3DEXPERIENCE®

HACKER VERBESSERN IHRE ANGRIFFSTECHNIKEN – VERBESSERN UNTERNEHMEN AUCH IHREN SCHUTZ?

Christoph Greis

EuroCentral Cloud Advocacy Director
Chris.Greis@3ds.com

DASSAULT SYSTEMES | The 3DEXPERIENCE® Company

AGENDA

- Die Situation
- Was wollen Unternehmen
- Die Antwort
- Die richtige Strategie

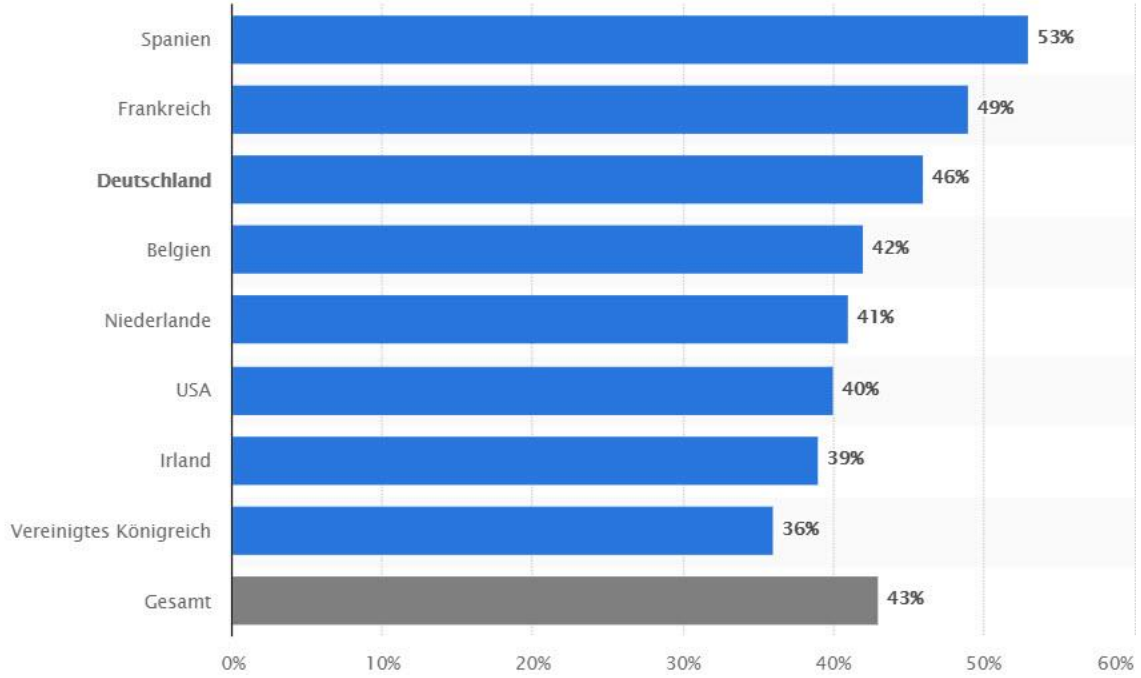
3DEXPERIENCE®

DIE SITUATION

DASSAULT SYSTEMES | The 3DEXPERIENCE® Company

WORÜBER REDEN WIR?

Cyberkriminalität Risiken bei europäischen Firmen



WORÜBER REDEN WIR?

Cyberkriminalität Risiken bei deutschen Firmen

Details can be found here: - https://www.bsi.bund.de/DE/Home/home_node.html

DATEN AUS DEUTSCHLAND

Aktuelle Zahlen

- Erfolgreiche Cyber-Angriffe **passieren jede 10 Sekunden** (Dunkelziffer höher)
- Gesamtschaden der deutschen Wirtschaft von **223 Milliarden €** (2021)
- 85 % der Cybersicherheitsverletzungen werden durch menschliches Versagen verursacht
- 94 % aller Schadsoftware wird per E-Mail zugestellt
- 71 % aller Cyberangriffe sind **finanziell motiviert**
- Aufklärungsquote liegt bei unter 30 %
- **Cyberversicherungen** erhöhen Ihre Vorrausetzungen oder **nehmen keine Kunden mehr an**

