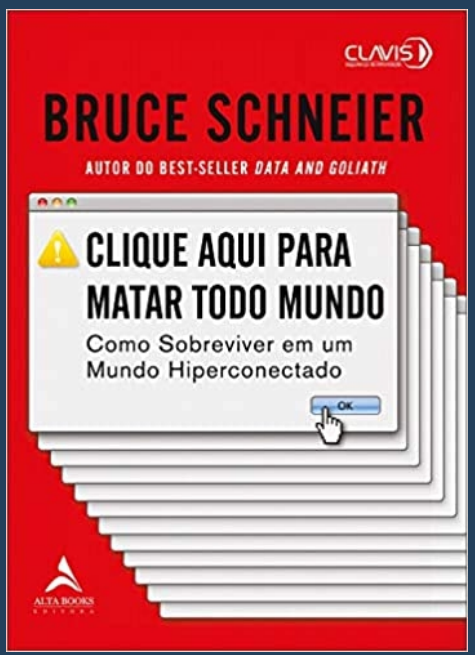

Clique Aqui Para Matar Todo Mundo

Clique Aqui Para Matar Todo Mundo: Como Sobreviver em um Mundo Hiperconectado
Ano de publicação: 2020
Autor: Bruce Schneier
288 páginas
Link para compra: https://amzn.to/3l8a0GD

A era digital veio para ficar e alterar todas as relações econômicas e sociais já conhecidas pela humanidade.

Todas essas alterações denotaram grandes impactos no cotidiano das pessoas em todas as partes do mundo, porém uma delas merece uma atenção maior, a disseminação de informações pela internet e seus dispositivos correlatos.

É sobre esse assunto e todas as implicações que Bruce Schneier fala em seu livro "Clique Aqui Para Matar Todo Mundo". Nesse sentido, o autor se propõe a desmistificar todo o processo de disseminação da informação e os riscos ocultos dessa nova tendência, como também, as formas de barrar seus malefícios.

Avaliação geral

8

8 Aplicabilidade
8 Inspiração
8 Inovação
8 Impacto nos resultados
8 Estrutura

Ideias principais do livro

- **Todos os seus equipamentos, hoje em dia, são computadores;**
- Nossas informações são compartilhadas a todo momento;
- Quase todas as relações são permeadas pela internet;
- Ações são necessárias para deixar a Internet+ mais segura;
- O Governo tem um papel muito importante para a segurança da informação.

Esse livro é indicado para quem?

O conteúdo da obra é indicado para profissionais de TI ou de segurança da informação, que buscam se atualizar sobre os possíveis ataques e riscos da internet e das novas tecnologias.

Ainda, também pode ser indicado para todos da sociedade civil que busquem estar seguros na hiperconectividade da era da informação.

Visão geral do livro

Overview: A Internet+

A era digital veio com tudo, e hoje, é possível dizer que as pessoas são rodeadas por computadores que desempenham diversas funções e podem ser comandados por meio de um smartphone ou outro computador. Isso é o que Bruce Schneier chama de Internet+, a possibilidade de tudo ser um computador, que permite a participação integral da internet no mundo físico.
Essa interação implica em **redes gerais e abertas de segurança**, que podem se tornar mais suscetíveis a ataques.
Nesse sentido o problema da segurança se torna uma guerra entre dois grupos:

1. Os que buscam atacar sistemas;
2. Os que se preocupam em manter a segurança.

De acordo com o livro "Clique Aqui Para Matar Todo Mundo", para entender os processos de segurança da Internet+, é necessário entender alguns aspectos tecnológicos, políticos, criminosos e comerciais que permeiam esse ambiente.
Alguns deles são:

- Manter a segurança de computadores ainda é uma tarefa difícil - a maioria dos softwares que integram essas máquinas são **inseguros e mal codificados**;
- A internet não foi projetada com um sistema de segurança em mente;
- A extensão dos computadores pode ser usada contra nós - todos os aparelhos são computadores passíveis de serem programados para realizar qualquer tipo de função;
- A complexidade dos sistemas computadorizados faz a defesa ser mais difícil que o ataque;
- Novas vulnerabilidades aparecem na interconectividade - desconhecidas propriedades aparecem diariamente na internet e aumentam a vulnerabilidade;
- **Computadores falham** de maneiras diversas;
- Ataques se tornam mais fáceis e rápidos - o que funcionou ontem para defesa, já pode não funcionar hoje e muito menos amanhã.

