

Deutschland beim Thema Datenschutz weltweit führend, angetrieben durch Richtlinien und Compliance

„nCipher 2020 Encryption Trends“ Studie beleuchtet zunehmende Herausforderungen für Unternehmen im Bemühen um die Sicherheit sensibler Daten aus Cloud, IoT und 5G

Minneapolis und Düsseldorf – 8. September 2020 – Während sich weltweit digitale Initiativen wie die Cloud oder das Internet der Dinge (IoT) beschleunigen und Datenmengen und -typen immer weiter ansteigen, nehmen deutsche Unternehmen beim Einsatz von Verschlüsselungslösungen für den Datenschutz eine führende Rolle ein. So die auf Deutschland bezogenen Ergebnisse der multinationalen „2020 Encryption Trends“ Studie, die das Ponemon Institut in Zusammenarbeit mit [nCipher Security](#), einem Unternehmen von [Entrust Datacard](#) und Weltmarktführer im Bereich Hardware-Sicherheitsmodule (HSMS), heute veröffentlicht. Die zum 15. Jahr in Folge durchgeführte Studie untersucht, wie und aus welchen Beweggründen Unternehmen weltweit Verschlüsselung einsetzen.

Gesetzliche Bestimmungen und hohes Sicherheitsbewusstsein

Mit zunehmender Nutzung der Cloud und IoT-Technologien haben zwei Drittel (66%) der deutschen Unternehmen übergreifende Verschlüsselungsstrategien eingeführt, weitere 28% verschlüsseln einzelne Anwendungen oder Datentypen. Damit nimmt Deutschland zusammen mit den USA weiterhin eine international führende Position beim Thema Datenschutz ein.

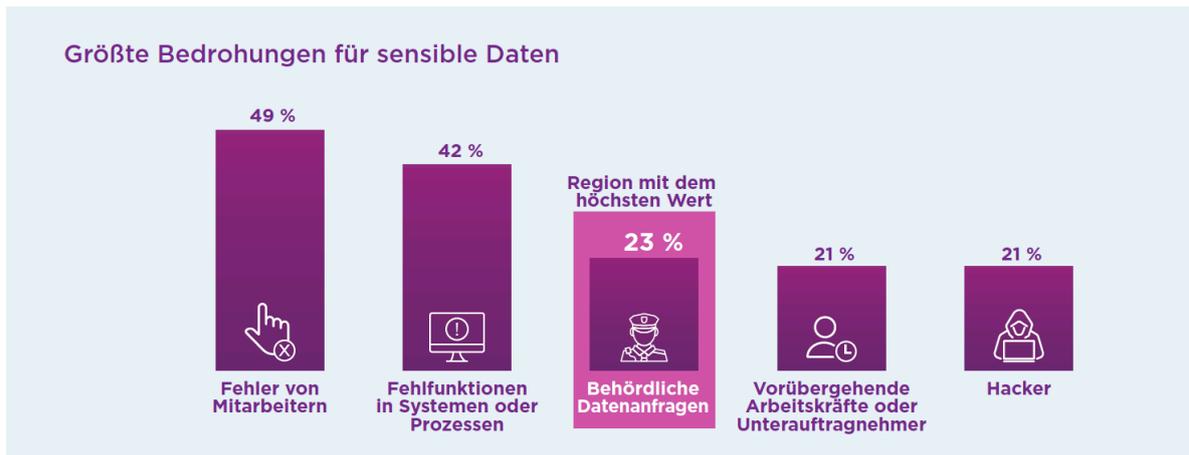
Der wichtigste Beweggrund für diese Vorreiterrolle liegt für deutsche Security-Verantwortliche mit 67% in der Einhaltung von Richtlinien wie zum Beispiel der Datenschutz-Grundverordnung (DSGVO) – während für ihre internationalen Kollegen der Schutz persönlicher Kundendaten und geistigen Unternehmenseigentums die Hauptursache für den Einsatz von Verschlüsselungslösungen ist. Einen Imageschaden durch öffentliche Bekanntgabe von Datenverletzungen fürchten in Deutschland nur 2% der Befragten, im Vergleich zu 15% weltweit.



