

Fünf Tipps gegen DSGVO-Bußgelder

Jede Woche ergehen rund 450 Millionen US-Dollar Strafe wegen Verstoß gegen die europäische DSGVO. Die britische Datenschutzbehörde ICO griff kürzlich hart durch. In Deutschland blieben Millionenbußgelder der Datenschutzbehörden der Länder bislang aus. Sophos gibt 5 Tipps zur Vermeidung von DSGVO-Verstößen.

Die Fluggesellschaft British Airways (BA) und die Hotelgruppe Marriott Hotels mussten ihre Verstöße gegen die europäische DSGVO teuer bezahlen. 229 Millionen US-Dollar Strafe für BA, 123 Millionen US-Dollar für Marriott.

Die Bußgelder zeigen, dass dank der DSGVO die Datenschutzbehörden, wie zum Beispiel die britische ICO (Information Commissioner's Office), heute nicht mehr wie Papiertiger dastehen, sondern handeln. So ist die Strafsumme für BA fast 400-fach höher als die bisherige Rekordstrafe der ICO von 645.999 US-Dollar. Die bekam übrigens Facebook ab, für seinen Cambridge Analytica Skandal.

Vor dem Hintergrund dieser neuen Rügen und enormen Summen hat Sophos noch einmal fünf wirkungsvolle Tipps zur Vermeidung von DSGVO-Verstößen zusammengestellt, die sich mit überschaubarem Aufwand für jedes Unternehmen umsetzen lassen.

Fünf Tipps für Unternehmen, DSGVO-Verstöße wie Datenverlust zu vermeiden:

1. **Patchen: so früh und so oft wie möglich.**

Es gilt, das Risiko, Opfer einer Cyberattacke zu werden, so gering wie möglich zu halten. Das geht am besten, indem man die Schwachstellen, die illegalen Eintritt ins System ermöglichen, behebt. Und zwar jede Schwachstelle.

2. **Persönliche Daten in einer Cloud sichern**

Eine Cloud möchte genauso ernstgenommen werden wie ein Computer. Deshalb: Unerwünschte Ports und Services schließen, Daten verschlüsseln und sicherstellen, dass geeignete Zugangskontrollen parat sind. Das ist nötig für sämtliche Umgebungen, inklusive Qualitätskontrolle und Entwicklungsumgebung.

3. **Zugang zu persönlichen Daten auf ein Minimum einschränken**

Die Strategie dahinter: Verkleinern der Angriffsfläche. Je mehr Daten man sammelt, desto mehr kann man verlieren. Deshalb sollten nur diejenigen Informationen behalten werden, die man wirklich braucht. Und zusätzlich sollten nur die Personen darauf Zugriff haben, die diese Dateien für ihre Arbeit benötigen.

4. **Schulungen für Mitarbeiter**

Jeder Mitarbeiter im Unternehmen, der in Kontakt mit persönlichen Daten kommt, muss wissen, wie man diese DSGVO-konform behandelt. Ob Handbücher, regelmäßige Schulungen oder Wikis – jedes Unternehmen sollte die Form finden, die zu ihm passt und seinen Mitarbeitern Sicherheit im Umgang mit Daten vermitteln kann.

5. **Dokumentation und Nachweis von Datenschutzbestimmungen**

Maßnahmen zum Datenschutz sollten gut dokumentiert sein. Für das Unternehmen zur Selbstkontrolle ebenso wie zur externen Überprüfung.

Pressekontakt:

Sophos

Jörg Schindler, PR Manager CEEMEA

joerg.schindler@sophos.com, +49-721-25516-263

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