Proteção de dados e segurança cibernética em um cenário pós-GDPR

#KingstonIsWithYou

Proteção de dados e segurança cibernética em um cenário pós-GDPR

Prefácio

Inúmeras empresas e organizações trabalharam muito, e contrataram muito, para se prepararem para o GDPR. Talvez a sua tenha sido uma delas. E ainda a natureza sempre em evolução das ameaças cibernéticas significa que você não pode parar e recuperar o fôlego. A conformidade com o GDPR não é um exercício de múltipla escolha, mas uma estrutura para você avaliar sua proteção de dados atual e suas iniciativas de segurança cibernética. Não há espaço para acomodação.

Neste pequeno eBook, nós reunimos o conhecimento de alguns dos analistas em segurança cibernética mais experientes do Reino Unido para discutir como a proteção de dados mudou desde a introdução do GDPR. Também incluímos o modo como as empresas estão instruindo seus funcionários sobre a necessidade de conformidade e discutindo como os departamentos de TI e provedores de tecnologia podem proteger melhor a infraestrutura de TI e instruir os usuários finais sobre os desafios de segurança emergentes.

Proteção de dados e segurança cibernética em um cenário pós-GDPR

Colaboradores

Este pequeno eBook foi compilado por cinco especialistas em proteção de dados e segurança cibernética.

Rob Allen
@Rob_A_kingston

Rob é o Diretor de Marketing e Serviços Técnicos na Kingston Technology e está na empresa desde 1996. Em sua função, Rob é responsável por supervisionar RP, Mídia Social, Marketing do Canal com a Mídia de Marketing Digital e Criativa para todas as marcas e produtos da Kingston.

Tara Taubman-Bassirian
@clarinette02

Tara possui múltiplos títulos: advogada, defensora, mediadora, pesquisadora, consultora, palestrante e escritora. Com um conhecimento incrível em áreas como privacidade, propriedade intelectual e proteção de dados, ela se destacou em diversas partes do mundo, em especial no Reino Unido, na França e nos EUA.

Rafael Bloom
@rafibloom73

Rafael é Diretor da Salvatore ltd. Nessa função, ele ajuda empresas a enfrentar as oportunidades e os desafios estratégicos, comerciais e processuais criados pelas mudanças tecnológicas e regulatórias.

Miriam Brown
@Kingston_MBrown

Gerente de Marketing Estratégico B2B da Kingston ela está na empresa desde 1997. Em sua função, Miriam é responsável pela estratégia, conteúdo e campanhas de marketing para todos os produtos B2B da Kingston.

Sally Eaves
@sallyeaves

A Prof. Sally Eaves foi descrita como uma 'força avançada na tecnologia ética. Ela traz consigo a experiência profunda dos cargos que exerceu como Diretora Executiva e Diretora de Tecnologia, como Mestre em Tecnologias Emergentes e como Consultora em Estratégia Global. Sally é uma importante e premiada oradora, autora, pesquisadora e influenciadora líder com ideias originais e autênticas.

Proteção de dados e segurança cibernética em um cenário pós-GDPR

Índice

Seção 1	Como a proteção de dados mudou desde o GDPR?	5 – 7
Seção 2	Como as organizações estão instruindo seus funcionários?	8 - 9
Seção 3	Os departamentos de TI podem proteger melhor os dispositivos?	10 - 11
Seção 4	Como os provedores de tecnologia podem melhorar processos e o entendimento?	12 - 13
	Resumo	14
	Sobre a Kingston	15

Seção 1 – Como a proteção de dados mudou desde o GDPR?

As empresas percorreram um longo caminho. Nos últimos dois anos, as equipes jurídicas se expandiram, o recrutamento de Profissionais de Proteção de Dados aumentou vertiginosamente[1] e cresceu a consultoria externa sobre privacidade de dados. A realização de avaliações do impacto da proteção de dados (DPIAs) agora é conhecida por milhares de organizações.

Mas há um longo caminho à frente.

