Segurança cibernética

*Por Rodrigo Leal de Siqueira**

Capítulo II

O problema existe, é real e precisamos combatê-lo

Como bem dito no capítulo anterior, a transformação digital é uma realidade. Os ciclos de inovação são cada vez mais curtos e menos pacientes. Uma startup faz a disrupção de algo em poucos dias, quebrando barreiras de anos de uma empresa tradicional.

Ter a informação correta, no tempo certo, com qualidade é uma necessidade, não mais um capricho. Para que estes pontos sejam atingidos, algo simples e mágico precisa ocorrer: a conectividade.

Estudos indicam que teremos "muitos" bilhões de dispositivos conectados até o final de 2025, inclusive nós. Ter sua vida monitorada a cada segundo será uma realidade, mas isso é um outro tópico a ser tratado posteriormente.

As facilidades que a conectividade nos trará são imensuráveis. Os dados monitorados e tratados podem virar informações valiosas para a predição de acidentes ou mesmo a mudança de uma atividade, somente com o correlacionamento de informações. Tudo isso em segundos.

Ao pensarmos na transformação digital como base ou pavimentação, devemos ter soluções contínuas de detecção de ameaças para acompanhar em tempo real tudo o que está acontecendo neste novo ambiente conectado.

Estamos no ano de 2022 e vivemos o mundo da hiperconectividade, só que agora também no processo produtivo/operativo das empresas. Vocês conectaram o que nunca foi conectado e a realidade atual é que criamos um landscape para ameaças perfeito, conectamos ambientes frágeis por natureza e isso não é um erro, é característica do negócio.

O gráfico da Figura 1 representa exatamente o contexto em que vivemos. As redes de TI/IT (Tecnologia da Informação) corporativas nascem protegidas com diversas soluções e sua camada de exposição, apesar de existir, é pequena. Ao olharmos para o ambiente de TO/OT (Tecnologia Operativa – Automação e Telecom), o cenário é completamente inverso, soluções de segurança cibernética pouco implementadas e a camada de exposição é muito grande. A diferença é que a camada de exposição no ambiente produtivo/operativo das empresas tem relação direta com dois temas de suma importância - vidas humanas e a lucratividade dos negócios.

Figura 1 - IT x OT no mundo de segurança.

O título deste artigo tem por base experiências reais e um estudo da Claroty que compartilha dados relevantes após a entrevista com mais de 1.100 profissionais de segurança cibernética das áreas de IT e OT, com dados reais do segundo semestre de 2021.

As principais descobertas deste estudo incluem os aspectos relacionados a seguir:

1 - Os ataques de ransomwares foram enormes e os pagamentos, incrivelmente, predominantes

• A crescente onda de ataques de ransomwares direcionados a organizações atingiu novos patamares e nenhuma organização está imune. Olhando mais de perto, a distribuição de ataques, em setores como petróleo e gás, água e resíduos e automotivo, 90% deles foram impactados por ransomware e 87% na indústria pesada e energia elétrica. Não surpreendentemente, quanto maior a organização, maior a probabilidade de um ataque, pois é aí que está o dinheiro;

• Surpreendentes 80% dos entrevistados experimentaram um ataque, com 47% relatando um impacto em seu ambiente de OT/industrial(ICS);

• Mais de 60% pagou o resgate e pouco mais da metade (52%) pagou $ 500.000 USD ou mais;

• Mais de 90% divulgaram os incidentes aos acionistas e/ou autoridades e 69% acreditam que a notificação do incidente deva ser obrigatória.

O que está impulsionando essa decisão de pagar o resgate? Como diz o ditado, "tempo é dinheiro". Independentemente da região, a maioria dos entrevistados estimou uma perda de receita por hora de inatividade em suas operações igual ou superior ao pagamento. Assim, o modelo financeiro parece favorecer o pagamento do resgate dada essa equação e o que está em jogo. Esse raciocínio também é provável porque, em uma base global, 69% dos entrevistados acreditam que deveria ser legal pagar resgates. Para mudar o cálculo financeiro, é necessário um sistema de incentivos e desincentivos que favoreçam melhores controles e governança de risco desde o início.

2 - A transformação digital, o trabalho remoto e a escassez de pessoal persistem

• A transformação digital continua a acelerar desde a pandemia e o trabalho remoto/híbrido continuará em 73% das organizações;

• Quase 90% estão procurando contratar, mas 54% dizem que é difícil encontrar candidatos de segurança de OT qualificados suficientes.

