ARTIGO

A IMPORTÂNCIA DOS FATORES HUMANOS PARA A CIBERSEGURANÇA

POR

Cristine Hoepers (CERT.br)

cristine@cert.br

O eixo Fatores Humanos do documento com os referenciais de formação para o curso de Bacharelado em Cibersegurança define que um profissional que vá atuar nessa área deve ter a competência de "*estabelecer um plano de mitigação de ataques de engenharia social e conscientização de usuário visando a proteção de dados pessoais e organizacionais*".

Para realmente entendermos a importância desse eixo e como podemos abordar essa missão de proteger o ser humano (que em nossa profissão chamamos casualmente de "usuário") e seus dados, convido o leitor a embarcar comigo em uma reflexão sobre como nossa evolução nos moldou, como esse conhecimento é essencial para construirmos qualquer plano de conscientização, qual o nosso papel como profissionais de computação, quais os desafios para um futuro com IA ubíqua e como devemos tratar **o ser humano como o elo principal da cadeia**, e não o elo mais fraco.

Do Fogo ao Smartphone

Uma das coisas mais fascinantes na história da humanidade é nossa habilidade de modificar nosso ambiente, principalmente através do domínio da energia e do desenvolvimento de novas tecnologias. Quase todos os saltos civilizatórios estiveram associados a uma quebra de paradigma na forma de produzir e utilizar energia que, por sua vez, leva à possibilidade de novas tecnologias, levando a avanços na produção, utiliza-

ção e armazenamento de energia, o que viabiliza novas tecnologias. Desde que os hominídeos dominaram o fogo, estamos nesse ciclo virtuoso de evolução [1].

Infelizmente, sempre que esses avanços ocorrem, não há como escolher somente os benefícios de uma tecnologia, pois ela também pode ser utilizada para fins negativos. Com a revolução da informação não foi diferente, pois temos um conjunto de tecnologias, baseadas em software, que foram desenvolvidas por seres humanos para o uso por seres humanos, não sendo possível prever os tipos de uso que a tecnologia terá.

Estamos em um momento desta evolução em que boa parte da humanidade anda diariamente com um computador conectado à Internet no bolso. Este computador, que chamamos de smartphone, nos permite facilidades que há menos de 20 anos eram inimagináveis: ter documentos pessoais à mão; ter uma biblioteca inteira num aplicativo; fazer uma chamada de vídeo com a família; ter um mapa com GPS e não se perder, mesmo numa cidade estranha; reservar hotéis e passagens; pagar contas; fazer compras on-line; acessar o banco; entre muitas outras possibilidades, incluindo atividades relacionadas ao trabalho. E todos esses serviços dependem, também, do acesso à Internet e da disponibilidade e confiabilidade dos sistemas em nuvem, que também são extremamente visados por atacantes, pois ali estão concentrados os dados de praticamente todos os cidadãos e empresas.

Ou seja, não é à toa que os atacantes também direcionam seus ataques a conseguir acesso aos serviços de nuvem e aos dispositivos de usuários finais, estes últimos visados inclusive para furto, considerando que são hoje a nossa carteira.

Fomos da Caverna ao Espaço, mas Ainda Somos Praticamente os Mesmos

Embora a tecnologia tenha evoluído exponencialmente nos últimos séculos, a cognição, os instintos e o raciocínio do ser humano ainda são muito similares aos do período Paleolítico. Nós achamos que as pessoas tomam decisões por motivos racionais (lobo frontal), mas a verdade é que na maior parte de nossa evolução, nós dependemos majoritariamente do nosso instinto de fuga e luta (sistema límbico). Com isso, nossas decisões são muito mais emocionais do que racionais. Mesmo sem saber, os atacantes exploram exatamente o fato de que nossas emoções falam mais alto que nossa razão [1, 2].

Em geral, quando uma pessoa "cai" em um golpe nos perguntamos como a pessoa não percebeu, pois era "lógico" que era um golpe, bastava refletir e analisar. E o uso dessas palavras já nos dá uma dica que a pessoa não raciocinou, ou seja, seu cérebro não ativou as áreas mais recentes de raciocínio lógico, mas sim houve ativação direta das áreas de reação emocional do sistema límbico, o que foi cunhado como sequestro límbico (do Inglês "*amigdala hijacking*" [3]).

Os ataques de engenharia social sempre existiram, e exploram exatamente essa característica do nosso cérebro, ao ludibriar a pessoa com o uso de ardis

combinados com uma reação emocional forte. No passado, quase todos os golpistas precisavam também ser bons atores, pois eles precisavam ficar cara a cara com as vítimas para convencê-las a comprar um bilhete premiado da loteria ou uma casa pré-moldada, mas que nunca seriam entregues.

Infelizmente, os sistemas informatizados tornaram mais fácil a vida dos golpistas, pois agora é necessário apenas ter uma história comovente ou amedrontadora, e combiná-la com a tecnologia, seja enviando mensagens, criando sites ou aplicativos falsos.