Um dos maiores desafios relacionados ao GDPR é que você não pode tirar o olho da bola. Na maioria das organizações, quase todos os membros da equipe, em determinado momento, poderiam violar as regras. O problema é ampliado em setores onde a força de trabalho é sobrecarregada ou existe um alto grau de autonomia - como cuidados médicos, educação e legal.

Na legislação, por exemplo, muitos advogados não pensariam nada sobre a troca de dados reservados através de um simples anexo de e-mail. Profissionais de saúde trocariam dados de um paciente ou os resultados de um exame de imagem utilizando endereços de e-mail não seguros. Em organizações com alto nível de estresse, tudo o que é preciso é uma pequena pressão extra na lista de tarefas para a conformidade ir para o espaço. A produtividade – parece – se sobrepõe ao protocolo.

Isso deve mudar.

Então há a questão de conscientização no setor beneficente. Com muita frequência, as instituições beneficentes pensam ser isentas do GDPR. Mesmo que entendam que o GDPR se aplica a todas as organizações privadas, públicas e do terceiro setor, essas instituições ficam, talvez compreensivamente, relutantes em desviar dinheiro de sua causa para investir em proteção de dados. Isso é nobre mas também ingênuo da parte delas. As possíveis multas por infringir o GDPR encobrem o provável gasto em TI.

Desde 2016 a demanda por Profissionais de Proteção de Dados (DPOs) aumentou vertiginosamente em mais de 700%.

Tara Taubman-Bassirian
@clarinette02

GDPR, Proteção de Dados e Consultoria de Propriedade Intelectual

"Muitas organizações do terceiro setor dizem: 'O GDPR não se aplica a nós, somos apenas uma instituição beneficiente." Até na conformidade do site, eu tento lhes dizer que não se trata de dados que desejam coletar, trata-se do terceiro que se permite que tenha acesso aos dados de seus visitantes."

1. Varonis: Um ano na vida do GDPR: Estatísticas e conclusões obrigatórias www.varonis.com/blog/gdpr-effect-review/ [accessed 11/26/2019]

Como a proteção de dados mudou desde o GDPR?

A minimização de dados é uma tendência encorajadora

Vivemos em uma era onde a coleta de dados é notória. "The Big Four" (Google, Apple, Facebook e Amazon) guardam enormes quantidades de dados de clientes. Pressupõe-se que outras organizações imitem as The Big Four e coletem o máximo de dados possível. E ainda, quanto mais dados você possui, maior o risco ao qual se expõe. Uma das tendências mais positivas vistas desde a introdução do GDPR é uma rebelião contra a coleta excessiva de dados. As empresas inteligentes adotam uma atitude de minimização de dados: se não precisar, não colete.

Tara Taubman-Bassirian
@clarinette02

GDPR, Proteção de Dados e Consultoria de Propriedade Intelectual

"A minimização de dados é provavelmente um dos melhores princípios do GDPR. A criação de um banco de dados significa criar riscos."

Rob Allen
@Rob_A_kingston

Diretora de Marketing e Serviços Técnicos, Kingston Technology

"Nós temos regras rígidas de exclusão de dados. Sim, dados críticos para os negócios devem ser armazenados corretamente. Mas e todo o resto? Depois de passado um ano. Qual a razão para manter os dados?"

Os benefícios se estendem além de apenas limitar os riscos. O marketing, por exemplo. Se o seu banco de dados de marketing não for limpo, você pode estar conservando dados obsoletos. Quando seu banco de dados chega em dezenas de milhares de pessoas e você realiza frequentes campanhas de marketing, os custos aumentam. Ele desvirtua as estatísticas de desempenho da sua campanha.

A minimização de dados se aplica também aos dados físicos. Cuidado com o que você imprime (como a digitalização de passaportes de clientes); cuidado com o que você escreve (como senhas de contas). E quando você precisar guardar uma cópia física de algo, conserve-a em lugar seguro. A pilha de documentos sobre sua mesa pode ser impressionante. Mas segura ela não é.

Rafael Bloom
@rafibloom73

Director, Salvatore Ltd.

"Estamos testemunhando um modo de pensar completamente diferente sobre a interface entre tecnologia e o que uma empresa está efetivamente fazendo. O nível de maturidade digital na liderança empresarial precisava desesperadamente acontecer."

