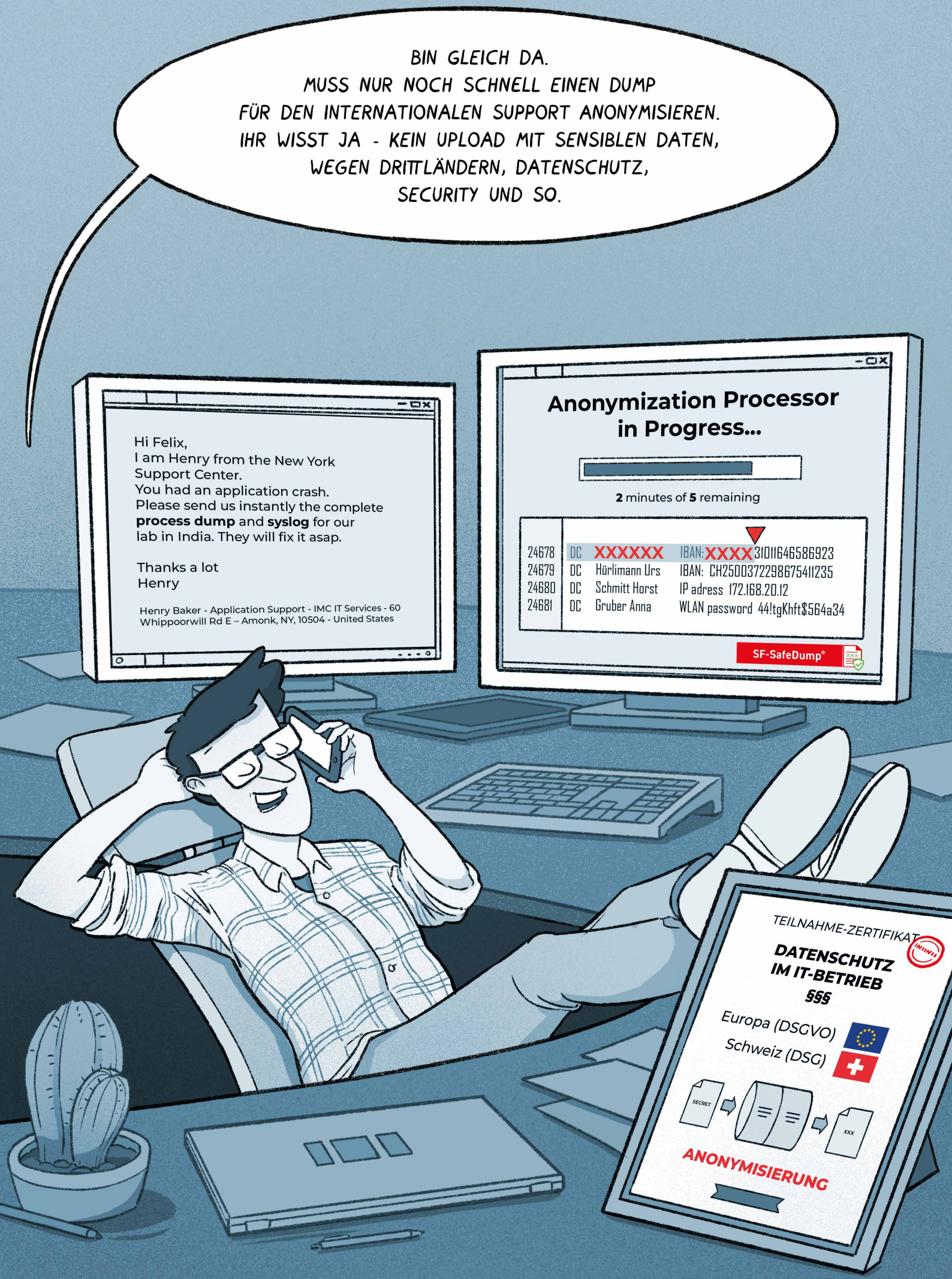
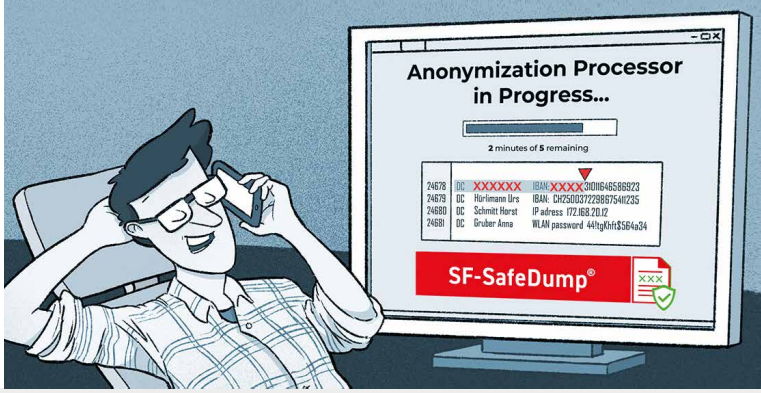