Overview: Os Paradigmas da Segurança

Existem **dois paradigmas** que permeiam a segurança, são eles:

1. O mundo de tecnologias físicas e letais (automóveis, aviões, indústria farmacêutica), nas quais tudo deve ser rigorosamente testado;
2. O mundo dos softwares, no qual o que se deve priorizar é o serviço rápido e ágil.

De acordo com o livro "Clique Aqui Para Matar Todo Mundo", no ambiente da Internet+ esses dois paradigmas estão a todo tempo colidindo, e para se proteger do choque desses processos é necessário realizar nos seus dispositivos o updating.
Esse update, ou, as atualizações que a concessora dessa inteligência disponibiliza, se preocupa em barrar certas falhas que são encontradas ao longo do tempo.
Entretanto, por diversas razões conhecidas, muitas pessoas ainda não realizam essas atualizações quando concedidas, como também, muitas empresas deixam de disponibilizá-las para certos tipos de dispositivos mais antigos.
Essas práticas relatadas acima, facilitam os ataques praticados por hackers.
Nesse sentido, a melhor solução seria a integração desses dois paradigmas, oferecendo softwares que contassem com a capacidade de ação ágil, porém, que houvessem **passado por processos rigorosos** e continuassem recebendo atualizações em possíveis falhas.

Overview: Os processos de autenticação

Ao fazer uso de algum sistema da Internet+ é necessário que provemos que nós realmente somos nós. Dentro deste processo, existem três tipos de autenticações:

1. **Por login e senha** (algo que você sabe);
2. **Por biometria** (algo que você é);
3. **Por dois aparelhos** (algo que você tem).

Ainda assim, é apontado por Bruce Schneier que existem maneiras de **hackear essas três formas de autenticação.**
A grande questão é o embate que existe nesse processo, já que ele precisa ser seguro e ao mesmo tempo de fácil utilização para os usuários, sendo também vital para qualquer aparelho da Internet+ saber qual o usuário da vez.
Nesse sentido, mesmo com o trade-off de segurança e conveniência, em algum momento ambas as tendências terão que se preocupar com a segurança.

Overview: Atribuição como ferramenta de controle

Atribuição é apenas a identificação de uma pessoa que não quer ser identificada.
Em alguns casos ela é fácil, pois pode-se associar a um cartão de crédito ou telefone nominal, o que ajuda as autoridades a **identificar o responsável por algum ato ilegal**.
Porém, ela também pode ser difícil, considerando que o processo de identificação é conhecido por muitas pessoas, e que alguns países não contam com sistema de vigilância para a internet.
Esse tipo de guerra anônima se mantém constante, já que muitas pessoas continuam cometendo erros, ou até mesmo crimes, mas desenvolvem habilidades com o uso da Internet+ para se manter anônimas.

Overview: Grandes instituições contribuem para a insegurança

A insegurança nas redes pode chegar a ser de grande interesse para corporações e para o governo de alguns países, que se aproveitam da função de retenção de informações dos computadores para poder ter acesso a dados pessoais.
De acordo com o livro "Clique Aqui Para Matar Todo Mundo", as ferramentas de busca da internet são o local **onde mais deixamos informações e preferências**, uma grande fonte para instituições interessadas.
Ainda, analisando essas questões, grandes corporações aproveitam para controlar os tipos de programas a que poderemos ter acesso.
Em relação ao governo, sua tentativa de vigilância se dá por razões políticas e sociais, de modo a exercer maior controle sobre sua população, por meio da cooperação de instituições de telecomunicação com agências de inteligência do governo.
Todo esse cenário rodeado de instabilidade e insegurança é admirado por criminosos, que usam desses aspectos para efetuarem seus ataques, que vão desde roubo de dinheiro a controle de sistemas.