DATEN AUS DEUTSCHLAND

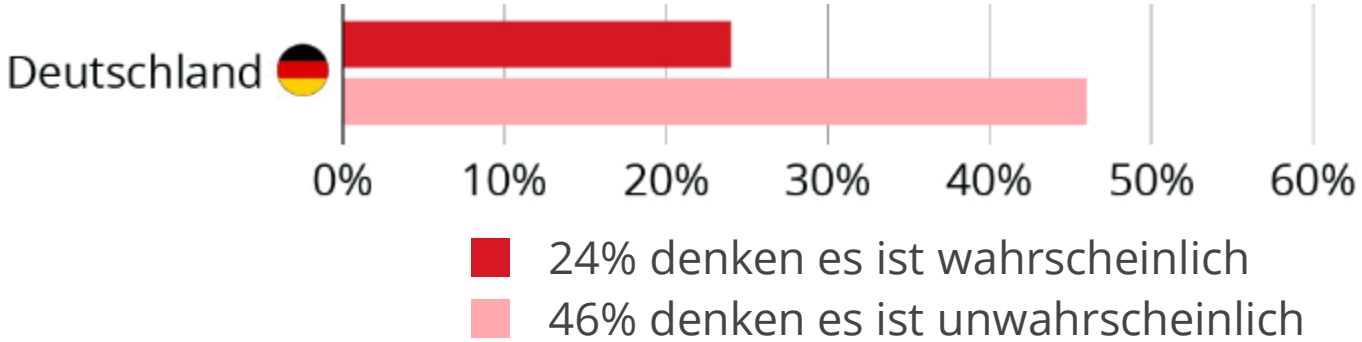
Quelle: https://de.statista.com

18.712 €

Durchschnittliche Kosten von Cyberattacken in Deutschland

46 %

aller deutschen Unternehmen haben in den letzten 12 Monaten eine Cyber-Attacke erlebt (15 Millionen registrierte Cyberangriffe)



Quelle: https://de.statista.com

LETZTES BEISPIEL AUS DER PRESSE

PROPHETE insolvent nach Cyber-Attacke

Am 25. November war der Fahrradhersteller Prophete das Opfer eines

NW+ Verluste waren zu hoch

Cyber-Attacke löst Insolvenz bei Fahrradhersteller Prophete im Kreis Gütersloh aus

PROPHETE – Historie

Seit über 100 Jahren immer eine Radlänge voraus.


Danke für die Statistik, Herr Greis – Und Nun?
DASSAULT SYSTEMES

WAS SIND DIE EIGENTLICHEN HERAUSFORDERUNGEN?

Neue Geschäfts-modelle

Lieferkettenrisiken

Transformation von Fertigungs-technologien

Fokus auf die Verbesserung der Produktlebenszyklen

Werkstoffe der Zukunft erkennen

Sich schnell ändernde Nachhaltigkeitse rwartungen

Der anhaltende Aufstieg des IoT

Alles als „as-a-service“

Wachsende Cyber-Risiken

Maximierung der Vorteile von Geschäftsöko-systemen

Erhöhte geopolitische Unsicherheit

Big Data

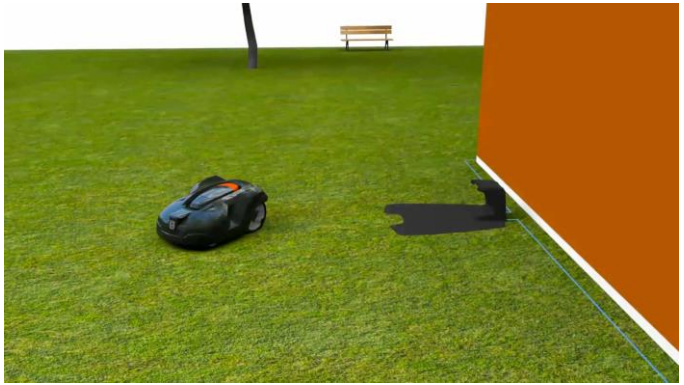
Der wachsende globale Fachkräftemangel

Der Wechsel von global zu lokal

Veränderte Kundenbeziehungen

DASSAULT SYSTEMES

WAS WOLLEN UNTERNEHMEN EIGENTLICH?




