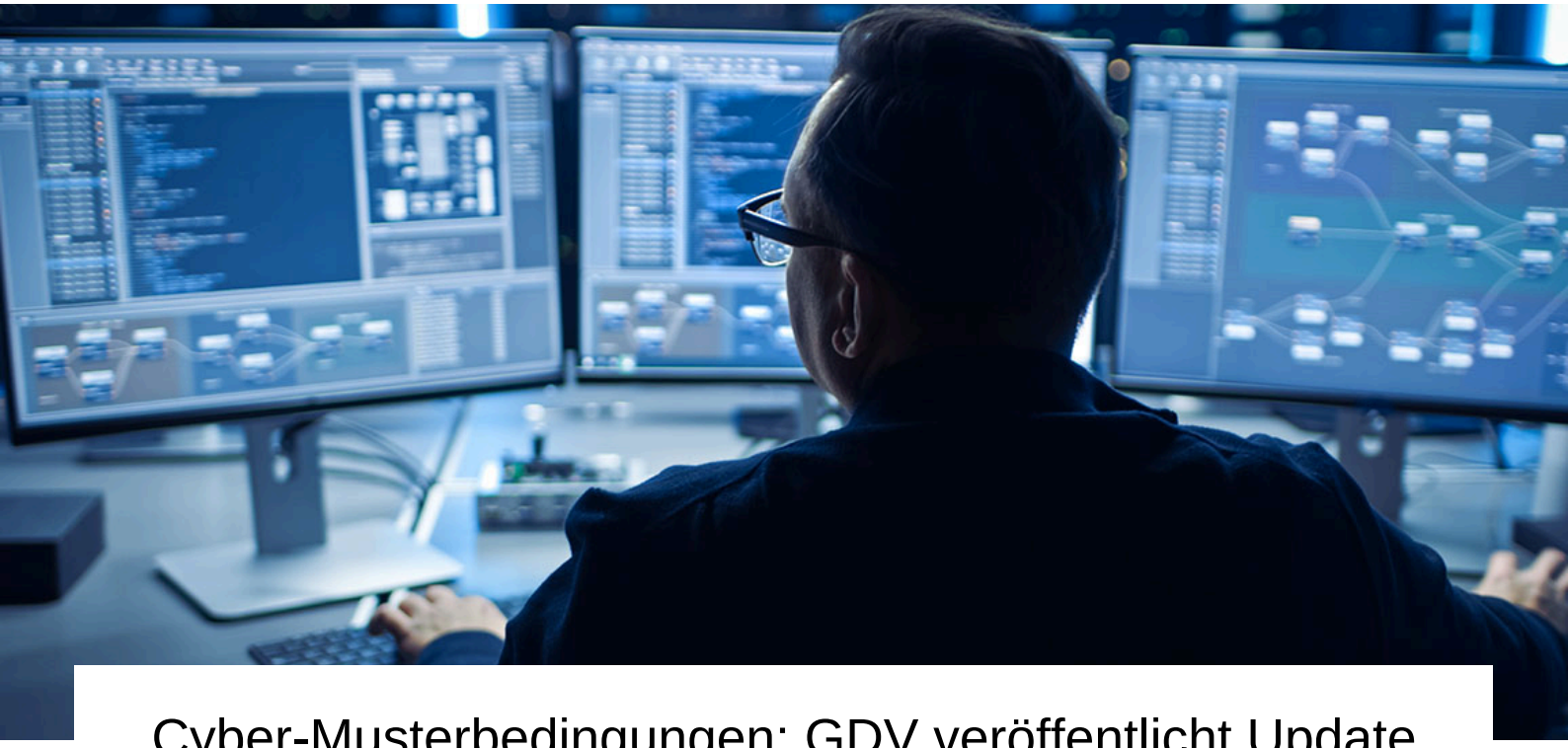

Cyber-Musterbedingungen: GDV veröffentlicht Update

Photo credit: depositphotos.com

Die neuen Musterbedingungen tragen diesen Entwicklungen Rechnung. An der grundlegenden Struktur einer Cyberpolice ändere sich hingegen nichts. GDV-Hauptgeschäftsführer Jörg Asmussen führt dazu aus:

Zu den Anpassungen der unverbindlichen Musterbedingungen zählen unter anderem die folgenden Aspekte:

Mobiles Arbeiten: Die neuen Musterbedingungen stellen klar, dass auch der Fernzugriff auf die Unternehmens-IT versichert ist.

