SANS SECURITY AWARENESS

Guia de Implementação de Segurança – Trabalhando em Casa com Segurança

Sumário executivo

Em decorrência do coronavírus, muitas empresas estão orientando seus funcionários a trabalhar de casa. Isso pode ser um desafio, pois grande parte delas não têm as políticas, a tecnologia e o treinamento necessários para garantir a segurança de uma força de trabalho remota. Além disso, muitos funcionários nunca tiveram a experiência de trabalhar de casa, ou podem se sentir desconfortáveis com a ideia. O objetivo deste guia é permitir que você treine essas pessoas rapidamente para que elas estejam o mais seguras possível. Caso tenha alguma dúvida sobre como usar este guia, entre em contato através do e-mail support@sans.org.

Como seus funcionários provavelmente já estão passando por um momento de estresse e de mudança, e sua empresa não possui tempo nem recursos ilimitados, este guia estratégico procura tornar o treinamento o mais simples possível. Recomendamos que você se concentre apenas nos riscos mais importantes e que terão maior impacto, os quais descrevemos abaixo. Pense neles como um ponto de partida. Você também pode adicionar outros riscos ou questões, caso queira. Mas lembre-se: quanto mais você exigir dos seus funcionários em termos de práticas, procedimentos ou tecnologias, menor a probabilidade de que eles consigam implementar tudo.

Como usar este guia

Recomendamos que você comece lendo o material neste guia e conferindo os links para os diversos materiais fornecidos, para ter uma ideia do que está disponível. Você verá que, para cada risco apresentado, nós temos uma variedade de materiais que podem ser usados para engajar e treinar sua organização. Assim, você poderá selecionar as modalidades que serão mais eficientes para as necessidades e a cultura da sua empresa. Terminando de ler este documento, leia também o Modelo de Comunicação e a Ficha Informativa que vieram junto neste kit para entender melhor os objetivos que você deseja atingir. Depois de ler a documentação, você precisará se coordenar com dois importantes grupos.

1. **Equipe de Segurança**: Colabore com sua equipe de segurança para compreender melhor quais são os riscos principais que vocês precisam administrar. Nós identificamos neste guia os riscos que acreditamos ser os maiores e mais comuns para funcionários trabalhando de casa, porém os riscos podem ser diferentes no seu caso. Um conselho: um erro comum por parte de equipes de segurança é tentar gerir todos os riscos e acabar sobrecarregando os funcionários com inúmeras políticas e exigências. Tente limitar os riscos que serão abordados ao menor número possível. Depois de identificar e definir os riscos prioritários, confirme as práticas para minimizar esses riscos. Como já mencionamos, se a sua empresa não possui tempo nem recursos para isso, coloque em

prática as orientações abaixo.

2. **Comunicação**: Depois de identificar os principais riscos humanos e as práticas fundamentais para minimizar esses riscos, colabore com sua equipe de comunicação para engajar e treinar seus funcionários quanto a essas práticas. Os programas de conscientização de segurança mais eficazes envolvem uma parceria forte com a equipe de comunicação. Se possível, tente incorporar alguém da comunicação à sua equipe de segurança. Ao se comunicar com seus funcionários, um estímulo eficiente para engajá-los é enfatizar que o treinamento não só vai protegê-los no trabalho, como também os ajudará a criar um lar ciberneticamente seguro, protegendo também sua família.

Em essência, ao trabalhar em conjunto com esses dois grupos, você tentará tornar a segurança o mais simples possível para seus funcionários, além de motivá-los, os dois elementos fundamentais para uma mudança de comportamento. Sugerimos até que você crie um Conselho Consultivo de pessoas importantes cujas opiniões são necessárias para a implementação do programa. Além das equipes de segurança e de comunicação, você também pode formar parcerias e se coordenar com outros setores, como o jurídico e os recursos humanos.

Pacote de download digital MGT433

O SANS Institute oferece o curso de treinamento de dois dias MGT433: Como criar, manter e mensurar um programa de conscientização de segurança de grande impacto. Esse curso intensivo fornece toda a teoria, as técnicas, a estrutura e os recursos necessários para criar um programa de conscientização de grande impacto, para que você possa gerenciar e mensurar com eficiência os riscos humanos. Como parte deste guia, estamos oferecendo acesso gratuito ao pacote de download digital do curso, com modelos e recursos de planejamento. Embora isso provavelmente vá muito além das necessidades desta iniciativa, esse material pode ser valioso para organizações maiores ou implementações mais complexas.

