OTRS Group

Resilienzsteigerung durch Nutzung von SaaS

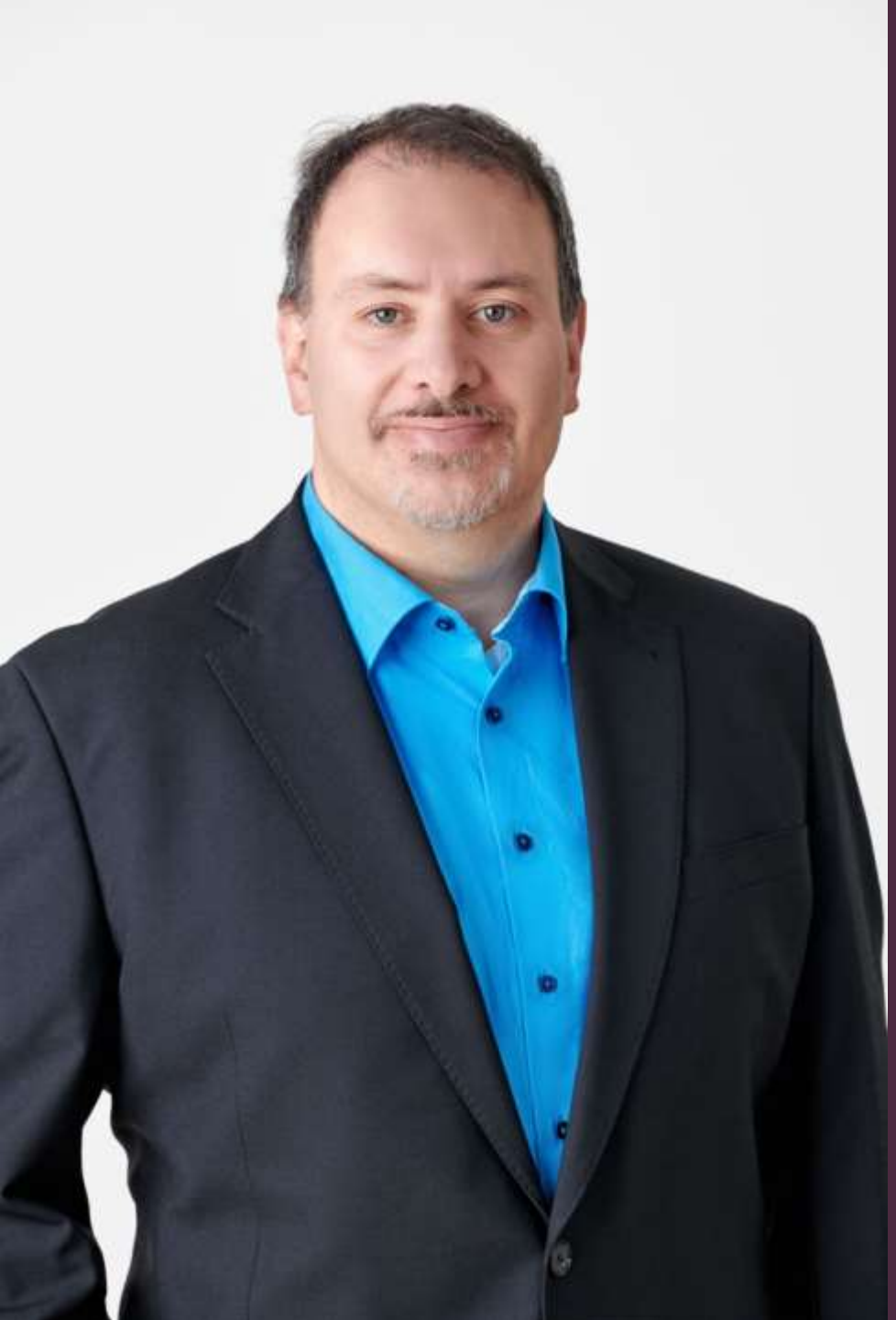
Jens Bothe
Vice President Information Security

STORM
powered by OTRS

Agenda

- Vita Jens O. Bothe
- Daten & Fakten OTRS Group
- Was versteht man unter…
- Resilienzsteigerung durch Nutzung von SaaS

