Seu Service Desk é o novo vetor de ataque - veja como defendê-lo. - Again

Data: 2025-10-02 15:35:27

Autor: Inteligência Against Invaders

O service desk é o novo perímetro

Os invasores não estão arrombando fechaduras – eles estão escolhendo pessoas. A maneira mais rápida dentro de muitas empresas ainda é o service desk. Agentes de ameaças como o Scatter Spider transformaram a engenharia social em uma ciência, e seus agentes de help desk são seu alvo principal.

Um telefonema convincente pode transformar uma redefinição de senha de rotina em acesso total ao domínio.

Os incidentes da MGM Resorts e da Clorox mostraram como uma chamada de engenharia social bem-sucedida pode ser devastadora, com um impacto comercial de nove dígitos e semanas de interrupção.

Isso não é um acaso; é o manual.

O treinamento ajuda, os controles decidem

Sim, o treinamento do agente é importante. Não, isso não vai te salvar sozinho. Os engenheiros sociais são especialistas em explorar humanos úteis sob pressão de tempo.

Scripts, “bom senso” e perguntas de desafio ad-hoc falham quando um invasor está calmo, preparado e persuasivo.

Se sua última linha de defesa é um agente sobrecarregado fazendo um julgamento, você já perdeu.

Ponto-chave: A verificação do usuário deve ser um **Fluxo de trabalho de propriedade da segurança**, não uma conversa de propriedade do agente.

Uma abordagem de fluxo de trabalho para verificação de usuários de help desk

Mudar a verificação da cabeça do agente para um formal **Fluxo de trabalho de segurança de TI** que seja consistente, registrado e aplicado:

- **Controlos obrigatórios:** Agentes **nunca** manipular ou exibir credenciais. O fluxo de trabalho sim.
- **Verificação baseada em função:** Alinhe a profundidade das verificações ao risco da persona (executivos, administradores, finanças, contratados, etc.). Funções de alto risco

exigem provas mais fortes.
- **Flexibilidade baseada em pontos:** A vida real acontece – os telefones morrem, as viagens interrompem o MFA. Use vários tipos de prova com pontuações que somam um limite de aprovação/reprovação.
- **Integração ITSM:** Mantenha o agente em sua ferramenta normal (por exemplo, ServiceNow). Os tickets iniciam o fluxo de verificação automaticamente e retornam o resultado + telemetria de volta ao ticket.
- **Reduza o estresse e o erro do agente:** Um fluxo de trabalho formal remove o fardo de ser um especialista em segurança de seus agentes. Eles não precisam mais fazer julgamentos de alto risco, levando a um tratamento de tíquetes mais rápido, consistente e menos estressante. Isso não é apenas uma segurança melhor; é um serviço melhor.

[VÍDEO/IFRAME REMOVIDO]

Qual é a aparência de “bom” (perfis alinhados ao NIST)

A maioria de nossos clientes começa com três perfis de verificação mapeados para o risco do usuário e fatores disponíveis. Poderia ser assim:

- **Perfil 1 (Usuário Padrão – Baixa Garantia): Para solicitações de rotina, como uma redefinição de senha para um funcionário padrão.**
    - Método: uma notificação por push para o aplicativo autenticador corporativo registrado (Okta Verify, MS Authenticator). Isso é rápido, familiar e aproveita a infraestrutura existente.
- **Perfil 2 (Usuário Privilegiado/Ação Confidencial – Alta Garantia): Para administradores de domínio, controladores financeiros ou qualquer pessoa que solicite uma alteração confidencial.**
    - Método: Requer dois fatores distintos. Por exemplo: Notificação por push do autenticador bem-sucedida
      E
      Um código único enviado para o endereço de e-mail corporativo registrado.
      OU responder a uma pergunta com base em um atributo não público do sistema HRIS (por exemplo, “Qual é o seu número de identificação de funcionário?”).
- **Perfil 3 (Contingência/Falha de MFA – Garantia Flexível): Para quando o usuário perdeu seu dispositivo MFA principal.**
    - Método: O usuário deve atingir 100 pontos em um menu de opções, evitando que sejam totalmente bloqueados.
        - Código único para e-mail pessoal no arquivo: (50 pontos)
        - Código único para o número de telefone pessoal no arquivo: (50 pontos)
        - Verificação do número de série do dispositivo a partir do MDM: (60 pontos)
        - responder a uma pergunta com base em um atributo não público do sistema HRIS (por exemplo, “Qual é o seu número de identificação de funcionário?”). (50 pontos)