Impacto da exposição: da C-suite para o cliente

A proteção de dados como um conceito regulatório existe há decadas. Mas as altas multas impostas até hoje a empresas incluindo Google[1], British Airways e a cadeia de hotéis Marriott[2] – e a cobertura da mídia que geraram - chamou a atenção da C-suite para o GDPR . Isso causou um efeito multiplicador, trickle-down no original.

1. Varonis: Um ano na vida do GDPR: Estatísticas e conclusões obrigatórias www.varonis.com/blog/gdpr-effect-review/ [accessed 11/26/2019]
2. The Guardian: Multas do GDPR: para onde irão as £300m da BA e Marriott? www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog [accessed 11/26/2019]

Como a proteção de dados mudou desde o GDPR?

Continuação...

Outra força acionadora por trás da adoção de forte proteção de dados é a empresa colaborativa. Agora as grandes empresas realizam uma ampla diligência prévia sobre a integridade da segurança de dados de potenciais fornecedores porque não desejam ser responsáveis por violação de dados por associação com seu nome.

Também existe um outro lado da maior conscientização comercial do GDPR: os clientes estão mais cientes dos seus direitos sobre os dados. E sabem que se uma empresa perde o controle sobre seus dados (note bem, não precisa necessariamente haver uma violação), eles têm direito a uma indenização. As empresas devem estar atentas.

Sally Eaves
@sallyeaves

CEO e Diretora,
Sally Eaves Consultancy

"A proteção de dados tornou-se um imperativo de negócios onde a confiança pode ser obtida ou perdida."

Seção 2 – Como as organizações estão instruindo seus funcionários?

Treinamento de Pessoal: palavras capazes de provocar bocejos em sua força de trabalho.

Maior razão para garantir que seu treinamento é envolvente. Uma força de trabalho instruída tem menos probabilidade de violar as boas práticas de proteção de dados. E se houver uma violação de dados, o gabinete do comissário da informação (Information Commissioner's Office - ICO) vai examiná-la mais favoravelmente em seu julgamento, se você puder provar que se empenhou para treinar sua equipe em segurança de dados.

Rafael Bloom
@rafibloom73

Diretor,
Salvatore

"Eu gosto de pensar em dados como um item da cadeia de suprimentos, onde sua procedência e todo o seu ciclo de vida precisam ser controlados de maneira apropriada. Está tudo bem reunir sua equipe em uma sala por meia hora e dizer a eles o que fazer, por favor não rasguem as coisas, por favor tenham uma senha decente. Com certeza, você reduziu o risco para a organização. Mas, mais tarde, há realmente uma diferença material além daquele pequeno impacto inicial que você meio que impôs às pessoas? Não."

Entretanto, em abril de 2019, a Ministra Digital Margot James sugeriu que três em dez organizações do Reino Unido treinaram as equipes para lidar com ameaças cibernéticas[1]. Está na hora de levar a sério o treinamento.

Tem a ver com criar cultura, não com treinamento de múltipla escolha

Treinamento é influenciar mudanças comportamentais e culturais genuínas e não marcar caixas. É fácil comprar um pacote de treinamento on-line com algumas perguntas fáceis sobre proteção de dados que ninguém sabe responder corretamente. Mas isso vai realmente ajudar a proteger sua organização?

A boa conduta em proteção de dados possui dois ingredientes básicos. Em primeiro lugar, treinamento inteligente e envolvente, configurado de acordo com os desafios exclusivos de sua organização. Em segundo lugar, reconhecer que o GDPR é uma questão de cultura do local de trabalho que influencia todos os funcionários diariamente. É fazer as coisas certas com os dados, conduzindo-os de modo correto através da organização. Os RH, por exemplo. Pense em todos os dados pessoais de candidatos que estão parados nos servidores de e-mail. A proteção de dados é responsabilidade de todos.

1. Intelligent CISO: Após um ano, qual foi o impacto do GDPR na segurança de dados? www.intelligentciso.com/2019/04/16/one-year-on-what-has-been-the-impact-of-gdpr-on-data-security/ [accessed 11/26/2019]

Como as organizações estão instruindo seus funcionários?