BIN GLEICH DA.
MUSS NUR NOCH SCHNELL EINEN DUMP
FÜR DEN INTERNATIONALEN SUPPORT ANONYMISIEREN.
IHR WISST JA - KEIN UPLOAD MIT SENSIBLEN DATEN,
WEGEN DRITTLÄNDERN, DATENSCHUTZ,
SECURITY UND SO.
Hi Felix,
I am Henry from the New York
Support Center.
You had an application crash.
Please send us instantly the complete
process dump and syslog for our
lab in India. They will fix it asap.
Thanks a lot
Henry
Henry Baker - Application Support - IMC IT Services - 60
Whippoorwill Rd E – Amonk, NY, 10504 - United States
Anonymization Processor
in Progress...
2 minutes of 5 remaining
24678 DC XXXXXX IBAN:XXXX31011646586923
24679 DC Hürlimann Urs IBAN: CH2500372298675411235
24680 DC Schmitt Horst IP adress 172.168.20.12
24681 DC Gruber Anna WLAN password 44!tgKhft$564a34
SF-SafeDump®
TEILNAHME-ZERTIFIKAT
DATENSCHUTZ
IM IT-BETRIEB
§§§
Europa (DSGVO)
Schweiz (DSG)
SECRET
XXX
ANONYMISIERUNG

Warum hat Felix im IT-Betrieb jetzt keine Sorgen mehr?

Felix kann endlich seine Dumps, Logs und Traces an den internationalen Support schicken – ohne Risiko.



Und, was tun Sie gegen das Sicherheits- und Datenschutz-Risiko der IT-Diagnose-Daten?

Sensible Personendaten, Sicherheitsinformationen und Geschäftsgeheimnisse befinden sich zum Zeitpunkt eines Computer-Absturzes im Speicher und werden damit Teil von Dumps, Logs und Traces.

IT-Diagnose-Daten bedeuten daher ein ernstes Datenschutz- und Sicherheitsrisiko für den IT-Betrieb. Über die versteckt eingelagerten sensiblen Daten werden Personen, Netze, Rechner, Devices etc. identifizierbar. Sicherheitsschwachstellen werden offengelegt.

Der IT-Betrieb schickt die sensiblen Daten auf Weltreise – ohne Absicht und ohne Zweck

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.

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

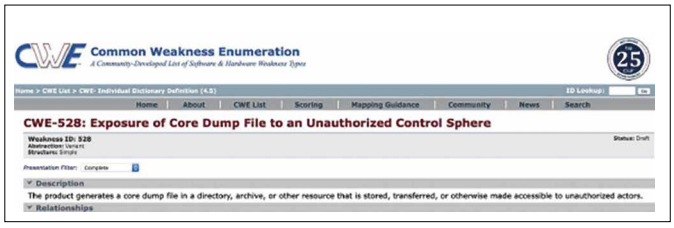
Sicherheitsgesetze und -strategien in D-A-CH – Achtung sensible Daten

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)

