A privacidade digital no futuro: previsões dos especialistas para a próxima década.

Quando o assunto é privacidade, o cenário nunca é o mesmo. Ameaças e prioridades mudam constantemente. Então, o quê as empresas devem saber sobre o que as espera na próxima década?

AUTOR
Marco Preuss

Sejam em celulares, smartwatches e até mesmogadgets. Hoje em dia dados pessoais estão em toda parte. Coletar informações pessoais faz os serviços melhores para os usuários mas, ao longo dos últimos anos, tivemos múltiplos casos que demonstraram os riscos desse hábito que se tornou tão tradicional.

Quando o assunto é privacidade de dados, é possível fazer uma comparação com um rio, afinal, você nunca entra no mesmo rio duas vezes. Isso porque preocupações, ameaças e prioridades estão sempre em movimento. Pensando nisso, quais serão as ameaças à privacidade que veremos na próxima década? E como as empresas podem se preparar para elas?

1. Governos vão acessar mais dados dos cidadãos sem pedir autorização

Já está acontecendo, mas, nos próximos anos, governos ao redor do mundo tendem a adotar leis que os autorizem a acessar mais e mais dados e informações de seus cidadãos. E vão dar diversas justificativas para isso, incluindo terrorismo, instabilidade e o fato de que esses dados já são explorados deliberadamente pelo setor privado.

2. A brecha entre regulamentação e realidade só crescerá

Embora a justificativa esteja clara, o aumento do acesso aos dados privados da população acarreta diversos riscos, principalmente o uso não-autorizado desses dados e o vazamento de informações.

Será um grande desafio para as entidades reguladoras saber adaptar seus parâmetros na mesma velocidade em que as novas tecnologias avancem. E as empresas também têm sido lentas para mudar o modo como lidam com dados do usuário. A única mudança significativa aplicada recentemente foi a prática de pedir o consentimento dos usuários sobre as formas como as empresas poderiam usar seus dados, o que agora é obrigatório em muitos países. Mas não é possível enxergar nenhuma tendência que direcione para o aumento da segurança para proteção de dados sensíveis do usuário.Ou seja, já existe uma grande distância entre a regulamentação e a realidade quando o assunto é privacidade. E isso tende a aumentar ainda mais, o que faz essa regulamentação parecer cada vez menos eficaz.

3. Ferramentas de contra-ataque criarão uma guerra virtual da privacidade

As tendências mencionadas acima vão encorajar os que pensam à frente inovadores a desenvolver novas tecnologias de proteção de privacidade. Os especialistas vão adotar esses métodos e mais tecnologias aparecerão para tentar burlá-los, dando início a uma batalha virtual.

Enquanto isso, os usuários se tornarão mais proativos e curiosos a cerca de sua privacidade. Existirá uma alta demanda para gerenciadores de senhas, redes privadas (VPNs) e tokens (geradores automáticos de senha) para sistemas de identificação de dois fatores (2FA).

No entanto, mecanismos de proteção como os tokens 2FA e os gerenciadores de senha cuidam só da fachada da casa. Ataques e problemas acontecem regularmente nos fundos, no backend. Essas ferramentas protegem o ambiente local, mas não são uma proteção eficaz contra ataques a sistemas como o armazenamento em nuvem (cloud). E, como as ferramentas baseadas na nuvem estão cada vez mais deixando de ser desnecessárias para se tornarem indispensáveis, os funcionários também terão que entender onde os riscos estão. VPNs protegem contra um certo tipo de roubo de dados, como endereço IP e geolocalização, por exemplo, mas não protegem contra usuários compartilhando dados com serviços como Google e Facebook.

4. Seguiremos sendo enganados por diversão

“O crescimento acelerado de games, testes e aplicativos que fazem o usuário compartilhar dados pessoais em troca de diversão não deveria ser tão subestimado.”

Cibercriminosos podem usar esse tipo de estratégia para atacar empresas, roubando dados pessoais de funcionários e usando esses dados para acessar sistemas e informações corporativas.

5. Veremos novos ataques a processos democráticos, mas também proteção contra a desinformação

Esse tipo de ataque já tem sido comum nos últimos anos e não há motivo evidente para que parem. Tecnologías capazes de falsificar a identidade visual e a fala de uma pessoa já existem e, com uma eleição presidencial nos Estados Unidos logo à frente, esses métodos devem infelizmente roubar a atenção do público e ser explorados por ambos os lados da disputa.

“Mas onde há ação, também há reação. Por isso, poderemos contar com novas ferramentas de confrontar aqueles que tentam manipular o público.”

6. Provedores da Internet das Coisas (IoT) aumentarão o investimento em segurança

Os últimos anos têm sido turbulentos para a indústria da segurança digital, já que ataques específicos à IoT, vazamentos de dados e campanhas de desinformação e fake news têm sido cada vez mais desafiadores.

Esses fenômenos incentivarão fornecedores a subir o nível de colaboração em prol da segurança. Amazon, Apple, Google e a Zigbee Alliance anunciaram que estão criando um grupo de trabalho para desenvolver e promover um padrão de conectividade gratuito e livre de royalties. Isso aumentará a compatibilidade entre produtos que usem IoT e criará uma base mais segura para seu uso. Espera-se que outras empresas sigam essa tendência.

Considerando tudo o que foi citado acima, é possível dizer que estamos frente a uma década muito interessante para a privacidade. Mas os desafios são significativos e as empresas terão um papel fundamental para assegurar a privacidade dos dados, não só de seus colaboradores, mas também dos consumidores.

A esperança é que novas soluções surjam na medida de novas ameaças. Enquanto isso, toda e qualquer empresa pode começar a fazer sua parte, simplesmente adotando iniciativas de capacitação e treinamento de segurança e privacidade para seus funcionários.