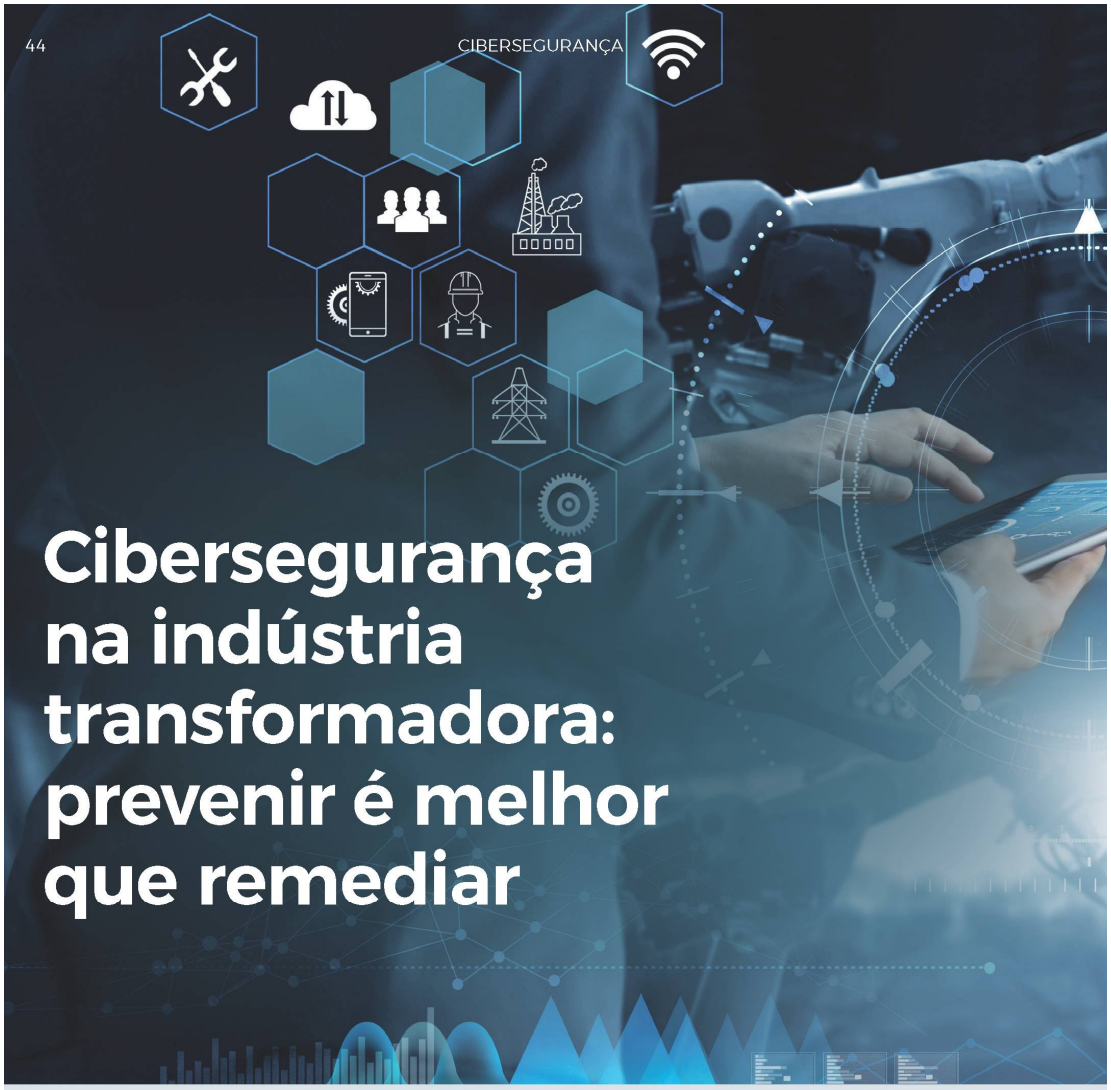

Cibersegurança na indústria transformadora: prevenir é melhor que remediar

Uma infraestrutura industrial que combina dispositivos TO com uma miríade de sensores e dispositivos IIoT é um problema de segurança. As vulnerabilidades e o perímetro de defesa aumentam a uma velocidade constante e as organizações devem criar planos de cibersegurança bem estruturados para mitigar os riscos de intrusão.