Há uma pessoa por trás dos dados

Na primeira seção observamos que os consumidores estão mais cientes dos direitos sobre seus dados. Um bom modo de posicionar o treinamento em proteção de dados é ajudar sua equipe fazer a conexão de que há sempre uma pessoa por trás dos dados. Peça a seus funcionários para pensar em todas as organizações às quais forneceram dados e perceber que proteção de dados está relacionada à privacidade pessoal.

Ter um plano de contingência

Sally Eaves
@sallyeaves

"A instrução contínua de funcionários sobre segurança e privacidade de dados é um imperativo para as empresas. Ela não deve ser uma sessão de treinamento isolada, uma vez por ano, mas uma experiência proativa, interativa e envolvente para que faça parte da experiência de trabalho diária. Os funcionários devem estar envolvido no diálogo sobre o que queremos mitigar, controlar e defender."

Miriam Brown
@Kingston_MBrown

"Acho interessante durante o treinamento quando você diz às pessoas: 'e se fossem seus dados?' Se o gerente do meu banco estivesse trabalhando de casa em seu laptop e tivesse informações reservadas naquele laptop, eu gostaria que estas estivessem em uma unidade criptografada."

Rob Allen
@Rob_A_kingston

"Trate os dados como se fossem seus."

Seção 3 –
Os departamentos de TI podem proteger melhor os dispositivos?

O trabalho remoto é o novo normal

Sua equipe provavelmente acessa seu mundo de trabalho de diversos dispositivos diferentes - incluindo dispositivos pessoais que podem facilmente ser deixados em um trem ou perdidos em um táxi. Seu desafio é encontrar um meio de ajudar sua equipe a trabalhar com eficiência sem ficar vulnerável a riscos de segurança e violações de dados. Só é preciso uma pessoa para derrubar todos os seus esforços na proteção de dados.

Sally Eaves
@sallyeaves

CEO e Diretora,
Sally Eaves Consultancy

"Dados precisam ser protegidos em trânsito, quando inativos e em uso - é crucial ter um plano abrangente de segurança, recuperação e eliminação de dados para englobar todos esses contextos. Chamar atenção para áreas de risco que frequentemente são subestimadas é especialmente importante, por exemplo, USBs não criptografado, utilizar e-mail para enviar anexos não criptografados e recursos de navegador expondo dados reservados do usuário. Com tantos dispositivos conectados e a evolução dos padrões de trabalho, é crítico assegurar que os dados armazenados em um telefone celular estão tão seguros quanto os dados armazenados em um servidor da empresa."

Autenticação de dois fatores

Para uma organização média, de longe a coisa mais fácil e eficiiente que se pode fazer é proteger o perímetro da sua rede – e isso pode ser tão simples quanto o uso de gerenciadores de senha e autenticação de dois fatores. Um bom exemplo da autenticação de dois fatores é quando solicitamos a um usuário uma senha em um laptop e também um código que foi enviado ao seu telefone celular depois que uma senha válida tenha sido fornecida.

VPNs e SSDs/USBs criptografados

VPNs são cada vez mais populares com SMEs. São especialmente importantes para a equipe que acessa dados da empresa em redes públicas de WIFI. Mas as empresas devem ser cuidadosas para não superestimar as capacidades das VPNs. Elas são parte, mas não a solução completa. Com muita frequência as empresas implantam VPNs, apenas para trabalhadores remotos para serem usadas em laptops ou notebooks sem qualquer criptografia de hardware. Quase todo mundo armazena arquivos em seu laptop. O que acontece se esse dispositivo é hackeado, perdido ou roubado? USBs e SSDs criptografados são apenas marginalmente mais caros do que as versões padrão. Implantar USBs criptografados e equipar seus notebooks com SSDs com criptografia de hardware resolve bastante os desafios do trabalho remoto. E se um dispositivo for perdido ou roubado, você pode ter certeza que ninguém terá acesso aos arquivos criptografados. Você pode até destruir remotamente USBs perdidos.

