3M | The experts in screen privacy.

DSGVO-Bereitschaft FAQ

Enza Iannopollo, Forrester Research

Enza Iannopollo ist Analystin im Bereich Security & Risk und zertifizierte Datenschutzbeauftragte (CIPP/E). Sie ist bei Forrester in den Bereichen Datenschutz, Analytik und Internet of Things tätig und fokussiert sich auf die Auswirkungen von Regelungen und deren zugrunde liegenden Technologien.

Die DSGVO ist eine der bedeutsamsten Änderungen der Datenschutzvorschriften der letzten 20 Jahre. Sie legt fest, wie Organisationen den Umgang mit personenbezogenen Daten ihrer Kunden, Mitarbeiter und Geschäftspartner dauerhaft handhaben müssen. 3M hat sich vor kurzem mit Enza Iannopollo von Forrester Research zusammengesetzt, um die Sicherheitsmaßnahmen, Richtlinien und Compliance-Programme im Zusammenhang mit dem Datenschutz zu besprechen, die viele Organisationen implementieren um den Vorschriften der DSGVO gerecht zu werden. Enza Iannopollo gab Einblicke in den Bereitschaftsgrad am Arbeitsplatz und unterstrich den Bedarf an physischen Sicherheitsvorkehrungen zum Schutz der Datensicherheit.

Was steht auf dem Spiel?

Organisationen erwarten Strafgebühren von bis zu 4 % ihres Jahresumsatzes bzw.

€20 Mio.

Enza Iannopollo sagte dazu:

F: Ist das Personal auf die Befolgung der DSGVO vorbereitet?

A: Unsere Zahlen zeigen, dass weltweit nur eines von drei Unternehmen auf die Anforderungen der Datenschutz-Grundverordnung (DSGVO) vorbereitet ist. Da die DSGVO am 25. Mai 2018 rechtskräftig wird, liegt es auf der Hand, dass viele Organisationen ihre Vorbereitungen schnell zum Abschluss bringen müssen.

Insbesondere sehen wir Firmen, die sich schwer tun, die Anforderungen der Implementierung und Dokumentation von Datenschutzschulungs und -sensibilisierungsprogrammen für Mitarbeiter zu erfüllen. EU-Vorschriften haben aufgezeigt, dass diese Programme eine Grundvoraussetzung für die DSGVO-Konformität sind. Wir haben ebenfalls festgestellt, dass Organisationen die den Anforderungen gerecht werden, die Datenschutzkultur ihrer Unternehmen deutlich verbessern konnten und damit die Anforderungen der Behörden übertreffen.

F: Sind Unternehmen in bestimmten Regionen besser vorbereitet als andere?

A: 34 Prozent der US-amerikanischen Firmen geben an, dass sie vorbereitet seien, verglichen mit 26 Prozent der Firmen in Europa.[1] Unternehmen, die nicht DSGVO-konform sind –bewusst oder unbewusst –gehen ein großes Geschäftsrisiko ein. Unternehmen, die davon überzeugt sind auf die Veränderungen ausreichend vorbereitet zu sein, dies aber nicht sind, gehen ein noch größeres Risiko ein.

Interessanterweise glauben mehr Unternehmen in den USA vorbereitet zu sein, als in Europa. Dies steht im Zusammenhang mit der extraterritorialen Wirkung der DSGVO. Die Vorschrift betrifft alle Unternehmen – ungeachtet des Standorts – die personenbezogene Daten von Personen mit Wohnsitz in Europa verarbeiten oder speichern. Das bedeutet, dass nicht nur europäische Unternehmen sondern auch viele Unternehmen mit Hauptsitz in den USA diese strikten Datenschutzregeln befolgen müssen.

Wir vermuten, dass ein oberflächliches Lesen der neuen Regeln in Verbindung mit irreführenden und unbegründeten Erwartungen einer schwachen Durchsetzung der DSGVO die eigene Wahrnehmung, bezüglich „DSGVO Readiness“, falsch beeinflussen könnten.

F: Welche physischen Sicherheits- und Datenschutzvorkehrungen fordert die DSGVO?

A: Die DSGVO ist eine prinzipienbasierte Vorschrift. Das heißt, die Regelungsbehörden legen den Organisationen keinen definierten Maßnahmenkatalog vor. Organisationen sollten DSGVO-Anforderungen stattdessen als eine Art “Wunschzustand” für ihre Praktiken im Zusammenhang mit der Handhabung von Daten betrachten. Es bedeutet auch, dass Organisationen spezifische Risiken identifizieren und bewerten müssen, die sie für die Konformität mit den DSGVO-Anforderungen mindern müssen.

