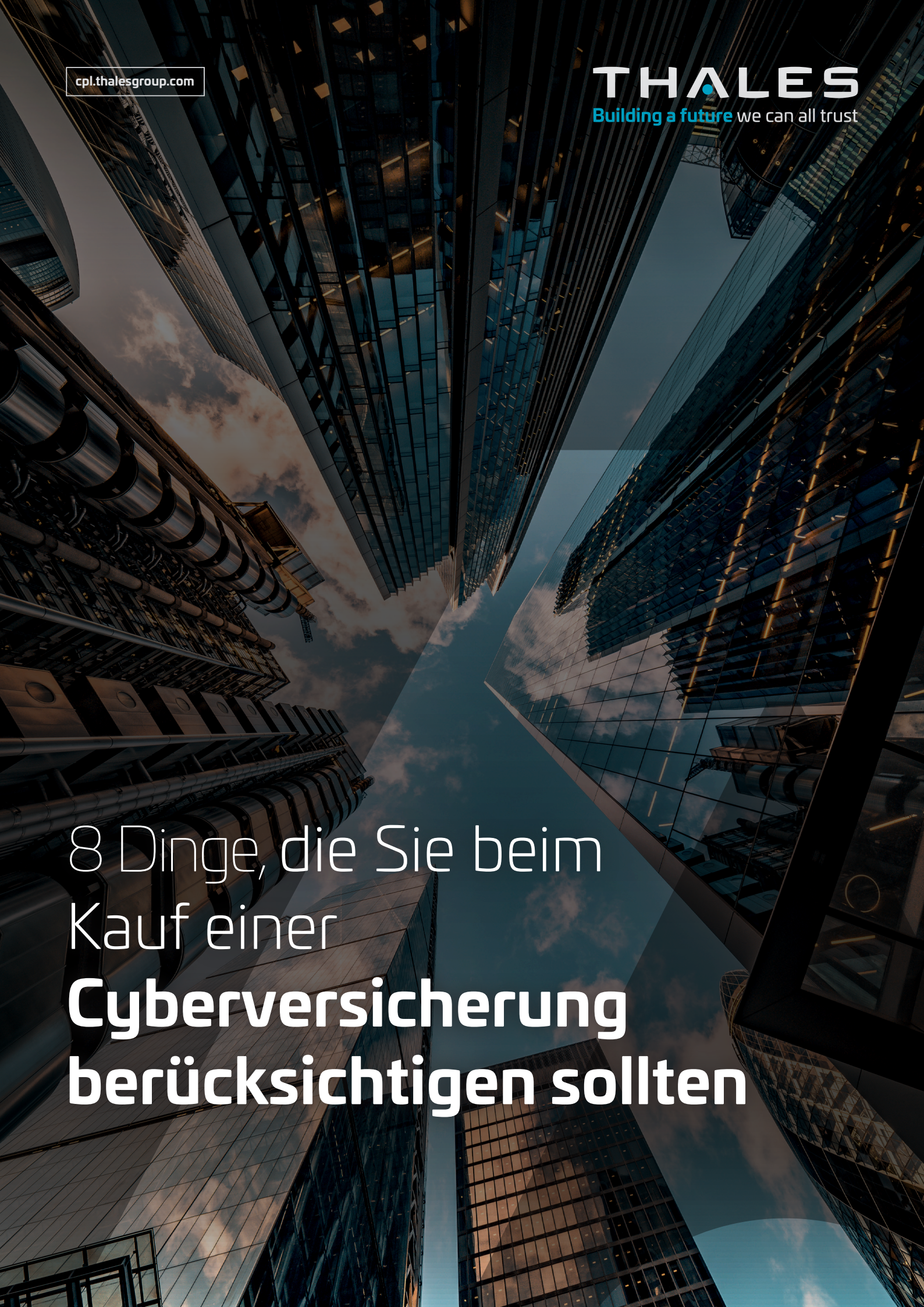


cpl.thalesgroup.com

THALES
Building a future we can all trust

8 Dinge, die Sie beim Kauf einer **Cyberversicherung berücksichtigen sollten**

Die Auswirkungen und Kosten von Cyberangriffen nehmen zu, insbesondere für kleine und mittlere Unternehmen. Um dieses Risiko für Unternehmen zu verringern, ist der Abschluss einer Cyberversicherung ein Muss. Das müssen Sie wissen, bevor Sie eine Cybersicherheitsversicherung abschließen:

