staylock

Nossos Serviços

Segurança da Informação

Os melhores profissionais para atuar no seu ambiente, criando uma atmosfera segura para que seus clientes e parceiros não fiquem desprotegidos e tenham total confiança em você.

Atuamos com LGPD, GDPR, PCI-DSS, ISO 27001, ISO 27701, SOX entre outras.

Pentest – Teste de Penetração

É essencialmente um método de teste usado para descobrir qualquer vulnerabilidade em seu sistema antes que os hackers possam detectar cada um deles e explorá-los. Simular um ataque em suas próprias defesas é a maneira perfeita de se certificar de que você está preparado no caso de um ataque real

staylock

Nossa missão é proporcionar ao cliente um ecossistema seguro acoplando o melhor da tecnologia com o melhor da humanologia.

Alguns de nossos serviços

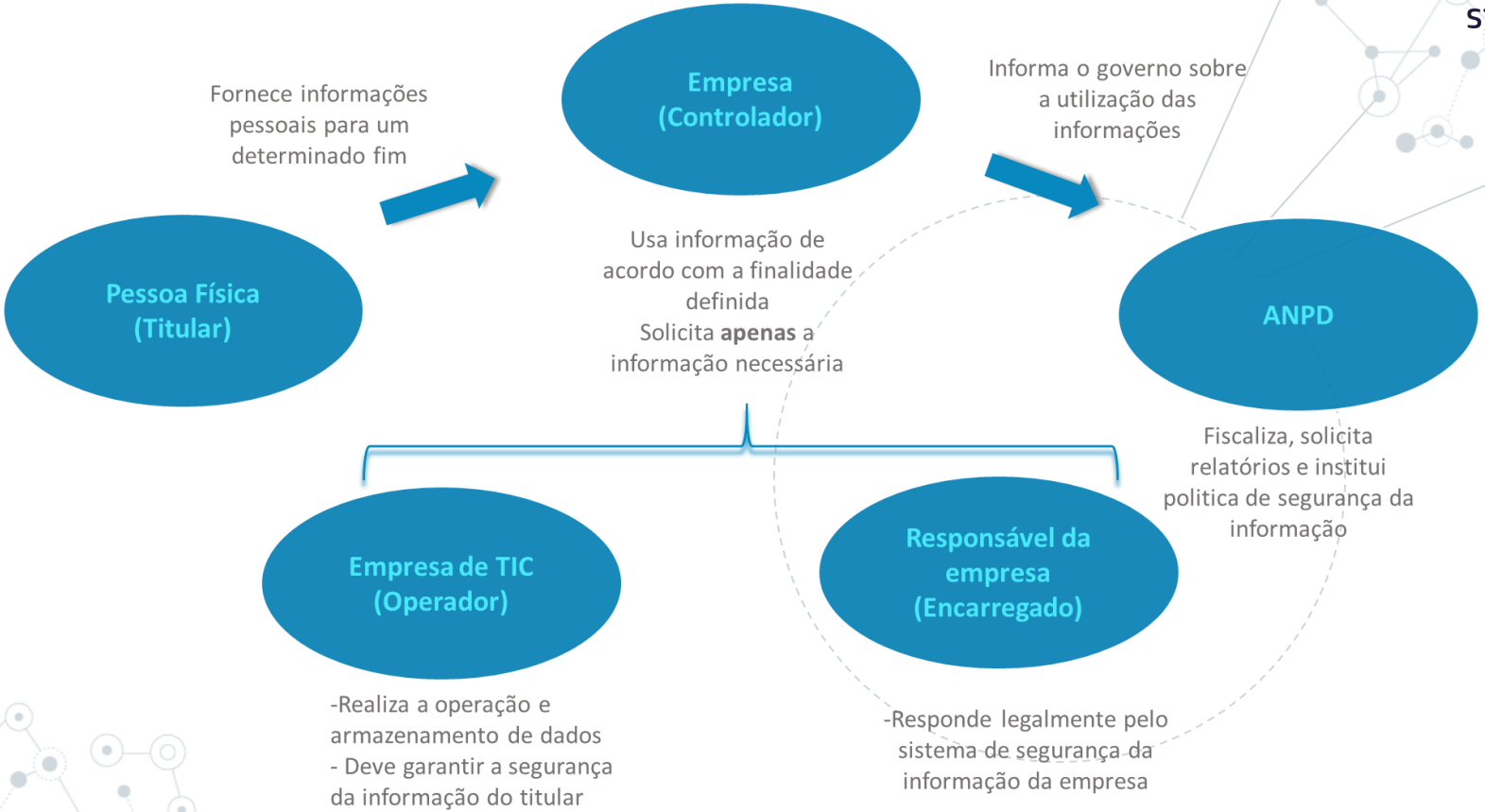
staylock

- Testes de Penetração
- DLP, SIEM, FIM, Firewall, IPS/IDS, Antivirus
- Workshops e treinamentos

Um pouco do que podemos oferecer.

Para você o que é Segurança da Informação?

LGPD – Lei Geral de Proteção de Dados



LGPD – Lei Geral de Proteção de Dados

Titular

- Poderá revogar a cessão dos dados a qualquer momento.
- É permitido ao titular solicitar informações a respeito da privacidade dos seus dados sempre que desejar, e deverá ser respondido com urgência.

Pessoa Jurídica

- Deverá pedir autorização para obtenção dos dados de forma clara.
