|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Clientes | Métodos e Procedimentos | Objetivo | Justificativa | Referencial bibliográfico |
|  |  | Prevenir ataques do tipo *zero-day,* através de dados presentes no NVD (*National Vulnerability Database*), que são mantidos pelo NIST (*National Institute of Standards and Technology*). Os dados presentes nesse site contém as vulnerabilidades, por fornecedores, anos e categorias. | Os ataques do tipo *zero-day*, são imprevisíveis. Isso devido porque essas falhas que permitem os ataques elas não foram divulgadas publicamente, e com isso o *software* não pode ser corrigido e os antivírus não conseguem detectar o ataque através da assinatura baseada em assinatura. Como as falhas podem ser divulgadas ou não prever elas é uma maneira te impedir que aplicações fiquem vulneráveis a ataques. | BILGE, LEYLA; DUMITRAS, TUDOR. Before we knew it: an empirical study of zero-day attacks in the real world (DOI:10.1145/2382196.2382284);  EGELMAN, SERGE; HERLEY, CORMAC; C. V. OORSCHOT, PAUL. Markets for Zero-Day Exploits: Ethics and Implications (DOI: 10.1145/2535813.2535818);  FOTI, PAOLO; ARMIN, JART; CREMONINI, MARCO. 0-Day Vulnerabilities and Cybercrime (DOI: 10.1109/ARES.2015.55);  KUMAR, PRATAP; K. SETH, RAVI. A Review on 0-day Vulnerability Testing in Web Application (DOI: 10.1145/2905055.2905357);  LAST, DAVI; Forecasting Zero-Day Vulnerabilities (DOI: 10.1145/2897795.2897813);  LUO, TIANYNUE; NI, CHEN; HAN, QING; YANG, MUTIAN; WU, JINGZHENG; WU, YANJUN. POSTER: PatchGen: Towards Automated Patch Detection and Generation for 1-Day Vulnerabilities (DOI: 10.1145/2810103.2810122). |
| Recursos necessários | Capítulos e seções |
|  |  |