1 Die Identität steht im Mittelpunkt moderner Cyberangriffe

Die Kompromittierung von Zugangsdaten ist der häufigste Angriffsvektor – 61 % der Datenschutzverletzungen sind auf gestohlene Zugangsdaten zurückzuführen. Kompromittierte Identitäten ermöglichen eine Vielzahl von Angriffen, einschließlich Ransomware. Die durchschnittlichen Kosten eines erfolgreichen Ransomware-Angriffs belaufen sich mittlerweile auf 4,62 Mio. USD, während die Gesamtkosten einer Datenschutzverletzung zwischen 2020 und 2021 um 10 % gestiegen sind. Diese Kosten beziehen sich auf vier Gruppen von Aktivitäten im Zusammenhang mit Datenschutzverletzungen: Aufdeckung und Eskalation, Benachrichtigung, Geschäftseinbußen und Reaktion auf die Datenschutzverletzung. Geschäftseinbußen machen den größten Teil der Kosten von Datenschutzverletzungen aus (38 %)[1]

> Die durchschnittlichen Kosten eines erfolgreichen Ransomware-Angriffs belaufen sich mittlerweile auf 4,62 Mio. USD.

2 Die Zahl der Forderungen an Cyberversicherungen sowie die Höhe der entsprechenden Prämien steigen.

Kleine und mittlere Unternehmen verlassen sich zunehmend auf digitale Technologien. Diese Abhängigkeit führt zu einem größeren Cyberrisiko. Wenn Technologie und Sicherheitsmaßnahmen versagen, ist eine Cyberversicherung für die Gewährleistung der Geschäftskontinuität entscheidend. Berichten zufolge wurden 2021 im Bereich Cybersicherheit mehr Versicherungsansprüche als zuvor gestellt[2]. Mehr Schadensfälle und höhere Verluste führen zu höheren Prämien – der Council of Insurance Agents & Brokers meldete im März 2022 einen durchschnittlichen Prämienanstieg von 34,3 % für Cyberversicherungen, womit zum ersten Mal seit den Ereignissen des 11. Septembers ein Anstieg dieser Größenordnung verzeichnet wurde[3]. Dieser Anstieg wird voraussichtlich auch im Jahr 2022 anhalten.

3 Kleine und mittlere Unternehmen sind am meisten gefährdet.

Cyberkriminelle werden immer raffinierter und ihre Taktiken immer ausgeklügelter. Kleine und mittlere Unternehmen sind durch diese Angriffe am stärksten bedroht, da ihnen die Kapazitäten – das Personal, die Technologie, das Budget – fehlen, um eine solide Cyberabwehr aufzubauen. Sie können schnell zu leichten Zielen für Kriminelle werden, die über komplexe Lieferketten größere Unternehmen angreifen möchten. Berücksichtigt man zusätzlich die regulatorische Landschaft mit ihren umfangreichen Sicherheits- und Datenschutzanforderungen, wird schnell deutlich, warum der Versicherungsschutz für kleine und mittlere Unternehmen ein existenzielles Thema ist.

1 Alle Statistiken sind dem Bericht IBM 2021 Cost of Data Breach entnommen, verfügbar unter https://www.ibm.com/security/data-breach.

2 Coalition, 2022 Cyber Claims Report, verfügbar unter https://info.coalitioninc.com/download-2022-cyber-claims-report.html

3 Commercial Property/Casualty Market Index, verfügbar unter https://www.ciab.com/resources/q2-p-c-market-survey-2021/

4 Was deckt eine Cyberversicherung ab?

Die Cyber-Risikoversicherung deckt die Kosten für die Wiederherstellung nach einer Sicherheitsverletzung, einem Virus oder einem Cyberangriff ab. Sie deckt auch Rechtsansprüche ab, die sich aus dem Angriff ergeben. Die meisten Cyber- und Datenschutzversicherungen bieten Schutz für Versicherte und Dritte.

