

Industrial Artificial Intelligence

Pioneering
a Smarter World

Never Waste a Good Crisis

Erfahrungsbericht und Lehren aus der Cyberattacke auf PSI
DIRK-Mitgliederversammlung Frühjahr 2025

PSI 

Safe-Harbour-Statement

This presentation may contain forward-looking statements regarding the business, results of operations, financial condition and earnings outlook of PSI Group. These statements may be identified by words such as “anticipate”, “believe”, “estimate”, “expect”, “forecast”, “intend”, “may”, “plan”, “project”, “predict”, “should” and “will” and variations of such words or similar expressions. These forward-looking statements are based on our current assessments, expectations and assumptions, of which many are beyond control of PSI Group, and are subject to risks and uncertainties. You should not place undue reliance on these forwardlooking statements. Should these risks or uncertainties materialise, or should underlying expectations not occur or assumptions prove incorrect, actual results, performance or achievements of PSI Group may materially vary from those described explicitly or implicitly in the relevant forward-looking statement. This could result from a variety of factors, such as the level of customer orders received, the demand for process control and optimisation software in the market, the timing of final acceptance of deliveries by customers, the condition of financial markets and access to financing for PSI Group, general conditions in the software market and macroeconomic conditions, cancellations, rescheduling or delays in projects, capacity constraints, extended sales and qualification cycles, misuse of systems or misbehaviour by own or subcontractors employees, misuse of systems or misbehaviour by customers, organisational failures, technical failures of own software and hardware systems, technical failures of 3rd party software and hardware systems and any other factors discussed in any reports or other announcements, in particular in the Risk Report in the PSI Group Annual Report. Any forward-looking statements contained in this document are based on current expectations and projections of the executive board based on information available the date hereof. PSI Group undertakes no obligation to revise or update any forward-looking statements as a result of new information, future events or otherwise, unless expressly required to do so by law.

PSI in a nutshell



55 Jahre

Gegründet 1969
IPO im Jahr 1998

Produktportfolio

Qualicision AI	Mehrsparten-Energie-Suite & SCADA – PSIcontrol / PSImarkets
	Metallurgische MES- & SCM-Suite – PSImetals
	MES- & ERP-System für die diskrete Fertigung - PSIpenta
	Lagerverwaltungs- & Logistiksuite – PSIWms
	ÖPNV-Depotmanagement-Suite – PSIdms

Standorte

17 Standorte

weltweit auf vier Kontinenten
1.700 Kunden

Finanzdaten

EUR 270 Mio.

Umsatz
2% EBIT

Unser Team

~2,310

23% weiblicher Anteil
35 Nationalitäten
Ø Zugehörigkeit 9,7 Jahre
Ø Alter 42,9 y

Industrieller Softwaremarkt

Zielmarkt von 106 Mrd. EUR



**Netz & Energie-
management**



**Prozess-
industrie**



**Diskrete
Fertigung**



Logistik



Mobilität

Alle Zahlen 31.12.2023

SCADA: Supervisory Control and Data Acquisition | MES: Manufacturing Execution System | SCM: Supply Chain Management
ERP: Enterprise Resource Planning | WMS: Warehouse Management System | DMS: Depot Management System

Die Krise ist da: Ad-hoc-Mitteilung und erstes Presseecho

PSI Software SE
Cyberangriff auf PSI

Ad-hoc | 15 Februar 2024 20:25

PSI Software SE / Schlagwort(e): Sonstiges
Cyberangriff auf PSI

15.02.2024 / 20:25 CET/CEST
Veröffentlichung einer Insiderinformation nach Artikel 17 der Verordnung (EU) Nr. 596/2014, übermittelt durch EQS News - ein Service der EQS Group AG.
Für den Inhalt der Mitteilung ist der Emittent / Herausgeber verantwortlich.

