1. RESUMO

Esta pesquisa foi feita com o intuito de abordar os principais vetores de ataque e vulnerabilidade presentes em ambientes de infraestrutura crítica. Ao final desta pesquisa será sugerida uma solução para estas vulnerabilidades utilizando a tecnologia Blockchain.

2. INTRODUÇÃO

Com o intuito de introduzir o assunto desta pesquisa, imaginemos que você (leitor) é dono de uma indústria voltada para a agricultura, na qual certas áreas devem ter uma temperatura específica e devem ser regadas em momentos específicos do dia, caso ocorra uma variação além do que é aceitável da temperatura ou falta/excesso de água no plantio, o resultado do produto/serviço que você fornece é severamente comprometido. Iremos abordar o assunto de tecnologia operacional (OT) que dentro deste assunto abordaremos o conceito de ICS (Industrial Control Systems)/SCADA (Supervisory Control and Data Acquisition).

3. Objetivos

Temos como objetivos demarcar os principais caminhos que os atacantes percorrem para iniciar um ataque à uma infraestrutura crítica, no seu caso, caro leitor, alguma automação da sua empresa de agricultura. Também devemos saber quais são os principais tipos de ataque voltados para os ICS e introduzir o conceito de Blockchain com o intuito de propor uma possível solução para mitigar estes vetores de ataque e vulnerabilidade.

3.1– Vetores de ataque

A imagem abaixo resume em porcentagem os pontos de acesso inicial ao ICS/SCADA.

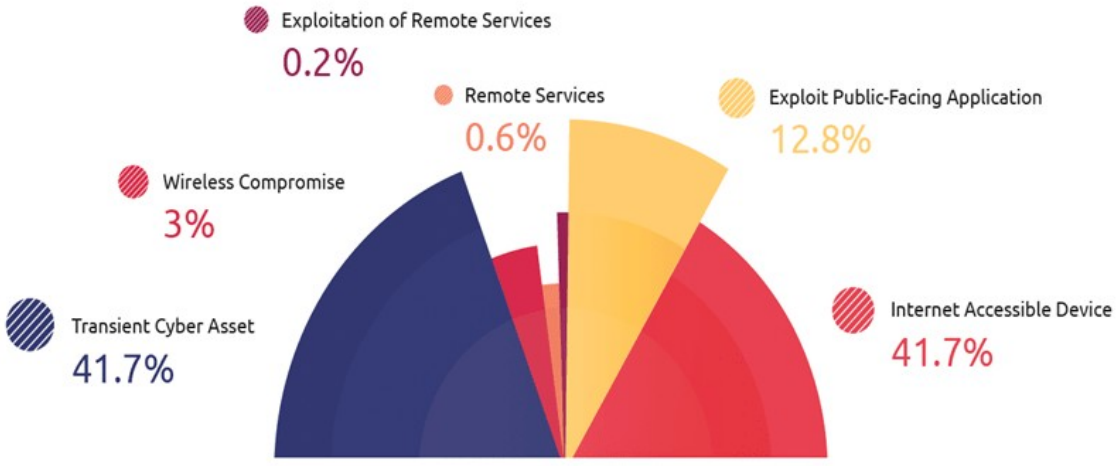

Figura 1: vetores de ataque

Fonte: https://www.trendmicro.com/pt_br/research/22/d/an-in-depth-look-at-ics-vulnerabilities-part-3.html

. Dispositivos acessíveis à Internet (Internet Acessible Device) e ativos cibernéticos transitórios (Transient Cyber Asset) estão vinculados para a maioria dos pontos de acesso inicial, com ambos em 41,7%.

. A exploração de aplicativos voltados para o público (Exploit Public-Facing Aplication) chega a 12,8%. É quando os atacantes usam um software voltado para a Internet, como aplicativos da web HMI ou SCADA, serviços de rede ou sistemas operacionais de ativos como ponto de partida para seu ataque.

. Além disso, os compromissos sem fio (3%), serviços remotos (0,6%) e exploração de serviços remotos (0,2%) foram os mais baixos. Isso não deve ser tomado como uma indicação de que as superfícies de ataque relacionadas não precisam ser protegidas.

3.2 – Vulnerabilidades ICS/SCADA

Uma das maiores vulnerabilidades encontradas estão relacionadas a uma codificação insegura, o que sugere que os fornecedores ou programadores não estão se preocupando com a segurança do seu produto, ou então, não estão verificando corretamente o seu código antes de lançá-lo. Um produto que deve ser muito bem manutenido é o SCADA pois ele é a interface gráfica do ICS, visto que qualquer alteração nele, alterará o produto ou serviço da empresa em questão.

Outra vulnerabilidade é a de injeção de dados que visa alterar os padrões de certas automações feitas pelo ICS (por exemplo alterar a temperatura das estufas de uma indústria de agricultura).

A figura abaixo exemplifica três interfaces de um sistema SCADA de uma indústria.