STORM
powered by OTRS



Vita Jens O. Bothe

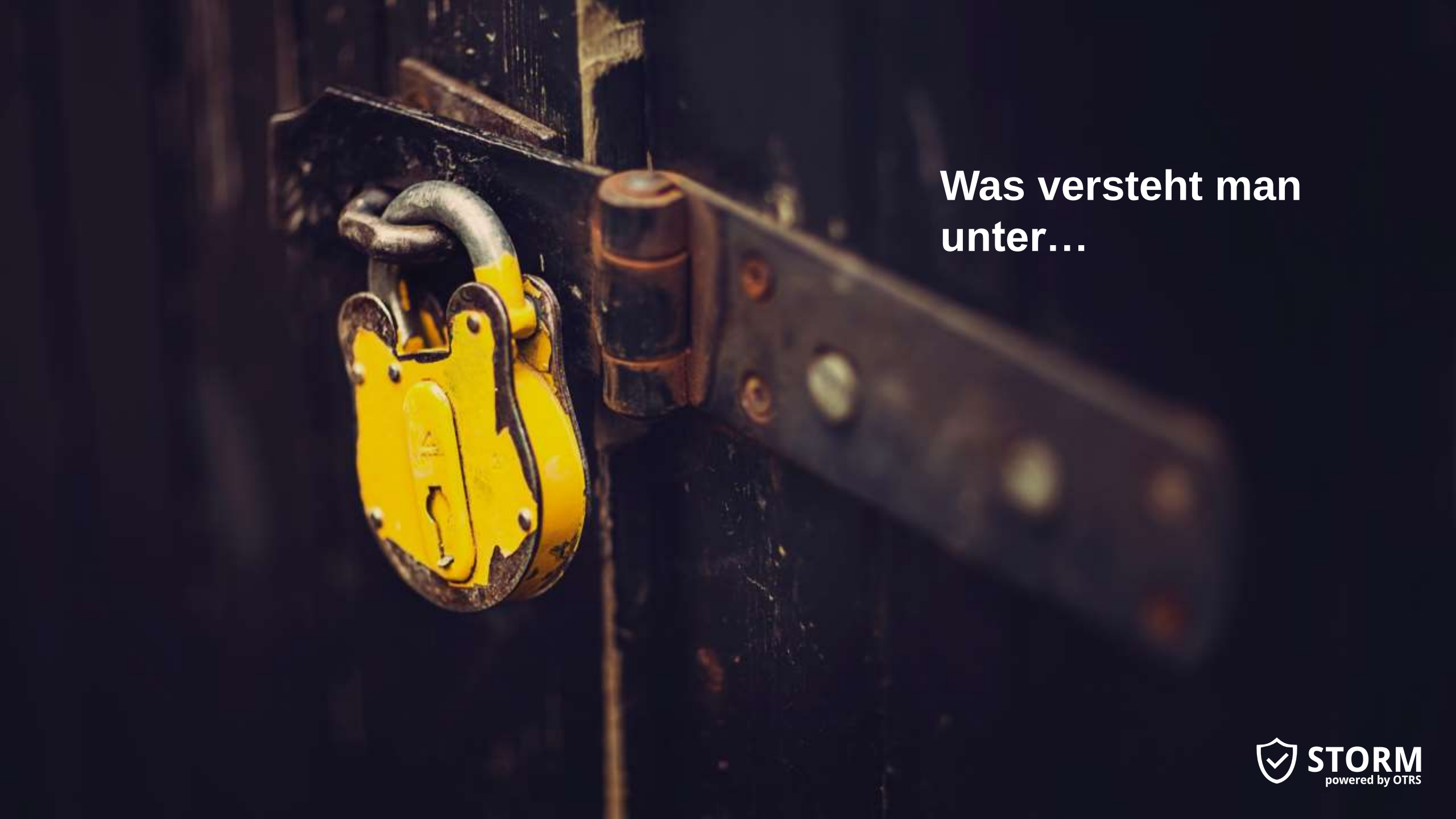
- Seit 2003 OTRS Anwender im Sicherheitsumfeld
  - Abusehandling
  - Schwachstellenmanagement
- Seit 2006 bei der OTRS AG
  - Betreuung der CERTs und Kunden aus dem Sicherheitsumfeld
  - Product Owner „**STORM** powered by **OTRS**“
  - Zuständig für die Informationssicherheit bei der OTRS Group
  - Leitung des OTRS PSIRT

