

APRESENTADO POR



# O desafio de garantir a segurança digital na movimentada via IoT

Security Operations Center é visto como principal estratégia de proteção, em mercado que avança com a chegada de novo carro conectado no Brasil



Nesta semana chega ao Brasil o Onix 2020, o carro conectado da Chevrolet. O veículo é um marco evidente da tendência de massificação da Internet das Coisas (IoT), que tende a se espalhar pelos objetos ao nosso redor, fora e dentro de casa. O Onix permite que motorista e passageiros usem o automóvel como *hotspot* de acesso à internet móvel *powered by Claro*.

Além da experiência de estar sempre conectado, o motorista evita a inconveniência de ver seu carro parar em função de problemas e deter que correr para fazer manutenções repentinas. A conexão 4,5G *powered by Claro*, que equipa o Onix 2020, envia continuamente para a Chevrolet, informações coletadas a partir de diversos sensores e dispositivos que equipam o veículo.

Para dar maior segurança aos dados que trafegam pela rede, o cartão SIM virtual (eSIM) é integrado ao módulo eletrônico do veículo, inviabilizando sua remoção. Todas as atualizações são feitas remotamente, sem que seja necessária qualquer intervenção do proprietário.

"Segurança é um dos principais temas quando se fala no avanço da IoT", pontua Rodrigo Viganó Hanstedt, gerente de projeto para IoT da Embratel. Usando os próprios carros como exemplo, é preciso lembrar que embreves, ruas, estradas e cidades inteiras estarão tomadas por automóveis conectados à internet. Cada um deles precisará estar protegido de ataques e invasões de hackers. Qualquer intruso nesta rede pode significar uma ameaça aos veículos

dentro dela, causando prejuízos para os motoristas e toda a mobilidade de uma cidade.

Justamente por isso, a Chevrolet utiliza o Serviço de Segurança para IoT da Embratel, que oferece proteção em tempo real para que sua conexão com o carro seja sempre segura. O responsável por garantir a segurança de motorista e montadora é o Security Operations Center (SOC) da Embratel, que monitora qualquer tentativa de invasão na rede.

"A Internet das Coisas não vai se desenvolver se pessoas forem atacadas e sofrerem com o roubo de dados ou com qualquer interferência na operação do sistema. Desde a década de 2000, previmos que esse boom de coisas conectadas poderia acontecer. A Embratel é pioneira na implementação de SOC", diz Elisabete Couto, diretora de Soluções de IoT da Embratel.

O SOC da Embratel utiliza tecnologias de Análise de Comportamento, Inteligência Artificial e Cognitiva, além de Machine Learning, para realizar a monitoração de todo o tráfego gerado pelo veículo, identificando desvios em padrões e possíveis ameaças à segurança da conexão. Se uma ameaça é identificada, medidas de mitigação são aplicadas, podendo chegar até ao bloqueio de um ou mais serviços do veículo.

O Serviço de Segurança da Embratel permite ainda o acompanhamento das monitorações por meio de relatórios para técnicos de segurança. Da mesma

forma, gera informações relevantes às áreas de negócio dos clientes.

## UMA DEMANDA CRESCENTE

De acordo com a Gartner, pelo menos um incidente grave de segurança será causado por falha na TI até 2020. Isso inclui todo tipo de serviço prestado em redes conectadas, incluindo os *smart cars*. Os dados que trafegam entre os pontos de interesse devem ser protegidos, como uma nova categoria de dados pessoais digitais, da mesma forma que protegemos nossos e-mails, senhas de sistemas e redes sociais ou históricos médicos.

A consultoria também aponta que, para uma organização ser capaz de combater com êxito o cibercrime no ambiente de ameaças — em que a internet estará em todas as coisas — a equipe e as soluções presentes no SOC, orientados pela inteligência

artificial, devem ser capazes de prevenir, detectar e responder efetivamente aos ataques.

A Gartner listou a implementação e amadurecimento de Centros de Operações de Segurança entre as sete principais tendências de segurança e riscos para 2019. De acordo com o relatório, dado o crescente impacto dos ataques de segurança e a elevada complexidade de suas ferramentas que geram alertas, empresas como a Embratel, que oferecem soluções digitais, procuram continuamente atualizar as tecnologias utilizadas em seus SOCs.

"Como fornecedores de Serviços de Segurança, trabalhamos com uma quantidade enorme de dados. Usamos inteligência artificial e machine learning aplicada ao perfil do cliente. Não só protegemos, mas tratamos e mineramos os dados para entender que tipos de ataques poderiam

ocorrer. Contamos ainda com bancos de dados internacionais de ameaças para antever problemas que podem já ter ocorrido em outras regiões com outras redes", conta Elisabete Couto.

Muitas empresas estão terceirizando o serviço de proteção de suas redes de IoT, na expectativa de obter resultados mais confiáveis, já que isso exige uma equipe própria trabalhando 24 horas. A escolha de um bom parceiro para fazer o monitoramento do seu ecossistema de IoT é a decisão natural, quando construir um SOC não está no seu *core business*.

## O PRÓXIMO PASSO

A evolução prevista para os carros conectados vai depender, entre outras coisas, da qualidade das redes e da segurança aplicada a IoT. Elisabete entende que o próximo passo é o carro autônomo. É esperado que os veículos que operam sozinhos sejam capazes de deixar as ruas mais seguras. Softwares, radares, sensores e câmeras tendem a ser, em conjunto, mais eficientes que humanos para detectar problemas que olhos e ouvidos podem não notar.

"Pode ser que a regulação demore. Mas, uma hora ou outra, o carro autônomo vai aparecer, principalmente nas estradas. É necessária uma legislação robusta que regule a utilização do serviço de carros autônomos. As soluções de segurança são fundamentais para garantir o funcionamento de uma infraestrutura inovadora como esta", conclui a diretora de Soluções de IoT da Embratel.

**"A IoT não vai se desenvolver se pessoas forem atacadas e sofrerem com o roubo de dados ou com qualquer interferência na operação do sistema"**

ELISABETE COUTO, DIRETORA DE SOLUÇÕES DE IOT DA EMBRTEL

**SOC REALIZA MONITORAMENTO E AÇÕES PROATIVAS E REATIVAS**

**Equipe trabalha 24 horas e sete dias por semana contra as ameaças**

**Algoritmos e Inteligência Artificial ajudam a identificar desvios de padrão**

**Em situações extremas, a comunicação pode ser interrompida**

**Sistema atua rapidamente para conter ou mitigar incidente, evitando maiores danos**

**Medidas como o Break the Glass bloqueiam instantaneamente serviços de conectividade**

CONTEÚDO PATROCINADO PRODUZIDO POR GLAB.GLOBO.COM