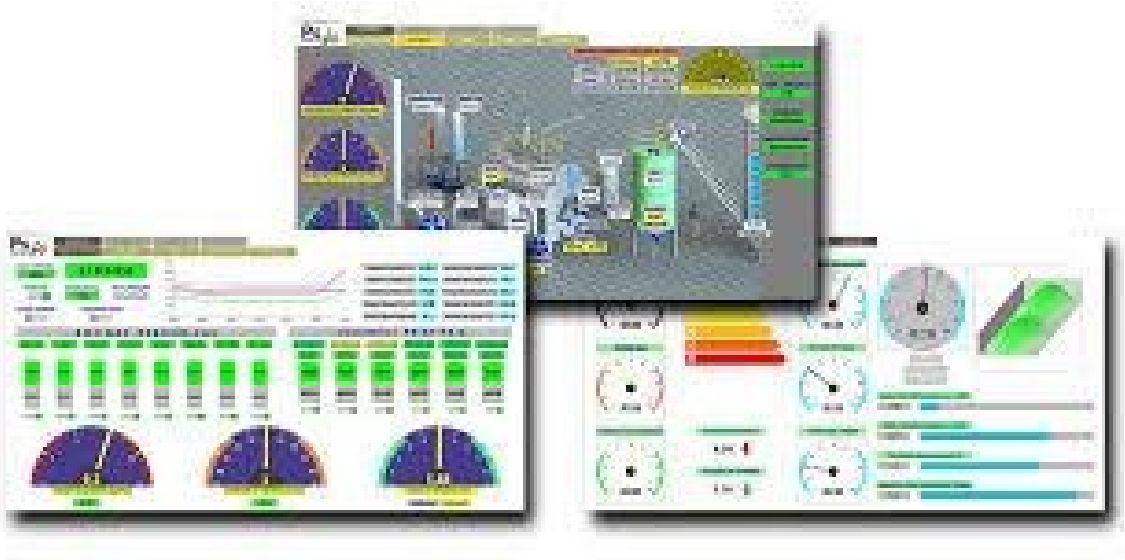

Figura 2: Exemplos de SCADA

fonte: https://www.marrari.com.br/engenharia/software-sistema-scada/

3.3 – Blockchain

A tecnologia de cadeia de blocos permite a descentralização desenvolvendo aplicações sobre uma rede par-a-par, por ser descentralizado todos podem ver o que trafega nesta rede (no caso ver os Hashes). Em uma cadeia de blocos, por exemplo o 4º bloco tem o hash do 3º e confirma a partir do “Proof-of-Work” se o hash é o mesmo, caso não seja o mesmo é acusado que tem alguma diferença no 3º bloco, ou seja alguém alterou algum dado que estava alí inserido.

Um dos diversos pontos positivos da utilização do blockchain é a transparência e a agilidade no tráfego de dados, além da indiscutível segurança proporcionada pela criativa implementação do uso dos Hashes para verificar a veracidade dos blocos. Caso uma empresa implemente uma rede blockchain em sua tecnologia operacional, a alteração de quaisquer tipo de dados só vão ser aceitos casos todos os integrantes da rede aceitem a mudança.

Em suma a utilização da tecnologia de cadeia de blocos melhora a segurança, a confiabilidade, a privacidade e a auditoria em sistemas críticos.

4. JUSTIFICATIVA

Com diversos problemas abordados, como os vetores de ataque e as vulnerabilidades dos sistemas de tecnologia operacional ICS/SCADA, podemos observar que uma das vulnerabilidades encontradas seria a possível troca de porta de um sistema SCADA, o que gera um considerável risco à infraestrutura crítica da indústria, visto que se alguém tentasse alterar algum dado pelo SCADA, alterando a porta 502 por exemplo, conseguiria o acesso. Com a utilização da tecnologia blockchain, esta alteração da porta do SCADA só seria permitida caso todos os integrantes desta rede fossem favoráveis a troca deste dado.

5. SOLUÇÃO

A solução não seria retirar estes protocolos automatizados do ICS/SCADA, mas sim reforçar a segurança deles, utilizando esta tecnologia de cadeia de blocos tornando a rede de infraestrutura crítica muito mais segura, transparente e ágil. Além do fator segurança, ao utilizar uma rede blockchain a industria/empresa que a utiliza ganha uma confiabilidade maior no mercado.

Portanto a rede blockchain, por sua descentralização, transparência, confiabilidade e segurança deve ser implementada na área de tecnologia operacional com o intuito de resolver as vulnerabilidades críticas do ICS/SCADA

6. BIBLIOGRAFIA

Mattos, Diogo M. F. Medeiros. ***Blockchain* para Segurança em Redes Elét Inteligentes: Aplicações, Tendências e Desafios.** UFF, rio de janeiro. 202

Henrique, João. **Descubra as 7 principais aplicações do blockchain e seu funcionamento.** Disponível em: https://www.voitto.com.br/blog/artigo/aplicacoes-d blockchain. Acessado em: 08/06/2022

TREND micro, 6 de abril de 2022. Disponível em: https://www.trendmicro.com/pt_br/research/22/d/an-in-depth-look-at-ics-vulnerabilities-part-3.html. Acessado em 08/06/2022.