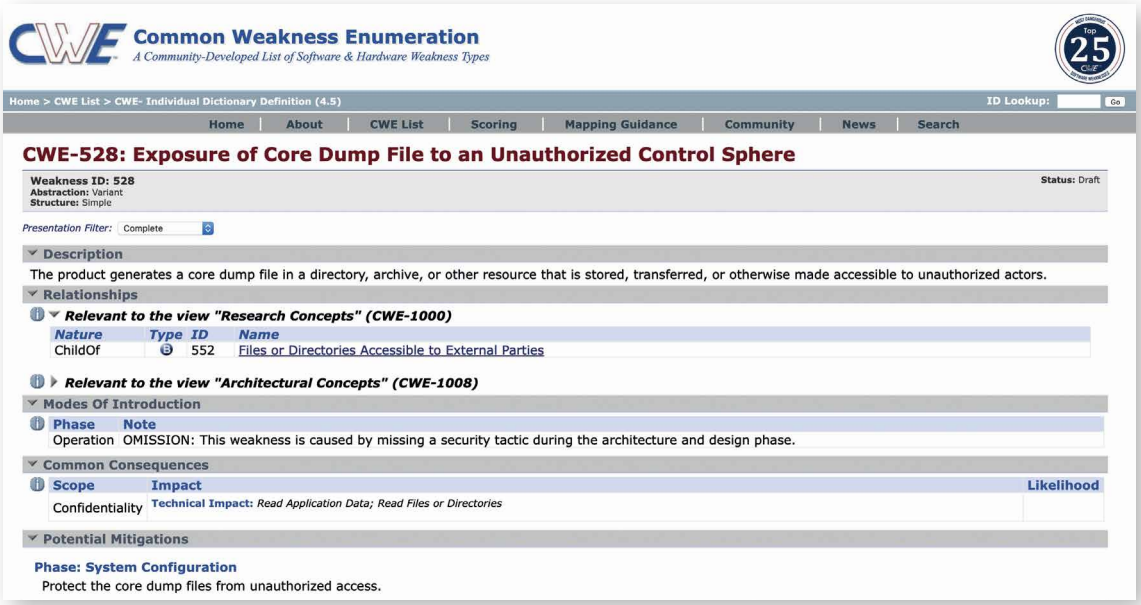


nvd.nist.gov/vuln/detail/CVE-2021-23211

„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-SiG 2.0 2021/2023 NIS2 (ab Oktober 2024)
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)

IT-BETRIEB

Verhindern Sie durch Anonymisierung den Abfluss sensibler Daten via Dumps, Logs und Traces

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

IHR ANONYMISIERUNGSPROZESS SOLLTE LOKAL, AUDITIERBAR UND QUALITÄTSGESICHERT SEIN

Achten Sie streng darauf, dass sämtliche Diagnose-Dokumentenformate einer Anonymisierung unterzogen werden, nicht nur Dumps, sondern auch Logs, Json-Files u.v.m. Für eine auditierbare Qualitätssicherung muss ein wiederholter Scan erfolgen. Es müssen entlastende Begleitdokumente erstellt werden. **Viele Hersteller-Tools oder Cloud-Lösungen scheiden dadurch aus** und stellen selbst ein Risiko für Ihre Entlastung dar (siehe S. 7).

Verhindern Sie Sicherheits- und Datenschutz-Risiken!

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-Betriebs-Mitarbeitende risikofrei und selbständig seine eigenen Diagnose-Dokumente lokal anonymisieren. SF-SafeDump läuft hoch performant auf dem Laptop.

Monitoring und Begleitdokumente um das Entstehen und Bearbeiten von IT-Diagnose-Daten liefern einen **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, IT-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 6 Abs. 4 revDSG und Art. 3 CYRV handeln.

- Die **automatisierte, lokale Anonymisierung sämtlicher 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. 7), 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 bearbeiten können.

IHR ANONYMISIERUNGSPROZESS DARF SELBST KEIN DATENSCHUTZRISIKO SEIN!

KEIN TOOL MIT PRODUKTIONSDATENBANK-ZUGRIFF!

