CENTRO DE CIBERSEGURIDAD INDUSTRIAL

EDIÇÃO 2021

Por que SOCs de TI e Híbridos não devem ser usados para proteger redes industriais

SÉRIE DE CADERNOS CCI. NÚMERO 6

Edição: 2021

ISBN: 978-84-123284-8-6

Paseo de las Delicias, 30 - 2º
28045 Madrid

+34 910 910 751
info@cci-es.org
www.cci-es.org

O Centro de Ciberseguridad Industrial (CCI) é uma organização independente, sem fins lucrativos, que tem como missão promover e contribuir para a melhoria da cibersegurança industrial, num contexto em que organizações de setores como a manufatura ou energia desempenham um papel fundamental na construção da sociedade atual, como pilares do Estado de bem-estar.

O CCI é, hoje, o ecossistema e o ponto de encontro das entidades -privadas e públicas e dos profissionais afetados, preocupados ou ocupados com a cibersegurança industrial; É também referência mundial em sua área de atuação, pela troca de experiências, pela dinamização dos setores envolvidos e pelo desenvolvimento de referenciais e boas práticas.

CONTROLES

Alt + seta para a esquerda para retornar à visualização anterior após acessar um hiperlink

Clique no nosso ícone e visite nosso site

Ao clicar nas bandeiras da primeira página, você poderá ver a atividade do CCI em cada um desses países.

Ao clicar no número da página você retornará ao índice

PATROCINADORES

PATROCINADORES **PLATINUM**

Telefónica Tech

PATROCINADORES **GOLD**

accenture
Check Point SOFTWARE TECHNOLOGIES LTD.
Entelgy Innotec SECURITY
FORTINET
paloalto NETWORKS
PHOENIX CONTACT
S2 GRUPO
STORMSHIELD

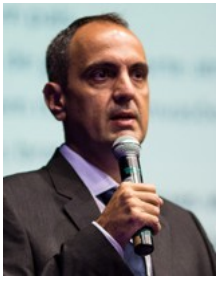
PATROCINADORES **SILVER**

CAPSA FOOD
kaspersky
Capgemini
S21 SEC
SIEMENS Ingenio para la vida
Sothis
TSK GRUPO
TECNICAS REUNIDAS
TÜV NORD

PATROCINADORES **BRONZE**

axians
Atos
CIC Consulting Informático
Deloitte.
DENEXUS
everis an NTT DATA Company
Getronics
gmv INNOVATING SOLUTIONS
LOGITEK
oylo Trust Engineering A ROCKWELL AUTOMATION COMPANY
SIA
tecnalia Corporación Tecnológica

AUTOR



Marcelo Branquinho

CEO E FUNDADOR DA TI SAFE

Engenheiro eletricista com especialização em sistemas de computação e MBA em gestão de negócios, sendo fundador e CEO da TI Safe. Especialista em segurança cibernética industrial. É autor de diversos livros técnicos e trabalhos publicados e frequente apresentador de estudos técnicos em congressos internacionais. Membro sênior da ISA Internacional, atua em diversos grupos de trabalho, como o da atual ISA/IEC-62443.

A série 'CCI Notebooks' é uma coleção de documentos de autores que compartilham sua experiência e opinião sobre tendências atuais e futuras.

Como organização independente, a CCI tem como objetivo dar voz a especialistas e colaboradores que agregam valor à cultura de cibersegurança industrial, gerando este espaço de troca de conhecimentos e experiências.

Nesse sentido, os 'Cadernos CCI' expressam, sob padrões de qualidade, uma contribuição do (s) próprio (s) autor (es).

