Wat is het verschil tussen Red Team en Blue Team cybersecurity?

SECURITY

Binnen het domein van cybersecurity en ethisch hacken zijn er verschillende soorten rollen te definiëren. Zo is er een onderscheid te maken tussen de bekende white hat hacker (ethisch hacker) en de black hat hacker (onethische hacker). Binnen de groep ethische hackers bestaan er ook verschillende rollen. Namelijk het ‘red’ team en het ‘blue’ team. Wat betekenen deze teams? Wat zijn de rollen van deze teams binnen cybersecurity en hoe zorgt het inschakelen van deze teams dat risico’s verkleind worden en de continuïteit wordt verhoogd? We lichten het graag toe in deze blog van Networking4all.

Red team vs blue team

Staat cybersecurity hoog op de agenda binnen uw organisatie dan heeft u vast wel eens gehoord van de offensieve en defensieve teams binnen cybersecurity. Het offensieve team, het red team, gaat in de aanval en probeert een doelwit te hacken. De defensieve kant, het blue team, probeert deze aanval te detecteren en verdedigt de systemen van het doelwit. Red team VS blue team dus.

Wat is het red team binnen cybersecurity?

Het red team zijn de cybersecurity specialisten die dus het doelwit proberen te hacken middels het uitbuiten van reeds bekende of onbekende kwetsbaarheden. Dit kunnen ethisch hackers zijn van bijvoorbeeld Networking4all die proberen doormiddel van een pentest kwetsbaarheden in de systemen van het doelwit te vinden. In scenario's waarin het red team tegen het blue team wordt ingezet kan er worden getest hoe security analisten in bijvoorbeeld het security operations center reageren op een aanval. De aanvallende gedachte van het red team vereist een set aan vaardigheden om real-time aanvalsscenario's zo nauwkeurig mogelijk na te bootsen:

Kennis over software en systemen: weet je hoe programma's, applicaties en systemen worden gebouwd, dan ben je beter in staat om mogelijke zwakke punten te identificeren.

Pentesten: een groot deel van de taak van het red team is het identificeren en proberen te misbruiken van kwetsbaarheden in een netwerk. Kortom: het ingaan van de aanval. Kennis van de juiste pentest tools en hoe deze ingezet kunnen worden is hierbij van belang.

Social engineering: de grootste kwetsbaarheid van een organisatie is vaak de mens in plaats van het netwerk. Social engineering technieken zoals phishing, vishing en de mystery guest kunnen soms de meest haalbare manier zijn om beveiligingsdefensies te omzeilen.

Dreigingsinformatie en reverse engineering: het kennen van de bestaande dreigingen en hoe deze uit te buiten is belangrijk voor een lid van het red team.

Creativiteit: het vinden van manieren om de defensie van het blauwe team te omzeilen vereist vaak het creëren van nieuwe en innovatieve vormen van cyberaanvallen. Creativiteit is een must!

Wat is de rol van het red team binnen cybersecurity?

In de meeste gevallen krijgt het red team een specifieke opdracht van de opdrachtgever. Een voorbeeld van een opdracht kan zijn: probeer toegang te krijgen tot onze salarisadministratie en/of onze klantgegevens. Hierin krijgt het red team afhankelijk van het scenario een bepaalde mate van vrijheid. Zo kan het red team dit doel proberen te behalen via enkel technische middelen, maar bijvoorbeeld ook door fysiek toegang proberen te krijgen tot locaties van de klant. Deze laatste

techniek is een vorm van social engineering. Door de vrijheid die het red team mogelijk kan krijgen kunnen nauwkeurig real-life aanvalsscenario's worden nagebootst.
Na het uitvoeren van een aanval voor een klant, wordt achteraf een uitgebreide rapportage opgeleverd. Hierin wordt inzichtelijk gemaakt wanneer welke aanvallen zijn uitgevoerd en wat het effect hiervan was.

Wat is het blue team binnen cybersecurity?

Het blue team zijn de verdedigende cybersecurity specialisten. Zij proberen op dagelijkse basis de cyberbeveiliging van één of meerdere organisaties te waarborgen en te verbeteren door middels verschillende soorten cybersecurity software activiteiten te analyseren, kwetsbaarheden en/of risico's te identificeren, deze op te lossen en vervolgens te monitoren of deze oplossingen effectief zijn.
Bij de grotere bedrijven wordt dit proces veelal vanuit een Security Operations Center (SOC) aangestuurd en uitgevoerd.

Wat is de rol van het blue team binnen cybersecurity?

Waar het red team vooral de aanval kiest is een belangrijke taak van het blue team dat zij een aanval van het red team zo snel mogelijk opmerken en tegengaan. Niet alleen als het gaat om een directe aanval op de systemen van een bedrijf, maar ook als het red team via social engineering informatie probeert te achterhalen en deze informatie misbruikt om toegang te krijgen tot de systemen van een bedrijf. Het blue team moet ervoor zorgen hackers altijd een stap voor te zijn om het risico op een geslaagde cyberaanval te verkleinen.

Risico’s verkleinen en continuïteit vergroten door de inzet van het red en blue team

Het nabootsen van realistische aanvalsscenario's door het red team tegen het blue team te laten strijden brengt handige inzichten in het weerbaarheidsniveau van de systemen en de security analisten binnen een organisatie. Door deze inzichten kunnen kwetsbaarheden worden verholpen en worden zwakke plekken versterkt. Dit verkleint de risico's op een geslaagde cyberaanval en verhoogd de continuïteit. Hieronder de belangrijkste voordelen van het uitvoeren van red team VS blue team:

Identificatie van kwetsbaarheden: het red team voert realistische aanvallen uit om kwetsbaarheden in de beveiliging van een organisatie te identificeren. Door deze kwetsbaarheden te ontdekken, kan het blue team vervolgens maatregelen nemen om de beveiliging van de organisatie te versterken en deze kwetsbaarheden te verhelpen.

Beperking van schade: het blue team kan snel reageren op aanvallen en eventuele schade beperken. Door vroegtijdig te detecteren en te reageren op aanvallen kan de impact van een aanval worden verminderd en de downtime van systemen worden beperkt.

Verhoogde bewustwording: door het uitvoeren van realistische aanvallen en beveiligingstesten, kunnen zowel het red team als het blue team de organisatie helpen zich bewust te worden van de mogelijke risico's en kwetsbaarheden. Dit kan bijdragen aan een cultuur van beveiligingsbewustzijn binnen de organisatie.

Voortdurende verbetering: het inschakelen van red team en blue team kan ook helpen bij het voortdurend verbeteren van de beveiliging van een organisatie. Het blue team kan leren van de aanvallen die het red team uitvoert en maatregelen nemen om de beveiliging te verbeteren.

Door het inschakelen van red team en blue team cybersecurity specialisten kan een organisatie de risico's mogelijk slagende cyberaanvallen verminderen en de continuïteit van de organisatie

vergroten. Het is belangrijk dat deze teams goed samenwerken en dat de aanbevelingen van het red team effectief worden opgevolgd door het blue team om de beveiliging van de organisatie te waarborgen.