Daten & Fakten
OTRS Group

2003	Deutschland	6	~111	> 11,8 Mio. €*
Gründung	Zentrale	Töchter	Mitarbeiter	Umsatz

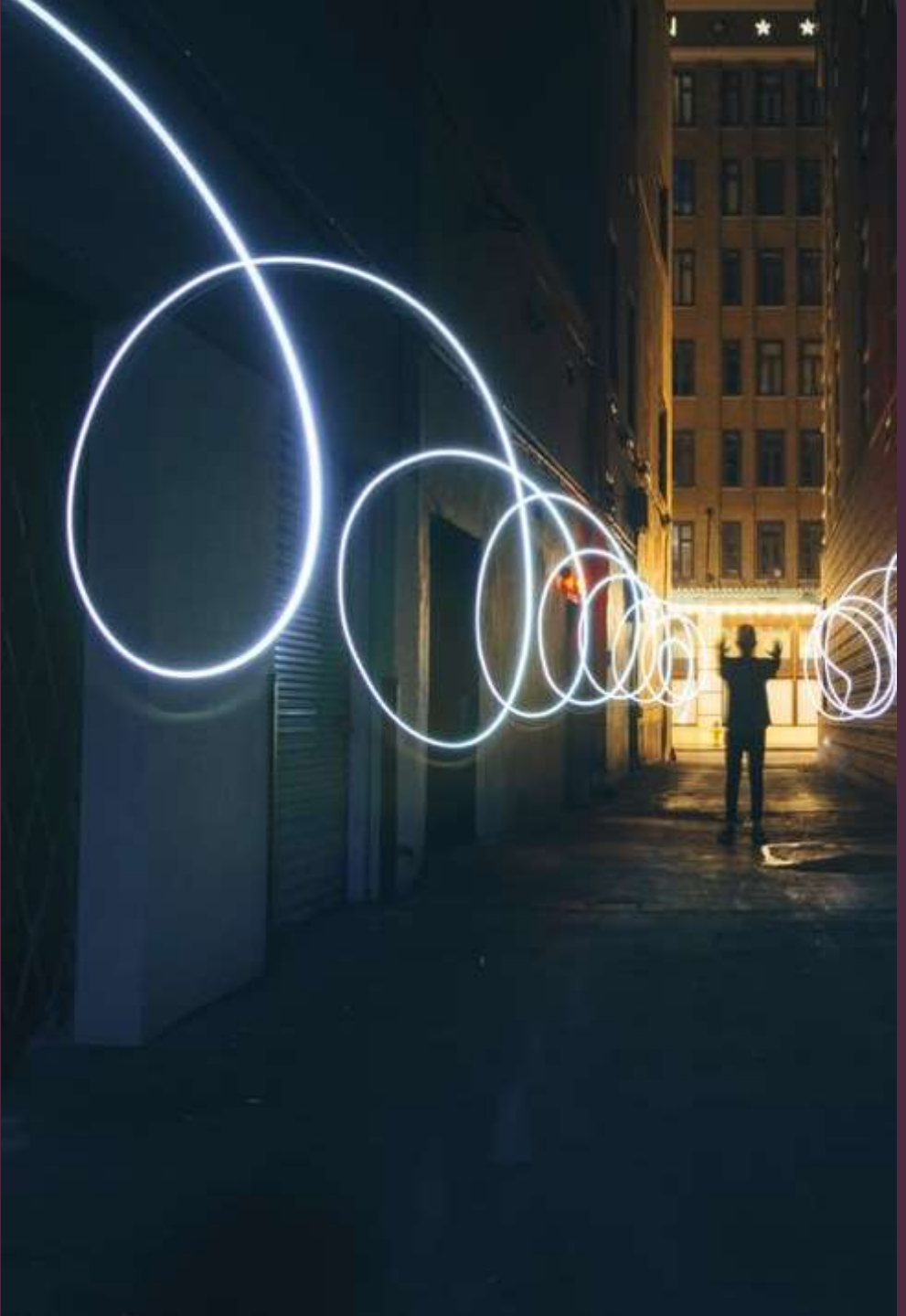
STORM
powered by OTRS

*Stand 2022



Was versteht man unter…

STORM
powered by OTRS

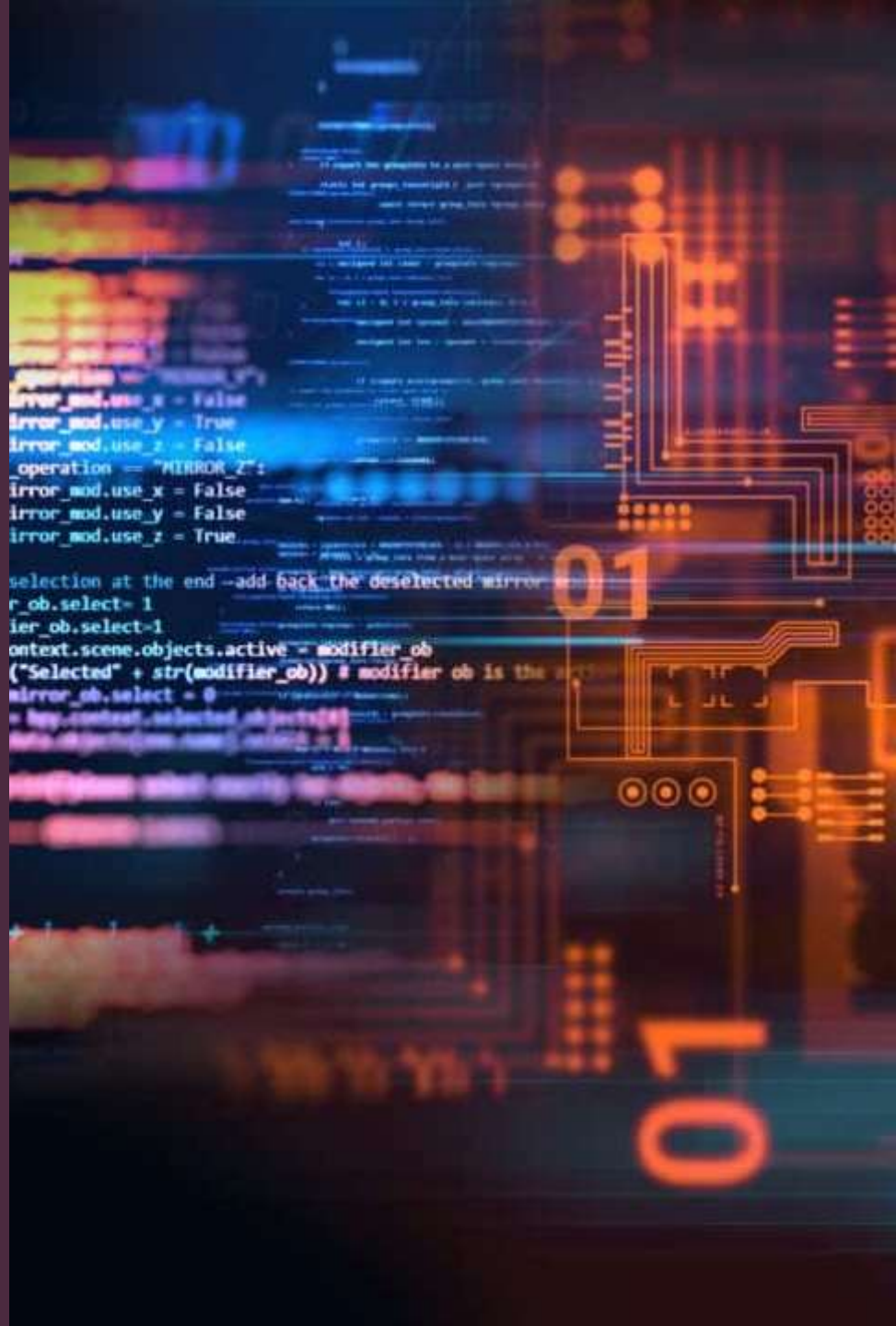


Resilienz
(lat. resiliare)

Die Fähigkeit eines Systems, nach einem Ausfall, einer Störung oder einem unerwarteten Vorfall in kurzer Zeit wieder in seinen normalen Betriebszustand zurückzukehren oder einen akzeptablen Betrieb aufrechtzuerhalten.