CONTEÚDO

RESUMO

Embora haja relações positivas entre redes de TI (Tecnologia da Informação) e de TO (Tecnologia de Operação), o viés operacional de sua segurança cibernética é bastante diferente. Enquanto o principal pilar da segurança cibernética de TI é a confidencialidade das informações, o principal pilar da segurança ciber- nética de TO é a disponibilidade. Isso significa que, para atingir seus objetivos de segurança cibernética,tais ambientes precisam se diferenciar em suas tecnologias, metodologias e estratégias. No entanto, hoje começam a surgir no mercado, Centro de Operações de Segurança (SOC – do inglês Security Operation Center) híbridos; ou seja, aqueles em que profissionais especialistas em segurança cibernética de ambientes de TI e de TO trabalham juntos para gerenciar a segurança das redes de TO. Este tipo de gestão híbrida oferece altos riscos à continuidade operacional das redes de TO. Este artigo apresenta uma explicação mais aprofundada sobre os diversos aspectos da gestão de segurança de redes operativas para demonstrar porque não é recomendado utilizar SOCs de TI e SOCs Híbridos para proteger redes industriais.

Palavras-chave: Tecnologia da Operação; Tecnologia da Informação; Segurança Cibernética.

INTRODUÇÃO

Os avanços tecnológicos dos últimos anos superaram quantitativa e qualitativamente as inovações científicas e práticas da humanidade. Entre seus destaques, está o desenvolvimento computacional e sua ramificada rede mundial de comunicação, a Internet.

Se por um lado as novas tecnologias trazem grandes benefícios para a sociedade, aproximando as relações humanas virtualmente e propiciando a troca de informações instantânea, por outro, atrai a atenção de criminosos cibernéticos interessados em roubar dados sigilosos e realizar ataques com objetivos políticos e financeiros.

É fundamental hoje que redes privadas de tecnologia de informação (TI) e de tecnologia de operação (TO) tenham um alto grau de segurança física e lógica, sobretudo quando são a base de infraestruturas críticas cujos danos podem afetar drasticamente a sociedade.

Uma rápida pesquisa no banco de dados Incident Hub mostra que, de 2015 a 2020, o número de incidentes cibernéticos em redes industriais obteve um surpreendente aumento de mais mil porcento (Figura 1).

Tipo de industria	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	**Total**
Orgãos Governamentais				1	4	2	26	30	35	63	51	**212**
Saúde pública		2				2	19	4	6	35	41	**109**
Manufatura crítica		1			1		1	2	1	12	32	**50**
Sistemas de transporte	2	9	4	2	2	1	2	4	4	5	15	**50**
Tecnologia da Informação								2		19	26	**47**
Servicios de emergência				1	2	1	13	7	7	7	3	**41**
Energía	6	1	3		2	1		3	2	3	15	**36**
Comunicações								6	1	12	15	**34**
Serviços financeiros								3	1	4	16	**24**
Alimentação e Agricultura								2		4	9	**15**
Instalações comerciais								5		3	5	**13**
Infraestruturas críticas	1		1							2	9	**13**
Águas e Resíduos	4	2	2				2		1	1	1	**13**
Petróleo	1	1	4								1	**7**
Indústria química		1								1	4	**6**
Educação											4	**4**
Indústria base de defesa										1	2	**3**
Marítimo / Naval										1	2	**3**
Favricação geral	1		1									**2**
Vários											2	**2**
Sector hoteleiro										1		**1**
Reatores, materiais e instalações nucleares											1	**1**
Total	**15**	**17**	**15**	**4**	**11**	**7**	**63**	**68**	**58**	**174**	**254**	**686**

Figura 1 – O TI Safe Incident Hub (https://hub.tisafe.com) consolida os incidentes cibernéticos em redes industriais que ocurreram desde 1982 até os dias atuais.

Pode-se notar que os casos relatados englobam diversos segmentos industriais. Incidentes de segurança em redes operativas de energia elétrica, de indústrias químicas e petrolíferas, entre outras, demonstram que os ataques cibernéticos se estendem indiscriminadamente pelas redes críticas que abastecem a sociedade.

Embora haja relações positivas entre redes de TI e TO, o viés operacional de sua segurança cibernética é bastante diferente. Enquanto o principal pilar da segurança cibernética de TI pende para a confidencialidade, o principal pilar da segurança cibernética de TO é a disponibilidade.

Incidentes de segurança cibernética em redes de TI podem ocasionar problemas em sistemas administrativos importantes de uma empresa e causar perdas financeiras e danos à imagem dela, mas não ocasionam a perda de vidas humanas e danos ao meio ambiente.