A Importância do Letramento Digital

Por trabalhar com segurança há mais de 25 anos, com bastante frequência me perguntam "Qual sistema é o mais seguro?". Minha resposta invariavelmente é "o sistema que você conhece, sabe como usar, mantém atualizado e com mecanismos de segurança".

Dito isso, conhecer e saber usar um sistema requer o que hoje se convencionou chamar de letramento digital. Infelizmente, o baixo letramento digital da população brasileira é uma realidade que torna mais difícil o uso seguro da tecnologia. Os dados da TIC Domicílios mostram claramente que, apesar de 84% da população declarar que usa a Internet regularmente, menos da metade possui habilidades básicas como copiar e colar textos ou ativar configurações de segurança e privacidade [4].

Os fatores humanos devem, ou ao menos deveriam, estar sempre em mente nas fases de projeto e desenvolvimento de qualquer tecnologia, pois ela será utilizada por pessoas que não são especialistas e precisaria ser dotada de boa usabilidade e acessibilidade. Porém, a realidade atual está longe de ser ideal, pois infelizmente a maior parte dos sistemas é complexa para a maior parte das pessoas, o que se reflete nesse baixo índice de habilidades por parte dos cidadãos.

O Marco Civil da Internet diz em seu artigo 26 que "*O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico*."[5] Porém, sabemos que o cidadão em geral chega ao mercado de trabalho com conhecimentos muito rudimentares de uso de tecnologia e quase nulos de uso seguro. As organizações, de forma geral, contratam os funcionários assumindo que entendem a tecnologia, mas vemos pela TIC Domicílios que o cenário está bem longe disso.

O Cenário Perfeito para a Engenharia Social

Dicas básicas de segurança que são parte de qualquer material de conscientização, como "acesse somente sites com https", "verifique se o endereço é o do site que você quer acessar" ou "use somente aplicativos oficiais", requerem conhecimentos sobre o sistema operacional e sua interface, o navegador, domínios na Inter-

net, o ecossistema de desenvolvimento de aplicativos, entre outros. Por consequência, vemos no dia a dia, que muitas campanhas de conscientização falham, pois as pessoas não têm os conhecimentos básicos de informática para entender o que está sendo ensinado.

O uso acelerado e ubíquo da tecnologia sem um letramento adequado leva ao cenário atual, em que os atacantes têm uma grande vantagem, pois eles podem criar esquemas elaborados de fraude, que se valem da dificuldade das pessoas de entender as interfaces e as mensagens que lhe são apresentadas. Some-se a isso técnicas como imprimir senso de urgência ou instigar medo, que levam a reações emocionais e não racionais, e temos o cenário perfeito para a engenharia social moderna.

Como ter Efetividade em uma Campanha de Conscientização

Para quem trabalha com segurança é chave entender não só as vulnerabilidades técnicas do mundo em que vivemos, mas também os fatores humanos que estão envolvidos, pois estes são parte do projeto e do desenvolvimento dos sistemas, da compreensão e uso da tecnologia e da motivação dos atacantes. E esses mesmos fatores humanos são os que nos fazem agir sem pensar em momentos de estresse, vulnerabilidade que é explorada em ataques de Engenharia Social.

Soma-se a isso o fato que as campanhas em geral focam em "o que" fazer, e não em "por que" fazer. Esse é um ponto que precisa ser repensado, pois somos movidos não por razão, mas sim por emoção e confiança [2]. Explicar "porque" uma medida é necessária e como pode ajudar a pessoa é tão importante quanto explicar como implementar uma medida. A pessoa precisa ver a necessidade e entender que ela será beneficiada tanto quanto a organização. Se não houver o entendimento do porquê uma medida é importante, ela será burlada no momento em que o usuário sentir que precisa mais agilidade no trabalho e que a medida está "atrasando" sua rotina.

Também **é importante focar no Princípio de Pareto**. Pergunte-se: "Quais são os 20% das medidas que podem reduzir 80% dos riscos?" Se uma pessoa for confrontada com uma lista enorme de medidas que "precisa" implantar e ficar com a sensação de que "ou implementa tudo ou não está protegido" a reação natural é pensar "então nem vale a pena fazer nada". N**ão podemos, como profissionais, anestesiar os usuários, nem educar pelo medo.** Precisamos ter uma postura positiva, constante e confiável, que leve as pessoas a querer nos procurar, apontar problemas e alertar o mais cedo possível de que algo pode estar errado.

Precisamos ter os usuários como nossos aliados, como parceiros que vão identificar quando as ferramentas falharem – e as ferramentas falham mais frequentemente do que gostaríamos de admitir. Precisamos mudar nossa mentalidade e entender que o usuário é o elo mais importante da cadeia, não o mais fraco. Os sistemas são feitos para que ele possa cumprir uma missão, uma tarefa. **As medidas de segurança não podem**

impedir o trabalho, senão serão burladas. E o usuário que entende o porquê segurança é importante e que se sente à vontade para procurar a equipe técnica quando encontra problemas é capaz de detectar incidentes enquanto ainda é possível mitigá-los e evitar os efeitos mais danosos.

