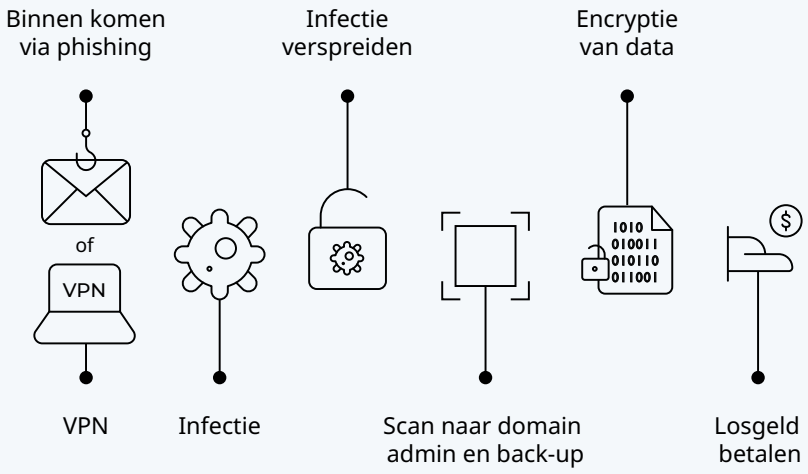
Ransomware
kwetsbaarheid-analyse

Met deze analyse wordt de gehele IT-omgeving van een organisatie onder de loep genomen door een ethisch hacker. Net als een kwaadwillende hacker trachten wij tot het hoogste beheerniveau te komen van een IT-omgeving.

Technische interviews zijn integraal onderdeel van het onderzoek; dit geeft ons inzicht in de opbouw van de infrastructuur.

Ook onderzoeken wij of we bij de back-ups kunnen komen en of deze veilig zijn bij een ransomware aanval. Al onze tests zijn gebaseerd op daad-werkelijke gebeurde ransomware incidenten.
De ransomware kwetsbaarheid-analyse wordt uitgewerkt in een rapportage met alle bevindingen en aanbevelingen. Iedere stap van de kwaadwillende hacker wordt gesimuleerd en onderzocht.

Anatomie van ransomware aanval



Technische stappen tijdens het Ransomware kwetsbaarheid-analyse proces

Kick-off

Voor aanvang van de kwetsbaarheid-analyse houden we een kick-off bijeenkomst. Bij deze kick-off wordt met de security officer en andere betrokken stake-holders nagegaan of alle benodigdheden voor de test aanwezig zijn (contactgegevens, adressen/URL's, toegang tot locaties, etc.). Het doel is dat alles klaar is om de uitvoer te kunnen starten.

Phishingtest

Op een afgesproken dag versturen we een phishingmail aan alle medewerkers, en meten de aantallen kliks en logins op een nep-website. Op een online dashboard worden de resultaten bijgehouden en is inzichtelijk welk besturingssysteem en welke browser de medewerkers gebruiken. Ook wordt de lengte van de wacht-woorden geregistreerd.

Publieke infrastructuurtest

Hierbij brengen we in kaart hoe de infrastructuur van de klant eruitziet, die via het internet bereikbaar is en of deze kwetsbaarheden bevat. Denk hierbij aan websites, VPN-verbindingen, en publieke servers voor bijvoorbeeld bestandsuitwisseling.

Interne netwerktest

Hierbij simuleren we wat er gebeurt als een aanvaller toegang weet te verkrijgen tot de IT-omgeving, bijvoorbeeld door een laptop aan het netwerk aan te sluiten of door te verbinden met de Wifi. We gaan op zoek naar kwetsbaarheden of andere mogelijkheden om ons horizontaal door het netwerk te verplaatsen.

Fase 4

Windows-domeintest

Hierbij testen we met een geldig gebruikersaccount het perspectief van de insider. We proberen op diverse manieren om de netwerk rechten te verhogen en om toegang te krijgen tot de kroonjuwelen van de organisatie. Wanneer er controle verkregen is over het hele netwerk, trachten we de back-up voorziening te isoleren.

Fase 5

Workshop/interview

Met een aantal uitvoerende IT'ers uit de organisatie nemen we door welke kwetsbaarheden zouden kunnen bestaan in het geval van een ransomware aanval, bijvoorbeeld ten aanzien van de back-ups. De ervaring leert dat it-architecten en netwerkbeheerders een eigen interpretatie over de back-up procedure hebben. Door dit in kaart te brengen kan je de beveiliging verbeteren.

Rapportagefase

Na afloop van de test schrijven we ons rapport in concept. Het eerste concept wordt intern gereviewed door een Principal Consultant. Het concept-rapport bieden we aan voor een gezamenlijke review.

Definitieve oplevering

Na de gezamenlijke review en de feedback vanuit de klant maken we het rapport definitief. Het rapport wordt via een beveiligd portaal geleverd aan de klant.

CCV CYBER PENTEST

Keurmerk Pentesting:

Per 1 juli 2021 is het nieuwe keurmerk Pentesting van het CCV (Centrum voor Criminaliteitspreventie en Veiligheid) ingevoerd. HackDefense is hierop gecertificeerd en voert dit keurmerk voor al haar beveiligingstesten.

Meer informatie over dit keurmerk vindt u op https://hetccv.nl/keurmerken/expert/keurmerk-pentesten/

HackDefense BV
Zijlbaan 28
2352 BN Leiderdorp
The Netherlands
+31 (0)71 204 0101
info@hackdefense.com