Respondendo a dúvidas dos funcionários

Além de se comunicar com seus funcionários e treiná-los, recomendamos fortemente que você faça uso de algum tipo de tecnologia ou fórum no qual possa responder às dúvidas das pessoas, de preferência em tempo real. Isso pode incluir um e-mail alternativo dedicado, canal no Skype ou Slack, ou algum tipo de fórum online, como o Yammer. Outra ideia é realizar uma transmissão online sobre segurança, podendo repeti-la várias vezes durante a semana. Assim, as pessoas podem escolher um horário mais adequado para elas, comparecer ao evento ao vivo, e talvez até fazer perguntas. O objetivo é tornar a segurança o mais acessível possível e ajudar as pessoas a esclarecer suas dúvidas. Essa é uma chance fantástica de engajar seus funcionários e tornar o tema da segurança mais abordável.

Aproveite essa oportunidade. Tenha em mente que, para isso ser eficaz, é necessário ter um gerente dedicado a moderar todos os canais de segurança e responder ativamente às perguntas.

Riscos e materiais de treinamento

Já identificamos os três riscos principais que você deve gerenciar para sua força de trabalho remota. Eles representam um ponto de partida, e provavelmente serão os mais importantes para você. Cada risco abaixo inclui links para diversos recursos que ajudarão na comunicação e no treinamento sobre o assunto. Nós fornecemos vários materiais de comunicação. Dessa forma, você pode selecionar aqueles que terão maior impacto na cultura da sua empresa. Além disso, quase todos os materiais vêm em vários idiomas. Se tudo isso for excessivo e seu tempo for extremamente limitado, recomendamos que você implemente os dois materiais listados abaixo, simplesmente.

1. Ficha informativa "Trabalhando em casa com segurança" (incluída no seu Kit de Implementação).
2. Vídeo "Criando um Lar Ciberneticamente Seguro" (inglês) também disponível em outros idiomas aqui

Engenharia Social

Um dos maiores riscos que os funcionários remotos terão de enfrentar, especialmente neste momento de mudanças dramáticas e ambiente de urgência, são os ataques de engenharia social. Engenharia social é um ataque psicológico no qual os atacantes enganam suas vítimas, induzindo-as a cometer um erro, o que será ainda mais fácil durante essa época de mudanças e confusão. A chave é treinar as pessoas para reconhecer o que é engenharia social, como detectar os indicadores mais comuns de um ataque, e como proceder, caso identifiquem um ataque. Não foque apenas em ataques de phishing por e-mail, mas também em outros métodos, como por telefonema, mensagem de texto, redes sociais ou fake news. Você encontrará os materiais necessários para treinar e reforçar esse assunto em nossa pasta Material de apoio sobre Engenharia Social. Além disso, aqui estão dois vídeos de Conscientização de Segurança do SANS para incluir como link, oferecidos em vários idiomas.

- Engenharia Social (inglês) também disponível em outros idiomas aqui
- Phishing (inglês) também disponível em outros idiomas aqui

Senhas fortes

Como mostra o Relatório de Investigação de Violação de Dados anual da Verizon, senhas fracas continuam sendo uma das causas principais de violações em escala global. Existem quatro práticas fundamentais para ajudar a gerenciar esse risco, listadas abaixo. Você encontrará os materiais necessários para treinar e reforçar essas quatro práticas fundamentais na nossa pasta Senhas.

- Frases secretas (observe que senhas complexas e senhas com expiração são ideias ultrapassadas).
- Senhas únicas para todas as contas
- Gerenciadores de Senhas
- Autenticação multifator. Também chamada de autenticação de fator duplo ou verificação em duas etapas

Sistemas atualizados

O terceiro risco consiste em assegurar que todas as tecnologias utilizadas pelos seus funcionários estejam com a versão mais recente do sistema operacional, das aplicações e aplicativos móveis. Para quem utiliza dispositivos pessoais, pode ser necessário habilitar atualizações automáticas. Você encontrará os materiais necessários para treinar e reforçar esse assunto nas nossas pastas e Malwares ou Criando um Lar Ciberneticamente Seguro.

