OUCH! | Mai, 2018

SANS SECURITY AWARENESS

Der monatliche Security Awareness Newsletter für Jedermann

DSGVO

Überblick

Sie haben vielleicht von einem neuen Gesetz namens “EU-DSGVO“ bzw. Datenschutzgrundverordnung gehört. Dieses Gesetz wurde von der Europäischen Union entwickelt und tritt am 25. Mai 2018 in Kraft. Es gilt für jede Organisation, die persönliche Daten von Personen mit Wohnsitz in der Europäischen Union (EU) handhabt, unabhängig davon, wo in der Welt sich diese Organisation befindet. DSGVO, oder in Englisch GDPR, verlangt von Organisationen die Wahrung der Privatsphäre und Sicherheit der personenbezogenen Daten von EU-Bürgern. Um die Einhaltung der DSGVO zu gewährleisten, müssen die wichtigsten Grundsätze verstanden und umgesetzt werden.

Menschen haben ein Recht auf Privatsphäre. Organisationen müssen ihre Privatsphäre respektieren, indem sie einschränken, welche persönlichen Daten sie sammeln und verarbeiten, und indem sie diese Daten schützen. Datenschutzverpflichtungen gelten für alle Informationen, die allein oder zusammen mit anderen Informationen verwendet eine in der Europäischen Union lebende Person identifizieren könnten. Diese Informationen können z.B. Adressen, Passnummern, Führerscheinnummern, finanzielle Details, Biometrie, Gewerkschaftsmitgliedschaften, Krankengeschichte, Standortdaten oder Informationen zur sexuellen, religiösen oder politischen Orientierung einer Person sein. Die Regelung gilt für eine “natürliche Person”, also eine lebende Person. Hier sind einige der wichtigsten Grundsätze der DSGVO, die befolgt werden sollten:

Personenbezogene Daten werden rechtmäßig, fair und transparent verarbeitet.

Den Menschen muss mitgeteilt werden, was gesammelt wird und zu welchem Zweck.

Personenbezogene Daten werden für festgelegte, eindeutige und rechtmäßige Zwecke erhoben. Sie dürfen nicht aus anderen Gründen verwendet werden, die diesen Zwecken zuwiderlaufen.

Personenbezogene Daten werden nur so lange aufbewahrt und verarbeitet, wie es für diesen Zweck erforderlich ist und nicht länger.

Persönliche Daten müssen aktuell und korrekt gehalten werden.

Personen haben das Recht, eine Kopie ihrer Daten zu erhalten oder können verlangen, dass ihre persönlichen Daten nicht mehr verwendet oder in einigen Fällen ganz gelöscht werden.

Organisationen müssen geeignete Sicherheitsmaßnahmen ergreifen, um personenbezogene Daten vor unbeabsichtigter oder unrechtmäßiger Zerstörung, Verlust, Veränderung oder Offenlegung zu schützen.

Darüber hinaus müssen Unternehmen sicherstellen, dass alle Mitarbeiter, die mit personenbezogenen Daten umgehen, angemessen geschult werden, um diese Daten umfassend zu schützen.

Die Maßnahmen zum Schutz personenbezogener Daten müssen ein dem sensiblen Charakter der Daten angemessenes Schutzniveau gewährleisten. Je größer das Risiko, das mit Daten verbunden ist, desto größer sollte der Aufwand und die Ausgaben für Maßnahmen zum Schutz der Daten werden. Diese Maßnahmen sollten regelmäßig überprüft und gegebenenfalls aktualisiert werden. Gut dokumentierte Aufzeichnungen über Datenschutz- und Sicherheitsentscheidungen und -maßnahmen helfen, die Einhaltung der Anforderungen nachzuweisen. Darüber hinaus sind Organisationen gesetzlich verpflichtet, Maßnahmen wie Verträge und Due Diligence-Prüfungen zum Schutz personenbezogener Daten bei der Übermittlung an externe Dritte oder insbesondere an Dritte außerhalb der Europäischen Union zu ergreifen. Im Falle eines Verstoßes gegen den Schutz personenbezogener Daten müssen Organisationen den Vorfall innerhalb von 72 Stunden nach Bekanntwerden melden. Die Nichteinhaltung von DSGVO kann zu Geldbußen von bis zu 4% des globalen Umsatzes führen, was sie zu einer der finanziell kostspieligsten globalen Regelungen der Welt macht.

Deutsche Ausgabe

Diese OUCH! Ausgabe wurde von Marek Kreul und René Wiedewilt aus dem Englischen übersetzt. Beide arbeiten für das CERT eines DAX-Konzerns und haben sich auf IT-Forensik spezialisiert. Sie haben langjährige Erfahrung im Bereich IT-Sicherheit und sind mehrfach GIAC zertifiziert.

Gastautor

Brian Honan *ist CEO von BH Consulting, einem unabhängigen Beratungsunternehmen für Cybersicherheit und Datenschutz in Dublin, Irland. Brian war als Spezialberater für das Europol Cybercrime Centre (EC3) tätig, ist Gründer von Irlands erstem CERT, und sitzt im Beratergremium verschiedener innovativer Sicherheitsunternehmen. Sie finden Ihn auf* www.linkedin.com/in/brianhonan *oder auf Twitter als* @brianhonan.

Weiterführende Informationen

GDPR erklärt (englisch):	http://gdprandyou.ie
Die DSGVO Regularien:	https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:32016R0679
OUCH! Übersetzungen und Archiv:	https://www.sans.org/u/D88