EFF'S SURVEILLANCE SELF-DEFENSE

Seu Plano de Segurança

https://ssd.eff.org/en/about-surveillance-self-defense

ELECTRONIC FRONTIER FOUNDATION

LOCALIZATION LAB

Tentar proteger todos os seus dados de tudo e a toda a hora não é prático e é exaustivo. Mas, não tenha medo! A segurança é um processo e, através de uma planificação cuidadosa, é possível criar um plano que seja o melhor para si. A segurança não se resume às ferramentas que utiliza ou ao software que descarrega. Começa com a compreensão das ameaças específicas que enfrenta e como as pode combater..

Em segurança informática, uma ameaça é um evento potencial que pode comprometer os seus esforços para defender os seus dados. Pode combater as ameaças que enfrenta determinando o que precisa de proteger e contra quem o precisa de proteger. Este é o processo de planificação da segurança, muitas vezes referido como "modelação de ameaças."

Este guia explica como elaborar um plano de segurança para as suas informações digitais e como determinar quais as melhores soluções para si.

Em que consiste um plano de segurança? Digamos que quer manter a sua casa e os seus bens seguros. Eis algumas perguntas que pode fazer, utilizando algumas palavras-chave como "activos" e "adversários" que voltarão a ser mencionadas mais tarde:

O que é que eu tenho dentro de casa que vale a pena proteger?

- Os activos podem incluir: jóias, aparelhos electrónicos, documentos financeiros, passaportes ou fotografias.

De quem é que os quero proteger?

- Os adversários podem incluir: assaltantes, colegas de quarto ou convidados.

Qual é a probabilidade de eu precisar de os proteger?

- O meu bairro tem um historial de assaltos? Qual é o grau de confiança dos meus colegas de quarto/convidados? Quais são as capacidades dos meus adversários? Quais são os riscos que devo considerar?

Quão graves seriam as consequências se eu falhasse?

- Tenho alguma coisa em casa que não possa substituir? Tenho tempo ou dinheiro para os substituir? Tenho um seguro que cubra os bens roubados da minha

casa? Há outras pessoas na minha vida cuja segurança ficará comprometida se estas ameaças ocorrerem?

Quanto trabalho estou disposto a fazer para evitar estas consequências?

- Estou disposto a comprar um cofre para documentos sensíveis? Posso dar-me ao luxo de comprar uma fechadura de alta qualidade? Tenho tempo para abrir uma caixa de segurança no meu banco local e guardar aí os meus objectos de valor?

Quem são os meus aliados?

- Existem pessoas com quem vivo que poderiam ajudar a proteger as coisas que me interessam? Há vizinhos que possam saber mais sobre o local onde vivemos e os recursos a que temos acesso?

Depois de fazer estas perguntas a si próprio, está em condições de avaliar as medidas a tomar. Se os seus activos são valiosos, mas a probabilidade de um arrombamento é baixa, então pode não querer investir muito dinheiro numa fechadura. No entanto, se a probabilidade de arrombamento for elevada, deve adquirir a melhor fechadura do mercado e considerar a possibilidade de acrescentar um sistema de segurança.

Talvez já esteja a começar a sentir que não existe uma resposta definitiva para estas perguntas. Em vez disso, tem de fazer julgamentos com base naquilo que valoriza e na probabilidade de alguma ameaça se concretizar. É essa a essência deste exercício: tomar decisões informadas com base na medição da gravidade do impacto das ameaças, na probabilidade de estas ocorrerem e na definição de prioridades relativamente às coisas que pretende proteger.

Como posso elaborar o meu próprio plano de segurança? Por onde devo começar?

Ao elaborar um plano de segurança, responda às seguintes seis perguntas:

1. O que é que quero proteger?
2. De quem é que os quero proteger?
3. Quão graves seriam as consequências se eu falhasse?
4. Qual é a probabilidade de eu precisar de os proteger?
5. Qual o grau de dificuldade que estou disposto a suportar para tentar evitar potenciais consequências?
6. Quem são os meus aliados?

Vamos analisar mais detalhadamente cada uma destas questões.

O que é que quero proteger?

Um " activo" é algo que valorizamos e queremos proteger. No contexto da segurança digital, um activo é normalmente algum tipo de informação. Por exemplo, podem ser os seus e-mails, listas de contactos, mensagens diectas, localização ou outros documentos. Os seus próprios dispositivos também podem ser activos

Faça uma lista dos seus activos: dados que guarda, onde são guardados, quem tem acesso a eles e o que impede os outros de acederem aos mesmos.

De quem é que os quero proteger?