Berlin, 15. Februar 2024 – Die PSI Software SE hat am 15. Februar 2024 festgestellt, dass es einen Cyberangriff auf die IT-Systeme der PSI gegeben hat. Die Gesellschaft hat als Reaktion die Systeme proaktiv vom Internet getrennt, um Datenschutzverletzungen und Datenbeschädigungen zu verhindern. Die IT-Systeme sowie der Umfang der Auswirkungen werden aktuell überprüft. Dabei wird mit höchster Sorgfalt auf die Datenintegrität geachtet. Die PSI Software SE setzt alles daran, dass die betroffenen Systeme so schnell wie möglich wieder zur Verfügung stehen.

Kontakt:
PSI Software SE
Karsten Pierschke
Leiter Investor Relations und Konzernkommunikation
Dircksenstraße 42-44
10178 Berlin
Deutschland

Tel. +49 30 2801-2727

Ende der Insiderinformation

Handelsblatt

PSI Software

Hacker legen wichtigen Dienstleister für Energieunternehmen lahm

Zu den Kunden von PSI Software gehören Versorger, Verkehrsunternehmen und Infrastrukturbetreiber. Das LKA ermittelt zu den Hintergründen des Cyberangriffs.

René Bender, Michael Verfürden, Kathrin Witsch
16.02.2024 - 17:52 Uhr aktualisiert



PSI realisiert Netzleitsysteme für namhafte Energieversorger. Foto: dpa

Düsseldorf. Nach einem Hackerangriff auf den für Deutschlands Infrastruktur wichtigen Dienstleister PSI Software SE hat das Landeskriminalamt Berlin (LKA) die Ermittlungen übernommen. Experten der für Cybercrime zuständigen Abteilung würden zu den Hintergründen ermitteln, bestätigte eine Polizeisprecherin dem Handelsblatt. Zu Details äußerte sie sich nicht.

Weitere Presseupdates und Linkedin-Feedback zur Krisenkommunikation

heise online > Security > Cyberangriff auf PSI Software: Kunden wohl nicht betroffen, Ermittlungen laufen

Cyberangriff auf PSI Software: Kunden wohl nicht betroffen, Ermittlungen laufen

Nach dem Ransomware-Angriff auf PSI Software, die unter anderem Dienstleister für den Energiesektor sind, laufen die Ermittlungen. Kunden wohl nicht betroffen.



(Bild: nitpicker/Shutterstock.com)

19.02.2024, 11:00 Uhr | Lesezeit: 1 Min. | Security
Von Marie-Claire Koch

Nach einem Ransomware-Angriff auf die IT-Systeme von PSI Software SE hat das Unternehmen die Systeme vom Internet getrennt, um "Datenschutzverletzungen und Datenschutzbeschädigungen zu verhindern". In diesem Zuge wurde zwischenzeitlich auch die Website offline genommen. Inzwischen hat PSI Software eine [statische Website mit weiteren Informationen zum Vorfall](#) eingerichtet.

Das Bundesamt für Sicherheit in der Informationstechnik und das Landeskriminalamt Berlin wurden umgehend informiert, wie der Sprecher von PSI Software, Karsten Pierschke, heise online sagte. IT-Forensiker und weitere Experten seien ebenfalls involviert, um den Umfang der Auswirkungen zu prüfen. Man achte "mit höchster Sorgfalt auf die Datenintegrität". Die betroffenen Systeme sollen "so schnell wie möglich wieder zur Verfügung stehen".



Sarah Fluchs · 2.

+ Folgen

Finally make and communicate cybersecurity decisions you can t...
1 Tag · Bearbeitet · 🌐

📢 Qualität der Krisenkommunikation, Anschauungsbeispiele #VARTA und #PSI 📢

Security-Vorfälle gab es in diesem Monat bei gleich zwei großen deutsche Unternehmen innerhalb weniger Tage: Am 13. Februar wurde ein Security-Vorfall beim Ellwanger Batteriehersteller VARTA bekannt, am 15. Februar einer beim Berliner Leittechnik-Softwarehersteller PSI.

