Waarom wil men een penetratietest?

“Waarom vindt u dat er een pentest (penetratietest) nodig is op uw product?” Als we die vraag stellen aan klanten die ons benaderen, dan krijgen we verschillende antwoorden, zoals “ik wil er zeker van zijn dat mijn product veilig is” of “wij moeten dat doen vanwege de ISO-certificatie”.

De antwoorden geven vaak niet meteen prijs wat precies de achterliggende reden is voor een penetratietest. Laten we eens kijken naar antwoorden die door klanten het vaakst gegeven worden.

Gemoedsrust. “We hebben er alles aan gedaan om te zorgen dat de data aan onze kant veilig is opgeborgen, maar is dat gelukt?”

Imago. “Het imago van onze organisatie loopt ernstige schade op als we worden gehackt of wanneer ons product beveiligingsproblemen blijkt te hebben.”

Financiële risico’s. “We slaan gevoelige gegevens op. We lopen een groot financieel risico als die in gevaar komen.”

Certificatie. “We hebben een ISO27001 certificaat nodig en dat vereist de uitvoering van een penetrat
ietest op regelmatige basis.”

Vertrouwen. “Wanneer we software aanschaffen, willen we bevestigd zien dat die niet kwetsbaar is voor misbruik.” Hetzelfde geldt voor de leverancier van software: “ik wil mijn klanten laten weten (en aantonen) dat de software niet kwetsbaar is voor misbruik”.

Waarom willen we de achterliggende redenen weten van een verzoek om een pentest uit te voeren?

Het simpele antwoord is: omdat we moeten begrijpen welke risico’s precies moeten worden

afgedekt door middel van
een penetratietest. Om een nuttig testrapport op te kunnen stellen, moeten we weten waar de klant bang voor is.

Achter elk van de bovenstaande vijf categorieën gaat minimaal één risico schuil dat de klant feitelijk zorgen baart. Een voorbeeld: een klant is bang dat gebruikers het systeem manipuleren in hun voordeel (zoals het aanpassen van toetsresultaten door studenten in een studentvolgsysteem). Met die wetenschap kunnen we de pentest goed richten op dat specifieke risico. We brengen specifiekekwetsbaarheden dan in kaart en dragen daarmee bij aan het reduceren van de risico's.

Dit artikel is eerder in het Engels geschreven door Polteq consultant Martijn de Vrieze en verschenen op zijn website over technical software testing.