- Qualquer evento que coloque em risco a privacidade dos dados deverá ser imediatamente comunicado ao titular.

Deverá comprovar legítimo interesse na obtenção dos dados.

Agência Nacional de Proteção de Dados (ANPD)

- Poderá solicitar relatórios de risco à privacidade sempre que julgar necessário.
- Ao encontrar qualquer irregularidade, tem o poder de aplicar as multas cabíveis.

Como se Adequar

staylock

Esteira de dados

Todos os dados deverão ser tratados com transparência e as informações das tratativas seguirem conforme acordado com o dono do dado.

Dados sensíveis

Dados que possam identificar uma pessoa, sendo esses: religião, etnia, saúde, orientação sexual.

Dados anonimizados

Um dado anonimizado é um dado sensível que foi tratado para que suas informações não possam ser vinculadas ao seu titular original.

O que o seu cliente vê x não vê

staylock

- **Atendimento**
- **Seu Produto**
- **Mindset**

- **Segurança da Informação**
- **DLP**
- **FIM**
- **Reports**

- **Treinamentos**
- **Esteira de dados**
- **Firewall**
- **Controle**
- **Confidencialidade**

Esteja preparado

Tipos de Teste de Penetração

staylock

White Box
Todas as informações do cliente sobre a rede, servidores, banco de dados e sistemas que estão inclusos no escopo do teste de invasão, e demais informações de acesso aos mesmos, são fornecidas para que possam ser realizados testes extensivos e com mais abrangência.
Testes.

