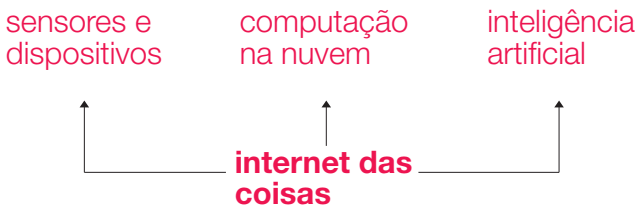
SEGURANÇA E PRIVACIDADE PARA A INTERNET DAS COISAS

POR QUE PRECISAMOS ENTENDER A IOT 'PARA ALÉM DA IOT'?

A Internet das Coisas (IoT) se tornou um sinônimo para cidades inteligentes, casas conectadas e sistemas industriais interconectados. No fim das contas, o que a IoT de fato representa? O número crescente de de dispositivos conectados à Internet e a expectativa de gerar mais de 200 bilhões de dólares em negócios até 2025 geram grande otimismo quanto ao futuro desse mercado. No entanto, desafios importantes, como o destino e tratamento dado à massiva quantidade de dados coletada por esses dispositivos e a segurança dos sistemas de IoT ainda precisam ser enfrentados. Este estudo analisa as características e riscos à segurança e à privacidade de três grupos de tecnologias que compõem a Internet das Coisas: (i) dispositivos e sensores; (ii) sistemas de inteligência artificial; e (iii) computação na nuvem.



Nesse contexto, a incorporação dos princípios da privacidade, proteção de dados e segurança no processo de desenvolvimento dessas tecnologias é central para o avanço e consolidação da IoT no Brasil em dois aspectos:

- Como um conjunto de tecnologias estratégicas que integram a elaboração de uma política de governo (Plano Nacional de IoT).
- Na condição de um importante ativo mercadológico, capaz de proporcionar inovações setoriais para a economia e conectividade do país.

Esses valores precisam ser inseridos na concepção e design dos produtos e também constantemente reavaliados de maneira que permaneçam relevantes. Para que o potencial da IoT se concretize, é necessário compreender como esses princípios se aplicam à operacionalização das tecnologias mencionadas.

COMO FIZEMOS?

A nota foi elaborada a partir do levantamento e análise das tecnologias que sustentam a IoT, e o mapeamento dos riscos multidimensionais associados a ela. Também contou com a organização de um grupo focal composto por especialistas técnicos e representantes da academia, sociedade civil e setor privado.

O QUE VOCÊ PRECISA SABER?

- A análise do uso de sensores e dispositivos, tecnologias de computação na nuvem e inteligência artificial indicou que, de modo geral, há pouca preocupação com o desenvolvimento de tecnologias seguras (security by design) e garantia da privacidade do usuário (privacy by design) no Brasil.
- A proliferação de dispositivos e sensores que captam e processam dados sobre pessoas, ambientes e eventos traz três desafios à segurança de indivíduos e de empresas. O primeiro é a ausência de padrões técnicos compartilhados entre indústria, agências regulatórias, desenvolvedores e provedores, o que é um obstáculo à interoperabilidade entre dispositivos. O segundo é a falta de garantias de que a performance de um dispositivo não extrapole a finalidade para a qual foi programado, nem o consentimento do usuário ou empresa que o utiliza. O terceiro é que problemas de segurança da IoT também se aplicam a dispositivos desconectados, pois nem todos os objetos requerem conexão com a Internet para se comunicarem.
- A rápida integração da nuvem a dispositivos de IoT nem sempre é acompanhada pelo incremento no nível de segurança em ambos os lados. Aos problemas de segurança comumente relacionados à nuvem, somam-se aqueles específicos de dispositivos de IoT, criando um ecossistema com novas configurações de vulnerabilidades e riscos.
- Os principais desafios para um sistema mais abrangente de governança da IoT são: a rápida difusão de sistemas ciber-físicos pouco seguros e a falta de atenção aos contextos cultural, socioeconômico e regulatório no Brasil.

QUER SABER MAIS?

Confira o artigo na íntegra aqui: https://igarape.org.br/seguranca-e-privacidade-para-a-internet-das-coisas/

INSTITUTO IGARAPÉ
a think and do tank

www.igarape.org.br

Ecossistema para a regulação para IoT baseado na privacidade e segurança desde a concepção

Natureza	Técnica	Regulatória e governança	Administração e gestão
Exemplos	PETs, uso de protocolos seguros (IPv6, TLS, HTTPS e MQTT), minimização da superfície de ataque, prazos de expiração para senhas por padrão, criptografia em serviços de nuvem, segurança por "camadas", respostas a incidentes, etc.	Regulação: Lei nº 13.709, de 14 de agosto de 2018 (LPDP), Plano Nacional de IoT, Código de Defesa do Consumidor, Lei de Acesso à Informação, Decreto 8.234 de 02 de maio de 2014 (regulação M2M). Portaria 1.729 de 31 de março de 2017 MCTIC (Estabelece a Câmara IoT, órgão multissetorial). Governança: Colaboração entre diferentes setores e a autoridade de supervisão para a determinação de necessidades e riscos referentes às tecnologias de IoT.	Assegurar o respaldo de setores de chefia; estandardizar processos de desenvolvimento seguro; gerenciar vulnerabilidades e segurança de projetos.
Objetivo	Garantir que hardware, software e middleware sejam seguros (resilientes contra ataques cibernéticos, preservando a integridade e confidencialidade das informações que processam) desde sua concepção e desenvolvimento.	Estabelecer princípios basilares para o desenvolvimento da IoT no país; regular a coleta e o uso de dados pessoais; garantir segurança jurídica; facilitar a coordenação inter-setorial; estimular a adoção de boas práticas; definir e aplicar penalidades.	Tornar o ambiente institucional favorável à adoção de medidas técnicas de reforço da privacidade e segurança; garantir que esses princípios sejam incorporados em toda a cadeia da organização (p.ex, para além da tecnologia).
Desafios	Criar estímulos positivos para que empresas, engenheiros e desenvolvedores adotem tecnologias seguras na prática.	Criar uma autoridade de proteção de dados independente e mecanismos de responsabilização e explicação; desenvolver uma jurisprudência sobre a interpretação da LPDP; realizar diálogos contínuos entre governo, sociedade civil e empresas para viabilizar a aplicação de medidas técnicas e administrativas; harmonizar a LPDP e a estratégia de transformação digital do governo e o Plano Nacional de IoT.	Conscientizar organizações sobre os custos de produtos e serviços inseguros, criar incentivos e formular estratégias para a adoção em escala da privacidade e segurança desde a concepção.