Über beide Vorfälle ist noch nicht viel mehr bekannt als das, was die Unternehmen selbst auf ihren Webseiten bekanntgegeben haben, in beiden Fällen ist die IT "vorsichtshalber" komplett down, und in beiden Fällen ist die Incident Response in vollem Gange.

Die Kommunikation auf den Unternehmenswebseiten aber ist ein schönes Lehrstück zum Thema Krisenkommunikation. Beide Unternehmen kommunizieren offen ihren Security-Vorfall und den groben Stand der Dinge. Das verdient Achtung!

👉 #PSI hingegen kommuniziert ziemlich lehrbuchartig.

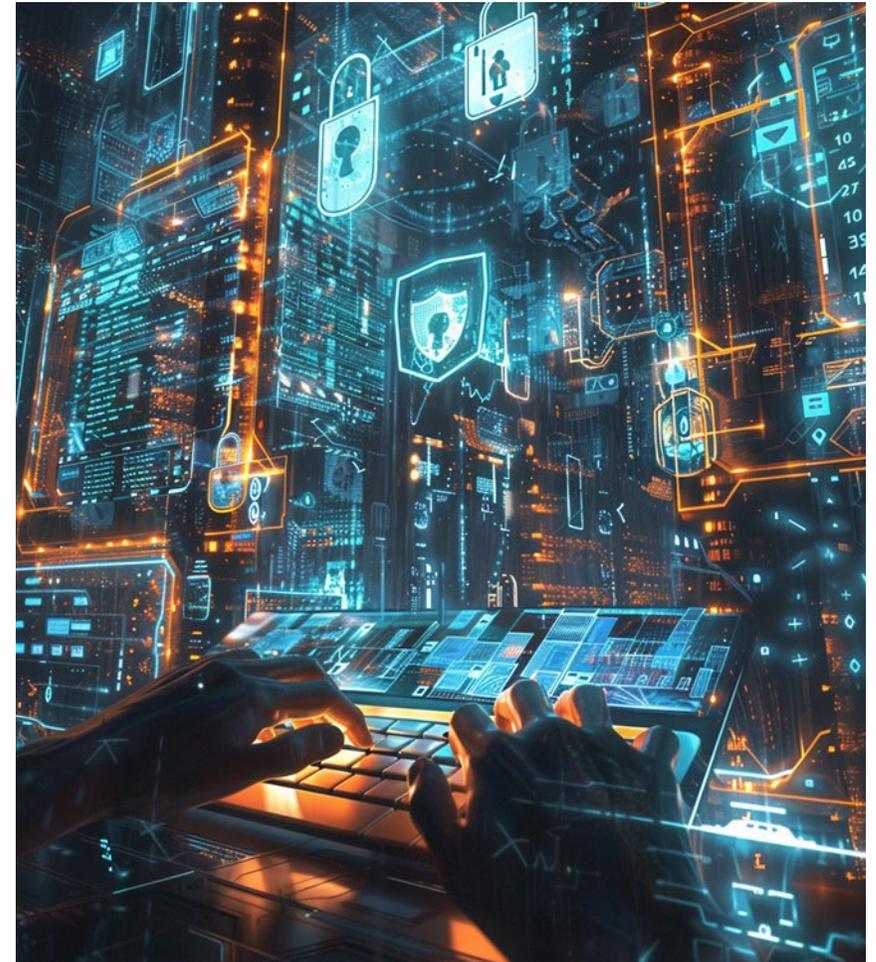
Die Unternehmenswebsite ist down, an ihrer Stelle wurde eine eigene Website für die Kommunikation des Vorfalls aufgesetzt, die regelmäßig um aktuelle Berichte ergänzt werden.

Die Informationen sind so gut strukturiert und erklärt, dass PSI das Kunststück gelungen ist, auf der eigenen Website besser zu informieren als in sämtlichen Medienberichten. Der Leser kann die Rekonstruktion des Vorfalls nachverfolgen, samt genauen Daten, Angriffsart, eingeleiteten Schritten, schon bekannten oder noch nicht bekannten Auswirkungen und Plänen für den Wiederanlauf. Chapeau, PSI!