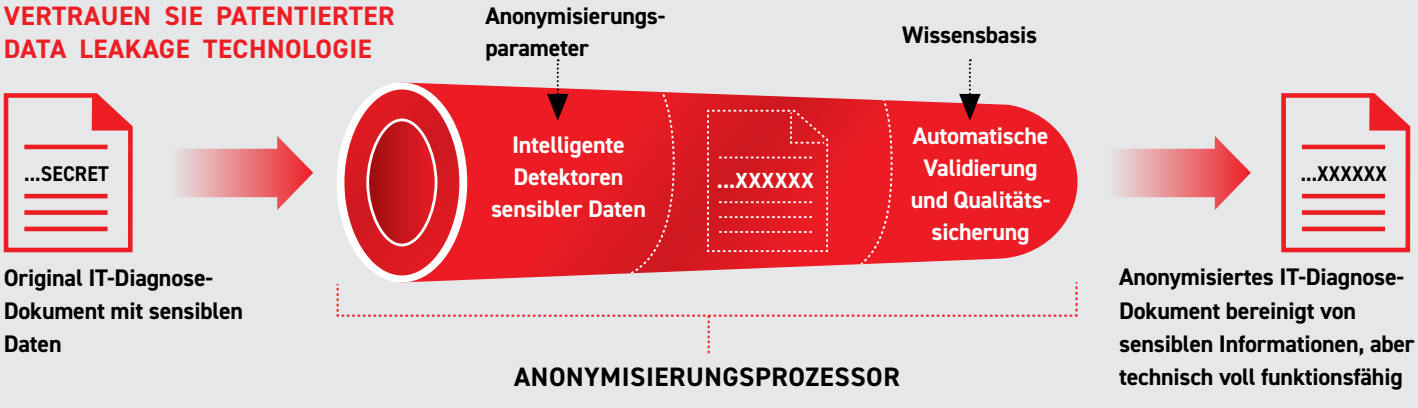
Eine sehr **wichtige Anforderung** an die implementierte Anonymisierungslösung ist folgende: Sie muss eigenständig alle relevanten Datentypen finden und darf nicht selbst ein Datenschutzrisiko darstellen. Die technischen Anonymisierungsprozesse sollten zum Beispiel **nicht vom direkten Zugriffsrecht 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 Mitarbeitenden 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 Auftragsbearbeitung 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 Bearbeitungsstufen 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



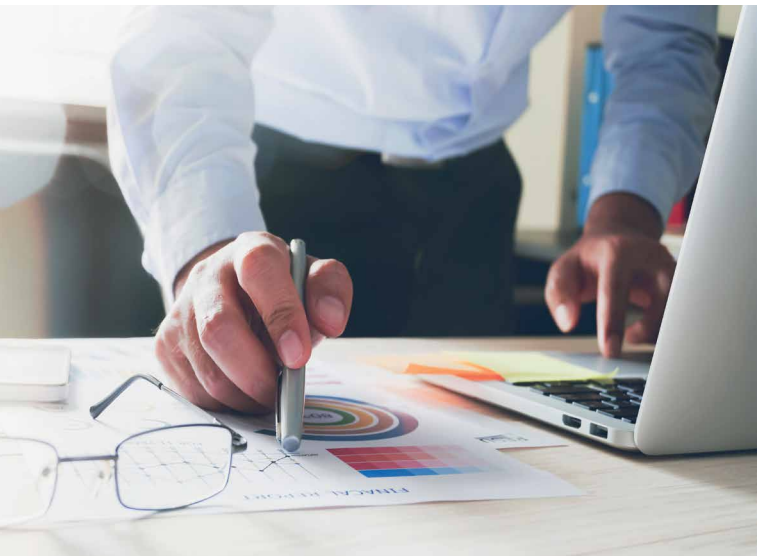
RISIKO-MANAGEMENT

Evaluieren Sie das Sicherheits- und Unternehmens-Risiko unterlassener Anonymisierung von Dumps, Logs & Traces

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.** Das geschätzte Risiko-Volumen liegt in Deutschland z.B. bei 5 Mio. IT-Diagnose-Dateien pro Jahr. Es berechnet sich aus 100 Uploads von IT-Diagnose-Dateien aus 50.000 Rechenzentren (nach Bitkom-Studie).

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. 7)!



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 Auftragsbearbeitung 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.

