expertenReport

Quelle: QBE Europe

NIS2: „Die Unternehmen haben ein hohes Eigeninteresse – es geht um ihre Cybersicherheit!“

Die EU hat mit der Verabschiedung der NIS2-Richtlinie eine wichtige Etappe in Richtung einer europaweiten Cyber-Sicherheitslandschaft absolviert. Doch was bedeutet das konkret für betroffene Unternehmen?

Herr Mairhofer, ab Oktober wird es für Unternehmen ernst – die NIS2 Richtlinie kommt. Was bedeutet das konkret?

Die NIS2-Richtlinie ist definitiv eine wichtige Entwicklung in der europäischen Cyber-Sicherheitslandschaft. Gegenüber NIS1 sind die zu erfüllenden Anforderungen an die Unternehmen gestiegen und auch der Kreis der Unternehmen, die unter diese Richtline fallen hat signifikant zugenommen. Die Mitgliedsstaaten müssen die Richtlinie bis zum 17.10.24 in nationales Recht umsetzen. Dabei dürfen sie die vorgegebenen Mindestanforderungen nicht unterschreiten. Auch wenn ein Teil der Vorgaben bei den betroffenen Unternehmen bereits Standard sein dürfte, werden die neuen Regelungen sicher einen guten Beitrag leisten, um die Cybersicherheit der europäischen Wirtschaft zu verbessern.

Mal ganz konkret gefragt: Was können Unternehmen schon heute tun, um den regulatorischen Anforderungen gerecht zu werden? Und ist die Angst vor Bußgeldzahlungen berechtigt?

Unternehmen sollten am besten direkt mit der Umsetzung der Maßnahmen anfangen, da der Aufwand je nach Ist-Stand erheblich sein kann. In Deutschland wird die Richtlinie mit dem NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) umgesetzt, das momentan nur in einem Referentenentwurf mit Stand 24.06.2024 vorliegt und somit noch Änderungen unterliegen kann. Unternehmen sollten allerdings beachten, dass keine weiteren Übergangsfristen vorgesehen sind. Theoretisch können Bußgelder also bereits ab Inkrafttreten des Gesetzes verhängt werden. Klar ist aber auch, dass es im Eigeninteresse der Unternehmen liegen sollte, die eigenen Systeme und Verfahren frühzeitig entsprechend den neuen Regelungen zu optimieren. Schließlich geht es ja darum, die eigene Cybersicherheit zu verbessern.

Verstanden. Welche Standards müssen betroffene Unternehmen Stand heute denn tatsächlich umsetzen?

Es gibt tatsächlich Mindeststandards, die erfüllt sein müssen. Dazu gehören unter anderem Konzepte in Bezug auf die Risikoanalyse und Sicherheit von Informationssystemen, Maßnahmen zur Bewältigung von Sicherheitsvorfällen und Aufrechthaltung des Betriebs. Auch Bereiche wie Schwachstellenmanagement, Zugriffskontrolle und Verschlüsselung sind relevant. Hinzu kommen noch die Themen Sicherheit der Lieferkette, gesicherte

Kommunikation und Cybersicherheitsschulungen – um nur ein paar Beispiele zu nennen.

Das klingt nach ganz schön viel organisatorischem und technologischem Aufwand! Worauf müssen sich Unternehmen einstellen, die die Maßnahmen nicht umsetzen können oder wollen?

Das kann unter der neuen Richtlinie schon richtig weh tun. Unter anderem können Unternehmen verpflichtet werden, die Öffentlichkeit über die Nichteinhaltung der Richtlinie zu informieren. Im Einzelfall können Vorständen oder Geschäftsführern der betroffenen Unternehmen sogar vorübergehend die Wahrnehmung von Leitungsaufgaben untersagt werden. Dazu kommen Geldstrafen: Je nachdem, was höher ist können hier Bußgelder bis 10 Millionen Euro oder bis zu 2 Prozent des globalen Jahresumsatzes verhängt werden. Sie sehen also, warum ich das Eigeninteresse der Unternehmen unterstreiche (lacht).

Solche Strafen wollen Unternehmen logischerweise umgehen. Wieso kann in diesem Zusammenhang auch eine D&O-Versicherung sinnvoll sein?

Die Geschäftsleitungen der unter NIS2 fallenden Unternehmen haben die Pflicht die geforderten Maßnahmen zu billigen und deren Umsetzung zu überwachen. Des Weiteren müssen sie regelmäßig an Schulungen teilnehmen. Eine D&O-Versicherung kann hier hilfreich sein, wenn die Geschäftsleitung wegen einer diesbezüglichen Pflichtverletzung in Anspruch genommen wird.

Ich habe gelesen, dass heute bereits mehr als 40 Prozent der Unternehmen wegen mangelhafter IT-Sicherheit keine Cyber-Versicherung abschließen können. Dieser Anteil würde sich mit in Kraft treten der Richtlinie noch einmal erhöhen, richtig?

Nein. Das Gegenteil ist der Fall! Unternehmen, die bisher aus Kosten- oder Aufwandsgründen auf eine Verbesserung der Cybersicherheit verzichtet haben und jetzt unter die NIS2-Regelung fallen, verbessern mit der Umsetzung der Maßnahmen auch ihre Chancen, eine Cyberversicherung abschließen zu können. Ein schöner Nebeneffekt der neuen Richtlinie.

Vielen Dank für das Gespräch, Herr Mairhofer!

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4929691/nis2-die-unternehmen-haben-ein-hohes-eigeninteresse-es-geht-um-ihre-cybersicherheit/