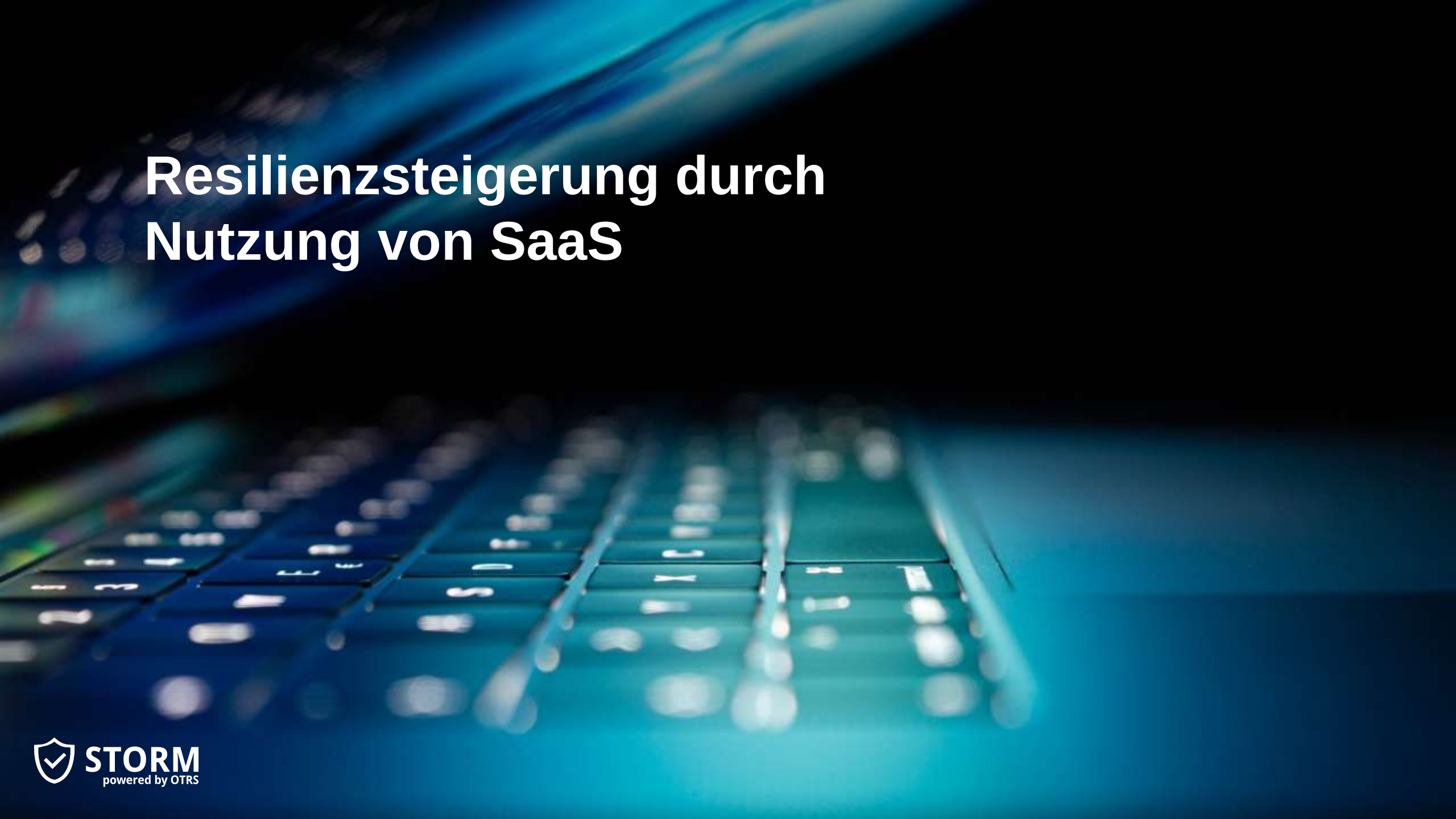
Software as a Service (SaaS)

Anwendungen, die durch einen Provider als Service bereitgestellt und deren Funktionalitäten z. B. über den Web Browser durch den Kunden genutzt werden.