Também é necessário ter cuidado com a linguagem, que precisa ser simples, e com o projeto e diagramação do material. Infelizmente, com o ambiente atual de excesso de informação em redes sociais, com mensagens curtas, a maior parte das pessoas não lerá textos grandes nem procurará por mais informações. Temos que fazer o projeto de folhetos, sites e aplicativos pensando que precisamos colocar a informação diagramada de forma a atrair o olhar, com imagens que complementem e chamem a atenção. As pessoas não lerão o material do início ao fim, elas passarão os olhos, e precisamos formatar a mensagem para esse novo leitor [6].

O que nos Aguarda no Futuro?

Algoritmos de inteligência artificial (IA) existem há décadas, mas um dos limitantes do avanço no uso era o fato de que não havia poder computacional para treinar os algoritmos e utilizá-los em tempo hábil para a maior parte das tarefas. Com a evolução da tecnologia esse cenário mudou e vivemos um momento em que os usos estão se tornando crescentes, para o bem e para o mal. É difícil dizer o que vai acontecer, mas dadas as capacidades e usos atuais, já temos alguns problemas à nossa porta.

Os profissionais que atuarão com segurança e conscientização terão pela frente o desafio de **ensinar mais que dicas de segurança,** precisarão **desenvolver o pensamento crítico dos usuários**. Será necessário pensar em como proteger dados sensíveis de vazamentos via ferramentas de IA em nuvem, sejam elas chats, ferramentas de auxílio para programação (os "co-pilots") ou quaisquer outras que surgirem.

O pensamento crítico será chave para diferenciar fatos de *deep fakes*, pois os criminosos poderão usar IA para automatizar várias partes do processo de Engenharia Social, reduzindo a interatividade necessária hoje e aumentando a credibilidade das mensagens. Além disso, tanto vídeo quanto áudio serão mais facilmente manipulados, requerendo perspicácia e pensamento crítico dos usuários para detectar fraudes.

Será necessário educar os usuários para esse cenário e esclarecer que os criminosos usarão os dados que eles mesmos colocam em redes sociais, pessoais ou de trabalho para treinar a IA, que poderá facilmente inferir relações de trabalho e de parentesco, e criar golpes personalizados sem interação dos fraudadores.

E será necessário que os profissionais aprendam a usar a IA a seu favor, seja incrementando ferramentas de detecção ou automatizando tarefas como buscas por vulnerabilidades e análise de segurança código, por exemplo.

Mas, mais que tudo, **é necessário que profissionais de cibersegurança incluam em sua formação a compreensão daquilo**

que nos faz humanos, tanto pontos fortes quanto pontos fracos, e adequem sua mensagem ao público ao invés de esperar que ele tente se adequar aos nossos jargões e nossa forma de lidar com a tecnologia. Recomendo a todos a leitura não só das referências deste artigo, mas também de outros materiais que tragam insights sobre como pensamos e porque agimos de determinadas maneiras. Seremos profissionais melhores se entendermos melhor nossos usuários, os seres humanos.

A tecnologia é feita de humanos para humanos - precisamos sempre nos lembrar disso!

Referências

1. VINCE, G. Transcendence: How Humans Evolved through Fire, Language, Beauty, and Time. New York: Basic Books, 2020. ISBN: 9780465094912.
2. SINEK, S. Start with Why: How Great Leaders Inspire Everyone to Take Action. London: Portfolio/Penguin, 2009. ISBN: 9781101149034.
3. ROWLES, R. Amygdala Hijacking and Social Engineering. Social-Engineer, LLC, 2023. Disponível em: https://www.social-engineer.org/social-engineering/amygdala-hijacking-and-social-engineering/. Acesso em: 23 mar. 2024.
4. CETIC.BR/NIC.BR. TIC Domicílios 2023 – Indivíduos. Disponível em: https://cetic.br/pt/tics/domicilios/2023/individuos/. Acesso em: 23 mar. 2024.
5. LEI Nº 12.965, de 23 de abril de 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 23 mar. 2024.
6. STIMAC, Stephanie. Design for Developers. New York: Manning, 2023. ISBN: 9781617299476.

CRISTINE HOEPERS é Gerente do CERT.br/NIC.br, é formada em Ciências da Computação pela UFSC e Doutora em Computação Aplicada pelo INPE. É, também instrutora autorizada do Software Engineering Institute, da Carnegie Mellon University, e ministra os cursos do CERT®/CC no Brasil. Em 2020 recebeu do M3AAWG, maior organização mundial de combate a abusos on-line, o prêmio anual Mary Litynski por seu trabalho para aumentar a resiliência da Internet. Atua nas áreas de Gestão de Incidentes, Privacidade, Implantação de CSIRTs, Honeypots e Combate a Fraudes na Internet.