DEVOTEAM CYBER TRUST DESTACA ESTRATÉGIA PEOPLE-FIRST SIMPLIFICANDO A LINGUAGEM EM CIBERSEGURANÇA

Níveis de alerta e processos claros de cada fase ajudam na resposta global nas organizações em defesa da cibersegurança

Lisboa, 23 de abril de 2024

Os desafios da cibersegurança: o fator humano

O panorama atual da cibersegurança é marcado por um conjunto cada vez mais complexo de ameaças, exigindo mais do que apenas defesas tecnológicas. Um fator crucial, mas frequentemente ignorado neste domínio, é o elemento humano, responsável por mais de 80% das violações da cibersegurança. Esta estatística realça uma vulnerabilidade significativa - a falha na sensibilização e no comportamento humano em matéria de cibersegurança.

Sendo a complexidade da cibersegurança uma barreira à sua compreensão torna-se evidente a necessidade de simplificação da sua linguagem através de soluções que ajudem as pessoas a entender e a orientarem-se melhor em como o que devem fazer para agir, dependendo da situação de alerta.

A Devoteam Cyber Trust reconhece que a tradicional concentração em soluções centradas na tecnologia e em programas periódicos de sensibilização está a revelar-se insuficiente. O que é necessário agora é uma mudança fundamental na abordagem - avançar para uma estratégia "People-First", de modo a realçar o papel do comportamento humano e da tomada de decisões como sendo fundamentais para reforçar as defesas da cibersegurança. Neste sentido, destacam-se os principais desafios humanos no ecossistema de cibersegurança:

1. **A barreira da mentalidade duradoura:** após uma formação periódica, os utilizadores têm uma tendência para voltar aos seus comportamentos originais. O impacto transitório das sessões de formação não consegue incutir uma consciencialização a longo prazo, levando a um lapso na vigilância e a um regresso a práticas menos seguras.

2. **O desafio da extensão:** embora os utilizadores sejam cruciais na identificação e comunicação de potenciais ameaças, manter este nível de envolvimento de forma consistente é um desafio. Existe uma falha entre a sensibilização esporádica e a participação ativa e contínua nos esforços de cibersegurança.
3. **Segurança como uma reflexão tardia:** a cibersegurança é vista como uma reflexão tardia e não como um aspeto integrante das operações diárias. Assim, os utilizadores podem dar prioridade à conveniência ou eficiência em detrimento dos protocolos de segurança, aumentando inadvertidamente a vulnerabilidade às ameaças cibernéticas.
4. **Ultrapassar a condescendência:** a benevolência em matéria de cibersegurança representa um risco substancial. Os utilizadores, uma vez familiarizados com determinados procedimentos ou protocolos, podem tornar-se menos vigilantes, subestimando a natureza evolutiva das ameaças cibernéticas.
5. **Criar uma cultura de segurança sustentada:** o desafio final reside na transformação da cultura organizacional para dar prioridade à cibersegurança de forma consistente. Ou seja, criar um ambiente em que a cibersegurança não seja apenas uma responsabilidade do departamento de TI, mas um aspeto fundamental na função de cada colaborador.

Perante os desafios anteriormente apresentados, tornou-se essencial encontrar uma solução com uma abordagem simples e acessível a todos os colaboradores das organizações. Em novembro de 2023, foi lançada a mais recente inovadora Alert Readiness Framework (ARF), desenvolvida pela Devoteam Cyber Trust, uma ferramenta vital para melhorar a ciber resiliência organizacional. **A Alert Readiness Framework é um mecanismo simples, no qual as organizações definem os seus próprios níveis de alerta adquiridos através de fontes de informação relevantes e qualificam cada uma delas atribuindo-lhes um peso e, assim, as organizações conseguem calcular o seu nível de alerta atual.**

A metodologia da ARF é revolucionária, uma vez que permite que as organizações passem de uma postura reativa de cibersegurança para uma postura proativa. Para tal, monitoriza o panorama cibernético, ajusta os níveis de alerta conforme necessário e garante a adoção de medidas adequadas e específicas para diferentes contextos, permitindo que as organizações se mantenham à frente de potenciais ameaças num estado de prontidão adequado e respondam eficazmente aos desafios cibernéticos em evolução. Neste sentido, a ARF apresenta vários benefícios estratégicos, de modo que todos tenham um papel e uma participação mais ativa no que diz respeito à cibersegurança dentro das organizações.

Rui Shantilal, Managing Partner da Devoteam Cyber Trust, afirma: "*A adoção da ARF significa uma mudança crítica para uma abordagem mais resiliente e centrada nas pessoas na área de cibersegurança. Esta framework não só aborda os desafios urgentes no panorama da cibersegurança, como também anuncia uma nova era em que as estratégias centradas no ser humano estão na vanguarda da proteção dos ativos digitais.*"

O Managing Partner da Devoteam Cyber Trust acrescenta, ainda, que "*Reconhecer e abordar o fator humano não é apenas divulgar informações; trata-se de promover uma cultura em que a cibersegurança é compreendida, valorizada e praticada por todos numa organização. Uma das principais vantagens da ARF é ser uma forma simples e efetiva.*"

A Devoteam Cyber Trust, uma empresa de consultoria de excelência com presença em 18 países da região EMEA, está excecionalmente posicionada para facilitar a implementação da Alert Readiness Framework. As organizações podem navegar com confiança nas complexidades da implementação da ARF, aproveitando os vastos recursos, a experiência e abordagem personalizada para melhorar a sua postura de segurança e resiliência cibernéticas.

Para aceder ao white paper com a informação completa sobre a Alert Readiness Framework, carregue **aqui**.

###

Sobre a Devoteam Cyber Trust

A Devoteam Cyber Trust é a unidade especializada em cibersegurança do Grupo Devoteam. Com mais de 800 especialistas localizados na região EMEA, o nosso objetivo é estabelecer a cibersegurança como um facilitador do sucesso dos negócios, em vez de um obstáculo. Utilizamos uma abordagem abrangente de Resiliência Cibernética, Segurança Aplicada e Gestão de Serviços de Segurança para proteger a jornada tecnológica de empresas de grande e média dimensão de todos os setores e indústrias. Desde 2009, anteriormente com a denominação INTEGRITY, a nossa equipa sediada em Portugal é especializada em fornecer Serviços Geridos de Segurança de ponta, que combina a sua expertise e tecnologia proprietária para reduzir de forma consistente e eficaz o risco cibernético dos nossos clientes. A ampla gama de serviços abrange Testes Persistentes de Intrusão, ISO 27001, PCI-DSS, Consultoria e Soluções de GRC e Gestão de Riscos de Terceiras Partes. Certificados em ISO 27001 (Segurança da Informação), ISO 27701 (Gestão de Informação Privada) e ISO 9001 (Qualidade), PCI-QSA e membros da CREST e CIS - Centro de Segurança na Internet, prestamos serviços a um número considerável de clientes, operando em mais de 20 países.

devoteam
Cyber Trust

Contacts
BE Ideas | Boutique PR Agency
Sofia Alcobia
sofia.alcobia@beideas.pt
T: + 351 962 615 717