HACK3R_
RANGER5

DESTAQUES DO SANS SECURITY AWARENESS REPORT 2022

Pergunte para qualquer profissional da área de segurança da informação e ele lhe confirmará que a System Administration, Networking and Security (SANS) é um dos institutos mais respeitados desse segmento. Com mais de 30 anos de existência, a SANS nasceu como uma cooperativa para fornecer programas de treinamento para especialistas do setor. Ao longo do tempo, se transformou em uma referência na área de cibersegurança, sobretudo por conta de seus cursos preparatórios, estudos, eventos e certificações na área de conscientização.

Como é de praxe, a organização publicou recentemente a mais nova edição de seu estudo anual sobre o assunto: o SANS Security Awareness Report 2022, fruto de uma longa pesquisa com mais de mil profissionais de conscientização ao redor do globo. O documento nos traz um panorama sobre os principais desafios, necessidades e o portunidades na área de segurança cibernética, tornando-se um guia essencial para aprimorar os programas de conscientização.

Como era de se esperar, os efeitos da pandemia do coronavírus (SARS-CoV2) na transformação digital continuam sendo alguns dos maiores desafios quando o assunto é condicionamento cultural dos colaboradores. O ambiente de trabalho híbrido e as distrações que os membros da equipe possuem em suas residências foram alguns dos entraves citados pelos profissionais entrevistados.

“As pessoas se tornaram o principal vetor de ataque para ciberataques em todo o mundo. Os seres humanos, em vez da tecnologia, representam o maior risco para as organizações, e os profissionais que supervisionam os programas de conscientização de segurança são a chave para gerenciar esse risco com eficiência”, explica Lance Spitzner, diretor do SANS Security Awareness e coautor do relatório.

HACK3R_
RANGERS

Nível de Maturidade

O Modelo SANS de Maturidade de Conscientização em Segurança nasceu em 2011 e se tornou rapidamente uma referência global para mensurar o nível de maturidade de um programa de conscientização em segurança da informação, determinando seu nível de complexidade dentro de uma escala de cinco estágios crescentes.

Globalmente falando, neste ano, houve um aumento de 8% na quantidade de programas no nível “Foco em Compliance”, o segundo na escala de maturidade da SANS. Nessa categoria, estão incluídos os programas que existem simplesmente para cumprir com o mínimo requisitado por normas regulatórias, o que os torna bastante deficientes, já que contam apenas com ações pontuais de educação.

Ao mesmo tempo, houve um declínio de 10% no número de programas na categoria “Promoção de Consciência e Mudança de Hábitos”, correspondente ao terceiro nível de maturidade, o mínimo aceitável dentro de uma corporação de acordo com os critérios da SANS.

Felizmente, apesar da queda, esse continua sendo o nível de maturidade mais comum, representando a maior parte das empresas entrevistadas na análise global. As únicas regiões nas quais os programas com “Foco em Compliance” ainda dominam são a Ásia (cerca de 43%) e, infelizmente, a América do Sul (cerca de 47%).

HACK3R_
RANGER5

As maiores preocupações

Quando o assunto são as principais preocupações dos profissionais de conscientização, não há grandes surpresas: o phishing permanece no topo do ranking das ameaças cibernéticas, com todas as suas variantes e vetores de disseminação (e-mail, SMS, ligações, entre outros).

Em segundo lugar, temos as campanhas de Business Email Compromise (BEC), também conhecidas por alguns como "fraude do CEO". Nesse tipo de golpe, o cibercriminoso personifica executivos de alto escalão da companhia para tentar se comunicar com outros colaboradores e obter ganhos ilícitos ao incentivar transações fraudulentas.

Por fim, a medalha de bronze fica para uma das ameaças mais temidas pelas empresas ao redor do globo: os ransomwares. A maior parte dos incidentes relacionados com o sequestro de dados se inicia com hábitos ineficientes de higiene cibernética, incluindo um colaborador que acaba caindo em um phishing ou que possui sua conta comprometida por usar uma senha fraca demais (seja por sua simplicidade, por ser a mesma usada em outros serviços ou por não estar acompanhada de um segundo fator de autenticação).

HACK3R_
RANGER5

Desafios enfrentados

Como já imaginávamos, o nível de maturidade de um programa de conscientização está ligado, de forma íntima, ao número de colaboradores dedicados integralmente às ações educacionais. As campanhas que atingem a mais alta categoria de maturidade, "Métricas Robustas", contam com pelo menos 3,5 full-time employees (FTE) trabalhando com foco total na campanha de conscientização. Ainda é raro, porém, encontrar corporações que disponham de recursos humanos exclusivamente para essa finalidade.

