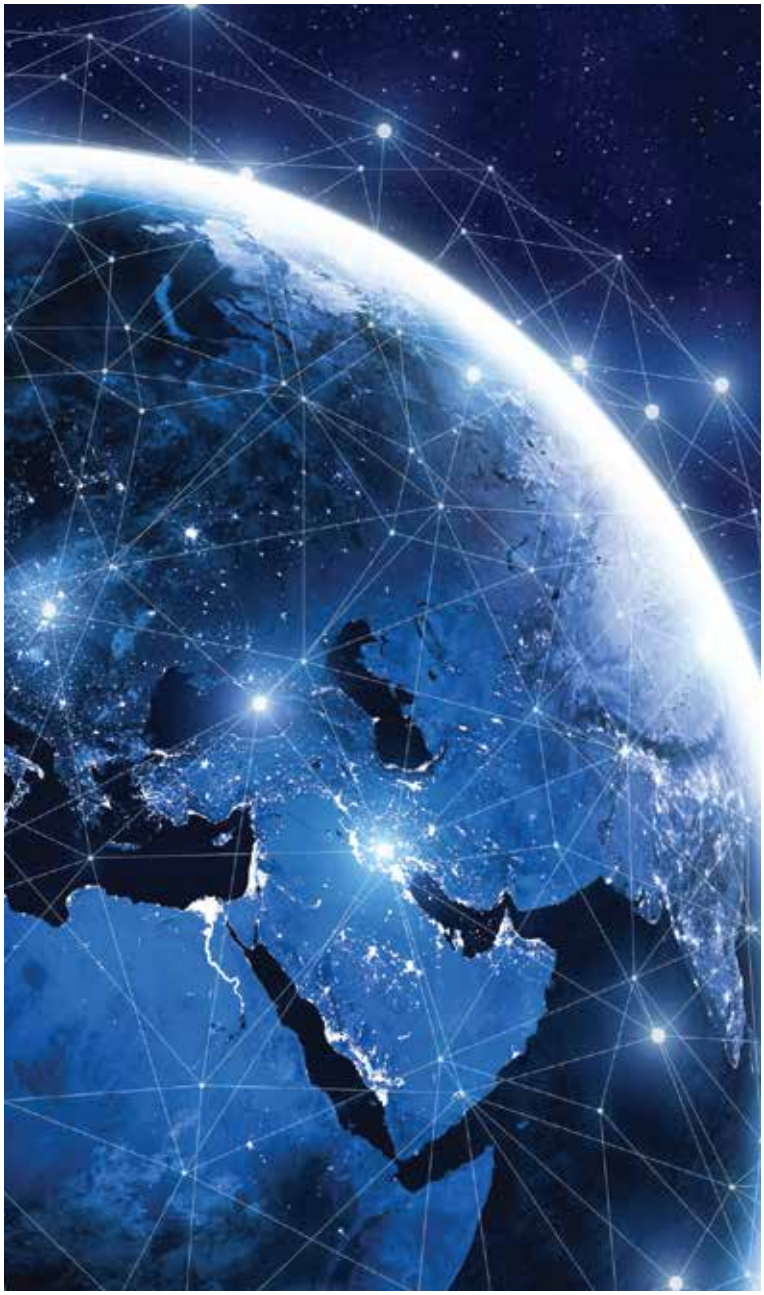
IoT - A Internet de Tudo: Construindo a ciber-resiliência em um mundo conectado



A Internet das Coisas (IoT) está em todos os lugares, prenunciando uma revolução tecnológica na velocidade da luz. De acordo com um Relatório da Oliver Wyman entre 50 e 100 bilhões de dispositivos deverão estar conectados à internet em 2020. Enquanto este rápido crescimento, sem dúvida, abrirá caminho para novas oportunidades, as organizações também devem se preparar para enfrentar novos desafios ligados à segurança. Você está preparado para a internet de tudo (IoE – internet of everything)?
Saiba mais sobre a onda de vulnerabilidades criada neste cenário, as novas soluções e regulamentações, como avaliar seu risco cibernértico e estar preparado para fazer face aos novos desafios no artigo: Internet de Tudo: Construindo a ciber-resiliência em um mundo conectado.