"Conheci certa vez um especialistas em segurança cibernética que tentou persuadir o CEO de uma empresa a adotar a autenticação de dois fatores e encontrou muita resistência: 'Não, não faremos isso, é desagradável, uma etapa extra, eu não quero isso.' Logo depois a empresa foi vítima de uma fraude de £40.000."

Rafael Bloom
@rafibloom73

Diretor, Salvatore Ltd

"No final o melhor método para aumentar a conscientização em segurança é abrir discussões com os funcionários para encontrar estratégias que sejam tanto seguras quanto produtivas."

Rob Allen
@Rob_A_kingston

Diretora de Marketing e Serviços Técnicos, Kingston Technology

Os departamentos de TI podem proteger melhor os dispositivos?

Servidores privados e MSPs

Um número crescente de grandes organizações está avançando para ter novamente seus próprios servidores no local. Isso significa ter total controle sobre as instalações do seu servidor, com nada armazenado na nuvem publicamente acessível. Existem também soluções de servidores híbridos onde dados não sigilosos ficam na nuvem, mas dados pessoais permanecem no local. Para SMEs e organizações do terceiro setor, pode ser muito dispendioso ter o próprio servidor. E é onde provedores de serviços gerenciados e servidores privados virtuais aparecem. Melhora o foco em segurança, sem inflar drasticamente seus custos operacionais.

Sinalização automática da data de expiração

Um dos princípios do GDPR é a necessidade de excluir dados antigos. Certos tipos de dados pessoais, por exemplo, não devem ser mantidos por mais de sete anos. E se você fosse avisado automaticamente quando os dados estiverem próximos de 'expirar'? Com o banco de dados certo, seria fácil para sua equipe de TI criar uma ação que enviasse automaticamente um e-mail para o DPO quando estivesse se aproximando a data de uma eliminação no sistema de retenção de dados.

Trabalhar com os fornecedores certos

Em se tratando de segurança de TI, existem inúmeros fabricantes e fornecedores. Faça sua pesquisa. A questão é ter um sistema instalado que venha de um fornecedor confiável com experiência específica em habilitar organizações em sua indústria ou setor. Assegure-se de que o(s) fornecedor(es) que escolher, não tenham apenas a tecnologia, mas também compreendam os desafios da implantação em relação à segurança de dados.

Seção 4 – Como os provedores de tecnologia podem melhorar processos e o entendimento?

TLC para o DPO

Desde 2016 a demanda por profissionais de proteção de dados (DPOs) aumentou vertiginosamente em mais de 700%.[1] Hoje, há mais de 500.000 DPOs empregados em toda a Europa – isso é seis vezes mais do que foi previsto em 2017.[2] E ainda a importância da função de DPO é frequentemente subestimada e banalizada.

Um DPO necessita de total visibilidade do cenário de segurança e privacidade de dados da sua empresa. É um emprego de tempo integral. E ainda em algumas organizações o 'DPO' é simplesmente um rótulo dado a um membro da equipe que entende melhor de tecnologia. Eles são responsáveis pela privacidade de dados de toda a empresa, tudo isso realizando as tarefas normais do seu trabalho diário.

A realidade é que precisamos disponibilizar uma série de serviços profissionais e ferramentas para apoiar essa nova geração de DPOs. Mesmo se você tiver um DPO em tempo integral, a segurança de dados avança depressa e sempre haverá desafios que exijam uma segunda opinião. Trabalhar com uma consultoria externa ou consultor em segurança de dados pode ajudar muito, mas primeiro você precisa que tudo esteja tão em ordem quanto possível internamente.

Clareza, contingência e coesão

Sua infraestrutura de TI somente é tão forte quanto seu elemento mais fraco. É por essa razão que em qualquer adição ao seu ecossistema de TI, seu provedor de tecnologia deve fornecer total clareza sobre as ameaças potenciais à segurança e orientação clara sobre como usar seu novo produto de forma segura.