„Unternehmen stehen heutzutage unter massivem Druck, ihre geschäftskritischen Informationen und Anwendungen vor einer Vielzahl an Bedrohungen zu schützen. Gerade an einem erfolgreichen Wirtschaftsstandort wie Deutschland ist das Bewusstsein für die vielfältigen Risiken von Datendiebstahl, Datenspionage und korrumpierten Informationen besonders hoch, die gesetzlichen Bestimmungen sind besonders umfangreich“, so Bernd Stamp, Solution Consultant & Tech Lead DACH bei nCipher Security, einem Unternehmen von Entrust Datacard. „Hierdurch erklärt sich die Vorrangstellung deutscher Unternehmen beim Thema Verschlüsselung. Zudem begünstigen die wirtschaftlichen Verhältnisse und ein generell hohes Sicherheitsbewusstsein den Aufbau hochsicherer IT-Infrastrukturen in Deutschland.“

Mehr Angst vor behördlichen Datenabfragen und Lauschangriffen als vor Hackern

Wie ihre internationalen Kollegen, sehen auch die deutschen Security-Verantwortlichen das größte Risiko für die Datensicherheit in Fehlern von Mitarbeitern (49%). Interessant: Gerade in Deutschland ist die Angst vor Bedrohungen durch Datenabfragen vonseiten der Behörden und Lauschangriffen durch Regierungen besonders hoch (23% und 14%, im Vergleich zu 12% bzw. 11% weltweit). Die Furcht vor Hackern ist jedoch geringer als im internationalen Vergleich (21% versus 29%).

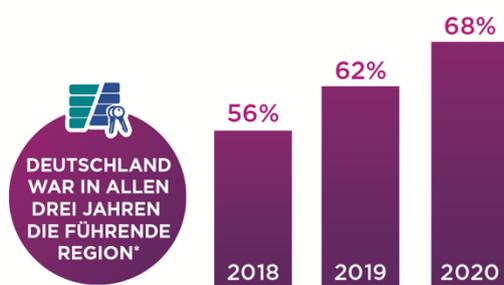


Datenermittlung als größte Herausforderung

Angesichts der explosionsartigen Zunahme und Verbreitung von Daten aus digitalen Initiativen, Cloud-Nutzung, IoT-Geräten und zunehmender Mobilität, stellt die Datenermittlung für 83% der deutschen Unternehmen mittlerweile die größte Herausforderung bei der Planung und Ausführung ihrer Verschlüsselungskonzepte dar. (Weltweit höchste Rate, der globale Durchschnitt liegt bei 67%).

Starke Verbreitung von Hardware-Sicherheitsmodulen für den Datenschutz und die Schlüsselverwaltung

nCipher Studie: deutsche Unternehmen weltweit führend beim Einsatz von HSMs



Hardware-Sicherheitsmodule (HSMs) als gehärtete, manipulationssichere Umgebungen zum Schutz sensibler Daten sind in Deutschland besonders weit verbreitet – und das bereits zum dritten Jahr in Folge. 68% der deutschen Befragten setzen HSMs ein, um mehr Vertrauen, Integrität und Kontrolle für geschäftskritische Daten und Anwendungen zu gewährleisten. 93% der Befragten geben an, dass die Bedeutung von HSMs als Teil ihrer Verschlüsselungsstrategie in den nächsten 12 Monaten weiter zunehmen wird. Genauso weit verbreitet sind HSMs aktuell nur in den USA und im Nahen Osten.

Konsequenterweise werden HSMs in Deutschland über alle Anwendungsarten hinweg häufiger eingesetzt als in anderen Regionen. So spielen sie eine wichtige Rolle bei der Verschlüsselung von Applikationen (69% vs. 46% weltweit), beim PKI-/Zertifikatsmanagement (68% vs. 30% weltweit), aber auch bei der Verschlüsselung von Public Clouds und BYOK-Konzepten (65% vs. 35% weltweit).