Questões adicionais a considerar

- **Wi-Fi**: Proteger seu ponto de acesso Wi-Fi. Esse assunto é abordado no material Criando um Lar Ciberneticamente Seguro. Além disso, considere assistir ao vídeo "Criando um Lar Ciberneticamente Seguro" (inglês) também disponível em outros idiomas aqui.

- **VPNs**: O que é VPN e por que você deveria utilizar uma. Recomendamos o OUCH newsletter [boletim OUCH] sobre VPNs.

- **Trabalhando Remotamente**: Isso vale para indivíduos que estejam trabalhando remotamente, porém FORA de casa, como em uma cafeteria, terminal de aeroporto ou hotel. Considere assistir ao nosso vídeo de treinamento "Trabalhando Remotamente" (inglês) também disponível em outros idiomas aqui.

- **Crianças e convidados**: Para reforçar a ideia de que sua família e convidados não devem acessar seus dispositivos de trabalho, considere assistir ao vídeo de treinamento "Trabalhando Remotamente" (inglês) também disponível em outros idiomas aqui.

- **Detecção e resposta**: Você quer que as pessoas comuniquem, caso acreditem que houve um incidente enquanto trabalhavam em casa? Se sim, o que você quer que elas comuniquem, e quando? Esse assunto é abordado em nosso material Invadido.

OUCH newsletters [boletins OUCH]

Além disso, considere usar os OUCH newsletters [boletins OUCH] disponíveis publicamente para complementar seu programa. Todos eles foram traduzidos para mais de vinte idiomas. Abaixo listamos os OUCH newsletters [boletins OUCH] que acreditamos que melhor complementam sua iniciativa "Trabalhando em Casa com Segurança". Você pode encontrar todos os boletins online no OUCH Security Awareness Newsletter Archives [Arquivo dos Boletins de Conscientização de Segurança OUCH].

VISÃO GERAL

Four Steps to Staying Secure [Quatro Etapas Para Estar Protegido]
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

Creating a Cybersecure Home [Criando um Lar Ciberneticamente Seguro]
https://www.sans.org/security-awareness-training/ouch-newsletter/2018/creating-cybersecure-home

ENGENHARIA SOCIAL

Social Engineering [Engenharia Social]
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering

Messaging / Smishing [Mensagens / Smishing]
https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks

Personalized Scams [Golpes Personalizados]
https://www.sans.org/security-awareness-training/resources/personalized-scams

CEO Fraud [Fraude do CEO]
https://www.sans.org/security-awareness-training/resources/ceo-fraudbec

Phone Call Attacks / Scams [Ataques e Golpes por Telefone]
https://www.sans.org/security-awareness-training/resources/phone-call-attacks-scams

Stop That Phish [Pare esse Phishing]
https://www.sans.org/security-awareness-training/resources/stop-phish

Scamming You Through Social Media [Golpes Através das Redes Sociais]
https://www.sans.org/security-awareness-training/resources/scamming-you-through-social-media

SENHAS
Making Passwords Simple [Simplificando as Senhas]
https://www.sans.org/security-awareness-training/resources/making-passwords-simple

Lock Down Your Login (2FA) [Proteja sua Conta]
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/lock-down-your-login

ADICIONAIS
Yes, You Are a Target [Sim, Você é um Alvo]
https://www.sans.org/security-awareness-training/resources/yes-you-are-target

Smart Home Devices [Dispositivos Residenciais Inteligentes]
https://www.sans.org/security-awareness-training/resources/smart-home-devices

Dicas Rápidas

Dicas e truques de fácil digestão que você pode compartilhar.