Fairerweise muss man anmerken, dass Kunden und Gesellschaft durchaus höhere Ansprüche an die Kommunikation von PSI haben dürfen als an die von VARTA. PSI verkauft Software (für kritische Infrastrukturen!), damit kann sich ein IT-Angriff potenziell direkt auf die IT (und OT) der Kunden fortpflanzen. Bei VARTA, die mit Batterien ein rein physisches Produkt verkaufen, ist das nicht der Fall.

Cyber Incident vom 14. Februar 2024

- Am 14. Februar wurden wir Opfer einer kriminellen Ransomware Attacke durch eine professionelle Hackergruppe.
- Die Gruppe agiert als "Ransomware as a Service-" (RaaS) Organisation und stellt hochspezialisierte Krypto-Trojaner zur Verfügung.
- Wir haben weder Kontakt mit den Erpressern aufgenommen, noch Lösegeld bezahlt. Es sind keine weiteren Lösegeldforderungen eingegangen, es gibt keine Hinweise auf Datenabfluss.
- Kundensysteme und Produkte waren nicht betroffen.
- Systemhärtung während der Incident Response und Wiederanlaufphase, kontinuierliche Investments und Ausgaben erforderlich (Personal, Services & Lizenzen/Subscriptions).



Situation zur Zeit des Incident und im weiteren Zeitverlauf

- Allgemeine Situation und Aktivitäten des internen Security Operations Center (SOC) der PSI Software SE
 - Kontext: Zunehmende Digitalisierung, steigende Anzahl kommerzieller Ransomware-Anbieter, geopolitische Spannungen
 - Überwachung der Angriffsabwehr, tägliche Einschätzungen & Maßnahmen, Tuning von Anti-Malware, Anpassung von IDS* & Schwachstellenmanagement, Anpassung interner Prozesse/Umgang mit IT-Assets und Notfallhandling
- 14./15. Februar 2024: Angriff und Notabschaltung aller externen und internen Verbindungen und Systeme des Unternehmens, Abstimmung der Kommunikation an den Kapitalmarkt, Behörden, Kunden, Partner und Mitarbeiter
- 15. Februar bis Juni 2024: Externer ERT*-Spezialist an Bord, hochintensive Sicherheitsprüfungen aller Systeme, forensische Analysen, Systemwiederherstellung und -härtung, kontinuierliche Kommunikation mit Kunden und Behörden
- 17. Mai 2024: Report an benannte Kontaktpersonen bei Kunden (meist CISOs*/ähnliche Rollen) und öffentlichen Einrichtungen (Bundesamt für Sicherheit in der Informationstechnik, Datenschutzbehörde, LKA, ...)
- Seit Juli 2024
 - Kommunikation mit Kunden und Behörden
 - kontinuierliche Einführung von Maßnahmen
 - schrittweise Produktivitätssteigerung

* IDS = Intrusion Detection Solution, ERT = Emergency Response Team, CISO = Chief Information Security Officer

Taktische Maßnahmen in der Incident Response

Krisenmanagement

- Schwerpunkte: KRITIS-Umgebung (Kritische Infrastrukturen), Datenabfluss, Kunden-/ Behörden- und Teamkommunikation
- Einbindung externes Emergency Response Team: Lead in der Forensik, Koordination und Beratung beim Wiederanlauf, Rückkopplung aller IT-sicherheitsrelevanten Entscheidungen
- Unternehmens-IT: Lead für zentrale Tätigkeiten, vermeiden von Re-Infektion, Rahmenbedingungen für Tätigkeiten im Feld, Entscheidungen für geänderten Neuaufbau

