Lei Geral de Proteção de Dados Pessoais- LGPD

Nesse artigo citamos as principais características dessa nova lei e como você pode implantá-la em conjunto com as soluções

DrayTek LGPD Compliance

A Lei Nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais - LGPD, inspirada na legislação da União Europeia "General Data Protection Regulation" - GDPR, entrou em vigor através do Decreto Nº 10.474 de 26 de agosto 2020, as punições e multas previstas pelo decreto só serão aplicadas a partir de agosto de 2021.

Os regulamentos cobrem como você lida e protege os dados (eletrônicos e outros) e incluem armazenamento, compartilhamento, uso, permissão, divulgação e exclusão.

Há muita publicidade e interesse da mídia no assunto, alertando as empresas para garantir que 'estão prontas'. Todo um setor surgiu para aconselhar sobre a LGPD e oferecer auditorias de conformidade em operações comerciais. Você não pode ser à prova de hackers, mas a LGPD tem tudo a ver de como reduzir seus riscos e mudar a cultura corporativa para estar mais consciente e assumir maiores responsabilidades.

Todas as empresas e organizações terão grandes responsabilidades em relação aos dados pessoais que estão armazenados sob seus cuidados.

O Brasil é um dos países que se destacam em ataques cibernéticos, em 3 meses foram contabilizados 15 Bilhões de ataques, de acordo com reportagem do site Canaltech de agosto de 2019.

A lei geral de proteção de dados (LGPD) regulamenta o uso e tratamento dos dados pessoais, tanto da iniciativa privada quanto do poder público, na tentativa de protegê-los contra vazamentos e uso indevido. Em caso de vazamento de dados, o usuário deverá ser avisado o mais rápido possível.

Com a LGPD, também foi criada a Autoridade Nacional de Proteção de Dados – ANPD que é o órgão da Administração Pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

Pontos principais da LGPD:

- Todos os dados pessoais coletados pela empresa de precisam de autorização para serem armazenados e utilizados;
- Os titulares dos dados têm direito ao acesso, informação, cancelamento, retificação, oposição e portabilidade de seus dados;
- As empresas responsáveis pelo tratamento de dados deverão nomear uma pessoa encarregada pela proteção de dados pessoais;
- Todas as atividades de tratamento de dados devem ser registradas em relatório;
- A LGPD também tem regras específicas para tratamento de dados sensíveis, dados de crianças e adolescentes, e, ainda, transferência internacional de dados;
- A nova lei também trata da realização de avaliação de impacto à proteção de dados;
- A lei determina punições para incidentes de segurança de dados, que vão de advertência a multa de até 2% do faturamento anual da empresa, limitado a R$ 50 milhões por infração incluindo empresas que não possuem estabelecimentos aqui no Brasil;

Como adaptar sua empresa a Lei LGPD?

- Procurar por um aconselhamento jurídico para analisar os impactos legais dessa nova lei.
- Criar um Comitê integrando as áreas de TI e Jurídica é uma boa prática para se enquadrar à nova lei de dados.
- Elaborar um Mapa de Riscos de Tratamento de Dados Pessoais.
- É preciso identificar, quando e onde todos os dados pessoais de funcionários, clientes e fornecedores são coletados, todos sem exceção: de uma simples data de nascimento a informações de folha de pagamento. Onde esses dados são armazenados? Quais são as camadas de proteção?
- Depois de executar o planejamento, inicie as ações corretivas. Reestruture as políticas de contratos e termos de privacidade, incluindo clausulas que esclareçam a finalidade do tratamento de dados. Sempre que um dado pessoal for coletado de forma física ou pela Internet, a pessoa precisa consentir, ou seja, assinar um termo de consentimento de uso desses dados. A empresa precisa ser transparente e o cliente deve saber como esses dados serão usados e armazenados.
- É necessário elaborar um programa de educação e conscientização dos funcionários da empresa. Eles precisam saber evitar vazamentos e ter a noção das responsabilidades e consequências do mau uso dos dados.
- Também será preciso definir, sobre quais setores realmente poderão ter acesso ao banco de dados e como eles poderão ser utilizados.

