3M | The experts in screen privacy.

Preparação para o GDPR Perguntas mais frequentes

Enza Iannopollo, Forrester Research

Enza é uma analista que trabalha na equipa de Security & Risk (Segurança e Risco) e é uma Profissional de Privacidade de Informação Certificada (CIPP/E). Na Forrester, o seu trabalho envolve a proteção de dados, privacidade, dados analíticos e a Internet das coisas, com um foco no impacto dos regulamentos e nas tecnologias subjacentes.

O GDPR (Regulamento Geral sobre a Proteção de Dados) é uma das mais importantes alterações na regulamentação da privacidade dos dados dos últimos 20 anos. Estabelece os procedimentos que as organizações têm de respeitar no processamento dos dados pessoais dos seus clientes, funcionários e parceiros empresariais numa base de continuidade. A 3M conversou recentemente com Enza Iannopollo da Forrester Research para debater as medidas de segurança, as políticas e os programas de conformidade com a privacidade que muitas organizações estão a implementar para passar a atuar em conformidade com os regulamentos como o GDPR. Enza falou-nos sobre a preparação no local de trabalho e realçou a necessidade de salvaguardas físicas para proteger contra ameaças à privacidade dos dados.

O que está em jogo?

As organizações podem ser alvo de coimas cujos valores ascendem até 4% do volume de negócios anual a nível mundial ou

€20 milhões

Eis o que nos disse:

P.: Estão os trabalhadores preparados para atuar em conformidade com o GDPR?

R.: A nível mundial, os nossos números revelam que apenas uma em cada três empresas está preparada para atuar em conformidade com o Regulamento Geral sobre a Proteção de Dados (GDPR). Como o GDPR entrará em vigor a 25 de maio de 2018, torna-se evidente que muitas organizações terão de se apressar para concluir os preparativos.

Mais concretamente, temos visto empresas que estão com dificuldades em cumprir com as exigências ao nível da implementação, com dificuldades no âmbito da formação para a privacidade dos documentos e também no âmbito dos programas de sensibilização dos funcionários. Os reguladores da UE indicaram que estes programas são essenciais para a conformidade com o GDPR. Entretanto, descobrimos que as organizações que já cumprem com este requisito melhoraram a sua cultura de privacidade empresarial e estabeleceram melhores práticas que, por vezes, vão além dos requisitos regulamentares.

P.: Há empresas de determinadas regiões que estão mais preparadas do que outras?

R.: 34 por cento das empresas dos EUA afirmam que estão preparadas, em comparação com 26 por cento das empresas na Europa.[1] As empresas que não estão em conformidade com o GDPR, independentemente de estarem ou não cientes desse facto, correm um grande risco empresarial. As empresas que acreditam estar preparadas, mas que, de facto, não estão, correm um risco ainda maior.

É interessante observar que existem mais empresas que acreditam estar preparadas nos EUA do que na Europa. Esta situação está relacionada com o efeito extraterritorial do GDPR. O regulamento aplica-se a todas as empresas, independentemente da respetiva localização, que processam ou detêm dados pessoais de residentes da União Europeia. Isto significa que além das empresas europeias, muitas empresas sediadas nos EUA também terão de estar em conformidade com estas normas de privacidade rigorosas.

Suspeitamos que a perceção de preparação das empresas possa estar comprometida, possivelmente devido a uma leitura superficial das normas e a expetativas enganadoras e infundadas de uma execução deficiente do GDPR.

P.: Quais são as salvaguardas físicas de segurança e privacidade exigidas pelo GDPR?

R.: O GDPR é um regulamento baseado em princípios. Isto significa que os reguladores não disponibilizam às organizações um conjunto de ações definitivas que devem respeitar. Em vez disso, as organizações devem encarar os requisitos do GDPR como uma espécie de "condição desejada" para as suas práticas de processamento de dados. Também significa que as organizações têm de identificar e avaliar determinados riscos que necessitam de mitigar para estar em conformidade com os requisitos do GDPR.

Para a identificação de riscos, as empresas têm de ter em conta todos os riscos apresentados pelo processamento de dados, em particular, devido à perda acidental ou ilícita, divulgação ou acesso não autorizados de dados pessoais transmitidos, armazenados ou, de outra forma, processados. Não interessa se uma divulgação de dados não autorizada ocorreu porque um pirata informático lançou um ciberataque sofisticado ao Web site de uma empresa ou porque um estranho tirou fotografias de dados extremamente sensíveis que estavam visíveis no ecrã do portátil de um funcionário. Ambas as situações representam sérios riscos e necessitam de estratégias de mitigação adequadas.

P.: A intrusão visual é um risco?

R.: Sem dúvida. Basta ter em conta o seguinte: as chaves que dão acesso ao reino de muitas organizações apresentam-se sob a forma de um nome de utilizador e de uma palavra-passe. Basta apenas olhar brevemente para um ecrã desprotegido para um indivíduo não autorizado obter esses dados e o consequente acesso. Além disso, o risco aumenta com o aumento da sofisticação da engenharia social.

