Compliance wächst schneller als die Kapazitäten der IT-Teams

Eine neue Sophos-Studie unter 5.000 IT- und Cybersecurity-Verantwortlichen zeigt: Regulatorische Anforderungen wachsen schneller als die Kapazitäten der Teams – mit direkten Folgen für Sicherheit und Betrieb.

Unternehmen in Deutschland, Österreich und der Schweiz stehen wie viele Organisationen weltweit vor der Herausforderung, eine wachsende Zahl an IT- und Cybersecurity-Vorgaben zu erfüllen. Eine aktuelle, von Sophos in Auftrag gegebene internationale Studie zeigt, wie stark regulatorische Anforderungen inzwischen in den Arbeitsalltag eingreifen und welche Folgen das für IT- und Sicherheitsteams hat.

Für die Untersuchung wurden Anfang 2026 insgesamt 5.000 IT- und Cybersecurity-Verantwortliche aus 17 Ländern und unterschiedlichen Branchen befragt. Die Ergebnisse zeigen: Compliance ist längst zu einer dauerhaften Managementaufgabe geworden, die erhebliche Ressourcen bindet und viele Organisationen an ihre Grenzen bringt.

Fünf Standards gleichzeitig und trotzdem selten Gewissheit
Im Median erfüllen Unternehmen aktuell fünf verschiedene Compliance-Standards gleichzeitig. Diese Bandbreite verdeutlicht, wie komplex die regulatorischen Anforderungen geworden sind.
Gleichzeitig fehlt vielen Organisationen die Sicherheit über den eigenen Status. 82 Prozent der Befragten geben an, besorgt zu sein, dass ihr Unternehmen nicht alle relevanten Vorgaben vollständig erfüllt. Fast ein Viertel äußert sogar große Bedenken. Nur 18 Prozent sehen sich auf der sicheren Seite.

Fast 40 Prozent der Arbeitszeit: Compliance verdrängt operative Sicherheit
Ein erheblicher Teil der verfügbaren Kapazitäten fließt in Compliance-Aufgaben. Im Schnitt wenden IT- und Cybersecurity-Teams 39 Prozent ihrer Arbeitszeit dafür auf. Dazu gehören unter anderem die Umsetzung von Anforderungen, interne Abstimmungen sowie die Dokumentation und Berichterstattung.
Dieser Aufwand fehlt an anderer Stelle. Die operative Sicherheitsarbeit gerät zunehmend unter Druck, weil Ressourcen gebunden sind.

Dynamische Anforderungen erschweren die Umsetzung
Viele Unternehmen haben Schwierigkeiten, mit den stetigen Veränderungen Schritt zu halten. 79 Prozent der Befragten empfinden es als herausfordernd, aktuelle Anforderungen zu verfolgen und umzusetzen. 19 Prozent beschreiben dies als sehr schwierig.
Die Vielzahl an Vorgaben führt zudem zu Überschneidungen: Ähnliche Anforderungen müssen mehrfach bearbeitet werden, was den Aufwand zusätzlich in die Höhe reibt.

Gleiche Pflichten, weniger Mittel: Kleinere Unternehmen besonders unter Druck
Vor allem kleinere Unternehmen stehen vor großen Herausforderungen. Sie sehen sich häufig mit einer vergleichbaren Anzahl an Regelwerken konfrontiert wie größere Organisationen, verfügen jedoch über deutlich weniger personelle und fachliche Ressourcen.
Das erhöht den Druck und erschwert eine nachhaltige Umsetzung der Anforderungen.

Je nach Branche und Land ein anderes Regelwerk – die Fragmentierung ist real
Die am häufigsten genannten Regelwerke sind ISO 27001/2 (51,2 %), GDPR (40,4 %), CIS (29,7 %), NIST CSF (23,8 %), PCI DSS (23,1 %), HIPAA (21,7 %), DORA (19,8 %) und NIS2 (16,1 %). Ihre Bedeutung variiert jedoch deutlich je nach Branche und Region.

So geben 66 Prozent der Unternehmen im Bereich Transport und Logistik an, sich an ISO 27001/2 zu orientieren, während dieser Anteil im öffentlichen Sektor bei 38 Prozent liegt. Auch zwischen einzelnen Ländern zeigen sich klare Unterschiede: In Spanien streben 60 Prozent der Unternehmen eine Ausrichtung an ISO 27001/2 an, in Mexiko sind es 35 Prozent.

Ein ähnliches Bild ergibt sich bei NIST CSF. In den USA orientieren sich 30 Prozent der Organisationen an diesem Framework, in Australien hingegen nur 13 Prozent.

Für Unternehmen im DACH-Raum ergibt sich daraus eine doppelte Herausforderung. Einerseits prägen europäische Vorgaben wie GDPR, NIS2 und künftig DORA das regulatorische Umfeld. Andererseits orientieren sich international tätige Unternehmen häufig zusätzlich an global etablierten Frameworks wie ISO 27001 oder NIST.

Das erhöht die Komplexität in der Umsetzung erheblich, da unterschiedliche Anforderungen parallel berücksichtigt und miteinander in Einklang gebracht werden müssen. Ein einheitlicher Ansatz ist in der Praxis selten ausreichend. Gefragt sind flexible, aufeinander abgestimmte Lösungen.

Wer nicht weiß, ob er compliant ist, hat ein Sicherheitsproblem
Ein zentrales Ergebnis der Studie ist die eingeschränkte Transparenz über den eigenen Compliance-Status. Viele Unternehmen gehen davon aus, die Anforderungen zu erfüllen, ohne dies sicher belegen zu können.

Diese Unsicherheit kann zu Lücken führen, die sowohl sicherheitsrelevant als auch betriebswirtschaftlich kritisch sind. Unentdeckte Schwachstellen erhöhen die Wahrscheinlichkeit von Cyberangriffen und Datenverlusten.

Von der Pflichtübung zur Managementaufgabe
Die Ergebnisse zeigen, dass Compliance weit über eine formale Pflicht hinausgeht. Sie entwickelt sich zu einer kontinuierlichen Managementaufgabe, die eng mit der Sicherheitsstrategie eines Unternehmens verknüpft ist.

Angesichts weiter steigender Anforderungen prüfen viele Organisationen, wie sie ihre Prozesse effizienter gestalten können. Dazu gehört auch die Zusammenarbeit mit externen Spezialisten, die zusätzliche Expertise und Entlastung bieten.

Weitere Einzelheiten beschreibt Sophos auf seinem Blog (in englischer Sprache): https://www.sophos.com/de-de/blog/is-compliance-complexity-outpacing-it-capacity

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

Pressekontakt:

TC Communications
Arno Lücht, +49-8081-954619

Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de