STORM
powered by OTRS

Resilienzsteigerung durch Nutzung von SaaS



STORM
powered by OTRS

Auswirkungen

- Ransomware-Attacke auf IT-Systeme eines OTRS On-Premise-Anwenders sorgte für wochenlangen Ausfall
- Services mussten neu implementiert werden, um Funktionalität wiederherzustellen
- ca. halbes Jahr später noch immer nicht alle historischen Daten verfügbar, Maßnahmen laufen weiter

SaaS als Fels in der Brandung

- OTRS SaaS-Anwender durch Ransomware-Attacke handlungsunfähig, da sämtliche Rechner und Server betroffen
- OTRS SaaS-System für ITSM lief unabhängig weiter, nach Deaktivierung der LDAP-Anbindung mit systembasierten Accounts voll nutzbar
- kurzfristige Erhöhung der Lizenzen und Systemressourcen, um Wiederherstellung des IT-Betriebes zu ermöglichen, z. B. Beschaffung und Installation neuer Rechner und Kommunikation mit internen Kunden

Vorbereitende Maßnahmen

- Festlegen der kritischen Services und Prüfung, ob als SaaS nutzbar
- Auswahl der passenden Vertragslevel, die zur tatsächlichen Nutzung passen (z. B. Service- und Reaktionszeiten)
- Erstellung eines Notfallplans unter Berücksichtigung der gesamten Infrastruktur inkl. SaaS-Systemen und Schnittstellen
  - Definition von SOP für bestimmte Ereignisse
  - Kontaktdaten, z. B. für den Support des Anbieters, redundant speichern
- Vorbereitete „Schatten“-IT
  - Stand-alone Notebooks, die nicht im Netz registriert sind, BYOD
  - Mobiltelefone
  - Alternative Kommunikationsmöglichkeiten via E-Mail, Chat und Online Meetings

Im Falle eines Vorfalls

- Kappung bestehender Verbindungen zwischen SaaS-System und betroffener Infrastruktur
- Aktivierung der systemeigenen Authentifizierung und Vergabe neuer Passwörter durch „Passwort vergessen“ Funktionalität
- Aktivierung der Fallback E-Mail-Adressen z. B. via Free Mail Provider
- Falls notwendig, Skalierung des Systems beauftragen
- Offene Kommunikation mit dem Dienstleister über den Vorfall

Zurück zum Alltag

- Nach Wiederherstellung einzelner Dienste
  - Prüfung, ob Backup-Verbindungen wieder zurückgebaut werden können und Rückbau dieser
  - Prüfung des System-Sizings
- Lessons Learned
  - Welche Dienste sollten ggf. anders aufgestellt werden?
  - Anpassungen von Dienstleistungen durch SaaS-Anbieter

Checkliste

- Festlegung der zukünftigen SaaS-Strategie und -Anbieter
  - Bewertung des Risikos insbesondere größerer Anbieter bzgl. Schwachstellen und Auswirkung
- Erstellung des Notfallplanes
- Aufbau einer unabhängigen Schatten-IT für Notfälle
- Unabhängige Zahlungsmittel, z. B. Kreditkarten für den Kauf von IT-Geräten, vorhalten
- Notwendige Informationen redundant, offline und extern vorhalten und regelmäßig prüfen und aktualisieren
- Regelmäßiges Üben des Notfallplanes
- Schulung der Mitarbeiter

STORM
powered by OTRS

Fazit

Um die Resilienz der IT zu erhöhen, sollten Unternehmen in Erwägung ziehen, sicherheitskritische Funktionen auf mehrere SaaS-Anbieter zu verteilen, um nicht von den großen Anbietern abhängig zu sein. Gleichzeitig müssen sie alternative Kommunikationswege und Systeme als Notfallvorkehrung bereithalten.

Besuchen Sie uns!

Halle 7
Stand 7-417

STORM
powered by OTRS