Os entrevistados relatam que a transformação digital acelerou desde o início da pandemia da Covid-19 e, em uma base global, algum nível de trabalho remoto continuará em 73% das organizações no futuro próximo. A transformação digital, o aumento inerente na conectividade entre as redes de TI e OT e o acesso remoto para os funcionários apresentam riscos ao criar vetores adicionais para invasores. Os resultados apareceram nas

manchetes e estimularam novos alertas do governo sobre o risco de conectar redes industriais a redes de TI e a necessidade de um estado elevado de conscientização e controles.

3 - Governança e supervisão executiva mostram uma liderança forte

• Mais da metade dos entrevistados dizem que o C-suite e o conselho de sua organização estão muito envolvidos na tomada de decisões e na supervisão de segurança cibernética;

• Mais de 60% estão centralizando a governança de TO e TI sob o CISO – uma prática recomendada;

• Mais de 65% classificam a estratégia de gerenciamento de vulnerabilidades de sua organização como moderada a altamente proativa, mas os ataques de ransomware são muito bem-sucedidos.

À medida que a transformação digital e o trabalho remoto continuaram ao longo de 2021, os ataques de ransomware nas redes de TI e OT/ICS foram desenfreados e os pagamentos foram significativos. Enquanto o modelo financeiro continuar favorecendo o pagamento e o resgate, essas ameaças continuarão. A única maneira de mitigar o risco é entender como tornar a hiperconectividade mais segura.

As lacunas em processos e tecnologia, algumas que existem há anos, devem ser abordadas. Felizmente, as organizações em todo o mundo têm uma forte liderança executiva e especialistas confiáveis em segurança cibernética no comando. Juntos, eles estão no caminho certo. Estendendo a governança para incluir redes de OT, alocando recursos adicionais e priorizando as melhores práticas e controles, eles estão construindo resiliência em meio à disrupção.

Como mencionado no capítulo anterior deste fascículo, "não existe bala de prata". As regras definidas pelo ONS e pela Aneel são apenas o início de algo que precisa ser contínuo e abrangente.

Ao olharmos para a rede operativa de um ambiente elétrico, devemos mirar cinco dimensões de suma importância, não somente casos de "ransomwares".

• A dimensão 1: entendimento do ambiente

Neste primeiro pilar, identificamos cada um dos ativos, seus protocolos, seus detalhes de configurações, seu perfil de comunicação, seu padrão. Todos os detalhes fim a fim em uma infraestrutura crítica por completo, mirando protocolos de OT, IOT, IIOT e IT para que tenhamos uma visibilidade fim a fim dos ativos.

Ainda neste primeiro pilar, quando falamos de inventário de ativos, devemos considerar inclusive as redes cascateadas como Profibus atrás dos dispositivos de OT.

O inventário realmente precisa ser profundo, inclusive a obsolescência dos ativos para ser agregada ao nível de risco da planta. Não se protege o que não se identifica.

• A dimensão 2: integridade de processos

Foi se o tempo em que um ataque era ocasionado somente por um vírus, um Trojan ou algo neste sentido. Atualmente, muitos problemas são ocasionados por ataques direcionados no ambiente operativo ou mesmo erros humanos.

Uma solução que, ao inventariar na dimensão 1, traga parâmetros e configurações dos ativos inventariados para que posteriormente sejam analisados continuamente para gerar um alerta após uma alteração é essencial para se detectar um ataque direcionado no ambiente operativo.

• A dimensão 3: segurança cibernética

Uma solução para segurança cibernética operativa precisa ser criada e direcionada para isso. Deve-se entender as características do ambiente operativo, suas particularidades, protocolos e drivers. Especialização para a proteção é a chave.

• A dimensão 4: segurança operativa

Aqui destacamos um pouco mais a especialização. É muito comum nos ambientes operacionais existirem soluções de backups específicas para PLCs, SCADAS, entre outros dispositivos.

Uma solução de segurança cibernética para este mundo deve trazer benefícios além dos tradicionais. Neste caso, o envio de informações para agregar a um backup o seu risco é de grande valia para se entender a criticidade de um Disaster & Recovery de um ambiente operativo.

• A dimensão 5: operação remota segura

Neste período de pandemia criou-se um grande vetor de ataque para as redes operativas. O trabalho remoto utiliza ferramentas tradicionais de IT no mundo de OT.