Kontinuität des Geschäftsbetriebs

- Kontinuierliche Lageerfassung, Entscheidungen auf Basis der Business Impact Analysis
- Regelmäßig angepasste Prioritäten (stündlich, täglich, wöchentlich) zwischen Leitungen der BUs* und zentralem Krisenstab
- Einbindung des Vorstands oder Krisenstabs in Kundenkommunikation und gemeinsame Maßnahmengestaltung

*BU = Business Unit

Strukturiertes Vorgehen im Wiederanlauf

Waschstraßen

- Strukturiertes Vorgehen zu „Waschstraßen“ inklusive entsprechender Anweisung, Dokumentation für Server und Clients
- Zusätzlich strukturiertes Vorgehen für Code-Washing

Wiederanfahren

- Vorsichtiges Wiederanfahren; den Umständen entsprechende Maßnahmen zur Absicherung und Schutz vor Reinfektionen oder erneutem Angriff

Zertifizierung

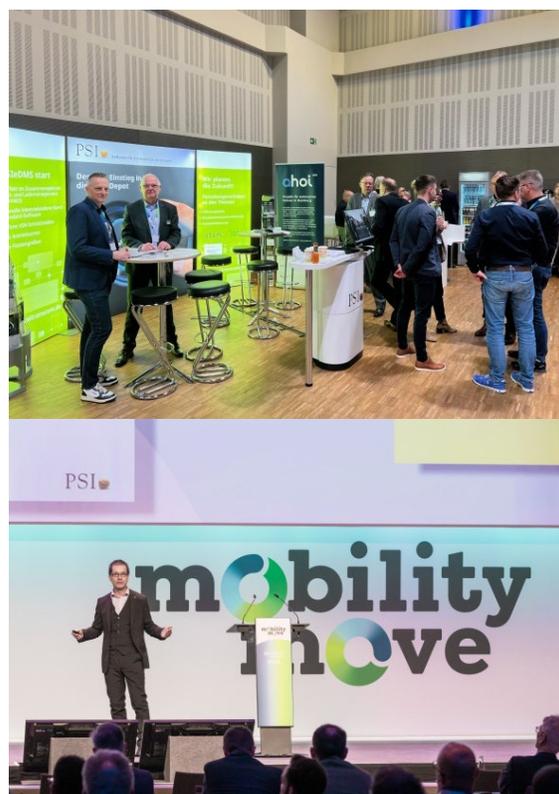
- Erfolgreicher Abschluss: Rezertifizierung ISO 9001 und Überwachungsaudit ISO 27001 in der Recovery Phase

Trotz der herausfordernden Situation haben wir unsere Vertriebs- und Marketingaktivitäten fortgesetzt ...

E-world energy & water
20. bis 22. Februar, Essen



mobility move
5. bis 7. März, Berlin



LogiMAT
19. bis 21. März,, Stuttgart



Hannover Messe
22. bis 26. April, Hannover



... und haben verschiedene Industrieawards erhalten

PSI mit PSIcontrol/Greengas unter den Finalisten beim Deutschen Innovationspreis 2024



PSI Automotive & Industry Sieger beim Factory Innovation Award in der Kategorie MES/MOM



Finanzkalender 2024

~~28. März 2024~~ → 4. Juni 2024:

Jahresergebnis/Geschäftsbericht 2023
Analystenkonferenz zum Jahresergebnis 2023

~~5. Juni 2024~~ → 26. Juli 2024:

Hauptversammlung (Präsenz)

~~30. April 2024~~ → 30. August 2024:

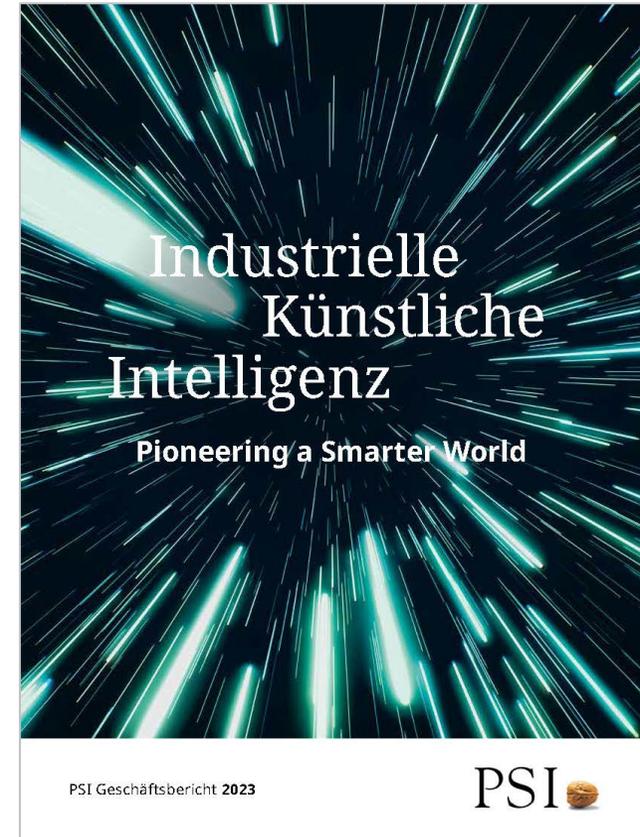
Bericht zum 1. Quartal 2024

~~31. Juli 2024~~ → 6. September 2024:

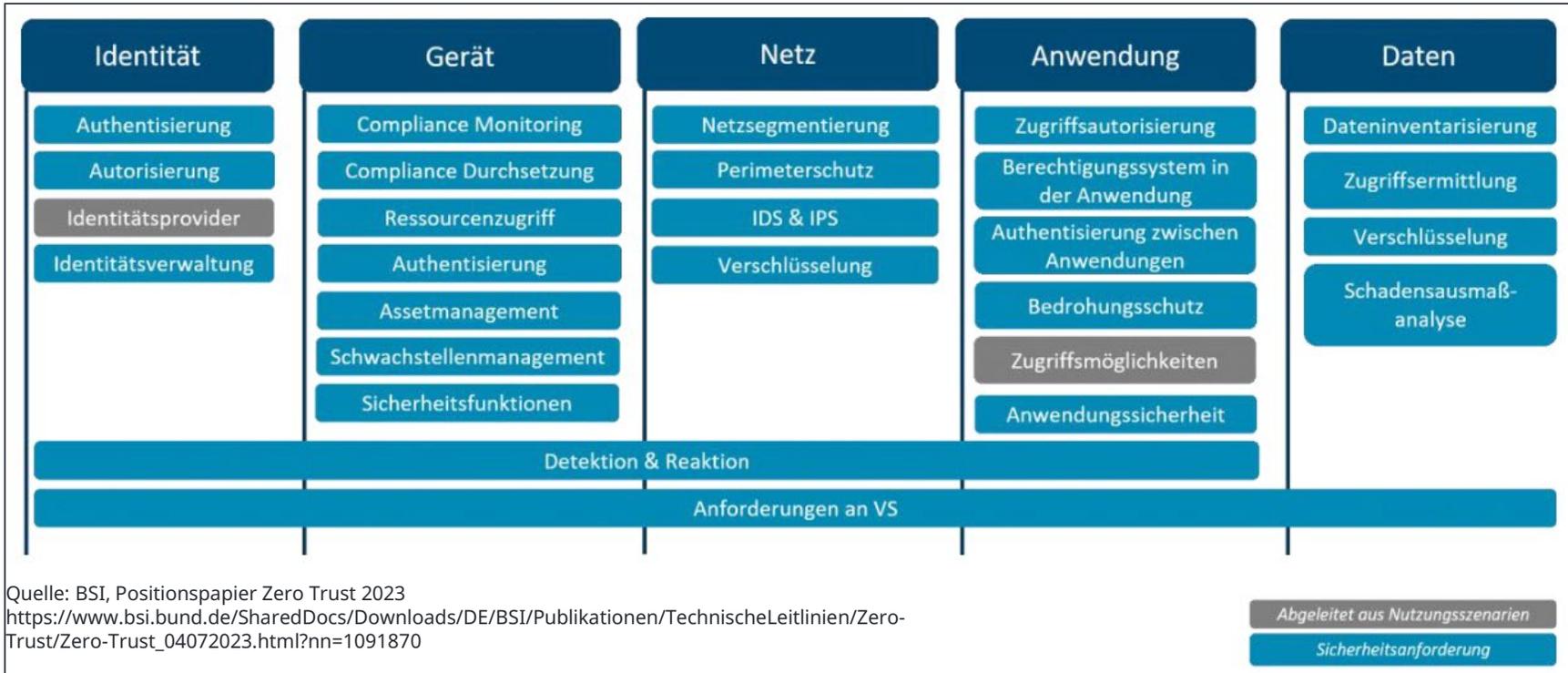
Bericht zum 1. Halbjahr 2024

31. Oktober 2024:

Bericht zum 3. Quartal 2024



Einführung Zero Trust und Total Security @PSI



Typische Grundprinzipien des Zero Trust-Modells:

Immer authentifizieren & autorisieren, zeitlich begrenzte Zugriffe mit geringstmöglichen Berechtigungen, Verstoß/Schwäche vermuten-überprüfen aller Sitzungen, Zugriffsversuche ...

Holistischer Ansatz Total Security @PSI: Verzahnung mit Security by Design, Physical Security

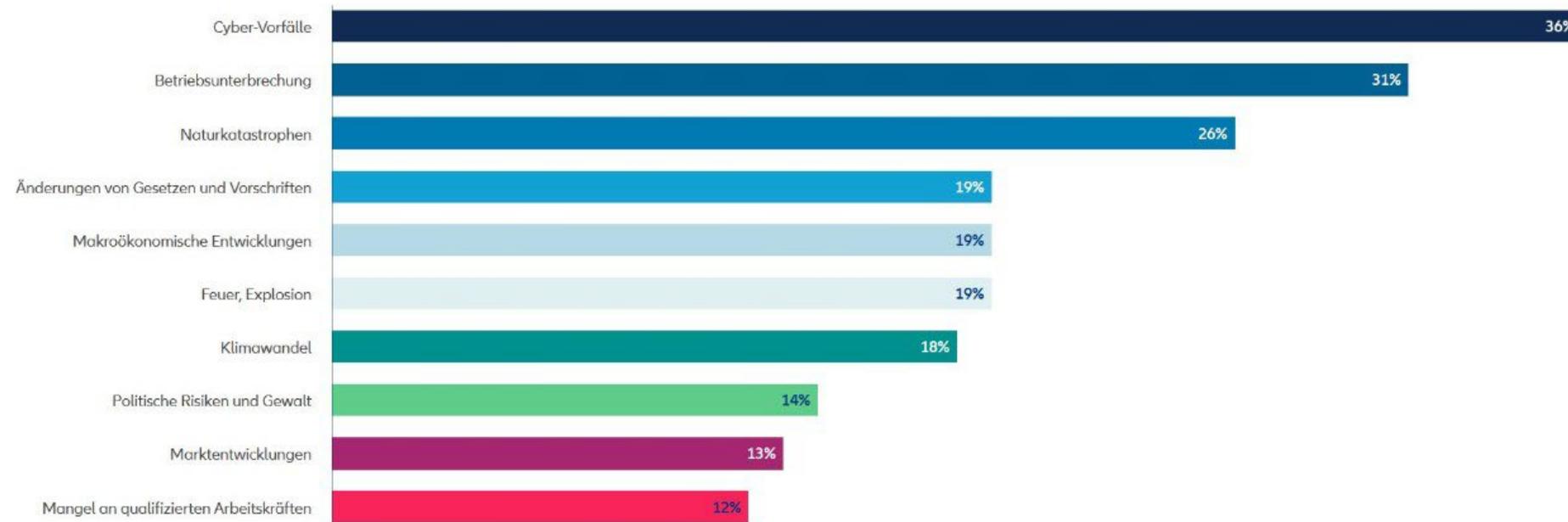
Cyberkriminalität als größtes Risiko für Unternehmen ...