Weitere wichtige Ergebnisse der 2020 Germany Encryption Trends Studie:

- 66% der deutschen Unternehmen geben an, dass sie eine konsequent angewandte Verschlüsselungsstrategie haben. Sie teilen sich damit den ersten Platz mit Unternehmen aus den USA. Weltweiter Durchschnitt: 48%.
- 67% der deutschen Unternehmen bewerten die „Einhaltung externer Datenschutz- oder Datensicherheitsvorschriften“ als einen Top-Treiber für die Verschlüsselung von Daten. Im Vergleich zu anderen Regionen (weltweiter Durchschnitt 47%) orientieren sich deutsche Security-Verantwortliche damit eher an externen Vorschriften als an tatsächlichen oder potenziellen Gefahren.
- Fast jedes deutsche Unternehmen (99%) betrachtet bei Verschlüsselungs-Lösungen die Durchsetzung von Richtlinien als wichtigstes Feature, im Vergleich zu 67% weltweit. Auch die Skalierbarkeit eines Systems wird als entscheidend betrachtet: 97% vs. 58% weltweit.
- Die größte Herausforderung bei der Planung und Durchführung einer Verschlüsselungsstrategie in Deutschland ist die „Ermittlung sensibler Daten“ (83%). Ein weiteres Problem liegt in unklaren Zuständigkeiten bei der Schlüsselverwaltung (weltweit höchste Rate von 93%, globaler Durchschnitt: 66%) und an einem Mangel an qualifiziertem Personal (63% gegenüber 57% weltweit).

Die **2020 Germany Encryption Trends Study** steht auf der Webseite von nCipher zum Download zur Verfügung: <https://tinyurl.com/yyhwxz75>

Die wichtigsten Ergebnisse werden in einem kurzen **Video** dargestellt: <https://youtu.be/aUrixY79wnl>

Sämtliche vorhandenen Materialien inklusive Bildmaterial finden Sie hier: <https://tinyurl.com/y363kj8l>

Methodik der Studie „Globale Verschlüsselungstrends 2020“

Die Studie „2020 Global Encryption Trends“ basiert auf Forschungsergebnissen des [Ponemon Institute](#) und erfasst, wie Unternehmen weltweit mit der Einhaltung von Vorschriften, zunehmenden Bedrohungen und der Implementierung von Verschlüsselung zum Schutz ihrer geschäftskritischen Informationen umgehen. Befragt wurden 6.457 IT-Experten aus verschiedenen Branchen in 17 Ländern/Regionen: Australien, Brasilien, Frankreich, Deutschland, Indien, Japan, Hongkong, Mexiko, Naher Osten (eine Kombination von Befragten aus Saudi-Arabien und den Vereinigten Arabischen Emiraten), Russische Föderation, Südostasien (Indonesien, Malaysia, Philippinen, Thailand und Vietnam), Südkorea, Taiwan, Großbritannien, USA und erstmals zwei neue Regionen, Niederlande und Schweden.

Über nCipher Security

nCipher Security, ein Unternehmen von [Entrust Datacard](#), ist ein führender Anbieter von universellen Hardware-Sicherheitsmodulen (HSM) und unterstützt weltweit Unternehmen dabei, Vertrauen, Integrität und Kontrolle für ihre geschäftskritischen Informationen und Anwendungen zu schaffen. Die heutige schnelllebige digitale Welt erhöht die Kundenzufriedenheit, verschafft Wettbewerbsvorteile und verbessert die operative Effizienz – gleichzeitig vervielfacht sie jedoch die Sicherheitsrisiken.

Die kryptografischen Lösungen von nCipher dienen der Sicherung neuer Technologien – Cloud, IoT, Blockchain, digitale Zahlungen – sowie der Einhaltung neuer Compliance-Mandate mittels der gleichen bewährten Technologie, auf die sich global agierende Unternehmen heute zum Schutz gegen die Bedrohung ihrer sensiblen Daten, ihrer Netzwerkkommunikation und ihrer Firmeninfrastruktur verlassen. Die Lösungen von nCipher schaffen Vertrauen für geschäftsentscheidende Anwendungen, gewährleisten die Integrität von Daten und ermöglichen Unternehmen eine umfassende Kontrolle – heute, morgen, jederzeit. www.ncipher.com

Folgen Sie uns auf [LinkedIn](#), [Twitter](#), [Facebook](#) und [Instagram](#) – suchen Sie nach „nCIPHERSecurity“.

Pressekontakte D/A/CH:

Alexandra Maiberger, amaiberger@pr-am.com, Tel: +49 179 4674 310

Lisa Ostermaier, sternschmiede@email.de, Tel: +49 152 0865 2080