No entanto, quando redes de TO são atacadas, as consequências são amplas e afetam diretamente o cotidiano das pessoas. Esta diferença fundamental no risco de incidentes de TI e TO já mostra que a segurança cibernética destas redes deve ser gerenciada por meio não apenas por meio de tecnologias diferentes, mas, também por meio de estratégias e pessoas com perspectivas, objetivos e formações técnicas diferentes.

Com isso, deduzimos de imediato a resposta em relação aos tipos mais adequados de centros de operações de segurança para cada tipo de rede. SOCs de TI são, majoritariamente, direcionados para redes corporativas cuja confidencialidade de dados (senhas, endereços, cartões de crédito etc.) é a principal preocupação.

SOCs de TO, também denominados SOCs industriais, são direcionados para redes cuja disponibilidade de sistemas de automação e controle (fornecimento de energia, água, comida, matéria-prima etc.) são o principal pilar de sua existência.

Resta, porém, uma dúvida em relação aos centros de operações de segurança híbridos; ou seja, aqueles que gerenciam e monitoram a segurança cibernética tanto das redes de TI quanto das redes de TO. Seria este tipo de SOC uma boa alternativa a ser adotada pelas empresas?

Essa dúvida será respondida por meio de uma análise mais aprofundada sobre as diferenças existentes nas pessoas, nas tecnologias e nos serviços gerenciados oferecidos pelo SOCs de TI, de TO e híbridos, como veremos adiante neste artigo.

PESSOAS

Semelhante à engenharia onde existem formações acadêmicas específicas que compartilham alguns fun- damentos em comum (engenheiro mecânico, civil, elétrico etc.), a segurança cibernética também exigeinstruções e formações exclusivas que variam conforme os objetivos que pretende alcançar, os clientes quedeve atender e os cibercriminosos contra os quais deve se proteger.

O oposto dessa exigência, isto é, a falta de formação apropriada em segurança cibernética de TO pode levar a problemas na operação de um SOC. Profissionais de um SOC de TO sem o devido conhecimento de tecnologias de automação ou mal-intencionados podem ser alvos de engenharia social e, assim, abrir caminho para invasões em plantas industriais.

Além disso, a equipe de um SOC industrial deve possuir estreitas parcerias com as fabricantes de software e hardware específicos utilizados nas plantas industriais e obter as certificações técnicas obrigatóriaspara operar devidamente a infraestrutura operativa e, com isso, garantir a máxima segurança cibernética possível.

A esfera "pessoas" engloba, além dos profissionais diretamente envolvidos com o chão de fábrica e com a sua segurança cibernética, os funcionários indiretos (administração, segurança física e patrimonial etc.) e os profissionais das empresas terceiras que fornecem os equipamentos e programas e que trabalham diretamente nas plantas industriais.

Uma boa forma de garantir a qualidade ao contratar um SOC industrial terceirizado é verificar se a empresa que provê os serviços possui atestados atualizados de capacidade técnica emitidos por pessoas jurídicas de seu segmento com serviços de SOC plenamente desenvolvidos e direcionados para redes de TO. Além disso, a empresa deverá demonstrar estar apta a gerenciar remotamente a segurança cibernética das redes industriais com soluções confiáveis e adequadas para esta finalidade.

Tais preocupações demonstram a necessidade de diferenciação entre os colaboradores de segurança cibernética de TO e de TI. Olhando para os cinco níveis da pirâmide de automação (modelo Purdue), cada profissional deve ser capacitado tecnicamente para operar soluções tecnológicas de segurança para proteger as soluções de níveis diferentes desta pirâmide (Figura 2).

Nivel Purdue	Infraestrutura	Segurança
4	Redes TCP/IP, MS, (AD, CA, etc.) Infraestrutura, Cloud, ERP, VoIP, etc.	SIEM, VPN, controle de acesso, NGFW, cópias de segurança, Ferramentas SOC, fontes de alimentação, gateways de segurança, pentesting…
3	MES, SAP PI	Gateways unidirecionais, ferramentas de acesso remoto
2	Sistemas de supervisão, protocolos industriais, ferramentas de engenharia e automação	EPP, Arquiteturas Zero Trust, cifra de dados
1	PLCs, IEDs, RTUs, redes automatizadas, comunicações em série	Firewalls industriais, Sistemas de detecção de intrusões Industriais
0	Sensores e actuadores, eletrônica	Hardware de segurança, segurança física

Figura 2 - Niveis de conhecimento tecnológico que devem possuir os profissionais de segurança cibernética de TI e TO para trabalhar em um centro deoperações de segurança.