A solução especializada para operação remota deve estar totalmente integrada aos padrões das redes operativas, mantendo toda a sua segmentação sem a necessidade de ajustes inseguros para uma operação remota na planta. Além disso, deve criar fluxos de aprovações para manutenções programadas, granularidade no acesso ao ativo de OT, gravação de vídeo de todas as atividades. Tudo isso ligado e interligado às dimensões 1, 2, 3 e 4 comentadas neste artigo.

mse engenharia

Há 42 anos **levando energia** para as principais **obras do país.**

Conheça as obras da mse.

Ano após ano estamos expandindo nossas operações e investindo em tecnologia, com soluções para atender obras industriais, de geração de energia, corporativas e de infraestrutura.

Acesse nosso site e entre em contato com nossa equipe de engenharia.

mse.com.br

mse

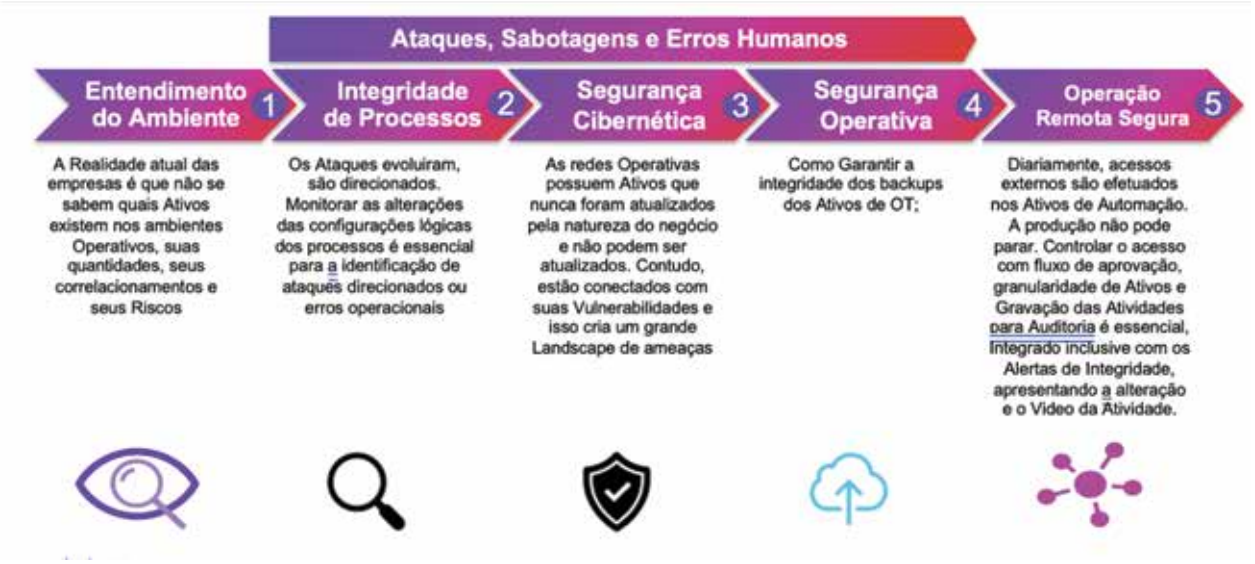

Figura 2 - As 5 dimensões.

A jornada é longa e contínua. Atender aos requisitos do ONS e da Aneel é apenas parte de uma grande jornada. Pensem na transformação digital e como o pilar especializado de segurança cibernética deve apoiar este ciclo contínuo de transformações exponenciais.

**Rodrigo Leal é graduado e mestre em engenharia elétrica. Possui MBA em Gestão de Projetos pela Fundação Getúlio Vargas (FGV) e curso de Gestão de Negócios da Era Digital pela Cesar School. Atualmente, cursa MBA Executivo de Negócios do Setor Elétrico pela FGV. Desde 2006 atua na Chesf, assessor do Diretor de Operação, coordenando vários processos da diretoria, incluindo os assuntos relativos à tecnologia operativa. Ocupa ainda a posição de vice-presidente do Conselho Diretor da UTC América Latina e Coordenador do Comitê de Tecnologia da Informação e Telecomunicações no Cigre-Brasil.*

Italo Calvano é engenheiro de computação, com especialização em Redes de Computadores, MBA e pós-graduação na COPPEAD com foco no mercado de energia. Atualmente, é vice-presidente da Claroty na América Latina, empresa especializada em segurança cibernética para infraestruturas críticas.