Firmen müssen bei der Identifizierung von Risiken vor allem den Prozess der Datenverarbeitung betrachten. Insbesondere infolge eines versehentlichen Verlusts oder einer unbefugten Weitergabe personenbezogener Daten, die übertragen, gespeichert oder auf sonstige Weise verarbeitet werden. Dabei spielt es keine Rolle, ob eine unbefugte Offenlegung von Daten erfolgt, weil ein Hacker eine ausgeklügelte Cyberattacke auf die Website eines Unternehmens verübt oder weil eine fremde Person hochsensible Daten auf dem Laptop-Bildschirm eines Mitarbeiters fotografiert. Beide sind gleichermaßen ernsthafte Risiken und erfordern geeignete Strategien um diese zu minimieren.

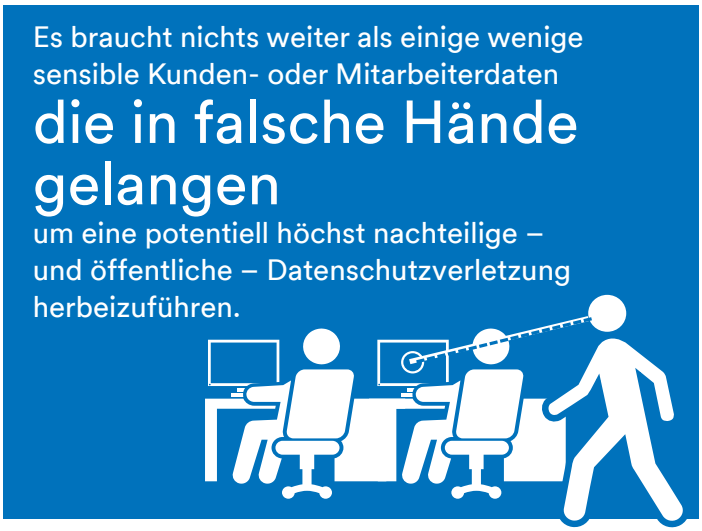
F: Ist visuelles Hacken ein Risiko?

A: Absolut. Denken Sie nur daran: Viele Unternehmen verwenden zum Schutz vor fremden Eingriffen einen Benutzernamen und ein Passwort. Ein Unbefugter braucht nur einen kurzen Blick auf einen ungeschützten Bildschirm zu werfen, um an diese Schlüssel zu gelangen und sich Zugang zu verschaffen. Das Risiko erhöht sich mit der zunehmenden Komplexität von Social Engineering.

Vor einer Weile wurde ein Journalist beim Arbeiten an Bord eines Flugzeugs gehackt.[2] Der Hacker konnte Einzelheiten über einen von dem Journalisten verfassten Artikel, persönliche E-Mails und bevorstehende Meetings beschreiben – alles Informationen, die er nach eigenen Angaben durch Hacken des Bord-WLAN-Systems erfassen konnte. Vielleicht konnte der Hacker diese Daten auch beim Betrachten des Laptop-Bildschirms des Journalisten erschleichen. Der Journalist war wütend, hat aber seine Lektion gelernt: während er an einem sensiblen Artikel arbeitete - in diesem Fall an einer Analyse der tiefen und weitreichenden Weigerung von Apple, einer Anfrage des FBI zum Entschlüsseln des Handys eines Terroristen Folge zu leisten - vergaß er, die Daten und sein geistiges Eigentum auf dem eigenen Gerät zu schützen. So wie dieser Journalist machen viele Organisationen den Fehler, das Risiko von Cyber- und visuellem Hacking zu unterschätzen.

F: Welche Vorteile bringt die Implementierung von technisch unaufwendigen Schutzmaßnahmen?

A: Nonstop-Nachrichten über massive Datendiebstähle lassen leicht vergessen, dass sich die heutige digitale Geschäftswelt weiterhin mit rein physischen Sicherheitsbedrohungen auseinandersetzen muss. Die Implementierung von physischen Sicherheitsmaßnahmen wie Videokameras zur Überwachung, Schlösser für Laptop-Taschen und Blickschutzfilter für Monitore, Laptops, Tablets und Smartphones bietet eine Reihe von Vorteilen. Beispielsweise stellen Blickschutzfilter eine solide Strategie zur Eindämmung von Datenschutzverstößen und Datendiebstahl dar. Es braucht nichts weiter als einige wenige sensible Kunden- oder Mitarbeiterdaten, um eine potentiell höchst nachteilige und öffentliche Datenschutzverletzung herbeizuführen.



Solche Maßnahmen dienen nicht nur der Einhaltung der DSGVO Verordnung, sondern auch anderer Regulationen. Zum Beispiel wurde vor einigen Jahren eine medizinische Assistentin einer Klinik der Universität von Iowa wegen eines Verstoßes gegen den Schutz von Patientendaten entlassen. Sie wurde des visuellen Hackens eines Kollegen bei der Durchsicht der Krankenakten eines Patienten beschuldigt, was ein Verstoß gegen den HIPAA ist.[3]

Physische Sicherheitsvorkehrungen wie Blickschutzfilter können als eine sichtbare Erinnerung der Mitarbeiter dienen, dass Sicherheit und Datenschutz zu den Prioritäten der Organisation zählen. Und wie immer geht es beim visuellen Datenschutz um mehr als nur die Befolgung der Regeln. Es geht um den Schutz der wertvollsten Aktiva eines Unternehmens.