Note que profissionais de segurança cibernética de TI devem normalmente possuir conhecimentos referentes apenas às tecnologias dos níveis 3 e 4, enquanto os profissionais de segurança de TO devem possuir conhecimentos que englobem todos os cinco níveis (de 0 a 4).

Ou seja, os profissionais que trabalham em um SOC de TO devem possuir uma gama de conhecimentos bem maior do que aqueles que trabalham em SOCs de TI, o que torna esse tipo de profissional muito difícil de formar internamente ou de contratar no mercado.

TECNOLOGIAS

As fraquezas e falhas humanas podem ser agravadas tanto com o mau uso de tecnologias industriais quanto pela gestão inapropriada de equipamentos de operação e de segurança. Em outras palavras, o uso incorreto de tecnologias de cibersegurança é muito perigoso e pode levar plantas industriais ao colapso.

Existem boas práticas comuns em segurança cibernética de TI que não devem ser aplicadas para a segurança de redes de TO. Como exemplo, o compartilhamento de serviços de rede de TI (tais como DNS e NTP, entre outros) na rede de TO representa uma grave falha de segurança, como advertido na norma ISA/IEC-62443.

> *O item 4.3.2 da norma ISA/IEC 62443-1-1 adverte que:*
>
> *As organizações que implementam soluções de segurança cibernética de tecnologia da informação (TI) para lidar com a segurança de sistemas de controle industriais podem não compreender totalmente os resultados da decisão. Embora muitos aplicativos de TI de negócios e soluções de segurança possam ser aplicados em sistemas industriais, eles precisam ser aplicados de maneira apropriada para eliminar consequências inadvertidas. Por esse motivo, a abordagem usada para definir os requisitos do sistema precisa ser baseada em uma combinação de requisitos funcionais e avaliação de risco, muitas vezes incluindo também a consciência de questões operacionais.*

Redes de TI e TO utilizam protocolos de comunicação diferentes. Enquanto as redes de TI são baseadas no protocolo TCP/IP, as redes de TO usam protocolos industriais altamente vulneráveis devido a diversos e complexos fatores relacionados à sua criação e à necessidade de respostas rápidas características de redes que operam em tempo real.

Diferentemente das redes de TI, as máquinas das redes operativas não podem ser atualizadas automaticamente por patches conforme novas vulnerabilidades são encontradas. Para realizar esta operação de segurança, é necessário planejamento, homologação com os sistemas de controle e monitoramento da planta industrial, testes em laboratório e, em alguns casos, suspender sua operação em paradas programadas que ocorrem com pouca frequência (semestrais ou anuais).

Diante desse cenário limitado, as redes de TO precisam ser protegidas com tecnologias e estratégias de segurança cibernética apropriadas para o uso industrial.

A equipe do SOC Industrial deve ter acesso restrito à rede de TO

> *O item 10.3.3 da norma ISA/IEC 62443-3-3 SR 5.1 afirma que*
>
> *Os sistemas de controle devem ter a capacidade de fornecer serviços de rede para as redes de sistemas de controle críticas, sem conexão com redes de sistemas de não-controle (redes de TI, corporativas e externas).*

De forma objetiva, os serviços e dados das redes externas necessários à operação das redes de controle devem ser depositados em servidores intermediários situados em uma DMZ entre as redes de TI e TO. Assim, nunca deve haver uma conexão direta entre os servidores e os clientes localizados na rede de TI com as máquinas na rede de TO.

O SOC Industrial deve ter sua atuação limitada às redes de TO, incluindo esta DMZ limítrofe, mas nunca à ativos localizados na rede de TI. Isso significa que SOCs híbridos representam, por possuir conexões tanto com as redes de TI quanto com as redes de TO, uma possível porta de entrada para atacantes que desejem acessar ou interromper as operações de uma rede industrial.