Ponta: Se a MFA não estiver disponível universalmente, prefira dados verificados pela empresa (atributos HRIS/IDP, postura do dispositivo, sinais geográficos/comportamentais) em vez de curiosidades pessoais adivinháveis. Mantenha uma lista curta e verificada e retire qualquer pergunta que vaze ou apareça em violações.

[IMAGEM REMOVIDA]

Detecte ataques antecipadamente, documente tudo

Quando a verificação reside dentro do fluxo de trabalho, você obtém resultados de segurança “gratuitamente”. Estes são alguns dos benefícios extras obtidos por nossos clientes:

- **Alerta antecipado:** Picos de falhas nas verificações contra o mesmo usuário ou função são fumaça antes do fogo — SecOps de alerta automático. Aviso automático contra contas suspeitas, mesmo usuário ligando em pouco tempo.
- **Trilha de auditoria:** Cada tentativa, fator, pontuação e resultado é carimbado de volta no ticket.
- **Conformidade:** Os relatórios automatizados demonstram controles consistentes em toda a mesa.

Plano de lançamento que não vai quebrar a mesa

Todas as organizações têm seus próprios princípios de projeto, mas estas são características comuns:

1. **Fatores de estoque + lacunas:** Quais usuários têm MFA? Quais não? Quais dados seguros são adequados para verificações de conhecimento?
2. **Defina 3 perfis:** Mapear para funções de baixo/médio/alto risco; Defina o limite de aprovação como 100.
3. **Integre com ITSM:** Acione o fluxo do seu ticket (por exemplo, ServiceNow) com ID de usuário + categoria; write-back de resultados e telemetria.
4. **Treine para o processo, não para a persuasão:** Os agentes aprendem uma coisa:**Acompanhe o fluxo de trabalho**.
5. **Meça e ajuste:** Acompanhe as taxas de falha, o tempo de resolução, os escalonamentos e as falsas rejeições. Ajuste a pontuação e as perguntas trimestralmente.

Uma nota sobre nossas ferramentas

Gerenciador de verificação de identidade (IVM) FastPass implementa este modelo: verificação obrigatória, baseada em funções e baseada em pontos, totalmente integrada ao ITSM.

Ele centraliza verificações, aplica políticas e retorna resultados + contexto para o tíquete para alertas, auditoria e conformidade.

Se você está enfrentando táticas no estilo Aranha Dispersa, esse é o tipo de proteção que as bloqueia no primeiro salto.

FastPassCorp auxiliou várias grandes organizações na implementação de um fluxo de trabalho seguro para usuários e ganhou uma experiência superior no campo documentada nos guias e vídeos disponíveis.

A conclusão

Você não vence a engenharia social com pôsteres mais bonitos e roteiros mais longos. Você o vence removendo a discrição, levantando provas e instrumentando o fluxo de trabalho que o invasor

está tentando explorar.

Faça isso e a central de atendimento deixa de ser um alvo fácil e começa a agir como um controle adequado.

Preocupado com a Aranha Dispersa?

Se você gostaria de saber como proteger sua central de serviços e agentes contra um Scatter Spider ou outro ataque de engenharia social?

Dê uma olhada em nossos vídeos e guias para implementar um fluxo de trabalho seguro de verificação de usuário **ou** Entre em contato conosco para uma reunião sobre sua situação**.**

Patrocinado e escrito por FastPassCorp*.*