Info Hacker

RESUMO QUINZENAL OFICIAL DA ACADEMIA HACKER

Red Team vs Blue Team

por Leila Maria Biggi de Souza Cavalcante

Será que uma empresa está realmente segura contra invasões? O que fazer para diminuir o risco de ciberataques? Uma boa opção é implementar estratégias de Security Red Team, Blue Team.

A crescente demanda pela eficiência na segurança da informação fez com que as organizações passassem a lidar com o assunto de forma mais estratégica. A formação de um Blue Team e um Red Team é um bom exemplo disso.

Com atribuições específicas, as equipes promovem um trabalho de cibersegurança em nível mais elevado nas empresas, onde cada uma tem sua importância, trazendo inúmeros benefícios.

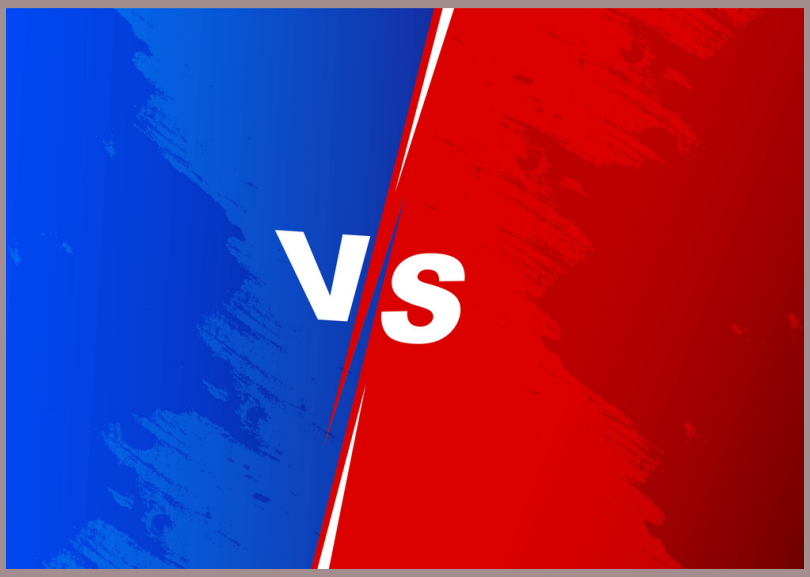

Image by Harryarts on Freepik

- O que é o **Red Team**?

O Red Team, em português, "*equipe vermelha*" são os responsáveis por simular um ciberataque contra uma empresa. Nesse caso, a ideia é tentar encontrar vulnerabilidades no sistema de forma antecipada, impedindo que criminosos usem a brecha para causar danos.

Inicialmente, os profissionais realizarão uma avaliação sobre o modelo operacional da companhia com o objetivo de montar um diagnóstico básico, catalogando quais são as principais falhas e riscos.

Nesse sentido, muitas empresas preferem contratar o Red Team externamente, visto que pessoas de fora conseguem enxergar os processos por outro ângulo e, consequentemente, pode ser mais fácil detectar os problemas menos óbvios.

Após a análise inicial, os profissionais começam os testes de segurança. Nessa etapa, as suas ações serão semelhantes às dos cibercriminosos, explorando todas as possíveis falhas na proteção.

Feito isso, é o momento de fornecer o relatório da investigação e dar as sugestões apropriadas para melhorar a segurança digital da empresa, que podem incluir:

- Atualização de sistemas;
- Política de mesas e telas limpas;
- Senhas mais seguras.

O que é o **Blue Team**?

O Blue Team, ou "*equipe azul*", é responsável por atuar na defesa contra uma invasão. Ou seja, caso a corporação sofra uma tentativa de invasão, o time azul é o encarregado de impedir que essa ação tenha sucesso.

Ele atua em conjunto com o Red Team para a manutenção da segurança digital. Ambas as equipes procuram identificar brechas na proteção que podem ser perigosas.

No entanto, diferente do time vermelho que acha as falhas e simula o ataque, o Blue Team trabalha arduamente para buscar uma solução para os erros.