O SOC de TO deve proteger redes com protocolos inseguros

As redes de automação utilizam protocolos não usuais no mundo de TI e denominados "protocolos industriais". Estes protocolos foram desenvolvidos para responder rapidamente e em tempo real às solicitações dos sistemas e aplicações. Por isso, eles normalmente não possuem recursos de segurança que possam causar delays na rede tais como como criptografia e autenticação. É importante notar que os profissionais de segurança de TI são acostumados com a prevenção e resposta a ataques conhecidos que exploram fragilidades do protocolo TCP/IP e desconhecem os riscos de ataques em protocolos industriais, não sendo costumeiro o monitoramento deles.

Além disso, misturar eventos de TI e TO em uma única ferramenta de monitoramento (como SIEMs ou similares) não é recomendado pois as quantidades de eventos de segurança (logs) em redes de TI são muito maiores que em redes de TO, fazendo com que os eventos de segurança de TO possam facilmente se perder em um volume gigantesco de dados. Com isso, a visibilidade fornecida por ferramentas tradicionais de SIEM (Security Information and Event Management) é limitada quando utilizada para monitorar eventos de redes de TI e TO simultaneamente.

Um SOC de TO deve usar ferramentas de monitoramento específicas para redes industriais, como IDSs Industriais por exemplo, levando em consideração as diferenças básicas de análise e monitoramento de dados nestes ambientes. Além disso, elas devem ser capazes de correlacionar os eventos específicos de redes de automação (por exemplo, correlacionar eventos de Firewalls com os eventos de anomalias detectadas por Sistemas de Detecção de Intrusão industriais).

Políticas e procedimentos comumente aplicados à segurança cibernética de redes de TI podem paralisar a operação uma planta industrial

Políticas de segurança de TI não são aplicáveis plenamente às redes de TO (como, por exemplo, senhas, patches, firewalls, IDSs comuns etc.). A implementação de estratégias erradas pode afetar diretamente a disponibilidade de uma planta industrial.

Procedimentos de segurança invasivos e corriqueiros no trabalho de um SOC de TI como, por exemplo, a análise de vulnerabilidades e testes de penetração (pentest), devem ser evitados em redes de TO. Além disso, todas as coletas e análises de dados em redes de automação devem ser feitas sempre de forma não intrusiva a fim de evitar que tais procedimentos afetem a performance da rede operativa e, consequentemente, a operação da planta industrial.

SERVIÇOS

O trabalho diário de um SOC de TO é preventivo e as ações de segurança devem ser feitas sempre em alinhamento com a equipe de segurança do cliente. Com isso, gera-se uma segurança reforçada uma vez que as ações de segurança são sempre executadas e quatro mãos (equipe do SOC de TO + equipe do cliente). Ressalta-se, no entanto, que em redes de TO normalmente não existem respostas imediatas a incidentes de segurança cibernéticos e também não são possíveis as automatizações de atualizações de segurança, como é costumeiro em SOCs de TI.

Nesses casos, os serviços de atualizações de segurança devem ser cuidadosamente revisados para não afetarão a rede em produção. Respostas erradas a eventos monitorados por um SOC podem levar a paradas operacionais em redes críticas, piorando o problema. Um profissional de segurança de TI pode, por falta de conhecimento, bloquear uma comunicação importante para uma rede de TO por considerá-la uma ameaça, por exemplo.

Além disso, centros de operações de segurança de TO requerem necessariamente recursos inexistentes em SOCs de TI. Um SOC Industrial precisa, por exemplo, ter um laboratório de segurança com simuladores capazes de testar novas versões de sistemas operacionais, aplicativos e atualizações de soluções de segurança cibernética antes de aplicá-las nas plantas industriais. Os SOCs de TI não possuem tais laboratórios industriais nem equipe de P&D certificada para conduzir testes e homologações em redes de automação, o que acarreta um grande risco e imprudência ao aplicar soluções de segurança em máquinas da rede de TOsem antes testá-las e homologá-las em ambiente adequado e controlado.

A INTEGRAÇÃO DA GESTÃO SEGURANÇA CIBERNÉTICA DE REDES DE TI E TO É POSSÍVEL?