F: Wie können Unternehmen den Datenschutz verbessern, um die positiven Kundenerfahrungen zu steigern?

A: Firmen, die robuste DSGVO- und Datenschutzprogramme durchführen, profitieren von einer Reihe geschäftlicher Vorteile, die über die Regelbefolgung hinausgehen. Dazu gehört die Bereitstellung eines erstklassigen Kundenerlebnisses. Die Art und Weise, wie Ihre Organisation die Daten ihrer Kunden schützt, kann sich direkt auf die Schaffung – oder Zerstörung – des grundlegenden Vertrauens der Kunden auswirken.

Wir wissen zum Beispiel, dass Kunden infolge von Datenschutzverletzungen zu Wettbewerbern überwechseln.[4] Des Weiteren zeigen unsere Untersuchungen des Verbraucherverhaltens im Zusammenhang mit dem Datenschutz, dass Personen sich weigern, eine Online-Transaktion abzuschließen, wenn sie in der Datenschutzerklärung eines Unternehmens etwas lesen, das ihnen nicht gefällt.[5]

Wenn Sie sich engagiert für den Schutz der Daten Ihrer Kunden einsetzen und Ihre Mitarbeiter dieses Engagement bei der Interaktion mit Kunden widerspiegeln, kann Sie dies von Ihren Wettbewerbern abheben.

F: Gibt es Unternehmen, die sich durch ihr Engagement für Datenschutz und Sicherheit hervorheben?

A: Datenschutz hat sich von einem Nischenthema für Rechtsabteilungen zu einem zentralen Wert für viele Organisationen gewandelt. CIOs und CMOs zählen heute zu den Führungskräften, die glauben, dass der Schutz von Datenbeständen vor Attacken und Missbrauch zu ihren höchsten Prioritäten gehören. Unsere Forschungsergebnisse zeigen, dass 23 Prozent der Fortune 100-Unternehmen Datenschutz zu einem Teil ihrer Bemühungen um unternehmerische Sozialverantwortung (CSR) gemacht haben.[6] Ca. 70 Prozent bezogen Datensicherheit in ihre CSR-Berichte ein.

23 % der Fortune 100-Unternehmen
haben Datenschutz zu einem Teil ihrer Bemühungen um unternehmerische Sozialverantwortung (CSR) gemacht.

Wir haben ebenfalls festgestellt, dass Firmen, die sich für Datenschutz und Sicherheit engagieren, von Offenheit und Transparenz hinsichtlich ihres Umgangs mit personenbezogenen Daten profitieren. Dies kann eine extrem vorteilhafte Wirkung auf die Schaffung von Vertrauen bei Kunden, Mitarbeitern und Geschäftspartnern haben. Die Geschäftsabwicklung im Einklang mit diesem Engagement ist jedoch nicht einfach. Organisationen müssen in vielen Fällen ihre Betriebsabläufe anpassen, um dieses Engagement zum Leben zu erwecken und eine Unternehmenskultur zu schaffen, die Datenschutz und Sicherheit als zentrale Werte anerkennt.

F: Stehen weitere Regelwerke wie die DSGVO an?

A: Ohne Zweifel: Die DSGVO signalisiert einen Trend. Wir haben vor kurzem eine neue Studie abgeschlossen, welche die Datenschutzregelungen und -praktiken von 54 Ländern analysiert.[7] Es ist klar, dass Regionen wie der asiatisch-pazifische Raum die DSGVO als eine mögliche Evolution lokaler Datenschutzregeln sehen. Elemente der DSGVO, wie zum Beispiel der Speicherort von Daten, werden ebenfalls in die Datenschutzregeln in Lateinamerika und Russland eingebettet. Auch das Europäische Parlament arbeitet an einer Neufassung der Anforderungen der gegenwärtigen Datenschutzrichtlinien für elektronische Kommunikation. Die Details müssen noch ausgearbeitet werden, aber geplant ist eine Ausrichtung der Anforderungen an die elektronische Kommunikation mit der DSGVO.

3M ist eine Marke der 3M Company. ©3M 2017. Alle Rechte vorbehalten.

[1]Forrester Business Technographics Security Survey, 2017
[2]Digital Trends, “Apple vs FBI shown in different light as journalist hacked mid-flight,” 25. Januar 2016
[3]Veriphyr, “Medical Assistant Fired for “Shoulder Surfing” and Breaching Patient Data Privacy,” 2011
[4]Ponemon Institute, “The Impact of Data Breaches on Reputation and Share Value,” Mai 2017
[5]Forrester Research Consumer Technographics European Online Benchmark Survey (Part 2), 2016
[6]Forrester Report “The Future of Data Security and Privacy: Growth And Competitive Differentiation,” 2017
[7]Forrester “Interactive Data Privacy Heat Map,” 2017

FORRESTER®