PUBLICIDADE

claranet

# A importância dos testes de cibersegurança

**A procura proativa de vulnerabilidades nos sistemas de TI das organizações tornou-se crucial para responder às ciberameaças cada vez mais complexas e globais. Mas nem todos os testes de segurança são iguais.**

**ANTÓNIO RIBEIRO**
**Cybersecurity Manager**
Claranet Portugal

**O Pen testing fornece uma camada de informação mais completa e profunda ao nível da segurança dos sistemas de TI e conta com uma componente humana na análise efetuada, que possui um papel importante na procura, identificação e exploração das vulnerabilidades encontradas.**

Imagine uma organização que lança uma App mas descura totalmente as questões de segurança durante a sua criação, lançando-a para o mercado ignorando que possui "portas de entrada" que os cibercriminosos poderão facilmente explorar; imagine agora essa mesma App a ser usada por milhares – ou dezenas de milhares – de utilizadores, que desconhecem as vulnerabilidades graves de segurança dessa aplicação e, por isso mesmo, colocam em risco os dispositivos e os sistemas da sua organização cada vez que a usam.

Este cenário, aparentemente exagerado e potencialmente catastrófico, não está muito longe da realidade de muitas organizações que desenvolvem aplicações sem contemplar a segurança do seu produto. E de muitas empresas que ignoram a importância de executar testes proativos de segurança nos seus sistemas de TI, deixando-os vulneráveis a vários tipos de ataques.

A verdade é que a complexidade cada vez maior dos ataques de cibersegurança e o aumento do perímetro de ataque dos cibercriminosos – gerado por mais pessoas em trabalho remoto e pelo aumento da mobilidade dos colaboradores –, tornou necessário a realização frequente de testes de segurança aos sistemas de forma proativa. Estes devem abranger tanto as organizações que disponibilizam ferramentas aos seus utilizadores e a outras empresas, como as organizações que simplesmente recorrem a apps de terceiros para assegurar as suas operações normais.

As soluções mais comuns para evitar estes riscos - testes de Vulnerability Assessment e os chamados Pen testing (Penetration testing) - estão longe de ser novas, mas são cada vez mais cruciais: os primeiros avaliam o grau básico de vulnerabilidade dos sistemas numa organização; os segundos exploram de forma mais profunda essas vulnerabilidades e o possível efeito que podem ter na continuidade dos negócios.

## Qual o teste de segurança mais eficaz?

Antes conhecer o que cada tipo de análise de segurança pode fornecer às empresas, é importante perceber que deverão ser sempre executados por um fornecedor de serviços de segurança com know-how consolidado nestes testes. Caso contrário, os sistemas irão continuar vulneráveis e, mais grave, transmitindo uma falsa sensação de segurança a quem os usa e administra.

**Vulnerability Assessment** – É um tipo de teste básico mas importante, que as organizações deverão solicitar com frequência, e que rapidamente poderá trazer resultados.

Em termos práticos é feito com uma ferramenta específica que procura vulnerabilidades conhecidas no software e no hardware de uma organização (servidores Web, portas, dispositivos, ferramentas de produtividade, entre outros), identificando problemas conhecidos e avaliando se os patchs de segurança estão atualizados.

Apesar de ser um ponto de partida válido para se perceber o nível de vulnerabilidade de um sistema, utiliza ferramentas standard e incide em vulnerabilidades conhecidas. Isto significa que um Vulnerability Assessment não explora as vulnerabilidades que deteta nem fornece indicação se a vulnerabilidade é, ou não, explorável – e de que forma -, obrigando assim a um nível mais profundo de análise.

**Pen testing** – Fornece uma camada de informação mais completa e profunda ao nível da segurança dos sistemas de TI e conta com uma componente humana na análise efetuada, que possui um papel importante na procura, identificação e exploração das vulnerabilidades encontradas.

É um teste mais complexo e dispendioso, mas que garante uma relação custo-benefício significativamente superior ao teste de Vulnerability Assessment – que também integra, embora sirva como ponto de partida para criar um perfil da empresa analisada.

A partir daqui, o teste pressupõe um leque de procedimentos que cruzam a procura e deteção automática de vulnerabilidades com a análise humana dos resultados, incluindo avaliação de padrões, histórico, informação detalhada sobre a intervenção e recomendações para solucionar as vulnerabilidades encontradas.

O Pen testing pode ser feito com vários níveis de autonomia por parte do Security Service Provider – tendo como base informação mais ou menos completa fornecida pelo próprio cliente, ou atuando "a partir do zero", sem qualquer tipo de informação prévia.

## A importância de testar

Qualquer organização que desenvolva software terá todas as vantagens em contemplar a segurança desde o início do respetivo projeto; assim como qualquer empresa que utilize essas soluções deverá submeter os seus sistemas a testes de segurança frequentes. Idealmente os testes deverão ser contínuos ou, pelo menos, anualmente e sempre que existam alterações significativas na infraestrutura usada.

Qualquer que seja a periodicidade, as preocupações com a segurança dos sistemas de TI deverão ser encaradas como um investimento e não como uma despesa, e fazer parte dos projetos desde o seu início. Caso contrário, os esforços para resolver qualquer problema de segurança a posteriori, poderão ter um custo muito superior.