Top 10 Geschäftsrisiken weltweit in 2024

Allianz Risk Barometer 2024

Basierend auf den Antworten von 3,069 Risikomanagement-Experten aus 92 Ländern und Gebieten (% der Antworten). Die Zahlen ergeben nicht 100%, da jeweils bis zu drei Risiken ausgewählt werden konnten.



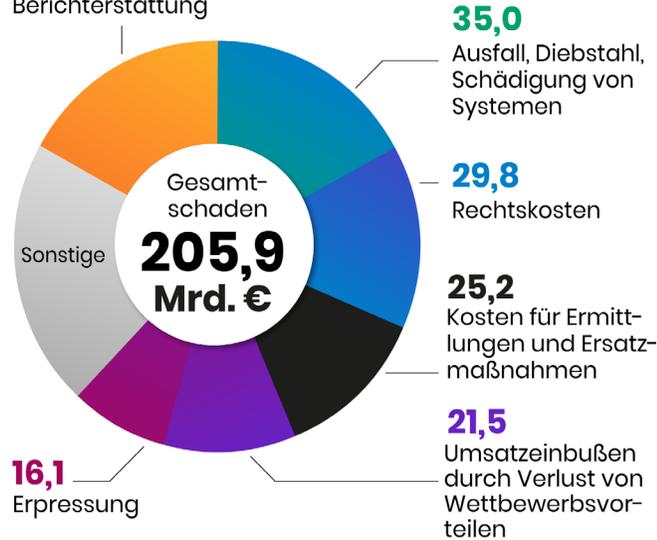
... und mit hohen Kosten verbunden

Was kostet die Cyberkriminalität Deutschland?

Schadenssummen im Zusammenhang mit Cyberkriminalität in Deutschland, 2023

35,3 Mrd. €

Imageschaden & negative Berichterstattung



ThePioneer

Quelle: Bitkom Research 2023

powered by statista

BUNDESLAGEBILD

Cybercrime 2023

Ransomware bleibt primäre Bedrohung mit enormem Schadenspotential

BKA

TOP 10 Ransomware-Varianten

1. → Lockbit
2. → Phobos
3. → BlackBasta
4. → Akira
5. → BlackCat
6. → MedusaLocker
7. → Play
8. → LokiLocker
9. → Qilin
10. → Royal; C3RB3R

Angriffe mit über

70

unterschiedlichen Ransomware-Varianten

Kriminelle Einnahmen

> 1,1 Mrd. US-Dollar

Festgestellte Lösegeldzahlungen auf Kryptowallets von Ransomware-Akteuren

Durchschnittlich gezahlte Lösegeldsumme
621.858 US-Dollar
Die Gesamtsumme der Lösegeldzahlungen ist 2023 stark angestiegen

Kennzahlen zu Ransomware-Angriffen im Jahr 2023

- a) Top 10 der relevantesten in Deutschland 2023 aktiven Ransomware-Varianten. Die Auflistung basiert auf einer Erhebung des BKA in den Bundesländern.
- b) Quelle: BKA
- c) Durchschnittlich festgestellte Lösegeldzahlungen weltweit. Quelle: Coveware (2023) Quartalsberichte 2023. Online abrufbar unter <https://www.coveware.com/blog>
- d) Einnahmen durch Ransomware-Angriffe. Quelle: Chainalysis (2024). The 2024 Crypto Crime Report

Kontakt



Karsten Pierschke

Leiter Investor Relations

✉ kpierschke@psi.de

☎ +49 30 2801-2727

PSI Software SE
Dircksenstraße 42-44
10178 Berlin
Germany