Kann mein Unternehmen nicht selber Vorsorge treffen?
DASSAULT SYSTEMES

VERTEILUNG DER VERANTWORTUNG

On Premise	IaaS*	PaaS**	SaaS***
Anwendungen	Anwendungen	Anwendungen	Anwendungen
Daten	Daten	Daten	Daten
Laufzeit	Laufzeit	Laufzeit	Laufzeit
Middleware	Middleware	Middleware	Middleware
Betriebssystem	Betriebssystem	Betriebssystem	Betriebssystem
Virtualisierung	Virtualisierung	Virtualisierung	Virtualisierung
Server	Server	Server	Server
Speicher	Speicher	Speicher	Speicher
Netzwerk	Netzwerk	Netzwerk	Netzwerk

Aufwand für Sicherheitsmaßnahmen

* Infrastructure-as-a-Service
** Platform-as-a-Service
*** Software-as-a-Service

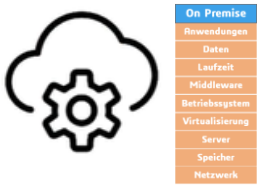
DASSAULT SYSTEMES

UNBEDINGTE AUFGABEN ZUR SICHERHEIT

Wie setzt das Ihr Unternehmen um?

BEDROHUNGS-ANALYSE

SYSTEM ARCHITEKTUR



SICHERER SOFTWARE ENTWICKLUNG LEBENSZYKLUS

BETRIEBS-SICHERHEIT

SICHERHEITSTANDARDS

STANDARD SICHERHEITSSTANDARDS

CYBERSICHERHEITSINSTITUTIONEN
Arbeitsmethoden

OWASP

cloud security alliance® CSA

National Institute of Standards and Technology U.S. Department of Commerce NIST

ANSSI

REFERENZEN ZUR CYBERSICHERHEIT
Werkzeuge

CVE Common Vulnerabilities and Exposures

MITRE | ATT&CK®

NIST Cybersecurity Framework

DASSAULT SYSTEMES

BEDROHUNGSANALYSE

Wie setzt das Ihr Unternehmen um?

Clear Web
- Forums & Communities
- Market Place
- News Group
- Social Media
- Malware & Attack Analysis

Dark Web
- Forums & Communities
- Market Place
- News Group
- Social Media

Threat Monitoring

- VIP & Executives
- Stolen Licenses
- Phishing Campaign
- Fake Malicious Apps & Websites
- Compromised User Accounts
- Data Leakage
- Employees Credentials
- Vulnerabilities
- Malware, Exploits & Zero-Days

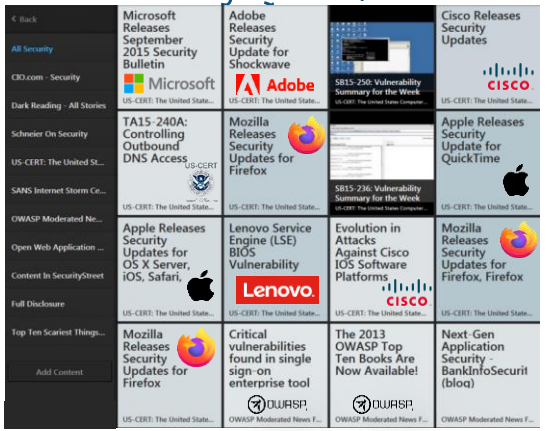
REAKTIV

Threat Intelligence

- Threat Actors
- Threat Activities
- Targets: Companies / Industries
- Threat Actors Operating Procedures
- Threat Actors Dynamics
- Threat Actors Motivation
- Attack Campaign