Integrar Centros de Operação de Segurança de TI e TO não significa a mesma coisa que estabelecer SOCs híbridos. Cada SOC deve gerir as soluções de segurança cibernética de seu tipo de planta (SOCs de TI paraplantas de TI e SOCs de TO para plantas industriais).

A integração da gestão deve ser feita em um nível mais alto, mantendo a autonomia de cada SOC, porém, em conjunto com as duas equipes de segurança para trocas de experiências e sugestões de melhoria através de um conselho global da empresa

O grande risco dos SOCs híbridos

Em uma rápida análise é possível constatar que um funcionário mal-intencionado de um SOC híbrido tem o poder de facilitar uma invasão de um hacker externo via internet ao liberar o acesso deste invasor pelos firewalls de TI e TO por ele controlados (Figura 3).

Este acúmulo de poderes nas mãos de funcionários de SOCs híbridos é algo financeiramente tentador e que pode viabilizar golpes por engenharia social, sequestros por Ransomware e uma enorme gama de ataques que podem levar à paralisação da planta industrial.

Ter provedores de SOCs de TI e TO com equipes diferentes aumenta a segurança e inviabiliza ataques externos e coordenados em direção à planta industrial. Desta forma, a gestão diferenciada da segurança das redes de TI e TO atua como uma muralha dupla de proteção que contribuirá, a seu modo, com um maior grau de proteção da infraestrutura industrial.