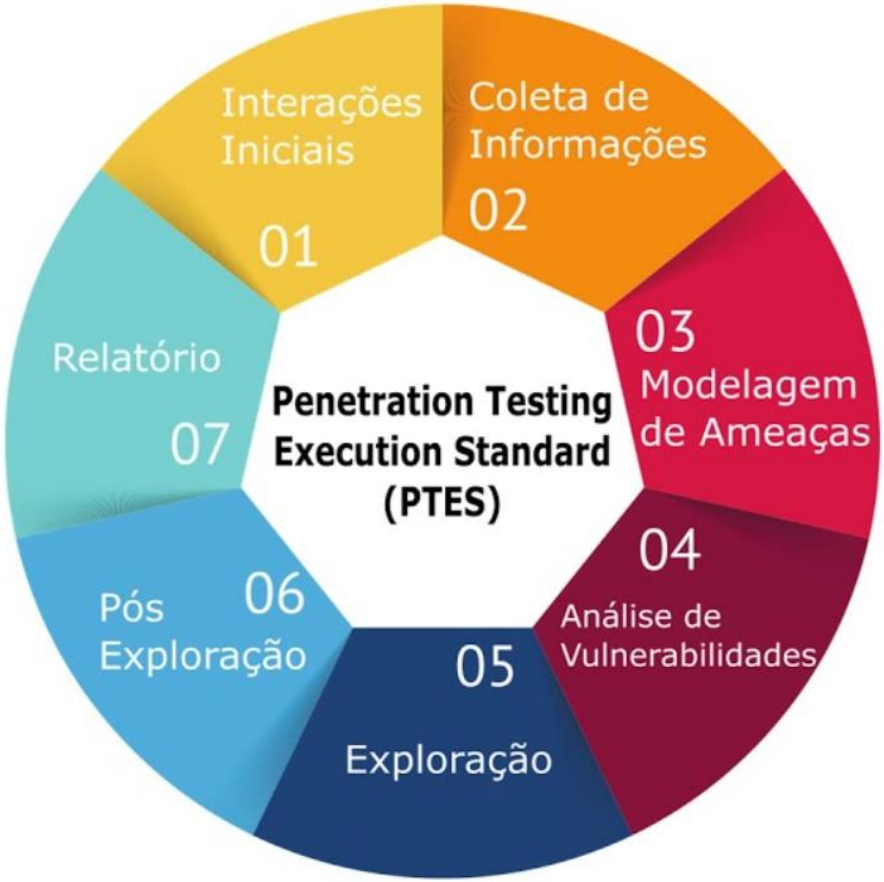
Grey Box
Esse tipo de análise pode ser considerado um mix dos anteriores, pois o analista de teste recebe alguma informação do cliente, como: dados da infraestrutura da rede ou acesso à determinado serviço web.

Black Box

É o tipo de análise mais próximo de um ataque externo, pois nenhuma informação vinda do cliente é fornecida ao analista de teste.

Sendo assim, todo e qualquer tipo de informação para a realização de um teste Black Box é adquirida através de técnicas específicas de hacking sobre os serviços disponíveis do alvo, identificando assim as vulnerabilidades e os possíveis danos causados por um ataque mal intencionado.