PROAKTIV

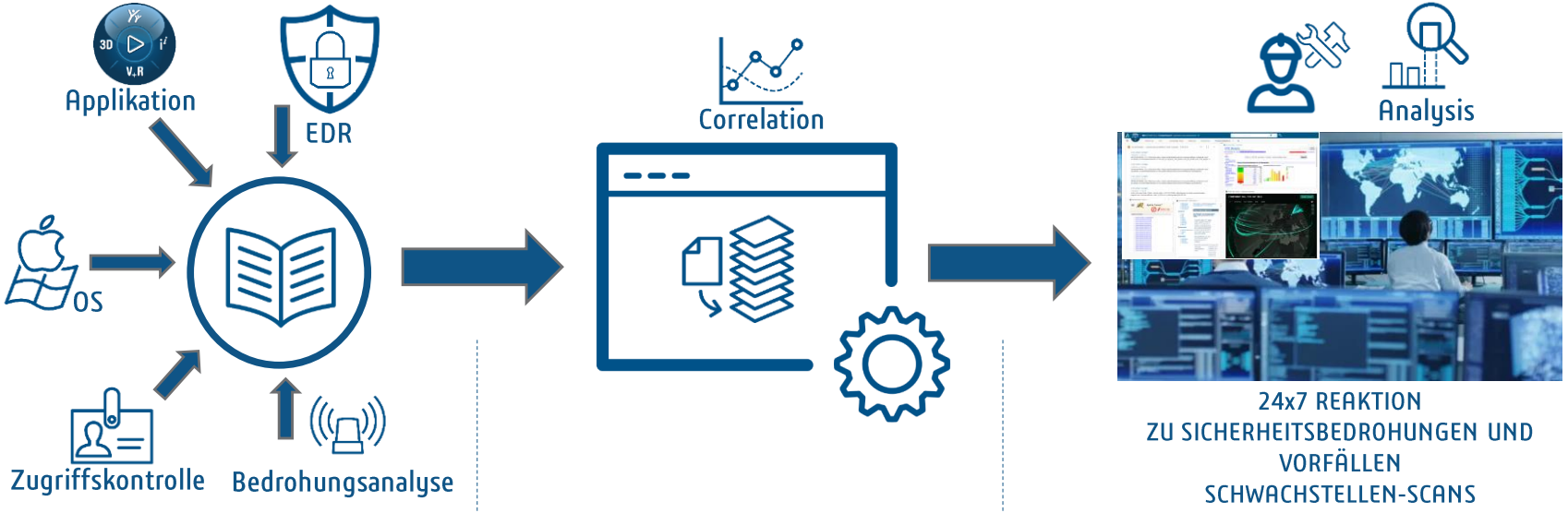
Zuverlässige Quellen / Feeds



DASSAULT SYSTEMES

SICHERER BETRIEB

Wie setzt das Ihr Unternehmen um?



Daten / Logs

Security Information and Event Management **(SIEM)**

Security Operation Center **(SOC)**

3DEXPERIENCE®

DIE ANTWORT

Die richtige Strategie

DASSAULT SYSTEMES | The 3DEXPERIENCE® Company

DIE RICHTIGE STRATEGIE: SOFTWARE AS A SERVICE

Ermöglicht Unternehmen eine Fokussierung
auf ihr KERNGESCHÄFT. Sie bietet Tools, die Kunden benötigen, wann sie sie brauchen und solange sie sie brauchen. Bleiben Sie agil und reagieren Sie schneller auf Anforderungen im geschäftlichen Umfeld.