Tara Taubman-Bassirian
@clarinette02

GDPR, Proteção de Dados e Consultoria de Propriedade Intelectual

"Eu tento explicar às pessoas que instalam câmeras CCTV em todos os lugares que isso não se trata necessariamente de segurança, porque geralmente estas são instaladas sem uma senha. Assim, você pode apenas se conectar a um a website, sentar e assistir. Ísso é na verdade dizer ao seu ladrão: 'venha e procure qundo eu não estiver aqui!"

1. Varonis: Um ano na vida do GDPR: Estatísticas e conclusões obrigatórias www.varonis.com/blog/gdpr-effect-review/ [accessed 11/26/2019]
2. The Guardian: Multas do GDPR: para onde irão as £300m da BA e Marriott? www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog [accessed 11/26/2019]

Como os provedores de tecnologia podem melhorar processos e o entendimento?

Existe a questão de contingência. O que acontece quando um produto alcança o fim de sua vida útil ou precisa de atualização? Os provedores de tecnologia devem fornecer orientação sobre a contingência relacionada a seus produtos que possam inadvertidamente comprometer os dados que contêm ou expor a segurança de todo o ecossistema de TI. Considere um exame de ressonância magnética, por exemplo. Ele pode vir em um SSD criptografado de quatro terabytes para armazenar imagens de pacientes. Mas o que acontece quando o armazenamento acaba?

Os provedores de tecnologia e as próprias organizações também devem proporcionar um ambiente de coesão digital e coesão de dados - ambos dentro da organização e ao trabalhar com fornecedores e parceiros externos. Isso é especialmente crítico para organizações multifacetadas, com muitos departamentos e localizadas em muitos locais como o NHS (Serviço Nacional de Saúde do Reino Unido).

Miriam Brown
@Kingston_MBrown

Gerente de Marketing Estratégico B2B na Kingston Technology

"Nós vendemos muitos produtos para o NHS - mas há diferenças definidas nos graus de confiança, quando perguntamos quais políticas e protocolos eles têm em vigor."

Explorando o horizonte

A tecnologia se move rápido, às vezes ultrapassando a segurança. Com as tecnologias emergentes, como pagamento atráves de reconhecimento facial na China, às vezes é o caso das organizações correrem para conseguir a tecnologia antes de considerarem as implicações potenciais de segurança e proteção de dados. A disponibilidade generalizada de redes 5G está a um ano ou dois à frente, onde a computação de ponta, ou edge computing, e silos de dados distribuídos se tornarão realidade. Os provedores de tecnologia devem ser capazes de ajudar as organizações a se beneficiarem das tecnologias emergentes sem comprometer sua própria integridade de dados e segurança de TI.

Sally Eaves
@sallyeaves

CEO e Diretora, Sally Eaves Consultancy

"Eu acredito que começaremos a ver uma mudança no GDPR após reduzidas as dores da implementação, para nos concentrar em otimizar os ganhos, como processos de TI aprimorados, backup e recuperação e maior segurança, e usá-los como um ponto de dferenciação em relação aos colegas do setor."

Resumo

O GDPR mudou as empresas para melhor, levando a privacidade de dados e segurança da rede à atenção da C-suite e clientes similares. A conformidade, no entanto, requer atenção constante em segurança de dados, dia e noite, de toda a sua força de trabalho. A natureza sempre em evolução da tecnologia e das ameaças cibernéticas significa que uma boa infraestrutura de segurança e um bom treinamento, apoiados por um suporte de consultoria em tecnologia e privacidade de dados, é definitivamente crítico para os negócios. Lembrar a equipe que sempre há uma pessoa por trás dos dados pode ajudar muito para incorporar uma cultura de proteção de dados entre o seu pessoal. E uma mudança cultural é muito mais eficaz do que exercícios de treinamento de múltipla escolha.

Sobre a Kingston

Com 32 anos de experiência, a Kingston possui o conhecimento para identificar e resolver seus desafios de trabalho remoto, tornando fácil para seu pessoal trabalhar com segurança de qualquer lugar, sem comprometer sua organização.

©2021 Kingston Technology Corporation, 17600 Newhope Street, Fountain Valley, CA 92708 USA. All rights reserved.
Todos os direitos reservados. Todas as marcas ou marcas registradas pertencem a seus respectivos proprietários.

#KingstonIsWithYou