Verletzung von Datenschutzgesetzen: Seit 2018 räumt die Datenschutzgrundverordnung (DSGVO) den Betroffenen eines Datenlecks ein Recht auf Schadenersatz ein. Da von einem solchen Datenleck oft viele Menschen betroffen sind, können diese Zahlungen sehr hoch ausfallen. Dieses Risiko wird in der Neufassung der Musterbedingungen mitversichert.

Krieg und staatliche Angriffe: Die Neufassung stellt klar, dass ein Krieg im Sinne der Bedingungen nicht den Einsatz physischer Waffengewalt voraussetzt. Schäden durch Kriegshandlungen sind auch dann ausgeschlossen, wenn der Krieg mit digitalen Mitteln geführt wird. Darüber hinaus formulieren die neuen Musterbedingungen einen Ausschluss für staatliche Cyberangriffe. Demnach sind Schäden ausgeschlossen, die eine direkte oder indirekte Folge eines erfolgreichen staatlichen Angriffs auf kritische Infrastrukturen sind.

Externe Dienstleister: Schäden infolge einer Störung bei externen Dienstleistern wie Cloud-Anbietern, Rechenzentren oder Software-as-a-Service-Lösungen waren vom Versicherungsschutz bislang ausgeschlossen. Diese Einschränkung wird in den neuen Musterbedingungen größtenteils aufgehoben: Werden beim Dienstleister gespeicherte Daten manipuliert, mit Schadsoftware infiziert oder für unberechtigte Personen zugänglich, besteht Versicherungsschutz. Weiterhin ausgeschlossen bleibt hingegen der Ausfall des Dienstleisters, also die fehlende Verfügbarkeit der Daten.

IT-Sicherheitsniveau: Die vom versicherten Unternehmen zu erfüllenden Obliegenheiten wurden neu formuliert, um den aktuellen technischen Stand abzubilden und das Verständnis beim Leser zu verbessern. Die Basis für ein angemessenes IT-Sicherheitsniveau bilden weiterhin die bekannten, einfach umzusetzenden Maßnahmen wie regelmäßige Datensicherungen, starke Passwörter, individuelle Zugänge, Virenscanner, Firewalls und schnell installierte Sicherheitsupdates.

Mittelstand: Unterschätzte Gefahren aus dem Web vs. Überschätzung des eigenen Sicherheitsniveau

Gerade in kleinen und mittleren Unternehmen würden die Gefahren aus dem Web häufig unterschätzt und das Niveau der eigenen IT-Sicherheit überschätzt.

Neben Wirtschaft und Versicherern müsse aber auch die Politik ihren Beitrag leisten, indem sie klare Zuständigkeiten und Rahmenbedingungen für mehr Cybersicherheit schaffe. Die zuständigen Behörden sollten großflächige Angriffe auf Privatpersonen und Unternehmen schnell erkennen, bekannt machen und idealerweise auch Hinweise zur Abwehr des Angriffs geben. Staatsanwaltschaften und Polizeibehörden sollten sowohl als Partner der Betroffenen agieren als auch einen hohen Ermittlungs- und Fahndungsdruck auf die Täter ausüben. „Erfolge im Kampf gegen Cyberkriminelle sind möglich – setzen aber eine gemeinsame Anstrengung aller Akteure voraus“, so Asmussen.

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4928721/cyber-musterbedingungen-gdv-veroeffentlicht-update/