DASSAULT SYSTEMES | The 3DEXPERIENCE® Company

EIN MODELL DER GEMEINSAMEN VERANTWORTUNG

Architektur, Ressourcen und Betriebs- **Verantwortung**

On-Premise

Kunde

Datensicherung & Disaster recovery
Betrieb/Überwachung/Gesundheitsprüfung
Bereitstellung & Verwaltung. Dienstleistungen
Hohe Verfügbarkeit/Skalierbarkeit
Voraussetzungen (DB, Middleware...)
Physische Cybersicherheit / Hardware / Umgebung

Software
Support und Updatebereitstellung

Gesichert & immer aktuell

SaaS

SaaS (Applikation)
Unterstützung und Aktualisierung
Plattform als Service (PaaS)
Infrastruktur als Service (IaaS)
DevSecOps / Cybersicherheit

Internetverbindung zum
Rechenzentrum
Mitarbeiter Sensbilisierung

DASSAULT SYSTEMES

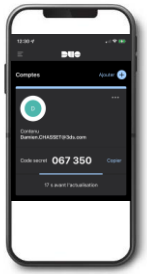
NOTWENDIGE SICHERHEITSEBENEN

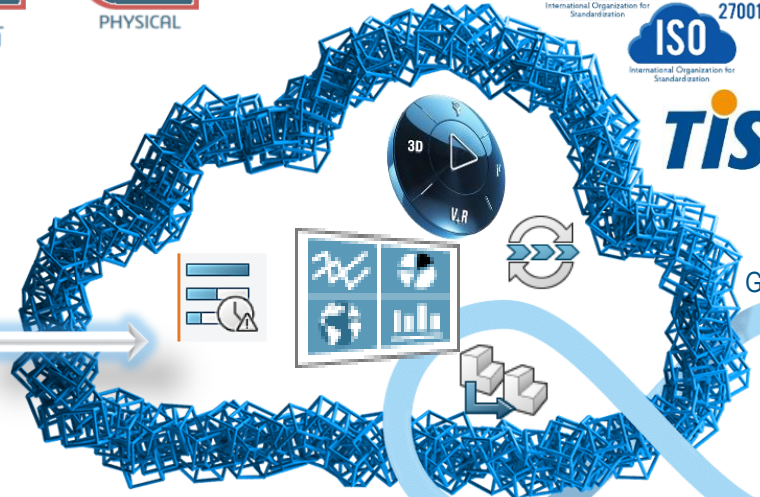
Internet

https

SSL/TLS V1.2 AES 256-bit

2 Factor Authentication





OWASP Open Web Application Security Project

ISO 9001

ISO 27001

TISAX®

GDPR* Compliant

DASSAULT SYSTEMES

REDUZIERTER TCO UND VORHERSAGBARE KOSTEN

Die größte Kostenblöcke

onPremise

Softwarehersteller liefert:
- Software
- Support

Kundenverantwortung
- Deployment & Update
- Operations/Monitoring/Health check
- Hochverfügbarkeit/Skalierbarkeit
- Backup & DRP
- DevSecOps
- Cyber Sicherheit
- DB, Middleware...
- Physische Cybersicherheit
- Physische Hardware
- Physische Umgebung

Personal + Fachwissen

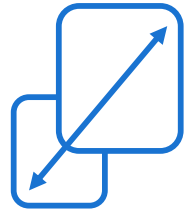
Hyperscaler

TCO

SaaS

Vertragsinhalte:
- Zugriff zur Lösung
- Support und Update
- PaaS
- IaaS

In der Kundenverantwortung:
- Internet Verbindung



VERTRAUEN IST GUT, ABER....

Security

Privacy

Regulatory

DASSAULT SYSTEMES

INFORMATIONSSICHERHEIT

Stellen Sie sich bitte nochmal diese Fragen

- Wie viele Tage Ausfall können Sie sich leisten?
- Was droht Ihnen bei Lieferverspätungen?
- Wie sind Sie vorbereitet, wenn Ihr Unternehmen still steht?

EINHEITLICHE SCHUTZSTRATEGIE?

Das muss ihr Software SaaS Anbieter bieten

Eine **einheitliche** Schutzstrategie umfasst die **Informationssicherheits-**, **Datenschutz-** und **Qualitätssicherung.** Der Anbieter muss sicherstellen, dass eine **sichere**, **stabile** und **skalierbare** Cloud-Plattform inklusiver **robuster Data-Governance-Prozesse** und ein inspektionsfähiges **Qualitätsmanagementsystem** angeboten wird.