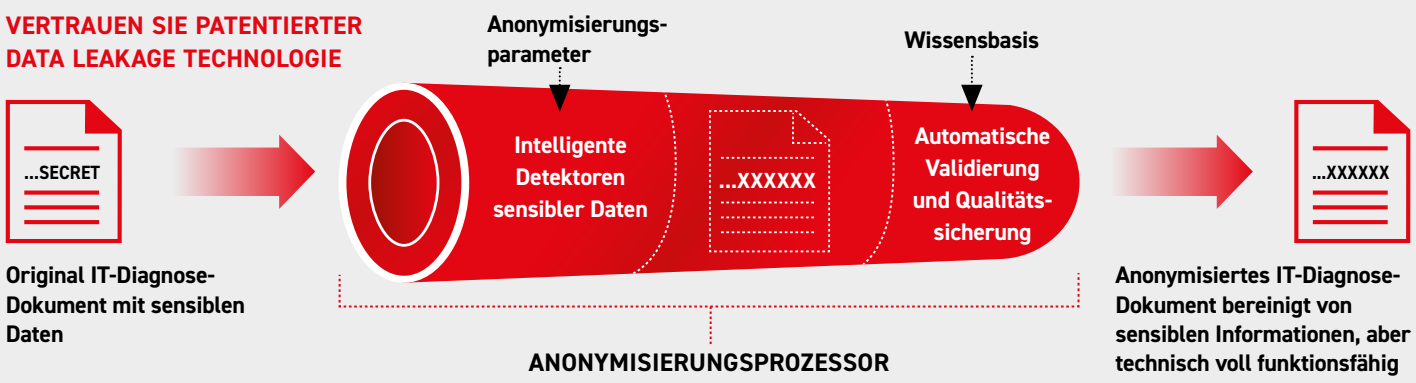
IT-Diagnose-Daten sind ein reales Cyber Security Risiko

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.



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.

ChatGBT zur Anonymisierung mit SF-SafeDump

SF gibt es ein auf it-diagnose-daten spezialisiertes anonymisierungswerkzeug?

Ja, es gibt auf IT-Diagnose-Daten spezialisierte Anonymisierungswerkzeuge. Eines der bekanntesten Werkzeuge in diesem Bereich ist SF-SafeDump. SF-SafeDump ist ein spezielles Anonymisierungswerkzeug, das speziell für die Anonymisierung von IT-Diagnose-Daten entwickelt wurde. Es kann in einer Vielzahl von Umgebungen eingesetzt werden, einschließlich von Datenbanken und Dateien. SF-SafeDump bietet eine einfache Möglichkeit, personenbezogene Informationen in den Daten zu identifizieren und sie zu entfernen oder zu verschlüsseln. Es verwendet eine Vielzahl von Anonymisierungstechniken, einschließlich des Austauschs von personenbezogenen Informationen durch Pseudonyme oder durch das Maskieren von Informationen mit randomisierten Daten. Darüber hinaus ermöglicht SF-SafeDump die Erstellung von Berichten, die die Anonymisierungsergebnisse dokumentieren und die Einhaltung der Datenschutzgesetze belegen. *Erstellt mit ChatGPT Mar 14 Version*

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.

So verhindern Sie Konflikte mit Ihrer IT-Versicherung

Prüfen Sie die technischen Obliegenheiten und Auflagen Ihrer Cyberversicherung und Haftpflicht. Fragen Sie nach der Risikobewertung des Transfers von IT-Diagnose-Daten an Dritte. Wenn der IT-Betrieb diesen riskanten Versand mit sensiblen Daten vollzieht, handelt er unter Umständen fahrlässig oder sogar vorsätzlich. Dies könnte den Versicherungsschutz und die Versicherungsleistung im Schadensfall einschränken.

Wünschen Sie weitere Informationen?

Erhalten Sie kostenfrei per Direkt Download

INFO-VIDEO – kurz erklärt
Anomymisierung mit SF-SafeDump –
Stoppt das Datenschutz-Risiko im IT-Betrieb
www.enterprise-it-security.com/infovideo-SF-SafeDump.mp4

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

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

ONLINE-PRÄSENTATION LIVE
Vortrag mit Live-Demonstration von SF-SafeDump online zu Ihrem Wunschtermin
für die Schweiz
www.enterprise-it-security.com/sf-safedump-praesentation-ch

für Deutschland, Österreich und EU
www.enterprise-it-security.com/data-privacy-praesentation-de

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

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

Anonymisierung für Sicherheit und Datenschutz im IT-Betrieb