visionware

“CIBERSEGURANÇA, UM PROCESSO DE MELHORIA CONTÍNUA”

A CIBERSEGURANÇA DEIXOU DE SER UMA OPÇÃO PARA PASSAR A SER UMA NECESSIDADE VITAL PARA A SOBREVIVÊNCIA E PROSPERIDADE DAS ORGANIZAÇÕES E INDIVÍDUOS NESTA ERA DIGITAL. OS PROFISSIONAIS DE CIBERSEGURANÇA TÊM O IMPORTANTE (E INSUBSTITUÍVEL) PAPEL DE FORTALECER A SEGURANÇA DOS CLIENTES E, POR CONSEQUÊNCIA, MANTER A INTEGRIDADE E CONFIANÇA NO SETOR.

Para proteger os clientes é necessário prevenir e analisar quais são os riscos, aferir quais os ativos críticos e compreender o que os cibercriminosos poderão tender a explorar. A ideia de um *hacker* jovem e inexperiente que trabalha sozinho é falaciosa; a realidade atual é que as organizações lidam com grupos cibercriminosos, organizados, experientes e implacáveis, com estratégias, recursos e tempo investido. Isto significa que é crucial garantir que a infraestrutura de segurança é robusta e também ágil o suficiente para combater as ameaças em constante evolução. A tecnologia avançada é assim um fator importante para que uma organização consiga proteger o seu negócio, colaboradores e clientes, contudo, a tecnologia por si só, não é, nem nunca será suficiente. As organizações terão de procurar estabelecer um modelo de governação de segurança que enquadre este tema diretamente numa ótica de gestão de risco diretamente com a camada de gestão. A segurança terá de ser vista de forma holística. Nesta linha de pensamento apontaria para a implementação de um Security Operations Center (SOC) como umas das soluções mais abrangentes, e que realmente faz toda a diferença em termos de deteção e resposta contra ciberataques.

BRUNO CASTRO, FUNDADOR & CEO DA VISIONWARE. ESPECIALISTA EM CIBERSEGURANÇA E ANÁLISE FORENSE

Para garantir a proteção dos clientes é também essencial, olhar para dentro e prevenir as ameaças internas. Para protegermos os nossos clientes é crítico antes de mais protegermo-nos também - ser o modelo e/ou o espelho da cibersegurança. É importante proteger computadores e dispositivos utilizados pelos vários colaboradores, incluído o *top management*. Todos estão sujeitos a tentativas de *phishing*, fraudes e exploração de vulnerabilidades. Incentivar a formação e o treino contínuos sobre as ciberameaças e as melhores práticas de segurança é fundamental. Os colaboradores e clientes devem estar cientes dos riscos e é importante que todos sejam capazes de identificar ameaças quando as veem. Também aplicar o princípio do menor privilégio, isto é, limitar o acesso de cada colaborador às informações necessárias para o seu trabalho. E claro, pode parecer cliché, mas a verdade é que as *passwords* são as primeiras linhas de defesa contra ataques e é importante que sejam complexas, secretas, exclusivas, e ainda, que incluam o uso de autenticação de dois fatores (2FA) como uma camada adicional de proteção.

A implementação regular de *backups* e a criação de planos de recuperação de desastres é também um fator crucial, na medida em que, garante que, em caso de comprometimento, os dados podem ser restaurados e assim minimizar os impactos operacionais. A deteção precoce é essencial na cibersegurança. Estabelecer sistemas de monitorização ativa de redes pode ajudar a identificar comportamentos suspeitos e possíveis ameaças antes que causem danos significativos. Realizar auditorias de segurança regularmente é também uma parte vital para identificar possíveis lacunas no sistema. Estas avaliações proporcionam *insights* críticos sobre áreas que necessitam de melhorias e garantem que as defesas permaneçam eficazes ao longo do tempo.

Tendo em consideração a volatilidade deste novo mundo cibernético, incluiria a implementação de um modelo de resposta a incidente e desastre. É fundamental que as organizações se testem a si próprias, nomeadamente, na sua capacidade de resposta a um ciberataque com sucesso. Não pode estar a criar modelos de resposta e procedimentos de reação no decorrer do ciberataque. O modelo de resposta tem de estar definido e minimamente testado.

A cibersegurança é uma batalha constante e em constante evolução. Colaborar com outros líderes do setor, partilhar informações sobre ameaças e estabelecer parcerias estratégicas fortalece a capacidade de resposta coletiva contra ciberataques e por acréscimo, torna o setor mais preparado para proteger os clientes.

Em última análise, a cibersegurança é um processo e um compromisso de melhoria contínua. Como líderes no setor, devemos assumir a responsabilidade de proteger os nossos próprios sistemas e, por conseguinte, os dos nossos clientes. Estas são apenas algumas das principais lições e orientações a adotar numa abordagem proativa em relação à cibersegurança, para que consigamos enfrentar os desafios contemporâneos e edificar um ambiente digital mais seguro e fiável. ◀