Overview: Aumento de riscos

A segurança da informação é baseada em uma tríade conhecida como **"CIA": confidencialidade, integridade e avaliabilidade.** Nesse panorama, as três coisas possíveis de se fazer com as informações de uma pessoa é copiar, modificar ou deletar.
Essas três palavras parecem inofensivas, mas quando vistas de um ponto macro podem trazer danos irreparáveis, tendo como exemplo um carro, que pode ter os breques desativados em um ataque hacker.
Além disso, Bruce traz a relevância que estão ganhando os algoritmos, sendo cada vez mais autônomos e poderosos.
Os algoritmos do tipo machine learning, os quais aprendem a se auto-alimentar de tempos em tempos, podem se tornar extremamente perigosos ao passo que, alguns passam a não precisar de supervisão humana.
Nessa mesma linha de perigo estão os supply chains, nos quais os ataques ocorrem na produção, distribuição e manutenção dos produtos que compõem a Internet+.
O autor ressalta que, avanços na tecnologia indicam mais possibilidades de ataque, e ainda, quanto melhores forem menos hackers serão necessários para esse trabalho.

Overview: Soluções

Bruce Schneier propõe algumas ações que **incentivem e melhorem a seguridade das tecnologias**. Dessa forma, vamos citar as melhores delas para cada categoria proposta.
Em **relação à dispositivos**, as 4 mais relevantes são:

1. Ser transparente na apresentação da seguridade do produto;
2. Produzir softwares com updates contínuos;
3. Contar com testes rigorosos;
4. Encriptar e autenticar informações.

Quando o assunto é **segurança da informação**, temos 3:

1. Minimizar a coleta de dados do usuário;
2. Deixar as informações anônimas sempre que possível;
3. Permitir aos usuários total acesso e controle de suas informações na rede.

Já em relação às **conexões de rede**, é possível citar 4:

1. Proporcionar uma conectividade segura aos usuários;
2. Auxiliar nas configurações dos dispositivos de rede;
3. Informar aos clientes possíveis ataques;
4. Educar os consumidores sobre as ameaças.

Para a **segurança da internet**, 2 se destacam:

1. Fornecer informações de roteamento autênticas e confiáveis;
2. Trabalhar com todo o tráfego de forma igualitária, sem distinção de serviço.

Sobre segurança de algoritmos, o livro "Clique Aqui Para Matar Todo Mundo" pontua que ainda não há uma solução clara para esse problema, porém a possibilidade de realizar auditorias, controles e ter transparência no sistema já ajudariam na causa.
Ainda, definir os limites do ciberespaço melhoraria a gestão de planejamentos de segurança da infraestrutura da Internet+, como também, começar a desconectar sistemas complexos, facilitaria no processo de seguridade.

Overview: Como manter a Internet+ segura

Na visão do autor, uma forma de deixar a internet mais segura é **criando políticas de incentivo** para que as concessoras sejam influenciadas a produzi-las dessa forma.
Nesse sentido, está incluso a criação de padrões, como o da venda desses produtos apenas com a certeza de que sejam seguros.
Aliado a isso, o esclarecimento das obrigações das empresas e dos clientes permite que o segundo grupo tenha mais conhecimento para cobrar padrões que não foram seguidos.
Outro ponto relevante, de acordo com Bruce Schneier, seria o esclarecimento da seguridade dos produtos quando efetuada a compra, em conjunto com uma **educação pública de maior qualidade**, a qual é vital para que as pessoas cresçam sabendo dos benefícios e malefícios da cibersegurança.
O livro "Clique Aqui Para Matar Todo Mundo" ressalta que a elevação do padrão de profissionais da área, treinados para trabalhar com mais pesquisas voltadas ao tema, iria ajudar não só na produção de sistemas mais seguros, assim como duradouros.

