Não sei

Alexandre Yuji Kajihara

2017

1 Introdução

O ataque de *zero-day* é um ataque cibernético que explora uma vulnerabilidade que não foi divulgada publicamente, e com isso não há defesa contra esse ataque, consequentemente não o *software* não pode ser corrigido e os antivírus não detectam devido a não ter assinatura [**?**]. Alguns tipos de ataques zero-day, permanecem desconhecidos até por 2,5 anos [**?**]. Quando as vulnerabilidades são descobertas ou são descritas em aviso público, os fornecedores de *software* lançam atualizações [**?**]. Além do que, um dos problemas é que depois de se lançados as atualizações, os usuários atrasam suas atualizações [**?**]. O preço das bulnerabilidades como a de plataformas, (Windows, iOS, principais navegadores) pode execeder mais de 100.000 dólares, dependendo da complexidade [**?**]. Atualmente, as explorações são incorporadas em arquivos não executáveis, como *.pdf, *.doc, *.xlsx [**?**]. Usuários que utilizam o antivírus podem ter mais cuidados com a segurança de seus computadores, e podem ser menos expostos aos ataques [**?**]. Ataques *zero-day* são ataques chamados de ataques específicos já que que visam um número limitado de organizções que possuem informações confidenciais que podem ser roubadas [**?**]. Além disso, os fornecedores de software dão preferência de corrigir vulnerabilidades que foram divulgadas ou estão prestes a declarar [**?**].

Os defensores da redes estão sempre a dois passos de trás dos invasores, já que devem se defender de falhas que não foram descobertas ou foram descobertas por atacantes [**?**]. A única vantagem é que os defensores sabem a localização provável e gravidade dessse ataque [**?**]. Uma maneira de se prevenir seria implementar sensores ou defesas cibernéticas, como *firewall* [**?**].

Os ataques de zero-day contra aplicações Web aumentaram [**?**]. Além disso, existem testes como o de *Web Application Penetration Testing* (WAPT), em que se as suas organizações não testam e não protegem de maneira adequadamente, terá seu aplicativo comprometido, ter dados roubados e danificar o desempenho da sua aplicação [**?**]. È díficil de prevenir, porque a informação só estará disponível quando o ataque tiver sido concluído [**?**]. Essas vulnerabilidades são muito desejadas por agências convernamentais, cibercriminosos e empresas de software [**?**]. Essas falhas podem ser em software ou sites [**?**]. As maneira para evitar os ataques *zero-day* seria utilizando Host Intrusion Protected Software (HIPS), em que não se depende de assinaturas, já que há um monitoramente das

atividades da máquina. Usar um bom antivírus, protegendo de ataques conhecidos e desconhecidos. Atualizar suas aplicações, em que se houver notificação de atualização de *software* atualize. Usar navegadores somente atualizados já que todos os navegadores empurram atualizações periódicas [**?**].

Referências

[1] Angelo Ciampa, Corrado Aaron Visaggio, and Massimiliano Di Penta. A heuristic-based approach for detecting SQL-injection vulnerabilities in web applications. In *2010 ICSE Workshop on Software Engineering for Secure Systems - SESS*. ACM, 2010.

[2] Marco Vieira, Nuno Antunes, and Henrique Madeira. Using web security scanners to detect vulnerabilities in web services. In *2009 IEEE/IFIP International Conference on Dependable Systems & Networks*. IEEE, jun 2009.