UMA ONDA DE VULNERABILIDADES

Os produtos da IoT são dispositivos ou objetos físicos incorporados aos produtos eletrônicos, softwares, sensores ou atuadores que podem se conectar à internet. Desde refrigeradores e brinquedos até dispositivos médicos e sistemas de controle industrial, os produtos conectados à internet estão transformando a maneira pela qual muitas indústrias conduzem os seus negócios, gerando eficiência e reinventando a experiência do consumidor.
Os dispositivos de IoT também fornecem às empresas inúmeros dados valiosos que podem ser sintetizados com as análises para aprimorar os produtos, penetrar em novos mercados e acessar os consumidores em potencial.

A explosão dos dispositivos de IoT está mudando de modo drástico o panorama do risco cibernético – e não necessariamente para melhor. Muitos especialistas em segurança acreditam que os dispositivos inteligentes estão criando uma onda de vulnerabilidades porque carecem, em geral, de sólidos recursos de segurança – ou, em alguns casos, mesmo de recursos básicos. Os dispositivos de IoT em geral também são precários no que tange o suporte regular do produto, como atualizações e patches, o que os torna especialmente vulneráveis a pontos fracos recentemente descobertos, como falhas ***Meltdown e Spectre***, na maioria dos processadores de computador.

A tecnologia inteligente também está conectando sistemas de computador e dispositivos que já estiveram separados ou não conectados diretamente à internet. Esta nova conectividade pode deixar as organizações ainda mais expostas às ameaças em expansão que ainda não foram totalmente levadas em consideração ou mitigadas. A empresa de cibersegurança Symantec, por exemplo, descobriu que, na média, os dispositivos de IoT são atacados uma vez a cada dois minutos nos horários de pico. E que mais da metade dos profissionais de segurança da internet pesquisados pela Tripwire, uma provedora de soluções de garantia da integridade, não se sente preparada para ataques à segurança que abusam, exploram ou aproveitam de modo maligno os dispositivos de IoT industriais não seguros.

O FBI adverte que, "quando um dispositivo de IoT está comprometido, os cibercriminosos podem facilitar ataques em outros sistemas ou redes, enviar emails de spam, roubar informações pessoais, interferir na segurança física e se aproveitar dos dispositivos comprometidos para participação em ataques de negação de serviço distribuído (DDoS)".

Exemplos recentes de ataques de IoT incluem:

- Infiltração de uma rede de cassinos dos EUA em 2017 por hackers que se conectaram a um fish tank (contador de fluxo de pessoas) conectado à internet dentro do prédio.
- Um ataque massivo de DDoS (negação do serviço distribuído) em 2016 contra uma empresa que administra o tráfego de DNS (Domain Name Server – Servidor de Nome de Domínio). Os invasores usaram uma botnet – uma rede de computadores infectada com malware – chamada Mirai para comprometer as câmeras conectadas à internet pelo mundo, o que interrompeu os serviços de muitos dos clientes da empresa.

UMA NOVA SOLUÇÃO DE IOT

Embora os fabricantes e provedores do serviço de IoT não possam eliminar totalmente o potencial para reclamações cibernéticas e de E&O referentes aos seus dispositivos conectados, eles podem assegurar uma cobertura de seguro eficaz que proporcione proteção robusta quando necessário. A Marsh desenvolveu um novo produto de seguro de IoT inovador – disponível através da Marsh Cyber CAT 3.0 como uma apólice independente ou por endosso – especificamente para empresas que projetam, fabricam e vendem produtos de IoT ao consumidor e à indústria, ou que prestam serviços relacionados a esses produtos.

