Internet das Coisas em um Mundo Conectado

UNIDADE 01

Regulamentações para Internet das Coisas

Olá, seja muito bem-vindo a primeira semana da disciplina de Internet das Coisas ao Mundo Conectado. Nesta semana iniciaremos uma recapitulação do que é internet das coisas e seu impacto na sociedade e avançaremos discutindo os desafios para a Internet das coisas, a necessidade de regulamentação e o papel dos governos.

A regulamentação da Internet das Coisas

Certamente você deve ter acompanhado nos noticiários que vez ou outra alguns serviços da internet acabam saindo do ar. A causa desta queda de serviço pode ser conhecido ataque distribuído de negação de serviço. Este ataque sobrecarrega os serviços de internet ao ponto de não conseguir atender mais os usuários. Estamos em um mundo cada vez mais conectado e dependente destas tecnologias. Desta forma é necessário uma maior regulamentação e participação de governos para que uma legislação clara e que extrapole fronteiras possa ser definida.

Com advento da internet das coisas, milhões ou bilhões de dispositivos estarão conectados simultaneamente na rede mundial sendo projetados e vendidos por empresas que estão espalhadas ao redor do mundo. Grande parte das indústrias não tem motivação adequada para intervir na elaboração de processos regulatórios. Para agravar esse cenário, muitos usuários são leigos e sequer sabem quais padrões e normas de segurança devem ser adotados por esses fornecedores para que garantam o nível mínimo de segurança. Grande parte desses dispositivos estão nas indústrias, no comércio, na saúde e em nossas residências. (SCHNEIER, B. 2016).

Primeiro podemos pensar em padrões de desenvolvimento. A pergunta que nos resta é: “será que os desenvolvedores adotam padrões de desenvolvimento de hardware e software que garantam o funcionamento desses dispositivos em nossas residências?”. Alguns anos atrás um famoso termostato vendido mundialmente apresentou um bug. Esse termostato poderia desligar durante o período de seu uso noturno. Para quem não sabe, um termostato é utilizado para manter a temperatura de uma residência. Agora imagine em um país onde a temperatura externa alcança -10 °C e enquanto o proprietário dorme o termostato simplesmente desliga. Ao acordar, o proprietário da residência pode encontrar sua casa a uma temperatura negativa, congelando todo o encanamento. Grande parte do software embarcado neste tipo de sistemas utiliza software desenvolvido por terceiros. Esta é uma característica do desenvolvimento de software moderno. Até mesmo uma charge sobre esta preocupação:

Charge sobre riscos de reutilização de código. (Fonte: Finding Critical Open Source Projects | Google Open Source Blog (googleblog.com))

Nesta ilustração podemos ver que toda a infraestrutura, apesar de tão moderna, pode estar dependendo de um único módulo frágil. Caso seja encontrado alguma vulnerabilidade neste módulo frágil, todos os demais sistemas dependentes poderão ser comprometidos. Possivelmente você também deve se lembrar que recentemente uma aeronave Boeing 737 Max apresentou problemas relativos a software, acarretando desastre aéreo.

Boeing 737 Max (Fonte:
The Banning of Boeing 737 MAX 8 Aircraft is Impacting Business Aviation - MoonJet Flight Support)

O segundo aspecto que merece atenção e a segurança ao acesso desses dispositivos. Sabemos que ao redor do mundo muitas pessoas ainda utilizam dispositivos conectados a internet com a senha padrão fornecida pelo desenvolvedor. Esses dispositivos podem estar sendo remotamente controlados por terceiros mal-intencionados, que espera o momento certo para realizar algum tipo de ataque cibernético. Em grande parte das vezes as pessoas sequer sabem que seu dispositivo está comprometido, pois continua aparentemente funcionando corretamente. Não apenas em nossas residências, mas esta é uma preocupação também da indústria e do comércio. Usinas elétricas e siderúrgicas também são foco de ataques. No início de 2021, a Companhia Paranaense de Energia Elétrica (COPEL) confirmou um desses tipos de ataque. Alguns servidores de rede ficaram indisponíveis e medidas de contingência tiveram que ser tomadas.

