PENSE COMO UM CIBERCRIMINOSO

Durante as operações cotidianas das empresas, cibercriminosos estão sempre procurando maneiras de invadir, explorar falhas e roubar informações.

Para se proteger, você precisa pensar como eles **para encontrar os diferentes vetores que podem ser explorados nos seus sistemas.**

6 ASPECTOS EXPLORADOS PELOS CIBERCRIMINOSOS

1 Roubo de equipamentos

Ameaça

Hackers roubam dados sensíveis.

80% do custo com o roubo de laptop está relacionado ao vazamento de dados sensíveis[1]

Mitigação

Criptografar todos os dispositivos e utilizar uma ferramenta de rastreamento para manter um inventário atualizado.

2 Falta de conscientização dos usuários

Uso de senhas frágeis e ataques de phishing.

85% das empresas já sofreram um ataque de phishing[2]

Mitigação

Fazer treinamentos e/ou campanhas de conscientização dos usuários.

3 Antivírus desatualizado

Novas variantes de vírus chegam diariamente.

390K novos códigos maliciosos são construídos diariamente.[3]

Mitigação

Mantenha o antivírus e vacinas atualizados, e use verificações heurísticas e de análise comportamental.

4 Software desatualizado

Software desatualizados podem estar vulneráveis a ataques automatizados.

APENAS **25%** dos usuários Microsoft® Windows® possuem completamente as correções aplicadas.[4]

Mitigação

Utilize uma ferramenta de gerenciamento de patches para manter os sistemas atualizados.

5 Websites maliciosos

Downloads automáticos ou acesso a sites de phishing que roubam credenciais de acesso.

195K domínios únicos foram usados para ataques de phishing em 2016.[5]

Mitigação

Implemente uma solução de filtro de conteúdo para não permitir que os usuários acessem sites de má reputação ou proibidos.

6 Ausência de monitoramento

Ataques, na maioria das vezes, passam por despercebidos.

205 DIAS Tempo médio que uma organização leva para descobrir que foi invadida.[6]

Mitigação

Implemente um sistema de monitoramento eficiente (SIEM), onde seja possível correlacionar os logs dos ativos, comportamentos anômalos e tentativas de acesso não autorizado.

Este Infográfico é uma tradução do original desenvolvido e disponibilizado pela empresa solarwinds - www.solarwinds.com

A solarwinds desde a sua fundação, em 1999, tem como missão fornecer produtos desenvolvidos especificamente para tornar os trabalhos mais fáceis para profissionais de TI, MSPs e profissionais da DevOps.

A 3Elos - www.3elos.com.br - é uma empresa brasileira de Segurança da Informação, visite-nos!

Notas:

1 Mobile Device Security: Startling Statistics on Data Loss and Data Breaches, ChannelPro Network. http://breachlevelindex.com/assets/Breach-Level-Index-Report-2016-Gemalto.pdf (accessed July 2017).
2 Phishing by the Numbers: Must-Know Phishing Statistics, 2016, Barkly. https://blog.barkly.com/phishing-statistics-2016 (accessed July 2017).
3 https://www.av-test.org/en/statistics/malware/ (accessed July 2017).
4 The 2016 Duo Trusted Access Report, Duo Security. https://duo.com/assets/ebooks/duo-trusted-access-report.pdf (accessed July 2017).
5 Domain Use and Trends. APWG. https://apwg.org//resources/apwg-reports/domain-use-and-trends (accessed July 2017).
6 M-Trends 2015: A View from the Front Lines, Mandiant. https://www2.fireeye.com/WEB-2015-MNDT-RPT-M-Trends-2015_LP.html (accessed July 2017).