

EVIL EYE



Evil Eye on täyden palvelun penetraatiotestauspaketti, joka räätälöidään aina jokaisen asiakkaan yksilöllisten tarpeiden mukaan ja jolla saadaan turvallisesti testattua toimiiko organisaation puolustusstrategia vakavia tosielämän hyökkäyksiä vastaan. Evil Eye on tehty simuloimaan oikeita skenaarioita.



Evil Eyessa etsitään pieniä tiedonjyviä, yhdistellään niitä ja haetaan parhaat hyökkäyskeinot testausta varten. Testauspaketti räätälöidään aina asiakkaan tarpeiden pohjalta. Toisin kuin penetraatiotestauksissa yleensä, valtaosa Evil Eyen testauksesta tehdään käsin. Käytämme penetraatiotestauksessa automaattisia työkaluja lähes ainoastaan pohjatiedon hankkimiseen. Käsin tehty työ on avain tehokkaampaan penetraatiotestaukseen ja realistisiin tuloksiin, jolloin testauksen laajuudesta ja laadusta voidaan varmistua.

Testausmenetelmistä ja määristä riippumatta testauksen tärkein anti on purkupalaveri, jossa tulokset ja havainnot käydään kohta kohdalta läpi asiakkaan kanssa. Samalla esitetään testauksen tuloksena tehdyt parannusehdotukset asiakkaan organisaatiosta ja infrastruktuurista löytyneille puutteille. Teemme myös räätälöidyt korjausehdotukset, joiden avulla havaitut puutteet saadaan korjattua kustannustehokkaasti.

Evil Eye -testauksessa hyödynnetään muun muassa tiedustelua, phishingiä, social engineeringiä ja kohdistettuja hyökkäyksiä. Suurimmalla osalla ei ole mitään hienoa nimeä, vaan käytämme kaikkia menetelmiä joita aidotkin hyökkääjät käyttävät. Työ suunnitellaan luovasti, sillä myöskään osaavat hyökkääjät eivät käytä toiminnassaan automaattityökaluja.

Verkkorikollisuus on muuttunut yhä enemmän rikollisen hyödyn tavoittelemiseksi. Tämän takia rikolliset kehittävät aina vain vaikeammin havaittavia hyökkäystapoja ja ovat entistä luovempia. Nykyään hyväksikäytetään muitakin kuin valtavirran ohjelmistoja ja tämä tuo lisää paineita haavoittuvuuksien hallintaan.

Selvitämme penetraatiotestauksessa kuinka houkuttelevana hyökkääjät pitävät yritystä. Testauksen yhteydessä kartoitamme asiakkaan tietoverkon infrastruktuurin mahdollisimman täydellisesti eri tiedonkeruumenetelmiä käyttäen. Näin saadaan aikaan realistinen kuva siitä, millaisena kohteena ulkopuoliset hyökkääjät asiakkaan näkevät.

Evil Eye -testauksen yhteydessä testataan myös kohdennettuihin hyökkäyksiin liittyviä skenaarioita. Sen kohdennetut hyökkäykset hyödyntävät avointa tiedustelutietoa, kuitenkin täysin vaaraa ja vahinkoa aiheuttamatta. Mitä tahansa osa-aluetta yrityksen tietoturvasuojassa voidaan testata. Evil Eyen avulla voidaan testata esimerkiksi henkilöstöä ja yrityksen tietoturvasuojaprosessit alusta loppuun. Samalla testaamme yrityksen tietoturvasuojauksen riittävyttä.



Tekemämme testaukset ovat tosielämän hyökkäysten tavoin suunniteltu herättämään mahdollisimman vähän huomiota. Tällöin saadaan samalla testattua mahdollisten IDS-järjestelmien toiminta ja herkkyys. Testaus voidaan tehdä myös kahdessa vaiheessa. Ensin suoritetaan testaus ilman asiakkaan infrastruktuurista saatua tietoa, jolloin nähdään tilanne ulkopuolisen hyökkääjän silmin. Tämän jälkeen voidaan suorittaa toinen testaus, jossa hyödynnetään asiakkaalta saatua tietoa infrastruktuurista ja suojausjärjestelmistä. Näin testauksen kattavuus ja tehokkuus saadaan maksimoitua.

Penetraatiotestaus sopii parhaiten yrityksille, joilla on useampia työntekijöitä. Kartoitamme myös mahdollisuuksien mukaan henkilöstön toimenkuvat ja toimintatavat, joita voidaan hyödyntää hyökkäykestauksessa. Varsinkin yritykset, joilla on julkisessa verkossa palveluita tai jotka käsittelevät luottamuksellista asiakastietoa tai rahaa, ovat harmittavan usein kohdennettujen hyökkäysten kohteena.

Penetraatiotestaus on hyvä toistaa vuosittain, jotta nähdään ovatko tehdyt muutokset ja koulutukset vaikuttaneet toivotulla tavalla ja vastaavatko ne vielä haasteisiin, joita jatkuvasti muuttuvat uhkakuvat aiheuttavat.



www.fitsec.com

info@fitsec.com