Cinco pontos adotados por muitas empresas de teste e auditoria (Cyber Essentials – UK Gov):

- Proteger a conexão com a Internet (roteador / firewall)
- Proteger seus dispositivos e softwares (configurações seguras para PCs, tablets, telefones, etc)
- Controlar o acesso aos seus dados e serviços (controle quem tem acesso aos seus dispositivos, a sua rede e servidor)
- Proteger contra vírus e outros malwares (produtos de hardware/software)
- Mantenha seus dispositivos e software sempre atualizados

Compromisso da DrayTek e IK1 Tecnologia com a LGPD

A DrayTek processa e armazena informações do cliente como parte do fornecimento de serviços e produtos. A DrayTek Corp. matriz em Taiwan e nossa empresa IK1 Tecnologia Ltda no Brasil, distribuidor autorizado para todo o território brasileiro dos equipamentos DrayTek, estão comprometidos com os requisitos da LGPD, incluindo segurança e manuseio de dados pessoais, requisitos de relatórios de violação, correção de erros, direitos de exclusão, requisitos de qualidade e seu direito de solicitar os seus dados mantidos em nosso poder. Quaisquer solicitações formais devem ser feitas ao nosso atual Diretor de Proteção de Dados.

A linha de equipamentos DrayTek e a LGPD:

As soluções DrayTek possuem mecanismos que atrelados as boas práticas de governança em TI, cumprem papel de fundamental importância para proteção de dados:

- ✓ Firewall com Inspeção de Pacotes (SPI), realiza o controle de entrada e saída serviços e protocolos da sua rede;
- ✓ Web Content Filter, garante o bloqueio de acesso a sites indevidos com conteúdos maliciosos;
- ✓ Spoofing Defense, impedindo que hackers se passe por outro dispositivo da rede com o objetivo de roubar dados, disseminar malware ou contornar controles de acesso;
- ✓ DoS Defense, inibi ataques de negação de serviço evitando sobrecargas na rede;
- ✓ IEEE 802.1x, em conjunto com os nossos Switches e APs, contribui para não autorizar acessos indevidos a rede como máquinas convidadas, invasores ou dispositivos não gerenciados que não executam uma autenticação bem-sucedida;
- ✓ VLAN IEEE 802.1Q, contribui com a segmentação da rede evitando a disseminação de um ataque com vírus, malware e ransomware para toda a rede da empresa;
- ✓ DNS Security, inibi consultas falsas de DNS que criam oportunidades para roubo de informações de terceiros ou alteração de dados em diversos tipos de transações como sites de bancos falsificados;
- ✓ DNS Filter, bloqueia o acesso a sites indevidos;
- ✓ Virtual Private Network (VPN), estabelece uma comunicação segura e criptografada para acessar a rede local da empresa sem estar fisicamente nela. Também é uma

excelente maneira de proteger e criptografar sua comunicação com a internet em redes públicas não confiáveis, como redes Wi-Fi de aeroportos;

As soluções DrayTek garantem sua performance (Throughput) com todos os recursos citados acima habilitados, possibilitando ter segurança e obter o melhor desempenho para a sua rede.

Requisitos de Segurança

O esquema mencionado anteriormente tem algumas recomendações específicas em relação a firewalls / roteador e todos esses são nossos métodos recomendados em nosso Guia de Segurança do Roteador, que recomendamos ler, compartilhar e seguir os conselhos contidos nele.

Cada dispositivo deve ser protegido por um firewall configurado corretamente, por profissional qualificado.

Altere todas as senhas administrativas padrão para senhas fortes.

Impedir o acesso à interface administrativa da Internet, a menos que haja uma necessidade de negócios clara e documentada e a interface seja protegida por uma lista de permissões de endereços IP ou 2FA (autenticação de dois fatores).

Bloquear conexões de entrada não autenticadas por padrão (stateful firewall).

Certifique-se de que as regras de firewall de entrada sejam aprovadas e documentadas por um indivíduo autorizado; a necessidade do negócio deve ser incluída na documentação remova ou desabilite regras de firewall permissivas rapidamente, quando não forem mais necessárias.

Use um firewall baseado em host em dispositivos (por exemplo, um firewall baseado em software em execução no próprio dispositivo) que são usados em redes não confiáveis, como hotspots Wi-Fi públicos.

Remova e desative contas de usuário ou administrador desnecessárias ou perfis / usuários VPN quando não forem mais necessários.

Instale atualizações de firmware "críticas" ou de "alta prioridade" o mais rápido possível.

Nosso guia de segurança do roteador mencionado anteriormente é realmente muito mais abrangente do que a lista acima.

Um CALDEIRÃO
de soluções tecnológicas