- As medidas mais eficientes que você pode tomar para proteger sua rede sem fio doméstica são alterar a senha padrão de administrador, habilitar a criptografia WPA2 e usar uma senha forte para a rede sem fio.
- Tenha cuidado com todos os dispositivos conectados à sua rede doméstica, incluindo monitores de bebê, videogames, TVs, eletrodomésticos, e até mesmo seu carro. Certifique-se de que todos esses dispositivos estejam protegidos por uma senha forte e/ou atualizados com a versão mais recente de seu sistema operacional.
- Uma das maneiras mais eficientes de proteger o computador da sua casa é se assegurando que o sistema operacional e os aplicativos estejam atualizados. Habilite atualizações automáticas sempre que possível.
- No fim, sua melhor proteção é o bom senso. Se um e-mail, ligação ou mensagem online parece estranho, suspeito ou bom demais para ser verdade, pode ser um ataque.
- Certifique-se de usar uma senha separada e única para cada uma de suas contas. Não consegue se lembrar de todas as senhas ou frases secretas? Considere usar um gerenciador de senhas para armazenar todas elas em segurança.
- A verificação em duas etapas é uma das melhores medidas que você pode adotar para proteger qualquer conta. Verificação em duas etapas é quando são exigidos tanto uma senha quanto um código enviado para o seu dispositivo móvel ou gerado por ele. Exemplos de serviços que têm como opção a verificação em duas etapas incluem

Gmail, Dropbox e Twitter.

- Phishing é quando um atacante tenta enganar você, induzindo-o a clicar em um link malicioso ou abrir um anexo de um e-mail. Suspeite de qualquer e-mail ou mensagem online que crie um senso de urgência, contenha erros ortográficos ou cumprimente você como "Caro(a) cliente".

Indicadores

Indicadores comportamentais são complicados para essa situação, pois é mais difícil mensurar como as pessoas se comportam dentro de casa. Além disso, alguns comportamentos não são específicos de trabalho (como proteger o dispositivo de Wi-Fi). No entanto, podemos mensurar o engajamento. Descobrimos que assuntos pessoais ou emocionais como esses podem ser muito engajantes, atraindo muito mais interesse do que outros assuntos. Sendo assim, indicadores como esses ainda podem ser valiosos.

- **Interação**: Com que frequência as pessoas fazem perguntas, publicam ideias ou pedem ajuda em algum dos canais ou fóruns de segurança que você hospeda?
- **Simulações**: Conduza algum tipo de simulação de engenharia social, como ataques de phishing, por mensagem de texto ou por telefone.

Para uma lista de indicadores mais abrangente, baixe a Matriz de Indicadores de Conscientização de Segurança interativa do pacote de download digital MGT433.

Licença

Autor do Kit de Implementação

Lance Spitzner tem mais de 20 anos de experiência na área de segurança com pesquisas de ameaças cibernéticas, arquitetura de segurança e conscientização e treinamento. Foi pioneiro nos campos da enganação e da inteligência cibernética, com sua invenção de honeynets e fundação do Honeynet Project. Como instrutor do SANS, ele desenvolveu os cursos MGT433: Conscientização de Segurança e MGT521: Cultura de Segurança. Além disso, Lance já publicou três livros sobre segurança, prestou consultoria em mais de 25 países e ajudou mais 350 organizações a criar programas de cultura e conscientização de segurança para gerenciar riscos humanos. Lance é um palestrante frequente, tuiteiro compulsivo (@lspitzner) e trabalha em diversos projetos de segurança comunitários. Antes de trabalhar com segurança da informação, Spitzner serviu na Força de Ação Rápida do exército americano e obteve seu MBA na Universidade de Illinois.

Sobre o SANS Institute

O SANS Institute foi criado em 1989 como uma organização para cooperação em pesquisa e educação. O SANS é o mais confiável e, de longe, o maior prestador de treinamento e certificação em segurança cibernética para profissionais de governos e instituições comerciais no mundo todo. Os instrutores renomados do SANS dão mais de 60 cursos diferentes em mais de 200 eventos de treinamento de segurança cibernética ao vivo, assim como online. A GIAC, uma afiliada do SANS Institute, valida as qualificações de profissionais por meio de mais de 35 certificações em segurança cibernética, práticas e técnicas. O SANS Technology Institute, uma subsidiária independente acreditada regionalmente, oferece cursos de mestrado em segurança cibernética. O SANS oferece inúmeros recursos gratuitos à comunidade de segurança da informação, incluindo projetos de consenso, relatórios de pesquisa e boletins, além de operar o sistema de alerta precoce da internet, o Internet

Storm Center. No coração do SANS moram os vários profissionais de segurança que representam diversas organizações globais, de corporações a universidades, trabalhando juntos para ajudar toda a comunidade de segurança da informação. (https://www.sans.org)