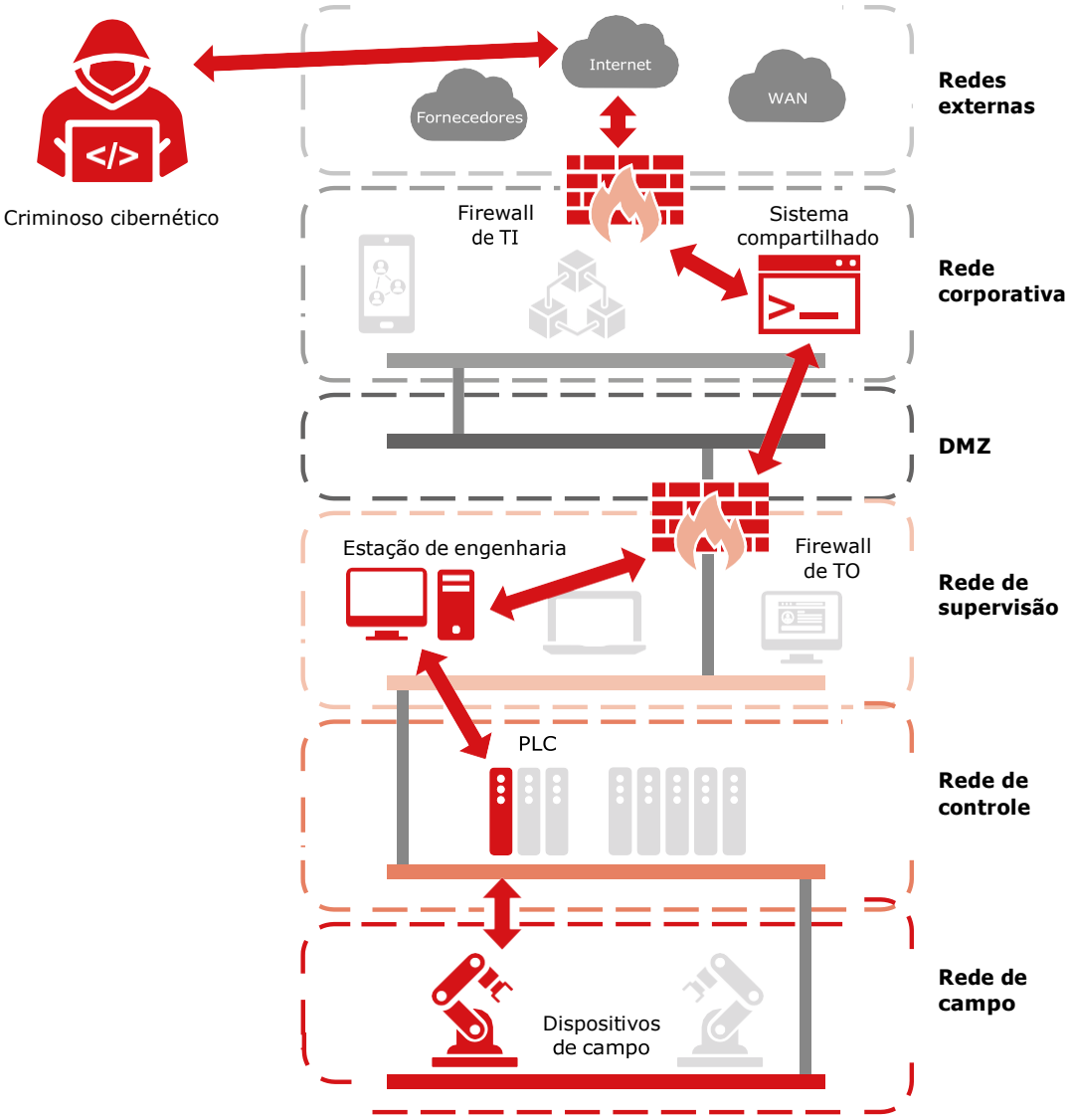


Figura 3 - Provedores de SOC de TI e TO devem ser diferentes e autônomos para evitarem ataques coordenados e erros de operação que podem paralisar a operação de redes críticas.

Essa estratégia com a autonomia de cada SOC impede que erros de configuração sejam propagados entre redes distintas e estabelece também uma melhor governança, permitindo que as equipes dos SOCs de TO e TI possam controlar a segurança cibernética das suas redes de forma independente.

Experiências aprendidas e informações relevantes de segurança devem ser compartilhadas entre os SOCs de TI e TO através de um comitê de segurança cibernética corporativa que deve estabelecer um processo integrado da gestão de riscos. Este comitê de segurança cibernética corporativa deve estar ciente sobre os potenciais impactos que a operação indevida de sistemas de TO pode causar sobre a empresa como um todo e até mesmo sobre a sociedade e o meio ambiente em ocorrências mais graves. Sua principal responsabilidade é alinhar os riscos cibernéticos com os riscos corporativos, além de fiscalizar e de estabelecer os papeis e objetivos que cada um dos setores deve assumir.

TERCEIRIZANDO A GESTÃO DE SEGURANÇA CIBERNÉTICA PARA UM SOC INDUSTRIAL

A oferta de profissionais experientes em segurança cibernética de TO não é farta no mercado atual. Existe uma carência global por profissionais com este perfil. Desta forma, compor um time para um SOC de TO interno é um grande desafio pois são necessários, no mínimo, 8 profissionais se revezando em esquema de turnos de trabalho para manter o gerenciamento e monitoramento das soluções de segurança em regime 24x7.

Em razão desta carência de profissionais, a terceirização da gestão de segurança industrial para uma empresa gabaritada é uma opção bastante interessante.

A tabela na Figura 4 apresenta um comparativo entre a composição de SOCs industriais internos (com funcionários da própria empresa) e a subcontratação de um SOC industrial externo:

Gestão através de um típico SOC interno	Gestão através de um SOC Industrial (TO)
Prosissionais internos	Time de elite de segurança cibernética industrial
Normalmente sobrecarregados com tarefas de TI e TO	100% focado em segurança cibernética industrial
Depende dos funcionários	Sempre disponível e escalável
Nível técnico Junior ou Médio	Nível especialista
Suvesso de detecçao indeterminado	Detecção de 100% das ameaças cibernéticas potenciais
Níveis 4, 3	Níveis 4, 3, 2, 1, 0
Poucas cestificações de segurança de TO	Time amplamente certificado e com experiência de projetos
Alto custo financeiro para implemantação e manutenção	Preços competitivos e compatíveis com os serviços prestados

Figura 4 - Comparativo entre a composição de SOCs industriais internos (com funcionários da própria empresa) e a subcontratação de um SOC industrial externo

CONSIDERAÇÕES FINAIS

Existem motivos plausíveis para não recomendarmos o uso de SOCs de TI ou Híbridos para proteger redes industriais. O simples motivo de abranger áreas e objetivos divergentes da TO, torna a gestão de segurança por estes SOCs um enorme risco para a segurança das redes industriais.