Para responder a esta pergunta, é importante identificar quem pode querer atacá-lo a si ou às suas informações. Uma pessoa ou entidade que represente uma ameaça aos seus activos é um "adversário ⓘ." Exemplos de potenciais adversários são o seu chefe, a polícia, o seu antigo parceiro, o seu concorrente comercial, o seu governo ou um hacker numa rede pública. Pode até incluir pessoas em quem confia e que podem acidentalmente comprometer os seus bens por serem descuidadas com os seus próprios planos de segurança

Faça uma lista de adversários potenciais ou conhecidos, ou daqueles que podem querer apoderar-se dos seus activos. A sua lista pode incluir indivíduos, uma agência governamental ou empresas. Dependendo de quem são os seus adversários, em algumas circunstâncias, esta lista pode ser algo que queira destruir depois de terminar a planificação da segurança.

Quão graves seriam as consequências se eu falhasse?

Existem muitas formas de um adversário obter acesso aos seus dados. Por exemplo, um adversário pode fazer com que o utilizador clique no link malicioso enviado para o seu e-mail que compromete o seu computador. Ou, mais simplesmente, pode ser alguém a fazer uma captura de ecrã das suas mensagens privadas e a utilizar essa informação contra si.

Os motivos dos adversários são muito diferentes, tal como as suas tácticas. Alguns podem ser altamente sofisticados do ponto de vista técnico, enquanto outros se assemelham mais a esquemas feitos para ganhar a sua confiança e, por fim, traí-la.

A planificação da segurança implica compreender quão graves podem ser as consequências se um adversário conseguir aceder a um dos seus activos. Para o efeito, deve considerar a capacidade do seu adversário. Por exemplo, o seu fornecedor de telemóveis tem acesso a todos os seus registos telefónicos. O seu governo pode ter capacidades mais fortes.

Escreva o que o seu adversário poderá querer fazer com os seus dados privados.

Qual é a probabilidade de eu precisar de os proteger?

O Risco é a probabilidade de uma determinada ameaça contra um determinado activo ocorrer na prática. Está associado à capacidade. Por exemplo, embora o seu fornecedor de telemóveis tenha a capacidade de aceder a todos os seus dados, o risco de publicar os seus dados privados online para prejudicar a sua reputação é baixo.

É importante distinguir entre o que pode acontecer e a *probabilidade* de acontecer. Por exemplo, existe a ameaça de o seu edifício desabar, mas o risco de isso acontecer é muito maior em São Francisco (onde os terramotos são comuns) do que em Estocolmo (onde não são).

A avaliação dos riscos é um processo pessoal e subjectivo. Muitas pessoas consideram certas ameaças inaceitáveis, independentemente da probabilidade de ocorrerem, porque a mera presença da ameaça, qualquer que seja a probabilidade, não vale o custo. Noutros casos, as pessoas ignoram os riscos elevados porque não vêem a ameaça como um problema.

Anote as ameaças que vai levar a sério e as que podem ser demasiado raras ou inofensivas (ou demasiado difíceis de combater) para se preocupar.

Qual o grau de dificuldade que estou disposto a suportar para tentar evitar potenciais consequências?

Não existe uma opção perfeita para a segurança. Nem toda a gente tem as mesmas prioridades, preocupações ou acesso a recursos. A sua avaliação de riscos permitir-lhe-á planear a estratégia certa para si, equilibrando a conveniência, o custo e a privacidade.

Por exemplo, um advogado que represente um cliente num caso de segurança nacional pode estar disposto a fazer mais esforços para proteger as comunicações sobre esse caso, como a utilização de correio electrónico encriptado, do que um membro da família que envia regularmente por email vídeos engraçados de gatos.

Anote as opções disponíveis para ajudar a mitigar as suas ameaças específicas. Anote se há restrições financeiras, técnicas ou sociais.

Quem são os meus aliados?

Tal como indicámos várias vezes ao longo deste guia, a privacidade e a segurança digital são um jogo de equipa que é melhor aplicado com a ajuda de outros. Isto não se deve apenas ao facto de haver poder nos números, mas porque a sua privacidade e segurança se sobrepõem a outras pessoas na sua vida. Se uma ameaça o afecta a si, pode também afectá-los a eles e vice-versa.

Considere a quem estende essa confiança. Por exemplo, considere se alguém pode ser uma "ameaça interna", uma pessoa da sua rede de confiança que pode trair a sua segurança de uma forma ou de outra. Mas não deixe que o medo de uma ameaça interna o desencoraje de estabelecer ligações com outras pessoas. Em vez disso, utilize-o como um guia para o incentivar a fazer planos cuidadosos e a certificar-se de que as outras pessoas do seu círculo também levam a segurança a sério.

Inicie um diálogo com outras pessoas que provavelmente partilham as mesmas preocupações. Chegue a alguns acordos partilhados sobre como cuidar uns dos outros e quais as informações que devem ser confiadas uns aos outros.

Planificação da segurança como uma prática regular

Não se esqueça de que o seu plano de segurança pode mudar à medida que a sua situação se altera. Por isso, é boa prática rever o seu plano de segurança com frequência.

Crie o seu próprio plano de segurança com base na sua situação específica. Depois, marque no seu calendário uma data no futuro. Isto irá levá-lo a rever o seu plano e a verificar se ainda é relevante para a sua situação.