O OTRS Group mostra como documentar os processos de segurança de TI de forma clara e legal

A nova Lei Geral de Proteção de Dados, que deveria entrar em vigor nesse mês de agosto, em função da Pandemia, foi transferida para maio de 2021. Com isso, as empresas ganham mais tempo para definir as estratégias, implementar os processos necessários e superar os desafios.

"Segundo o Índice LGPD ABES (Associação Brasileira de Empresas de Software), cerca 60% das empresas brasileiras não estão prontas para a LGPD. Dado o tamanho do país, há uma grande necessidade de ação em relação a dados uniformes. As empresas devem aproveitar a oportunidade de implementar a LGPD o mais rápido possível, com a ajuda de sistemas digitalizados, o que pode lhes proporcionar uma importante vantagem competitiva, inclusive para manter negócios com empresas da União Europeia, onde já foi implementada a GDPR", Jens Bothe, especialista em segurança do Grupo OTRS.

E como fornecedor líder de soluções para gerenciamento de processos e comunicações e especialista em ambientes de segurança, o OTRS Group fornece cinco recomendações para ajudar as empresas a se adequar as normas:

1- Comece pequeno

A maioria das grandes empresas possui processos já definidos e as chamadas equipes de defesa cibernética em uso. No entanto, muitas pequenas e médias empresas ainda precisam elaborar suas estratégias. Para isso, é aconselhável começar "pequeno": criar um Gabinete de Comunicação de Incidentes de Segurança é útil e é fundamental dedicar uma pessoa ou equipe de contato responsável por eventos relacionados à segurança. Isso pode criar documentação centralizada que mantém todos cientes do que está acontecendo.

2- Consulte especialistas experientes

As empresas nem sempre têm tempo para verificar todos os regulamentos para determinar se são relevantes para seus negócios. Portanto, não hesite em consultar especialistas externos experientes com perguntas sobre diretrizes e padrões aceitos.

3- Defina claramente os processos de segurança de TI

É importante que todas as empresas estabeleçam processos e responsabilidades claros para lidar com eventos relacionados à segurança. As seguintes perguntas devem estar entre as consideradas:

- Como você define um incidente de segurança?
- Quando exatamente um incidente precisa ser relatado?
- Quais dados ou processos devem ser protegidos?
- Qual é o impacto potencial do incidente?
- Quem deve ou pode ser informado de um incidente?
- Em que ordem e em que prazo a comunicação deve ocorrer?

4- Crie processos digitais centralizados

Para documentar os eventos de segurança e as etapas correspondentes tomadas para mitigar a situação de maneira segura, estão disponíveis sistemas como o STORM da OTRS AG. Eles agem como a espinha dorsal técnica dos processos de segurança de TI, suportam a comunicação relacionada a incidentes e armazenam a documentação em caso de auditorias posteriores. Eles possibilitam definir processos específicos para cenários de ameaças, conceder aos usuários acesso baseado em função e habilitar a comunicação criptografada entre usuários claramente autenticados, para que os ataques sejam tratados rapidamente e a documentação adequada seja

capturada.

5- Enxergue a segurança de TI como um processo contínuo

Uma vez estabelecidos, os processos de segurança de TI se tornam uma parte cotidiana de suas atividades de negócios. No entanto, deve-se considerar que os regulamentos, processos e requisitos podem mudar repetidamente. É por isso que as empresas devem se manter atualizadas. Se você deseja desenvolver seu know-how de segurança e desenvolver uma equipe de segurança de TI em sua organização, deve se conectar com outros agentes de segurança e ficar a par das mudanças no setor.

"Nem todas as empresas estão preparadas para isso", diz Luciano Alves de Oliveira, Diretor Geral da OTRS Brasil. "O Covid-19, por exemplo, foi o tema mais explorado para ataques cibernéticos durante o primeiro semestre de 2020, que atingiram organizações em todos os setores de atividade, incluindo governos, indústria, saúde, prestadores de serviços, infraestruturas críticas e consumidores. Na América Latina, durante o primeiro trimestre, foram registradas mais de 9,7 bilhões de tentativas de ataques cibernéticos, sendo 1,6 bilhão somente no Brasil. O número coincide com o aumento exponencial de profissionais que adotaram o home office nos últimos meses. A LGPD responde a isso e exige relatórios oportunos de incidentes de segurança. É por isso que é essencial que as empresas registrem os incidentes de TI e documentando-os legalmente", complementa Oliveira.

Sobre a OTRS AG

O OTRS Group é o fabricante e o maior fornecedor mundial do conjunto de gerenciamento de serviços OTRS, premiado com o selo de aprovação SERVIEW CERTIFIED TOOL.

Oferece soluções flexíveis para gerenciamento de processos e comunicação para empresas de todos os tamanhos, economizando tempo e dinheiro. Entre seus clientes estão Lufthansa, Airbus, IBM, Porsche, Siemens, BSI (Escritório Federal de Segurança em Tecnologia da Informação), Instituto Max Planck, Toyota, Hapag Lloyd e Banco do Brasil (Banco do Brasil). OTRS está disponível em 40 idiomas. A empresa é composta pela OTRS AG e suas seis subsidiárias OTRS Inc. (EUA), OTRS S.A. de C.V. (México), OTRS Asia Pte. Ltd. (Cingapura), OTRS Asia Ltd. (Hong Kong), OTRS do Brasil Soluções Ltda. (Brasil) e OTRS Magyarország Kft. (Hungria). A OTRS AG está listada no conselho básico da Bolsa de Frankfurt. Para mais informações, consulte www.otrs.com.