Overview: Últimas Considerações

É pontuado na obra que o Governo é uma peça chave para possibilitar a segurança da informação nos países, já que sua atuação influente tem poder de auxiliar na criação das políticas e padrões mencionados.
Além disso, haveria a possibilidade da **criação de um órgão atuante que fiscalizasse todos os aspectos da Internet+** para averiguar se tudo está sendo implementado corretamente e de maneira segura.
Ainda que essa regulamentação pareça difícil, pelo aspecto complexo e dinâmico da internet, é muito importante focar em trazer um uso saudável e não ofensivo desse sistema, inclusive pelos órgãos competentes.
Em todo esse ambiente, é importante pensar na relação Governo vs indústrias, definindo limites entre os dados trocados entre as mesmas e impondo mais força nas regulamentações.
Assim, é possível dizer que a segurança da informação está se tornando um assunto crítico, e todos os países devem aderir iniciativas para controlá-la, porém, é desconhecido os efeitos que as medidas adotadas em um país podem causar em outro.
Existem ações que os consumidores podem fazer por si só, para aumentar sua segurança online, muitas delas envolvendo pesquisa sobre a segurança dos produtos, o tipo de troca de informações que existe nele e a busca por sistemas de vigilância.
A humanidade é movida pela confiança, por isso, o livro "Clique Aqui Para Matar Todo Mundo", salienta que o governo e as empresas precisam ganhar a confiança dos usuários, **operando com transparência e integridade.**
Por fim, Bruce aponta que não sabe qual o futuro da Internet+ ou de seus consumidores, entretanto, seus efeitos são inegáveis e para barrá-los precisaremos da união de políticas e da tecnologia em prol de um sistema mais seguro.

O que outros autores dizem a respeito?

No livro "**A Arte da Guerra**", a importância da informação é constantemente tratada pelo autor Sun Tzu, já que promove uma vantagem competitiva para seu exército. Entretanto, para obter estas informações, o uso da espionagem é muito escolhido.

Tom Chatfield, autor de "**Como Viver na Era Digital**", afirma que, hoje em dia, um conteúdo na internet se torna relevante não mais pelo endosso de um especialista no assunto, mas pela popularidade que ele alcança junto ao público. Essa abordagem abre margem para que a massa consumidora seja alvo de manipulação.

Daniel H. Pink, autor de "**O Cérebro do Futuro**", afirma que, graças à fusão da riqueza, tecnologia e aumento da conexão de pessoas por meio de telefones e internet, o mundo está transicionando para uma nova era que vai além do conhecimento; é preciso criatividade, empatia e emoção.

Certo, mas como aplicar isso na minha vida?

Durante a explicação dos malefícios que permeiam o sistema da informação, o autor aponta algumas iniciativas que podem minimizar seus danos.

Assim, é possível iniciar com pequenas ações, se atentando primeiro para a segurança pessoal e conscientizando as pessoas mais próximas.

Se você gostou desse livro, aproveite para conhecer nosso acervo completo com centenas de Pocketbooks dos maiores sucessos nas áreas de gestão, marketing e vendas, liderança, estratégia, desenvolvimento pessoal e empreendedorismo!

Clique e acesse agora: www.pocketbook4you.com

O conteúdo apresentado acima traduz a visão e análise crítica da nossa equipe de redatores, respeitando os fundamentos de propriedade intelectual no Brasil (artigo 8, inciso I). Nenhuma parte do livro está sendo copiada. São conteúdos únicos e exclusivos, sempre dando créditos aos autores e indicando o link para aquisição da obra completa. A PocketBook4You respeita o código de direitos autorais de acordo com o estabelecido na legislação brasileira, Lei 9.610/98. Este conteúdo é de propriedade exclusiva da PocketBook4You e está protegido pela Lei de Direitos Autorais em seus artigos 46, I, (a) e em seu artigo 47, isso porque não se trata de reprodução e também não lhe implicam qualquer descrédito, pelo contrário, o direito moral é protegido e, como ressaltado anteriormente, o leitor recebe um link para adquirir a obra. É proibida a reprodução deste material sem a autorização da empresa.