Certificação Hacker-Secured

"O certificado que protege o utilizador contra o roubo de dados pessoais e de fraude na utilização de cartões de crédito."

A segurança da infraestrutura dos sites é uma questão particularmente sensível, à qual não se pode ficar indiferente, até porque por vezes as vulnerabilidades podem inadvertidamente serem introduzidas pelos administradores quando executam alterações nas políticas do firewall, criando vulnerabilidades para hackers, worms ou cavalos de Tróia. A única solução é vigiar proactivamente a rede por forma a conhecer as ameaças e implementar as medidas necessárias antes que os atacantes se aproveitem delas. Para além deste aspecto é importante também transmitir ao utilizador final que poderá navegar no site com segurança.
Foi a pensar nestes aspectos que a MarketWare lançou o certificado digital Hacker Secured. Este foi idealizado e concebido não só com o intuito de facultar mecanismos que permitissem aos administradores das redes vigiarem proactivamente e preventivamente toda a sua rede, como também, transmitir confiança e garantia aos utilizadores, que estão protegidos contra o roubo de dados pessoais e de fraude na utilização de cartões de crédito.
Desta forma, o Hacker-Secured, validará através de auditorias diárias, semanais ou mensais aos sites, com intuito de passar nos testes de segurança do FBI/SANS. Sempre que o site respeitar os requisitos mínimos impostos pelas melhores práticas de segurança, será atribuído o certificado Hacker-Secured. Perante esta situação o utilizador terá a garantia que em 99% dos casos não haverá intrusões. 

Descrição das Auditorias As auditorias diárias serão realizadas em três fases: Scan de detecção de portos vulneráveis, testes de penetração de rede, teste de análise completa das aplicações web. Com esta auditoria é possível executar de forma contínua e pró-activa a monitorização da segurança dos sistemas, reduzindo significativamente o tempo de investigação e o tempo de descoberta das vulnerabilidades existentes. Realidade que contribuiu para uma resolução mais rápida dos problemas caso esses ocorram e a disponibilização do factor de confiança ao utilizador final.

1ª Fase – Scan de Detecção de Portos VulneráveisA primeira fase consiste na realização de um scan que visa a análise global da rede a fim de detectar os Portos TCP e UDP que estão abertos e susceptíveis a ataques.

2ª Fase – Testes de Penetração de Rede Numa segunda fase serão analisados todos os Portos abertos para determinar exactamente os serviços que estão a correr, incluindo o tipo e a versão específica. Pretende-se analisar em detalhe todas as vulnerabilidades de todos os

serviços, como o DNS, SMTP, SSH, FTP, HTTP, e SNMP, utilizando métodos de assinatura ou de avaliação de resposta. Serão ainda utilizadas técnicas de detecção de intrusão e penetração de firewalls, a fim de garantir uma análise com a maior precisão.

3ª Fase – Teste de Análise Completa das Aplicações Web Nesta terceira fase pretende-se analisar o nível de aplicações web.

De acordo com a Gartner, 70% das quebras de segurança surgem a este nível. Aqui todos os serviços HTTP e domínios serão testados de maneira a identificar os módulos potencialmente perigosos, parâmetros de configuração, CGIs e outros scripts. O site será percorrido a fim de encontrar formulários que são utilizados para identificar vulnerabilidades, tais como, revelação de código e cross-site scripting. Análises genéricas e específicas de software serão executadas para detectar vulnerabilidades de configuração que estejam relacionadas com erros no código.