Fases do Teste de Penetração



Quando de ser feito o Teste de Penetração

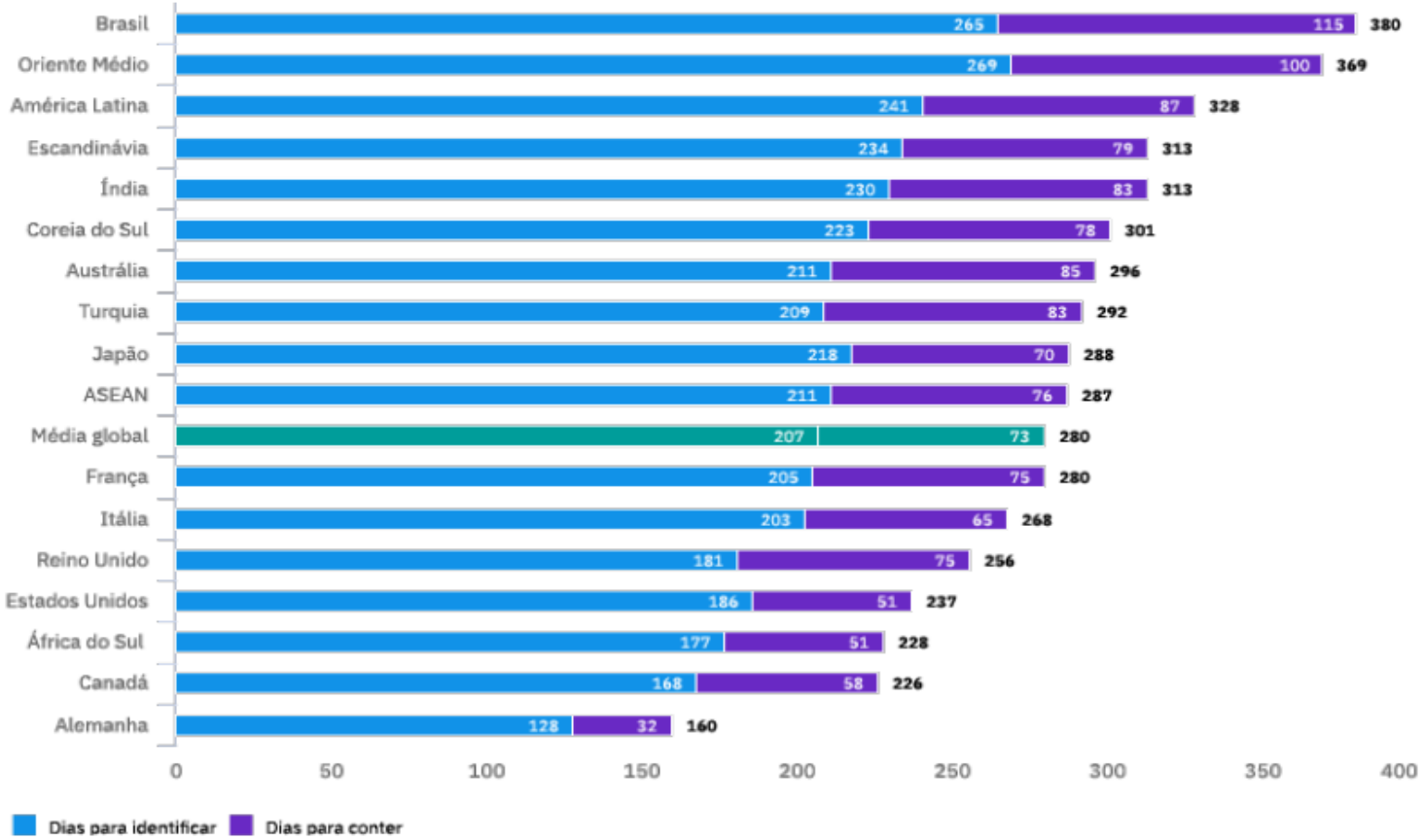
staylock

A realização deste tipo de teste deve ser frequente, dentro de intervalos programados, ou sempre que ocorrerem mudanças drásticas no ambiente físico ou lógico da rede. Pode parecer exagero, mas não é, pois as constantes mudanças na área de tecnologia, com novos recursos, novas ferramentas e novas soluções apresentadas dentro de um intervalo de tempo cada vez menor, trazem consigo inúmeros riscos, que podem ir desde vulnerabilidades não detectadas ou não previstas nos sistemas, até a adaptação de uso e pouco conhecimento das pessoas na operação do novo recurso. Somado a isso, temos uma constante evolução de ameaças provenientes de pessoas mal intencionadas que encontram nestas brechas oportunidades para obter algum tipo de vantagem, especialmente financeira.