Mafalda Simões Monteiro

As Tecnologias Operacionais (TO) já cá andavam muito antes de se falar em Indústria 4.0. Cumpriam a sua função primordial sem perigo. Mas as Tecnologias de Informação (TI) entraram em força nos chãos de fábrica. Sensores e dispositivos IIoT, o 5G, o Edge computing, a cloud, combinados com TO e ainda com recursos a mão-de-obra à distância permitiram aumentar a competitividade, a produtividade e reduzir custos. Esta convergência das TI e das TO está a aumentar a superfície de ataque, as vulnerabilidades e a agravar um ambiente de ameaças já de si complexo, abrindo portas à entrada de um volume maior de malware que

Os sistemas de produção legados, que desempenhavam as suas funções primordiais na perfeição, mas sem ter em conta a cibersegurança, tornaram-se num problema na era da Indústria 4.0. Uma infraestrutura que integra TO num ambiente repleto de sensores e dispositivos IIoT tem vulnerabilidades que devem ser mitigadas.

pode provocar prejuízos elevados ou até mesmo obrigar à paragem da produção.

Para o evitar, "as soluções de cibersegurança têm de ser robustas para responder aos desafios do segmento de IIoT", defende Gabriel Coimbra, group vice president e country manager da IDC.

No entanto, muitos dos dispositivos legados "estão congelados no tempo, executando sistemas operativos antigos, não podendo receber patches ou atualizações. Outros são incapazes de executar software de segurança e até há equipamentos soldados para evitar que alguém lhes faça alterações", diz John Shier, senior security advisor da Sophos.

Além disso, as empresas têm de estar em conformidade com o Regulamento Geral de Proteção de Dados (RGPD) e devem começar a "adaptar as suas metodologias, políticas e sistemas de gestão interna e externa de ciber-risco para estar em linha com as obrigações da Diretiva NIS2 [Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho]", em vigor desde janeiro, e que deverá ser transposta para o ordenamento jurídico nacional nos próximos 21 meses, alerta a advogada Inês Antas de Barros, sócia da Vieira de Almeida. As normas serão apertadas e haverá multas por incumprimento.

COMO DEFENDER-SE DAS CIBERAMEAÇAS

O combate às ciberameaças neste ambiente com várias camadas de tec-

nologias distintas integradas num só sistema tem de começar tão cedo quando possível, independentemente de a empresa já ter sido atacada ou não. É apenas uma questão de tempo até ser vítima.

A posição privilegiada da indústria transformadora na cadeia de abastecimento, acompanhada de infraestruturas desatualizada e sem segurança, é motivo de atenção dos cibercriminosos que aproveitam as falhas para entrar nos sistemas. Gabriel Coimbra explica que é importante interiorizar que os riscos de cibersegurança se encontram em qualquer etapa da jornada da IIoT e que os criminosos aproveitam a menor vulnerabilidade.

"A segurança em IoT deve estender-se além do perímetro tradicional da empresa", explica o analista. "Deve existir uma plataforma integrada e automatizada para melhorar a eficiência operacional, reduzir os custos e maximizar a segurança", acrescenta. É necessária a atualização da segurança da rede, a encriptação, a criação de uma camada adicional de monitorização da rede e o aumento o controlo de acesso especificamente para novos dispositivos IIoT.

Para o ajudar a fazer estes planos, o Centro Nacional de Cibersegurança (CNCS) concebeu e mantém atualizado o Quadro de Referência Nacional de Segurança Cibernética (EC QNRCS). Este quadro permite às organizações implementar corretamente as suas práticas de cibersegurança organizacional, processual, tecnológica e humana. Através desta análise de risco é possível "identificar o que tem de se proteger, quais os processos associados, quais as tecnologias que suportam os processos, fazendo-se em seguida o plano de mitigação", descreve António Gameiro Marques, diretor geral do Gabinete Nacional de Segurança Portugal (GNS) e do CNCS.

Esteja ainda atento aos desafios jurídicos e operacionais. É exigida "uma abordagem holística das várias vertentes", assinala Inês Antas de Barros. A dimensão jurídica é incontornável nas perspetivas preventiva e de resposta a incidentes, detalha a advogada da Vieira de Almeida.