Questionados sobre os principais desafios de manter um programa de educação eficaz, as três respostas mais populares estavam relacionadas à falta de tempo e de equipe: "Falta de tempo para gerenciamento de projetos", "Limites no tempo de treinamento para engajar colaboradores" e "Falta de equipe".

"Esses desafios foram e ainda são agravados pela COVID-19. Perguntamos aos entrevistados como a pandemia os impactou. Suas duas principais respostas foram de que ela não só criou um ambiente muito mais distraído e uma força de trabalho sobrecarregada, mas também gerou um cenário no qual os ataques cibernéticos baseados no fator humano tornaram-se mais frequentes e eficazes", explica a SANS.

HACK3R_
RANGER5

O que é preciso para ter sucesso?

O SANS Security Awareness Report 2022 elenca três requisitos básicos para que um programa de conscientização seja eficiente e cresça de forma gradual na escala de maturidade:

- Suporte da Liderança: os programas mais maduros são aqueles nos quais a alta diretoria da empresa oferece suporte aos profissionais de conscientização. Trata-se de uma constatação que permanece inalterada nas últimas três edições do relatório. É crucial engajar as diretorias, explicando de forma didática as prioridades estratégicas de um programa de conscientização e fazendo um alerta para os impactos que um baixo nível de maturidade pode causar.
- Tamanho da Equipe: gerenciar o risco humano não é uma questão tecnológica, é uma questão humana. Logo, não é surpresa alguma que os programas bem-sucedidos possuem equipes mais robustas e focadas exclusivamente nesse setor. Infelizmente, ainda é comum encontrar corporações que não enxergam a necessidade de ter um Security Awareness Officer (SAO) na equipe, valendo-se de profissionais técnicos para cuidar dos programas de conscientização.
- Frequência: novamente, como poderíamos imaginar, os melhores programas são aqueles com um nível consistente na frequência de ações educacionais. Eis a importância de manter uma comunicação clara com o board de diretores a respeito das métricas e indicadores de performance, de modo a auxiliar os executivos de alto escalão a entender e enxergar o valor desse investimento.

HACK3R_
RANGER5

Discrepâncias salariais

Por fim, uma constatação interessante do relatório é que, embora o nível médio de compensação salarial do profissional de conscientização tenha sido de US$ 110.309 anuais (um aumento com relação ao ano superior), aqueles que trabalham exclusivamente com programas de educação recebem, em média, US$ 86.626 — US$ 30 mil a menos do que os profissionais que dividem seu tempo entre manter os programas rodando e realizar outras tarefas. Estes recebem anualmente, em média, US$ 117.584.

“Acreditamos que a resposta é o valor percebido. Os dados sugerem que aqueles que trabalham em meio-período, muitas vezes, já fazem parte da equipe de segurança ou da TI, e a conscientização em segurança é simplesmente mais uma de suas outras responsabilidades. Seu salário mais alto pode ser um reflexo do fato de que eles são compensados por outras habilidades técnicas de segurança”, propõe a SANS.

“Aqueles que se dedicam em tempo integral à conscientização muitas vezes têm formação não técnica, como comunicação, e são remunerados especificamente pelo seu papel de sensibilização para a segurança, que muitas vezes não é tão valorizado quanto a maioria das outras funções dessa área”, complementa.

Conclusões

No geral, o relatório da SANS ressalta a importância de envolver as lideranças para demonstrar a criticidade de gerenciar o fator humano perante o aumento no número de ameaças cibernéticas. É fundamental receber suporte de outros departamentos e alterar a percepção geral das empresas sobre o papel da conscientização em segurança da informação.

“Os programas de conscientização de segurança mais maduros não apenas mudam o comportamento e a cultura de sua força de trabalho, mas também medem e demonstram seu valor para a liderança por meio de uma estrutura de métricas”, aponta Spitzner.

“As organizações não podem mais justificar um treinamento anual para preencher a lacuna de conformidade. Continua sendo fundamental que as empresas dediquem equipes, recursos e ferramentas suficientes para gerenciar o risco humano de forma eficaz”, conclui o especialista.

TESTE A NOSSA PLATAFORMA
GRATUITAMENTE DURANTE 15 DIAS!

HACKERRANGERS.COM.BR

HACK3R_
RANGERS

Bibliografia
SANS 2022 Security Awareness Report (SANS, junho de 2022)