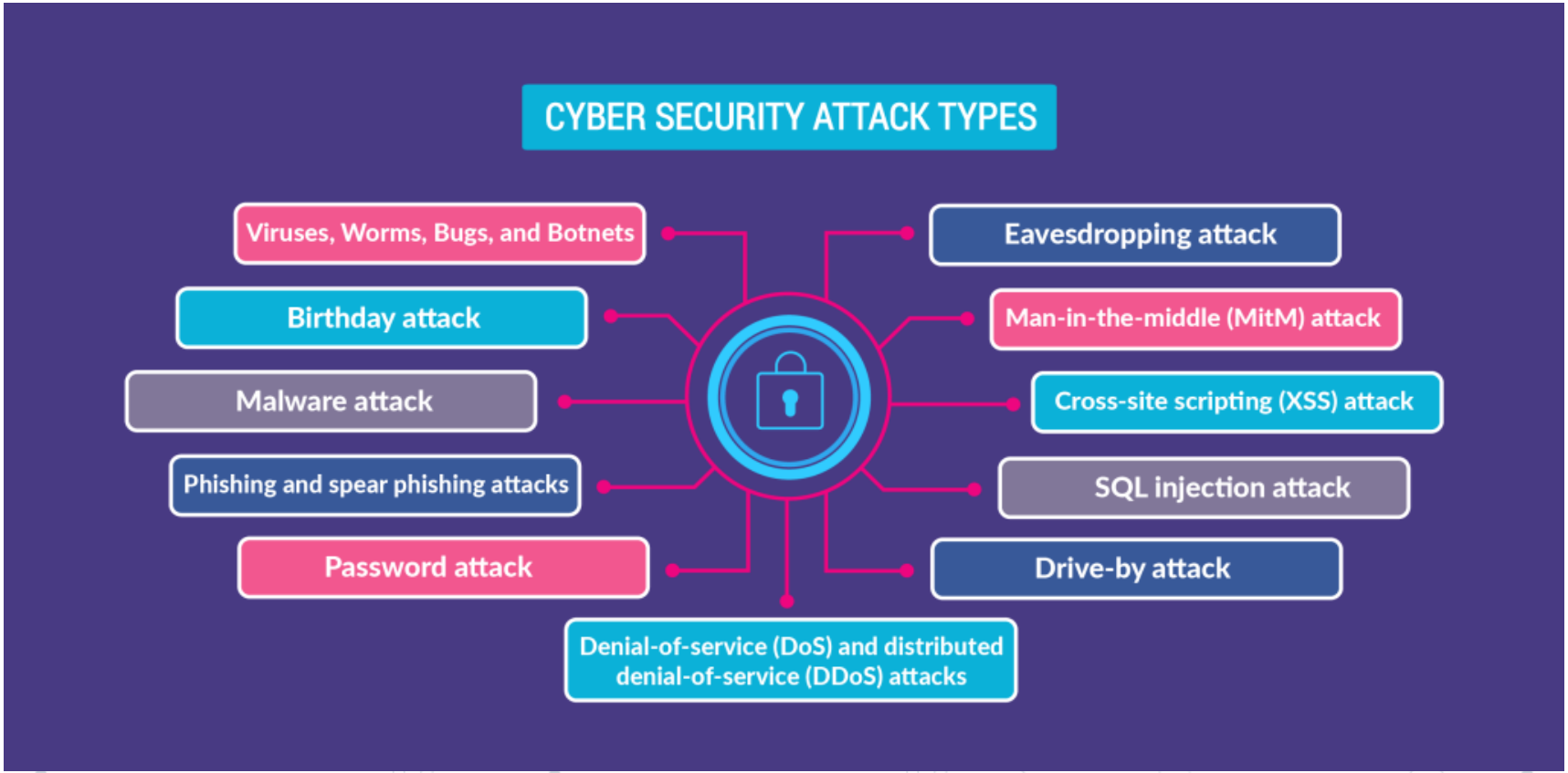
Algumas metodologias informam em seus requisitos com que frequência devem ser realizados os testes. Como exemplo, temos as empresas ligadas ao setor de Cartões de Crédito, que coletam, processam, armazenam e/ou transmitem informações destes cartões, obrigadas a adotar a norma PCI-DSS, que exige da organização a realização de testes de penetração anualmente e varreduras de vulnerabilidades trimestrais ou quando há mudanças no ambiente de rede.

Tempo médio para identificar e conter um vazamento de dados por país ou região

Medido em dias



Do que estamos te protegendo




Login:
Password:


staylock

Obrigado!

Perguntas?

Você pode me encontrar:

luis.magalhaes@staylocksec.com