Uma terceira preocupação é a longevidade de alguns dispositivos eletroeletrônicos. Com advento da internet das coisas, temos a expectativa que muitos dispositivos em nossas residências estejam conectados à rede mundial. Quando pensamos em um smartphone, sabemos que os usuários trocam, em média, a cada três anos. Mas quando falamos de

uma geladeira, geralmente esta tem uma vida útil superior a 10 anos. Será que o fabricante desta geladeira continuará dando suporte pela rede a um dispositivo com uma vida tão longa? Será que por 10 anos este fabricante fará atualizações de segurança em seus dispositivos?

Uma quarta preocupação que temos é com relação ao volume de dados coletados. Aos termos bilhões de dispositivos ligados à rede mundial, é natural que tenhamos um volume proporcional de dados sendo gerados. Como transformar esses dados em informações realmente úteis? De fato, os usuários não querem saber que a temperatura de sua geladeira estava -4,2 °C às 3h52 da madrugada. O que os usuários querem saber é se a geladeira está funcionando corretamente. Surge assim a necessidade de uma engenharia voltada à análise de grande volume de dados: conhecida como Big Data.

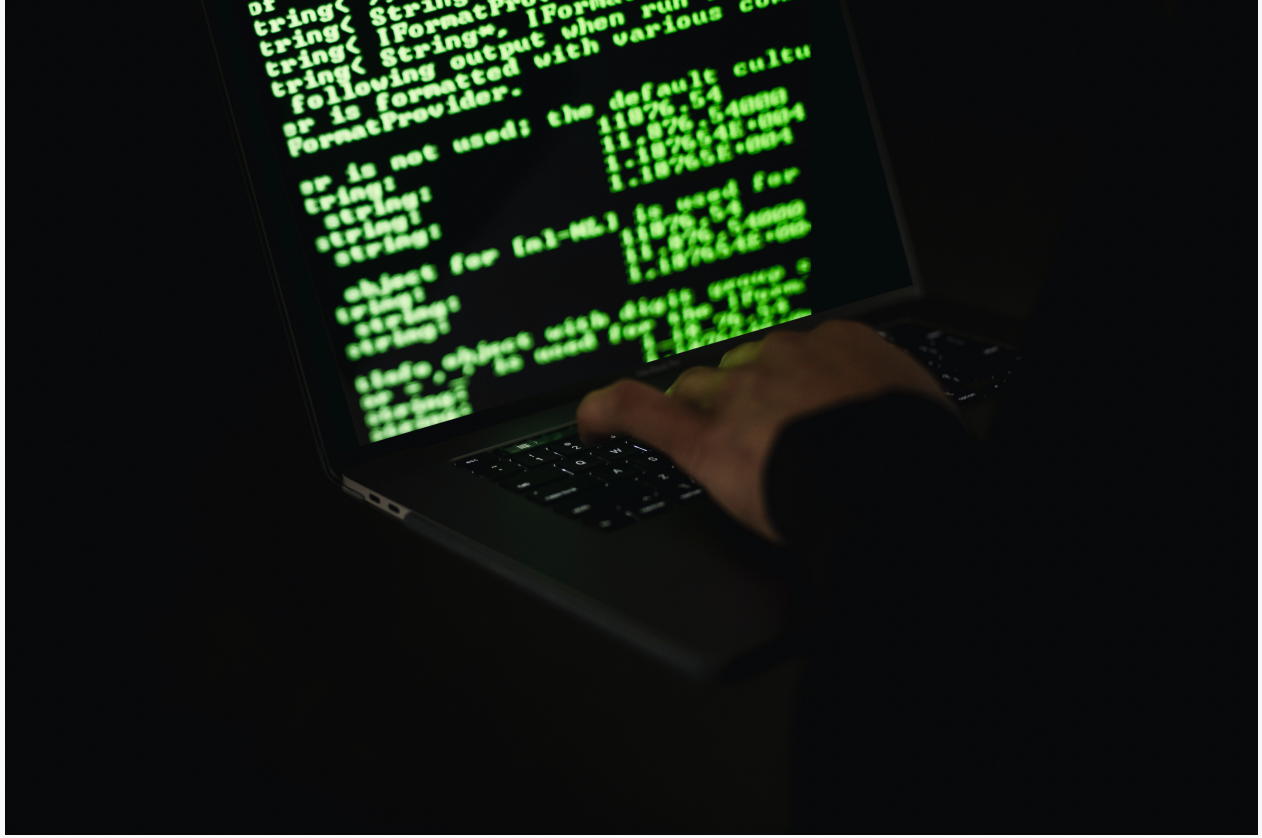

Foto de **Sora Shimazaki** no **Pexels**

Por fim, para que tudo isso funcione adequadamente, é necessária a criação de leis e procedimentos recomendados. De nada adianta descobrirmos que alguém cometeu um crime cibernético se não pudermos imputar a ele esta responsabilidade. Mas resta uma pergunta: quem pode regular efetivamente a internet das coisas? Sabemos que normas serão necessárias, mas se “engessarem” demasiadamente a liberdade para criação de dispositivos, estas normas poderão inviabilizar a Internet das coisas (BUTTLER, P. 2017).

Governos do mundo todo precisam estabelecer padrões mínimos para desenvolvimento e manutenção de dispositivos ao redor do mundo. Esses padrões não devem apenas dizer o que as empresas não podem fazer. Devem também ajudar e orientar as empresas a desenvolver esta tecnologia em um mundo de incertezas. Assim, as agências governamentais podem assumir três categorias: como usuário final; como provedor