Além disso, a equipe azul também é responsável por criar táticas que visam diminuir os impactos e prejuízos, caso a organização possa sofrer problemas com a segurança.

Algumas das funções do Blue Team:

- Avaliação de risco;
- Capacidade de resposta;
- Automação de segurança;
- Gerenciamento de incidentes.

A existência do Blue Team é essencial para garantir a cibersegurança da empresa, visto que são esses profissionais que estruturam a arquitetura de defesa que faz sentido para as circunstâncias da organização.

Purple Team

Além das equipes vermelha e azul, ainda existe a "*equipe roxa*". O Purple Team é a união dos serviços prestados pelas equipes. Então, em vez de trabalhar com a oposição entre team red vs team blue hacking, a ideia da equipe roxa é utilizar as vantagens das metodologias de análise tanto de ataque como de defesa para aumentar a segurança digital da empresa.

O funcionamento do Purple Team é pautado por meio da comunicação contínua entre as equipes. Assim, por meio de feedbacks valiosos, o time roxo pode montar uma operação de segurança.

Referências:

https://www.strongsecurity.com.br/blog/blue-team-e-red-team-entenda-o-que-sao-e-a-importancia-de-cada-um/

https://acaditi.com.br/red-team-e-blue-team/

https://br.claranet.com/blog/o-que-e-red-team-blue-team-e-purple-team-cyber-security

TPM 2.0

por Felipe Vasconcelos

O TPM, Trusted Platform Module, em sua versão 2.0, é uma ferramenta que ganhou popularidade nos últimos tempos, dado que a Microsoft tornou o seu uso obrigatório no Windows 11. Mas o que é o TPM 2.0?

O TPM é um chip físico, acoplado à placa mãe, que busca garantir mais segurança ao computador, principalmente o sistema operacional. Ele serve para guardar dados sensíveis ao processo de inicialização, como por exemplo chaves criptografadas, adicionando uma camada de segurança física. De acordo com a Microsoft: "As funções mais comuns do TPM são para medições de integridade do sistema e uso e criação de chaves". Uma das utilizações mais comuns do TPM é o armazenamento seguro e criptografado de hashes geradas na inicialização da máquina, de modo a isolar essa informação sensível de outros componentes que podem ser invadidos. Essa informação só pode ser acessada pelo próprio chip, de modo que nem mesmo o firmware consegue ter acesso direto às informações armazenadas.

A diferença entre as versões 2.0, atual, e 1.2, anterior, se resumem a um suporte mais diversificado de algoritmos de criptografia, superando o RSA e SHA1 que eram oferecidos pela versão 1.2.

O TPM 2.0 não é uma tecnologia recente, estando presente em placas mães que foram lançadas há mais de 4 anos. Para saber se o seu computador tem suporte a TPM 2.0, basta ir nas opções da BIOS, ativando a opção TPM 2.0, se ela existir. Se a mesma não existir, é possível adquirir o chip físico avulso e instalar em sua placa mãe. Também é possível adquirir as placas mães que já venham com o chip.

A ideia de um hardware exclusivo para guardar dados sensíveis não é criação da Microsoft, já que existem soluções semelhantes como o Secure Enclave utilizado pela Apple para finalidades semelhantes e com o Android oferecendo um suporte parecido dentro do processador. Porém, a Microsoft se destaca por ser um dos principais sistemas operacionais a ter como requisito obrigatório a sua utilização.

Referências:

https://learn.microsoft.com/pt-br/windows/security/information-protection/tpm/trusted-platform-module-overview
https://www.techtudo.com.br/dicas-e-tutoriais/2021/06/tpm-20-o-que-e-e-como-ativar-o-chip-para-instalar-o-windows-11.ghtml
https://canaltech.com.br/windows/tpm-20-saiba-o-que-e-o-componente-necessario-para-instalar-o-windows-11-188186/

Info Hacker - Edição 017
25/10/2022

Produção
Equipe Info Hacker

acha.ufal

Edições Anteriores

https://github.com/Academia-Hacker/Info-Hacker