Como visto, enquanto a segurança de TI está preocupada com a confidencialidade, exigindo procedimentos específicos para isso, a segurança de TO está preocupada, sobretudo, com a disponibilidade dos sistemas industriais.

Cada SOC (TI e TO) deve atuar de maneira independente. Ambos devem trocar informações através de um comitê de segurança cibernética corporativa que garantirá uma rotina segura para a empresa, sobretudo para aquelas infraestruturas críticas cujos serviços são essenciais para a sociedade e cujas vulnerabilidades podem resultar em grandes perdas econômicas e graves danos para o meio ambiente.

Por isso, as metodologias, as tecnologias, os serviços e as formações acadêmicas são significativamente diferentes entre tais profissionais e devem respeitar suas áreas de competência.

Concluindo, a segurança cibernética de redes industriais deve ser feita exclusivamente por centros de operação de segurança de TO e, de preferência, por SOCs especializados e disponíveis a todo momento. Ao ser estabelecido pela alta gestão da empresa, tais profissionais devem garantir que as operações industriais mantenham seu funcionamento correto e continuem beneficiando a sociedade.

BIBLIOGRAFIA

› BRANQUINHO, M.; BRANQUINHO, T. **Industrial Cybersecurity.** Rio de Janeiro: Alta Books, 2021.

› BRANQUINHO, M. et al. **Industrial automation and SCADA Cybersecurity.** Rio de Janeiro: Elsevier, 2014.

› BOUSQUET, Antoine J. **The Scientific Way Warfare: Order and Chaos on the Battlefields of Modernity.** New York: Columbia University Press.

› COBERT, E.; KOTT, A. (Eds.). **Cyber-security of SCADA and Other Industrial Control Systems.** Adelphi: Springer, 2016.

› GODOY, Eduardo P. et al. "Design and implementation of an electronic architecture for an agricultural mobile robot". **Brazilian Journal of Agricultural and Environmental Engineering,** v. 14, n. 11, 2010.

› GROOVER, M. **Automation, production systems, and computer integrated manufacturing.** USA: Prentice Hall.

› HESS, L. G. **Impacts and challenges of industrial automation in small enterprises: the case of the matrix workers of the chicken production chain.** Porto Alegre: Unisinos, 2018 [master's thesis].

› KNAPP, Eric. **Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems.** New York: ELSEVIER, 2011.

› LUCIANO,E. M; TESTA, Mauricio Gregianin: **"Information technology governance controls for outsourcing business processes: a proposal from COBIT".** JISTEM - Journal of Information Systems and Technology Management,v.8, n. 1, 2011.

› MACAULAY, T.; SINGER, B. **Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS.** London/New York: CRC Press, 2011.

› NAKAMURA, E. T.; of GEUS, P. L. **Network security in cooperative environments.** Novatec Publishing House: São Paulo, 2007.

› ROCKENBACH, S. **Architecture, automation, and sustainability.** Porto Alegre: UFRGS, 2004 [master's thesis].

› PESCIO, P. H. **Analysis of the integration of automation technology applied to the paper making process.** São Paulo: USP, 2016 [master's thesis]**.**

› SILVA, E.B. da. **Methodology for planning the convergence of Information Technology (IT) & Automation Technology (TA) in industrial processess.** São Paulo: USP, 2013 [doctoral thesis].

› SOUZA, J. de; WILBORN, F.; KALSHNE, N. **"Use of automation for quality control in the industry".** Espacios, v. 34, n. 10, 2013.

› STALLINGS, William. **Foundations of Modern Networking.** Indianapolis: Pearson, 2016.

› VANALLE, R.M.; SALLES, J.A.A. **"Relationship between automakers and suppliers: theoretical models and case studies in the Brazilian automotive industry".** Management & Production, v. 18, n. 2, 2011.

Paseo de las Delicias, 30 - 2º
28045 Madrid

+34 910 910 751

info@cci-es.org
www.cci-es.org
blog.cci-es.org
@info_cci