de infraestrutura; e como órgão regulador. Como Joe Mariani afirma, a internet das coisas pode se tornar uma caixa de pandora se não adequadamente administrada (MARIANI, J. 2017).

Conclusão

Nesta semana retomamos o conceito básico de Internet das coisas, sua importância na sociedade, seu impacto em várias áreas e seus desafios. Também abordamos a preocupação de regulamentar tanto o seu desenvolvimento como sua utilização, e quem pode fazê-lo.

Referências

SCHNEIER, B. Seu termostato conectado por Wi-Fi pode desligar toda a Internet. Precisamos de novos regulamentos. The Washington Post, Washington, 2016. Disponível em: <https://translate.google.com/translate?act=url&depth=2&hl=pt-BR&ie=UTF8&prev=_t&rurl=translate.google.com&sl=en&sp=nmt4&tl=pt-BR&u=https://www.washingtonpost.com/posteverything/wp/2016/11/03/your-wifi-connected-thermostat-can-take-down-the-whole-internet-we-need-new-regulations/&xid=17259,15700023,15700124,15700149,15700168,15700173,15700186,15700189,15700201>. Acesso em: 3 jun. 2021.

BUTTLER, P. Quem pode regular a IoT? CSO Online, Estados Unidos, 2017. Disponível em: <https://translate.googleusercontent.com/translate_c?act=url&depth=1&hl=pt-BR&ie=UTF8&prev=_t&rurl=translate.google.com&sl=en&sp=nmt4&tl=pt-BR&u=https://www.csoonline.com/article/3216110/internet-of-things/who-can-regulate-the-iot.html&xid=17259,15700023,15700124,15700149,15700168,15700173,15700186,15700189,15700201&usg=ALkJrhgUw5dasQrIyoNJxTJFrXpPmTYoJg>. Acesso em: 3 jun. 2021.

MARIANI, J. Guiando a IoT para a segurança. Deloitte Insights, Estados Unidos, 2017. Disponível em: <https://translate.google.com/translate?sl=en&tl=pt&js=y&prev=_t&hl=pt-BR&ie=UTF-8&u=https%3A%2F%2Fwww2.deloitte.com%2Finsights%2Fus%2Fen%2Ffocus%2Finternet-of-things%2Fregulating-iot-technology-role-of-government.html&edit-text=&act=url>. Acesso em: 3 jun. 2021.