

DATALAN

INOVÁCIE PRE ŽIVOT



ZIŠŤOVANIE ZRANITEĽNOSTÍ A PENETRAČNÉ TESTOVANIE

Otestujte sa ako hacker



Venujete dostatočnú pozornosť bezpečnosti informačných systémov?

Chcete vedieť, ako ste na tom s bezpečnosťou IT systémov vo Vašej firme? Potrebujete sa na svoju bezpečnosť pozrieť z pohľadu hackerov? Chcete mať prehľad o nepodporovaných a neaktualizovaných systémoch vo svojej sieti? Ak áno, odborníci z DATALANu otestujú, na akej úrovni je bezpečnosť vo vašej firme a či nie ste vystavení možnému riziku.

Zisťovanie zraniteľností a penetračné testy predstavujú testovanie bezpečnosti informačného systému prostredníctvom nástrojov a postupov, ktoré sú bežne využívané hackermi cielene napádajúcimi dostupné informačné systémy.

Nepodporované a neaktualizované systémy v sieti predstavujú potenciálne riziko pre bezpečnosť. Zraniteľnosti, ktoré sa nachádzajú v týchto systémoch, môžu byť využité rôznymi útočníkmi na prienik do siete, kedy môže dôjsť k odcudzeniu dôverných informácií alebo k spôsobeniu iných škôd v sieti.

Komu je riešenie určené

Služba „Zisťovanie zraniteľností a penetračné testovanie“ je určená pre všetky typy organizácií nezávisle od veľkosti, komplexnosti alebo jej obchodného zamerania. Je vhodná pre každú firmu, ktorej podnikanie a beh je závislý na IT systémoch a na ich bezpečnosti.

Testovanie z pohľadu útočníka

Testovanie môže byť vykonávané buď z pohľadu vonkajšieho alebo interného útočníka.

V prípade odhaľovania vonkajších zraniteľností sú na známe zraniteľnosti kontrolované služby zákazníka, ktoré sú prístupné na jeho verejných IP adresách z Internetu. Ide o kontrolu úrovne zabezpečenia elektronických služieb, ktoré sú poskytované v prostredí internetu.

Pomocou interného zisťovania zraniteľností sa detegujú a identifikujú vnútorné zraniteľnosti, ktoré sú útočníkom prístupné, ak sa nachádzajú priamo vo vnútornej sieti zákazníka alebo sa do tejto siete dokážu dostať vzdialene po prekonaní perimetrových ochrán. Na vzdialený prístup do lokálnej siete postačuje aj kliknutie na nevinný phishing e-mail. Na vnútorných systémoch sú zisťované známe zraniteľnosti, chýbajúce aktualizácie a nepodporované verzie programov.

Testy sú vykonávané pomocou automatických nástrojov na zisťovanie zraniteľností. Následne sú nájdené zraniteľnosti podrobené manuálnemu testovaniu využitím rôznych exploitov. Ide o dodatočné potvrdenie nájdenej zraniteľnosti a o jej využitie na preniknutie do systému.

Okrem zraniteľností informačného systému sú počas testu preverené aj schopnosti bezpečnostných prvkov detegovať a zamedzovať pokusy o prienik do informačného systému.

Riešenie od DATALANu prináša

- Komplexná správa o stave bezpečnosti systémov vo firme spolu s návrhmi na nápravu
- Pri opakovanom testovaní je možné sledovať trend vývoja bezpečnosti systémov vo firme
- Splnenie legislatívnych požiadaviek na zisťovanie zraniteľností firemných systémov
- Pohľad na bezpečnosť systémov z pohľadu útočníka

Výhody nášho riešenia

- Komplexný prehľad o IT infraštruktúre z pohľadu bezpečnosti
- Odhalenie potenciálne nebezpečných a neaktualizovaných systémov v sieti
- Testy potrebné pre súlad so Zákonom o kybernetickej bezpečnosti a so Zákonom o informačných systémoch verejnej správy
- Podrobná záverečná správa spolu s navrhovanými opravnými opatreniami



Kontaktujte nás

DATALAN, a. s.
Einsteinova Business Center
Krasovského 14
851 01 Bratislava 5

Tel.: 02 502 577 77
Fax: 02 502 577 00
Email: info@datalan.sk

www.datalan.sk

DATALAN

INOVÁCIE PRE ŽIVOT