Há um ano, um jornalista foi vítima de pirataria informática enquanto trabalhava num avião.[2] O pirata informático conseguiu descrever detalhes sobre um artigo que o jornalista estava a escrever, os e-mails pessoais que tinha enviado e as reuniões de trabalho agendadas. O pirata afirmou que todas estas informações foram obtidas ao piratear a rede de Wi-Fi do avião. Contudo, também é possível que possa simplesmente ter olhado para o ecrã do portátil do jornalista e, dessa forma, ter obtido as informações. O jornalista ficou revoltado, mas entendeu a mensagem: enquanto trabalhava num artigo sensível, neste caso em particular, um artigo que dissecava as repercussões profundas e de grande alcance da recusa da Apple em aceder ao pedido do FBI para desencriptar o telemóvel de um terrorista, esqueceu-se de proteger a privacidade e a propriedade intelectual do seu próprio dispositivo. Tal como aconteceu com este jornalista, muitas organizações cometem o mesmo erro de subestimar os riscos da intrusão visual e da pirataria informática.

P.: Quais são as vantagens da implementação de salvaguardas físicas de baixa tecnologia?

R.: Devido às inúmeras notícias sobre violações de dados de grande escala, é fácil esquecermo-nos de que as empresas digitais da atualidade continuam a ter de enfrentar desafios de segurança física. Há várias vantagens associadas à implementação de salvaguardas físicas, tais como câmaras de videovigilância, cadeados para as malas de portáteis e filtros de privacidade para monitores, portáteis, tablets e smartphones. Os filtros de privacidade, por exemplo, são uma sólida estratégia de mitigação de violações de privacidade e de dados. Basta que os dados sensíveis de clientes ou de funcionários sejam expostos aos olhos errados para ocorrer uma violação de dados extremamente prejudicial e altamente publicitada.

Além disso, estes filtros também estão em conformidade com outros regulamentos além do GDPR. Por exemplo, uma médica assistente foi despedida de um hospital da Universidade de Iowa há alguns uns anos por ter violado as normas de privacidade dos dados dos pacientes. Foi acusada de intrusão visual a um colega de trabalho enquanto este examinava o registo médico de um paciente, o que constitui uma violação da HIPAA (Lei de Portabilidade e Responsabilidade de Seguros de Saúde).[3]

As salvaguardas físicas, tais como os filtros de privacidade, podem servir como um lembrete visual para os funcionários de que as melhores práticas de segurança e privacidade são prioritárias para a organização. Além do mais, à semelhança de outros aspetos da privacidade visual, não se trata apenas de respeitar os requisitos de conformidade. Trata-se de proteger os ativos mais valiosos de uma empresa.

P.: De que forma é que as empresas podem tirar partido da privacidade para proporcionar uma experiência de cliente superior?

R.: As empresas que estão a levar a cabo programas sólidos no âmbito do GDPR e da privacidade estão a obter várias vantagens empresariais para além da conformidade. Proporcionar uma experiência de cliente superior é uma

delas. Os procedimentos de proteção dos dados dos clientes da sua organização podem ter um impacto direto na criação ou na destruição do sentimento de confiança subjacente que os clientes depositam em si.

Por exemplo, sabemos que os clientes mudam para a concorrência em resultado de uma violação de privacidade.[4] Além disso, o nosso estudo sobre as atitudes dos consumidores em relação à privacidade sublinha que 30 por cento dos indivíduos se recusam a efetuar uma transação online se lerem algo que lhes desagrada no aviso de privacidade da empresa.[5]

Se existir um compromisso em proteger os dados dos seus clientes e os seus funcionários o reconhecerem e refletirem nas suas interações com os clientes, esse compromisso pode distinguir a organização perante a concorrência.

P.: Existem empresas que se destacam pelo seu compromisso para com a privacidade e segurança?

R.: A privacidade deixou se ser um tópico de nicho para os departamentos jurídicos e passou a ser um valor essencial para muitas organizações. Atualmente, os CIOs e os CMOs estão entre os executivos para quem a proteção dos ativos de dados contra ataques e utilização indevida é uma das principais prioridades. O nosso estudo revelou que 23 por cento das empresas Fortune 100 incluíram a privacidade nos seus esforços de responsabilidade social corporativa (RSE).[6] Cerca de 70 por cento incluiu a segurança nos respetivos relatórios de RSE.

23% das empresas Fortune 100

incluíram a privacidade nos seus esforços de responsabilidade social corporativa (RSE).

Também notamos que as empresas empenhadas na privacidade e segurança obtêm benefícios pela sua abertura e transparência quanto à forma de processamento dos dados pessoais. Isto pode revelar-se uma forma extremamente valiosa de gerar confiança entre os clientes, funcionários e parceiros empresariais. Contudo, trabalhar em conformidade com este compromisso não é uma tarefa simples. Muitas vezes, as organizações têm de alterar a sua forma de funcionamento para fazer destes compromissos uma realidade e estabelecer uma cultura empresarial que reconheça a privacidade e a segurança como valores essenciais.

P: Há mais regulamentos como o GDPR a serem elaborados?

R.: Não restam dúvidas: o GDPR é indicador de uma tendência. Recentemente, concluímos um novo estudo que analisa as práticas e os regulamentos de privacidade de 54 países.[7] Torna-se evidente que regiões como a Ásia-Pacífico encaram o GDPR como uma possível evolução das normas de privacidade locais. Elementos do GDPR, como o local de residência dos dados, também estão a ser incorporados em normas de privacidade de dados na América Latina e na Rússia. Por fim, o Parlamento Europeu está atualmente a trabalhar na atualização dos requisitos da Diretiva Privacidade Eletrónica atual. Ainda é necessário trabalhar nos detalhes, mas o plano consiste em alinhar os requisitos da privacidade eletrónica com o GDPR.

[1]Forrester Business Technographics Security Survey, 2017
[2]Digital Trends, "Apple vs FBI shown in different light as journalist hacked mid-flight", 25 de janeiro de 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", maio de 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®