Lembre-se ainda daquele que é normalmente referido como o elo mais fraco da cibersegurança: as pessoas. É fundamental envolver os colaboradores no plano de mitigação de risco, com planos de formação focados nas atitudes, nos comportamentos, na sensibilização e educação. O fator humano será a ignição de mais de metade dos incidentes de cibersegurança significativos em 2025. E nem sempre inadvertidamente. "Cerca de 74 % dos empregados dizem que estariam dispostos a ignorar regras de cibersegurança se tal os ajudasse ou à sua equipa a atingir um objetivo de negócio", revela um estudo de 2022, do Gartner.

Acompanhe também o desenvolvimento do Cibersecutiry Act da UE que irá certificar processos de cibersegurança, procure selos de maturidade digital e lembre-se que pode complementar o seu plano de mitigação de riscos com seguros de cibersegurança, partilhando o risco com as seguradoras.

O QUE FAZER EM CASO DE INCIDENTE OU INCUMPRIMENTO

No caso de ser vítima de ataque, por exemplo por ransomware, ponha em marcha o plano de recuperação de desastres e continuidade de negócio e decida se paga ou não o resgate.

A transparência é fundamental. Deve manter os seus colaboradores, fornecedores, clientes e outros parceiros informados como fez a Vodafone Portugal no ano passado, ou o fabricante de alumínio Norsk Hydro, em 2019. Caso contrário poderá ter, além dos prejuízos do ataque, problemas de reputação.

Gameiro Marques recomenda ainda a participação dos incidentes à Polícia Judiciária. Essa informação poderá contribuir para investigações em curso e para o desmantelamento de organizações criminosas. Além disso, as empresas devem partilhar entre elas a informação dos ataques e das soluções encontradas. Muitas vezes, a solução de uma empresa pode ajudar outra a libertar-se dos efeitos do ataque. Com esta cooperação proactiva, as

Tal com os pombos voltam às esplanadas para comer o pão oferecido pelos clientes, também os criminosos voltam a atacar se receberem o resgate. Ao pagar não resolve o problema e está a financiar o crime.

empresas "estão a proteger a comunidade e a si próprias", conclui Gameiro Marques.

É caso para dizer que o segredo nem sempre é a alma do negócio.

Para cumprir o RGPD, a indústria transformadora já tem de levar a cabo uma avaliação do risco de segurança e pode ser multada se não tiver um plano de ação atualizado para o caso de um incidente grave. Com a Diretiva NIS2, as obrigações vão aumentar.

RANSOMWARE: DESACONSELHÁVEL PAGAR RESGATE

Um ataque de ransomware tem como principal objetivo encriptar dados valiosos para uma empresa para, em seguida, ser feito um pedido de resgate (ransom em inglês).

A indústria transformadora é aquela que paga resgates de ransomware mais elevados, esta é a principal conclusão de um estudo Sophos. O custo médio de pagamento de resgates ascende a mais de 2 milhões de euros, mais do dobro da média global (cerca de 812 mil euros).

De acordo com a S21Sec, este ano, "os ataques de ransomware vão continuar a aumentar em número e complexidade", predominando o modelo de negócio de ransomware as a service, através do qual um grupo de cibercriminosos disponibiliza o seu programa, bem como a sua infraestrutura de suporte, para utilização por outros grupos afiliados/comissionistas explica José Luis Silva, head of integration da S21sec.

A indústria transformadora paga muito pelos resgates, mas, apenas 33 % das organizações faz essa opção, ainda segundo a Sophos. E tal é um bom sinal, pois a generalidade dos especialistas desaconselha o pagamento do ransomware, embora refiram que o pagamento é uma decisão de gestão de risco para a organização.

António Gameiro Marques (CNCS) defende que não se deve pagar, para evitar voltar a ser atacado.

José Luis Silva, vai mais longe, alertando que o pagamento, "além de não resolver o problema, é um financiamento para o negócio dos cibercriminosos".

No entanto, John Shier considera que "pagar um resgate é uma escolha bastante individual, envolvendo muitos fatores. Algumas empresas optam por pagar por necessidade (porque não tinham backups dos dados roubados), enquanto outras pagam para tentar manter o incidente em segredo", conclui. ■