Versicherungsschutz für Versicherte	Versicherungsschutz für Dritte
Beschädigung oder Verlust von Daten	Haftung für Netzwerksicherheit und Datenschutz
Einnahmeverluste	Haftung für Medien
Cybererpressung/Ransomware	Regulatorische Verfahren
Reputationsschäden	

Wenn Sie Cyberrisiken versichern, ist die entsprechende Versicherung weltweit gültig. Die Zuständigkeit für die Beilegung von Streitigkeiten wird jedoch in den Vertragsbedingungen festgelegt. Wie jede andere Art von Versicherung, die Sie abschließen können, bieten auch Anbieter von Cyberversicherungen eine Vielzahl von Policen mit unterschiedlichem Deckungsumfang an, je nach den Risiken Ihres Unternehmens.

> Die Zahl der unterschiedlichen Cyberversicherungen ist im Durchschnitt um 34,3 % gestiegen und wird auch 2022 weiter ansteigen.
>
> Council of Insurance Agents & Brokers

5 Regulatorische Anforderungen, die sich auf Richtlinien zur Cybersicherheit auswirken

Auch nach Einführung der DSGVO der EU erweitert sich die regulatorische Landschaft. Die folgenden Anforderungen wirken sich auf Ihre Cyberversicherungen aus und machen es notwendiger denn je, dass Sie Cyberrisiken versichern.

Die Executive Order on Improving the Nation's Cybersecurity von President Biden[1]

- „Entwicklung eines Plans zur Umsetzung der Zero-Trust-Architektur"
- „Bei der Migration hin zu Cloud-Technologie sollte auf Zero-Trust-Architektur gesetzt werden"
- „Agenturen sollten im größtmöglichen Umfang eine Multi-Faktor-Authentifizierung und Verschlüsselung für Data-at-Rest und Data-in-Transit einführen"

Das Memorandum on Moving the U.S. Government Toward Zero Trust Cybersecurity Principles des Office of Management and Budget (OMB)[2]

- „Agenturen müssen zentralisierte Identitätsmanagementsysteme für Benutzer der Agentur einsetzen, die in Anwendungen und gemeinsame Plattformen integriert werden können"
- „Für Mitarbeiter, Auftragnehmer und Partner der Agentur ist eine Phishing-resistente MFA erforderlich"

Die Guidelines on Information and Communication Technology Security and Governance der European Insurance and Occupational Pensions Authority (EIOPA)[3]

- „Um eine sichere Kommunikation zu gewährleisten und Risiken zu verringern, sollte der administrative Fernzugriff auf kritische IKT-Systeme nur dann gewährt werden, wenn starke Authentifizierungslösungen zum Einsatz kommen"
- „Die Unternehmen sollten Authentifizierungsmethoden durchsetzen, die robust genug sind, um angemessen und effektiv sicherzustellen, dass die Richtlinien und Verfahren zur Zugriffskontrolle eingehalten werden."

Die Publikation Boosting your Organization's Cyber Resilience der ENISA[4]

- Schützen Sie alle aus der Ferne zugänglichen Dienste mit Multifaktor-Authentifizierung. Unternehmen sollten die Verwendung von SMS und Sprachanrufen als Authentifizierungsmethoden vermeiden. Stattdessen sollten sie „die Bereitstellung von Phishing-resistenten Token wie Smartcards und FIDO2 (Fast IDentity Online) Sicherheitsschlüsseln in Betracht ziehen."
- Alle Benutzer müssen die Multifaktor-Authentifizierung nutzen, wenn sie von einer Anwendung unterstützt wird.

Die Cyber Security Strategy der Regierung des Vereinigten Königreichs: 2022 to 2030[5]

1 https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

2 https://www.whitehouse.gov/omb/briefing-room/2022/01/26/office-of-management-and-budget-releases-federal-strategy-to-move-the-u-s-government-towards-a-zero-trust-architecture/

