INSPIRING A SAFE AND SECURE CYBER WORLD.

Tendências em Gestão de Riscos para Aplicações Web e Mobile

Anderson Dadario, CISSP, CSSLP

Site: https://dadario.com.br

Twitter: @andersonmvd

Quem sou eu?

Anderson Dadario, CISSP, CSSLP

Instrutor Oficial da (ISC)2

Empresas Anteriores:

Mondido (Sueca), Walmart E-Commerce, KPMG

Posto frequentemente no meu blog sobre segurança para aplicações web.

Todos temos algo a proteger

- Informação;
- Reputação;
- Status de conformidade;
- E o emprego também...

Como estamos protegendo estes ativos?

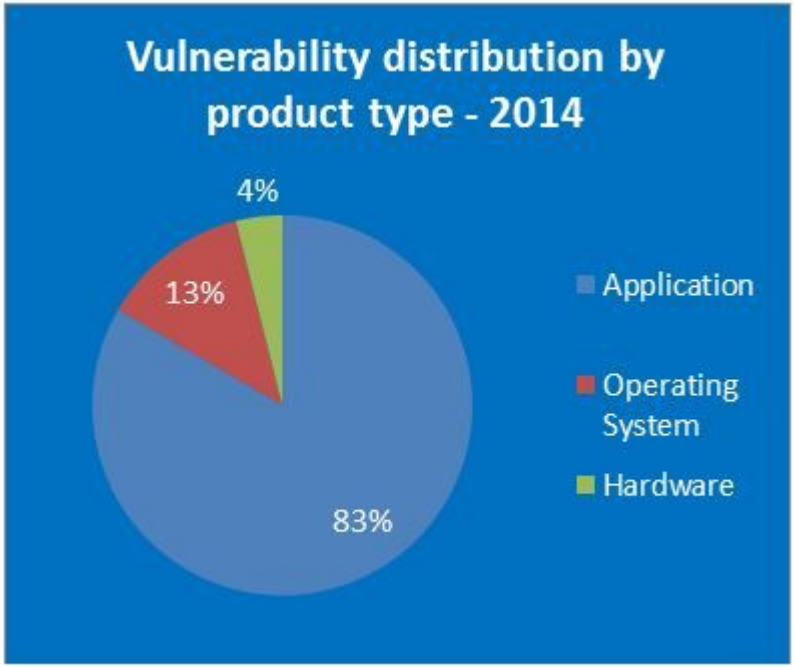
- Firewall layer 3?
- Proxy reverso?
- *Intrusion Detection System* (IDS) ?
- *Intrusion Prevention System* (IPS) ?
- Time de segurança de plantão 24/7?
- Política de segurança da informação?
- Bloqueio às entradas USB nos computadores?
- Antivírus?
- Pentest?

Assim não dá

Os itens anteriores podem ajudar sim, mas se é tudo que temos, nossa proteção é bem fraca.

Aplicações são o alvo #1

- Fonte: http://nvd.nist.gov/



+ Relacionados à Segurança de Aplicação

- Firewall layer 3?
- **Proxy reverso?**
- *Intrusion Detection System* (IDS) ?
- *Intrusion Prevention System* (IPS) ?
- Time de segurança de plantão 24/7?
- Política rígida de segurança da informação?
- Bloqueio às entradas USB nos computadores?
- Antivírus?
- **Pentest?**

Uma nota

- Google e Facebook já gastaram milhões de dólares pagando pesquisadores de segurança; Acham mesmo que um *Web Application Firewall* (WAF) poderia evitar tantas falhas?;

- Se essas empresas com pessoas super inteligentes produzem código com tantas falhas, o que dizer da empresa que você trabalha?

Cenário Global

Sim, adolescentes provavelmente conseguem comprometer a sua empresa sem grandes esforços.

Nos países mais desenvolvidos o cenário pode ser melhor, mas não está muito diferente. Veja se vocês se identificam:

Afirmações Familiares?

Anderson Dadario likes this 9d

Andrew Case
Volatility Core Developer

A few infosec truths that most companies miss:

- Pentests only give you a narrow view into how attacks *might* occur

- Real attacks have 0 scope & time restrictions

- Application whitelisting will never stop a real attacker

- Encrypted databases are useless against real attackers

- Enterprises are impossible to secure if every web browser is allowed to render ads & has Flash installed

- Blocking USBs is useless if employees can access Gmail

- If you can't stop ransomware then stopping worrying about APT

- If you aren't MITM'ing SSL then you don't have a DLP program show less

Unlike · Comment · Share · 331 33

Essa lista está incompleta

Por exemplo “proteção de perímetro” não existe mais.

Com o Bring Your Own Everything, dados são salvos no Dropbox, dados de usuários vão para o serviço de email marketing na nuvem e muito mais.

O que fazer então?

Proteger segurança em todas as vertentes, mas lembrar que aplicação é o alvo #1.

Para proteger aplicação, o time de segurança precisa conversar com o de desenvolvimento.

E essa conversa requer conhecimento que nenhuma ferramenta consegue prover por completo.

Crie conhecimento em comum

Desenvolvedor não sabe proteger a senha armazenada. Ele não tem senso comum?

Senso comum requer **Conhecimento em comum** e Conhecimento em comum requer **Treinamento**.

Segurança precisa de capacitação primeiro para depois capacitar outras áreas.

Por fim

Com conhecimento, segurança pode:

- Entender como adicionar segurança em todo o ciclo de desenvolvimento do software;
- Falar a mesma língua do desenvolvedor;
- Proteger os ativos que tem que ser protegidos.

Presente para poucos e Futuro

- Segurança integrada com o Build Pipeline;
- Desenvolvimento in-house de algumas aplicações de segurança, e.g., para resposta a incidentes;
- Cultura de Segurança da Informação disseminada entre todos os colaboradores;
- *Threat Hunting*: busca ativa por ameaças.
- Inteligência Artificial aplicada à S.I.;

Obrigado

Anderson Dadario, CISSP, CSSLP
Site/Blog: https://dadario.com.br
Twitter: @andersonmvd