Enquanto ambiguidades ou exclusões podem limitar ou impossibilitar a cobertura sob apólices tradicionais cibernéticas ou de E&O, o produto de IoT da Marsh fornece cobertura explícita e sob encomenda para:

- Erros e omissões no projeto e na fabricação dos dispositivo de IoT, inclusive aqueles que resultam em eventos de segurança ou privacidade para os clientes.
- Erros e omissões na prestação de serviços ao produto de IoT.
- Despesas com extorsão de ameaças direcionadas contra os produtos de IoT ou o seu uso.
- Custos ou despesas para mitigar, reduzir ou evitar reclamações potenciais.

O produto de IoT da Marsh também pode minimizar as exposições a determinados riscos para dar suporte ao investimento e à inovação da IoT, acelerando a sua trajetória de crescimento.

As variações da botnet Mirai continuam a provocar a destruição nos dispositivos de IoT. Por exemplo, no início deste ano, os hackers usaram o código da botnet Mirai e a energia de processamento dos dispositivos conectados – inclusive smartphones e smart TVs – para minerar o Monero, um tipo de moeda digital criptografada. Os especialistas em segurança advertem que os hackers continuarão a atacar os dispositivos de IoT para a mineração de criptomoedas.

Os ciberataques que interferem na operação apropriada de determinados dispositivos de IoT, como veículos ou dispositivos médicos conectados à internet, também podem apresentar um perigo para a vida humana e a propriedade. A US Food and Drug Administration (FDA), por exemplo, advertiu os pacientes com certos marca-passos de que eles estariam vulneráveis caso fosse enviado um código de computador para esvaziar a bateria do marca-passo ou modificar as frequências cardíacas. Os pesquisadores "white-hat" também apontaram a existência de ciberataques bem sucedidos contra veículos conectados à internet.

CONSIDERAÇÕES REGULADORAS

Os legisladores ficaram atentos a uma lista crescente de ataques de IoT e advertências nos noticiários. Em 2017, a legislação bipartidária foi introduzida no Senado dos EUA para melhorar a segurança dos dispositivos conectados à internet. Entre outras providências, esta legislação exigiria que os fornecedores de IoT que conduzem negócio com o governo dos EUA assegurassem que os seus produtos atendem aos vários requisitos de segurança. A legislação projetada para melhorar a cibersegurança de veículos autônomos e dispositivos médicos conectados à internet também está em andamento no Congresso. Agências do Poder Executivo, como a National Highway Traffic Safety Administration, também estão se envolvendo, emitindo diretrizes sobre segurança para carros e caminhões habilitados para a internet.

A regulamentação da IoT não está limitada aos EUA. O Reino Unido, por exemplo, divulgou um relatório em março que estabelece as diretrizes para ajudar a garantir que os dispositivos de IoT estejam "protegidos pelo projeto", com a segurança embutida desde o início.

PREPARANDO-SE PARA A REVOLUÇÃO DA IOT

As empresas que projetam, desenvolvem, fabricam ou prestam serviço aos dispositivos ou produtos de IoT devem levar em conta uma série de exposições cibernéticas potenciais. Elas incluem:

- Responsabilidade devido a suposto defeito no projeto ou na fabricação.
- Responsabilidade devido a uma falha na conectividade.
- Responsabilidade devido à falha na segurança.

- Responsabilidade na prestação de serviços para o produto de IoT.
- Demandas de extorsão contra os seus clientes ou contra a empresa.
- Investigações regulatórias, multas pecuniárias e multas contratuais.

As empresas que colocam em funcionamento ou que usam os dispositivos de IoT também podem estar sujeitas a riscos cibernéticos, inclusive violações de dados, interrupção dos negócios e despesas adicionais, restauração de dados, extorsão, danos materiais e lesões corporais de uma suposta vulnerabilidade na segurança ou violação da privacidade.

Para proteger a sua empresa desses riscos, a Marsh conta com uma equipe de especialistas que podem ajudar a você a avaliar as suas exposições cibernéticas de IoT e analisar as suas apólices cibernéticas e de erros e omissões

AVALIANDO SEU RISCO CIBERNÉTICO DE IoT

A Marsh Risk Consulting oferece um conjunto de serviços de cibersegurança moldados para os riscos de tecnologia de uma organização, inclusive voltados a Internet das Coisas (IoT).