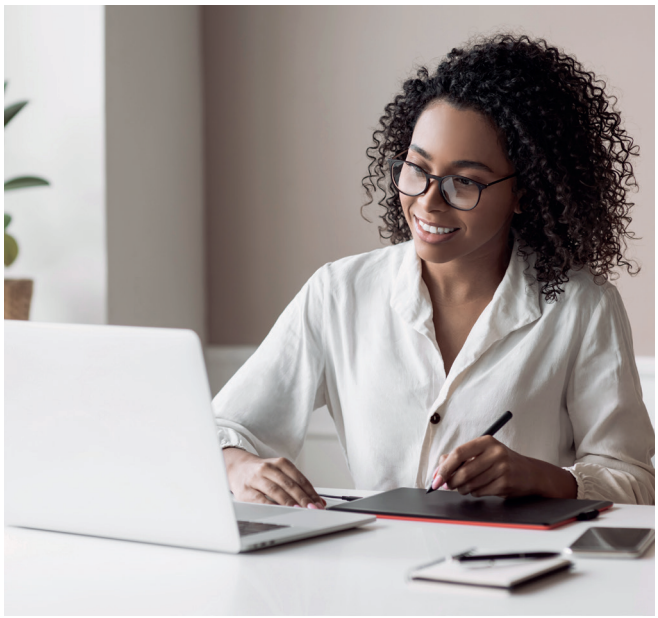
3 https://www.eiopa.europa.eu/document-library/guidelines/guidelines-information-and-communication-technology-security-and_en

4 https://www.enisa.europa.eu/publications/boosting-your-organisations-cyber-resilience

5 https://www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030

6 Best Practices zur Reduzierung von Haftung und Prämien

Die Versicherer möchten kein Geld verlieren und prüfen die Cybersicherheitspraktiken eines Unternehmens mit der gebotenen Sorgfalt, bevor sie es versichern. Sie können die Prämien senken, wenn Sie gute Cybersicherheitsverfahren anwenden, um Verstöße zu vermeiden. Sowohl Sie als auch Ihr Versicherer möchten nicht, dass es in Ihrem Unternehmen zu Vorfällen im Zusammenhang mit Cybersicherheit kommt. Die Best Practices umfassen unter anderem:



- Implementierung einer Multifaktor-Authentifizierung
- Schärfung des Bewusstseins für Cybersicherheit durch regelmäßige Schulungen
- Effektive Verwaltung von Drittparteien und Lieferanten
- Verschlüsselung Ihrer Daten an jedem Ort
- Stetige Aktualisierung Ihrer Software und Firmware
- Entwicklung und Erprobung eines Reaktionsplans für Zwischenfälle
- Durchführung regelmäßiger Penetrationstest

7 Wichtige Faktoren für die Auswahl der richtigen MFA-Lösung

„MFA ist eine der wichtigsten Cybersicherheitspraktiken, um das Risiko von Verstößen zu verringern – Branchenstudien haben ergeben, dass ist die Wahrscheinlichkeit der Kompromittierung eines Kontos bei Benutzern, die MFA aktivieren, um bis zu 99 Prozent geringer ist[1]." Daher wird die Multifaktor-Authentifizierung von mehreren Vorschriften empfohlen oder gefordert und ist eine Voraussetzung für den Abschluss einer Cyberversicherung. Selbst wenn ein Unternehmen alle anderen Anforderungen erfüllt hat, hat es Schwierigkeiten, eine Versicherung zu bekommen, wenn es keine MFA bereitstellt.

> MFA ist eine der wichtigsten Cybersicherheitspraktiken, um das Risiko von Verstößen zu verringern – Branchenstudien haben ergeben, dass ist die Wahrscheinlichkeit der Kompromittierung eines Kontos bei Benutzern, die MFA aktivieren, um bis zu 99 Prozent geringer ist[1].

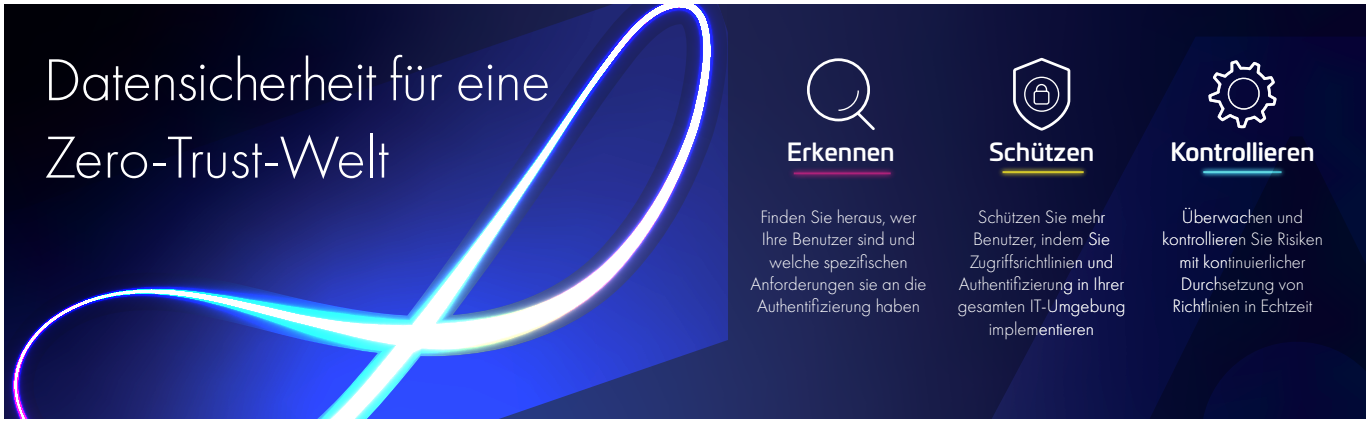
Wenn Sie sich fragen, welche MFA-Lösung für Sie am besten geeignet ist, sollten Sie sich für eine Lösung entscheiden, die:

- verschiedene Authentifizierungsmethoden anbietet, einschließlich Methoden wie FIDO und PKI-basierte MFA, die Schutz vor Phishing bieten,
- die Gesamtkosten für Bereitstellung und Betrieb senkt (eine schnelle Inbetriebnahme von MFA stellt sicher, dass Ihre Cyber-Versicherungspolice rechtzeitig erneuert wird),
- Flexibilität und Skalierbarkeit durch Integration mit On-Premise- und Cloud-Anwendungen bietet.

1 CISA Alert (AA22-074A), https://www.cisa.gov/uscert/ncas/alerts/aa22-074a

8 Schützen Sie sich mit MFA- und Zugriffsverwaltungslösungen von Thales vor Cyberangriffen

SafeNet Trusted Access von Thales ist ein Zugriffsverwaltungs- und Authentifizierungsdienst. Er stellt sicher, dass Ihre Benutzer nicht zum Ziel von Cyberangriffen werden, indem Sie die Authentifizierung auf alle Benutzer und Anwendungen mit unterschiedlichen Authentifizierungsfunktionen ausweiten können. Darüber hinaus versetzt er Sie in die Lage, den Zugriff auf alle Anwendungen mit geeigneten Richtlinien zu kontrollieren, die unter den gegebenen Umständen die richtige Authentifizierungsmethode für den richtigen Benutzer durchsetzen.



Mit seinen umfassenden und leistungsstarken Authentifizierungsfunktionen erfüllt SafeNet Trusted Access die spezifischen Anforderungen der verschiedenen Benutzer, indem es für jeden Benutzer die geeignete Authentifizierungsmethode bietet. SafeNet Trusted Access bietet kontextabhängige/adaptive und moderne Authentifizierungsfunktionen über hochsichere FIDO-Geräte sowie Push- und musterbasierte Authentifizierung an. Damit können Sie den sicheren Zugriff auf alle Apps und Benutzer erweitern und geben den Benutzern die Möglichkeit, sich überall und unter allen Umständen zu authentifizieren.

In Ihrer Umgebung integriert

SafeNet Trusted Access lässt sich reibungslos und flexibel in IT-Umgebungen integrieren. Der Dienst wird als SaaS oder im Hybrid-Modus bereitgestellt und bietet die Vorteile eines modernen, richtlinienbasierten Zugriffs mit Security by Design. Automatisierte Workflows und die vom Benutzer initiierte Registrierung gewährleisten Fernsupport für Tausende von Benutzern unabhängig davon, wo sie sich befinden, während verschiedene Integrationsmethoden sicherstellen, dass Sie jede Anwendung schützen können – ob in der Cloud oder On-Premises.

Über die SafeNet-Lösungen für Zugriffsverwaltung und Authentifizierung von Thales

Die branchenführenden Lösungen für Zugriffsverwaltung und Authentifizierung von Thales verwalten und sichern den Zugriff auf ihre IT-, Web- und Cloud-basierten Anwendungen zentral. Durch den Einsatz von richtlinienbasiertem SSO und universellen Authentifizierungsmethoden sind sie in der Lage, Sicherheitsverletzungen effektiv zu verhindern, sicher in die Cloud zu migrieren und die Einhaltung gesetzlicher Vorschriften zu vereinfachen.

Von SafeNet Trusted Access unterstützte Authentifizierungsmethoden