REVISION

Prüfen Sie ab sofort den Sicherheits- und DSG-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 Personendaten und sicherheitsrelevanten Informationen vor unerlaubter Weitergabe, Einsicht und Bearbeitung. 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 DSG-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. 7)

DATENSCHUTZ

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

Als Datenschutzverantwortlicher müssen 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 UND ZWECKFREI 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 Auftragsbearbeitungen 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 Zwischenbearbeitungs- und Weiterreichinstanzen, bis Dumps und Logs das Labor des Herstellers erreichen. Das Restrisiko und eine dafür mögliche **Rückgriffshaftung** steigt mit jeder weiteren involvierten Partei. Wenn Sie gemäss Art 6 Abs.4 revDSG personenbezogene Daten anonymisieren, reduzieren Sie das Risiko eines Datenschutzverstosses.

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. 7).
- 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. **Müssen 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 Mitarbeitender 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 sämtliche Diagnose-Datenformate und führt mit lokaler Anonymisierung zur **Vermeidung von Datenschutzverstössen.**

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 MITARBEITENDEN GEBOTEN

Es muss ausgeschlossen werden, dass Softwareentwickler und Applikationsverantwortliche bei Banken, Versicherungen oder Sozialdatenbearbeitern 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 Mitarbeitenden 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.

RISIKO FÜR IT-SICHERHEIT, CYBER- UND D&O-VERSICHERUNG

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. Prüfen Sie die Obliegenheiten Ihrer Cyber-Risk- und D&O-Versicherungen.

BEDEUTUNG FÜR KRITISCHE INFRASTRUKTUREN (KI)

Betreiber Kritischer Infrastrukturen (KI) müssen 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. Auf den Schutz dieser kritischen Infrastrukturen (KI) der Schweiz richtet sich die Nationale Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022.

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. 7).

Ihr Schutz gegen unerlaubten Datenabfluss, DSG- und Sicherheits-Verletzung

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

- ✓ IT-Sicherheit und Datenschutz für Diagnose-Daten, wie ihn die **DSG** fordert
- ✓ **Lokale Anonymisierung** sensibler, personenbezogener Daten in Dumps und Logs
- ✓ Verhinderung von Data Leakage durch **Eliminierung des Datenlecks** IT-Diagnose-Datei
- ✓ **Vermeidung von DSG- bzw. DSGVO-Verletzungen und Bussen** durch unerlaubte Übermittlung sensibler Daten
- ✓ **Juristische Absicherung der Auftragsbearbeitungen** mit den Herstellern durch Verhinderung gesetzeswidriger Datenabflüsse
- ✓ **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
- ✓ Datensicherheit auch beim **Inhouse-Zugriff** auf IT-Diagnose-Daten, wenn Entwickler Dumps und Logs der Produktionssysteme analysieren müssen.
- ✓ Beitrag zur **Erfüllung der Obliegenheiten und Auflagen ihrer IT-Versicherung.** Vermeidung von Fahrlässigkeit oder Vorsatz im Hinblick auf Versicherungsschutz und Versicherungsleistung der Cyber-Versicherung.
- ✓ Unterstützung bei der **Erfüllung der Security- und Compliance-Verpflichtungen aus MITRE, PCI, NIST**, dem Bundesamt für Informatik und Telekommunikation BIT, dem Nationalen Zentrum für Cybersicherheit (NCSC) sowie SOX, EUROSOX, ISO, BASELII/III, SOLVENCYII, FERC, DOD und HIPAA
- ✓ Lösung zur Handhabung von **personenbezogenen Randdaten in Protokolldateien gemäß Art. 57** des Regierungs- und Verwaltungsorganisationsgesetzes **(RVOG)**.
- ✓ Schutz der **kritischen Infrastrukturen (KI)** der Schweiz, wie von der **Nationalen Strategie zum Schutz der Schweiz vor Cyber-Risiken (NCS) 2018–2022** gefordert.
- ✓ 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. 7).
- ✓ Abteilungsübergreifende Compliance-Absicherung und damit Entlastung für Geschäftsleitung, Revision, Risiko-Management, IT-Betrieb, IT-Sicherheit, IT-Einkauf und Datenschutz

Anonymisierung sensibler Daten in IT-Diagnose-Dateien – Stoppt das Datenschutz-Risiko im IT-Betrieb

Video hier direkt ansehen

https://www.enterprise-it-security.com/info-video-de/Hei

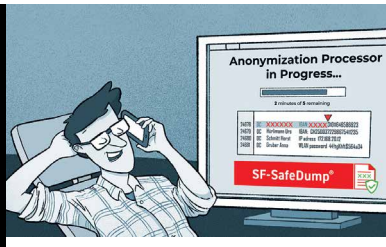
SF-SafeDump®

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