AVALIAÇÕES DE RISCOS CIBERNÉTICOS

As avaliações de risco cibernético podem ajudar as empresas a entender melhor os riscos de ponta a ponta associados ao uso dos dispositivos de IoT, como os processos automatizados de fabricação ou produção. Podemos dar pontuações qualitativas aos riscos cibernéticos, de uma forma que se interliguem às estruturas de gestão de risco empresarial existentes.

PROGRAMA DE GESTÃO DE FORNECEDORES

Podemos trabalhar com você conduzindo uma análise minuciosa do seu programa de gestão de fornecedores, incluindo o monitoramento continuado. Esta análise pode ajudar na avaliação das exposições cibernéticas relacionadas aos fornecedores da sua empresa, entre outras coisas, manutenção, teste e atualizações da missão crítica dos sistemas de controle industrial.

CBIQ – QUANTIFICAÇÃO DA INTERRUPÇÃO DO NEGÓCIO CIBERNÉTICO

A análise da CBIQ dos panoramas de interrupção do negócio, inclusive aqueles impulsionados pelas exposições de IoT, pode ajudar na identificação de questões não resolvidas que possam justificar um aumento nos investimentos de mitigação do risco ou transferência de risco. Este procedimento pode ajudar na compreensão da sua exposição ao risco cibernético em termos financeiros e informar sobre as suas decisões quanto aos limites do seguro cibernético, investimentos de mitigação cibernética e retenção de risco.

(E&O) para assegurar a cobertura e os limites apropriados para os produtos e serviços de IoT. As apólices atuais não contemplam itens relacionados a dispositivos e eventos de IoT, dando margem para ambiguidades e o dilema generalizado de "silent cyber", em que a cobertura pode estar disponível por não estar explicitamente excluída. Por exemplo, as apólices de E&O de tecnologia podem ter cobertura disponível para os produtos de IoT, caso a definição de "produtos de tecnologia" esteja escrita de modo amplo, mesmo quando a definição não inclui especificamente os produtos de IoT.

Ao analisar as suas apólices de seguro e planos de resposta ao evento cibernético, leve em conta as seguintes questões:

- A sua organização quantificou as perdas potenciais (ou os custos) de um evento cibernético relacionado à IoT?

- As suas apólices de seguro fornecem cobertura suficiente para uma falha na manutenção ou na prestação de serviços do seu produto de IoT, como atualizações de software, pacotes de serviço, patches e outros lançamentos de manutenção?

- A sua cobertura para extorsão cibernética inclui demandas aleatórias feitas por clientes e originadas de falha na sua segurança ou serviço?

- As suas apólices de seguro cibernético, de bens patrimoniais e de responsabilidade civil geral e os planos protegem de modo adequado a sua empresa de quaisquer exposições cibernéticas potencializadas pelos dispositivos de IoT?

Durante esta análise, examine o texto das suas apólices e planos para determinar se os dispositivos de IoT e os serviços estão excluídos ou separados de definições importantes como "sistema de computador", "produto de tecnologia" e "serviço profissional". As empresas também deverão analisar a cobertura de suas apólices de responsabilidade civil geral e de bens patrimoniais, mantendo um olhar atento na atividade reguladora pertinente à medida que os requisitos de segurança evoluem rapidamente para acompanhar o ritmo da inovação.

MARSH

Para mais informações sobre os riscos cibernéticos de IoT e as estratégias relacionadas de gestão de risco, entre em contato com o seu representante da Marsh, ou com:

CARLOS SANTIAGO
Líder da Marsh Risk Consulting Brasil
+55 (11) 3532-7711
carlos.santiago@marsh.com

RONALD AMTHOR
Líder FINPRO da Marsh LAC
+55 (11) 3532-7479
ronald.amthor@marsh.com