Secura
A BUREAU VERITAS COMPANY

Red Teaming

Uw organisatie ligt onder vuur. Het aantal gerichte cyberaanvallen neemt toe, net als de complexiteit van aanvallen. Digitale fraude, ransomware, aanvallen op de toeleveringsketen: dit zijn maar een paar van de dreigingen die op u af komen. Hoe goed is uw cyberverdediging opgewassen tegen vijandige actoren? Test het met Red Teaming.

Om uw organisatie voor te bereiden op cyberaanvallen heeft u niet alleen beveiligingscontroles nodig. Het is ook belangrijk dat uw Blue Team goed reageert op deze zeldzame, maar ingrijpende gebeurtenissen. De grootste winst van een Red Teaming-oefening, naast het vinden van onbekende kwetsbaarheden, is de kans om uw verdedigers een echte aanval te laten meemaken - in een veilige setting.

Wat is Red Teaming?

Red Teaming is een beveiligingsdiscipline die uit de militaire wereld komt en die complete cyberaanvallen simuleert. Zo meet u de effectiviteit van uw cyberverdediging tegen vijandige aanvallers. Uw verdedigers oefenen en verbeteren hun detectie- en reactievermogen, in een gecontroleerde omgeving. Tot slot kan het Red Team gaten in uw beveiliging blootleggen, omdat de oefening zich richt op de organisatie als geheel, zonder de beperkingen van een reguliere penetratietest.

Stel, u wilt weten of u geraffineerde spearphishing-aanvallen kunt herkennen, of Advanced Persistent Threats (APT's) kunt detecteren. Er is maar één manier om daarachter te komen: de aanvallen uitvoeren zoals een vijandige aanvaller dat zou doen, om zo deze processen te testen. Het Red Team simuleert de aanval. Het Blue Team, verantwoordelijk voor de verdediging, kan op allerlei manieren (of helemaal niet) betrokken zijn. Het White Team (de waarnemers) kan waar nodig escaleren en de-escaleren.

Het Red Teaming proces

1 Fase 1 | Planning en voorbereiding

Het proces begint met plannen en zorgvuldig voorbereiden. Een projectmanager stelt samen met de Red Team lead en het White Team een agenda en 'rules of engagement' op. Tijdens de oefening wordt dit schema gevolgd en waar nodig aangepast. Risico's en scenario's worden continu beoordeeld. Het Red Team communiceert doorlopend met het White Team, via wekelijkse vergaderingen, een beveiligde chatgroep en aanvullende gesprekken. Dit betekent dat het White Team volledige controle heeft over de aanval.

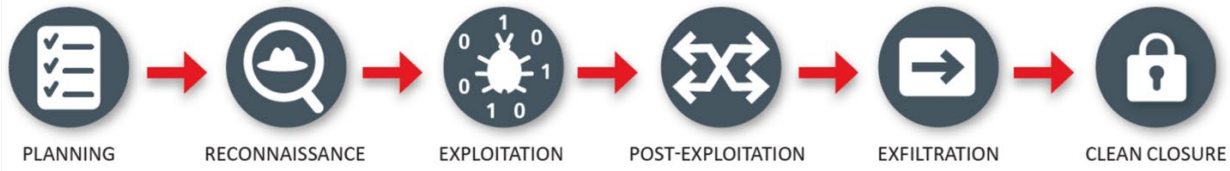
2 Fase 2 | De aanval

Na de voorbereiding gaan onze securityspecialisten in de aanval. Zij proberen op elke mogelijke manier toegang te krijgen tot uw zogenoemde 'kroonjuwelen.' Afhankelijk van het doelwit gebruikt Secura een combinatie van social engineering en aanvalstechnieken op computernetwerken, zoals een vijandige aanvaller dat ook in het echt zou doen. Technieken die we gebruiken zijn mystery guest, phishing, vishing, aanvallen via internet en aanvallen op computernetwerken in uw interne netwerken.

3 Fase 3 | Clean Closure

Als de aanval voorbij is, begint de zogenoemde 'clean closure', of afsluiting. Tijdens deze fase ruimen we allereerst de digitale restanten van de uitgevoerde aanvallen op. Ook verzorgen we voor het Blue Team één of meer evaluatiesessies. In een workshop lopen we de tijdlijn in zijn geheel nog eens langs, zodat zij daarvan leren. Het eindresultaat van deze fase is een gedetailleerd technisch rapport en een compleet beeld van hoe goed u eigenlijk beveiligd bent.

Dit zijn de fases van Secura's kill-chain voor Red Teaming-oefeningen:



De verschillende teams

RED TEAM

Het Red Team speelt de rol van de vijandige aanvaller, die de cyberveiligheid van de organisatie uitdaagt.

BLUE TEAM

Het Blue Team is verantwoordelijk voor het verdedigen van de netwerken, systemen en applicaties. In het team zitten zowel security professionals als beheerders die systemen en applicaties configureren.

WHITE TEAM

Het White Team is de schakel tussen het Red Team en het Blue Team. Binnen de organisatie zijn alleen de mensen in dit team op de hoogte van de oefening. Het White Team is cruciaal voor het slagen van de aanvalssimulatie.

PURPLE TEAM

Soms is het trainen van het Blue Team belangrijker voor de organisatie dan het echte real-world testen. Dan kunt u kiezen om een Purple Team samen te stellen. Hierin werken Red en Blue Team nauw samen om gaten in uw detectie op te sporen.

Vormen van Red Teaming

Red Teaming wint aan populariteit in alle sectoren, van financiële instellingen tot publieke organisaties en zelfs de vitale industrie. Secura is van mening dat er niet één Red Teaming-programma is dat bij iedere organisatie past. Daarom gebruikt Secura serviceniveaus voor Red Teaming, met elk een verschillende diepgang en duur. In overleg met onze Red Team managers kunt u kiezen welk serviceniveau het beste bij uw organisatie en budget past. Alle serviceniveaus werken met het MITRE ATT&CK-framework en bieden de mogelijkheid voor een Purple Teaming-opstelling (een gecombineerd team van Red en Blue).

RT Modular

Bent u klaar voor de volgende stap na een pentest? Bij deze modulaire aanpak maken we slim gebruik van de voordelen van Red Teaming **door alleen de meest relevante aanvallen voor uw organisatie te kiezen.** De geheime methodes van het Red Team zijn ondergeschikt aan het behalen van uw doelstellingen. Omdat we vooraf **meer informatie krijgen over uw organisatie**, is dit een voordelige optie om de digitale veiligheid van uw organisatie te testen.

RT Core

Red Teaming Core is een **volwaardige aanvalssimulatie voor middelgrote tot grote bedrijven met een eigen Blue Team**. Deze oefening combineert analyse en verkenning tot uitdagende aanvalsscenario's. Die scenario's zijn gebaseerd op levensechte threat actors. Secura bootst deze groepen na door dezelfde Technieken, Tactieken en Procedures (TTP's) te gebruiken zoals beschreven in het MITRE ATT&CK Framework. Om binnen een aantrekkelijk budget te blijven, bespreken we vooraf zogenaamde Leg Ups. Daarmee kan de oefening doorgaan als de verdediging op een bepaald gebied al toereikend genoeg is om het Red Team te vertragen.

RT Pro

De Pro-variant van Red Teaming is bedoeld voor organisaties met zeer volwassen Blue Teams en een hoge cyberweerbaarheid. Een volwassen organisatie aanvallen vereist veel meer inspanning van het Red Team – bijvoorbeeld met malware die uw EDR-oplossing omzeilt. Hier werkt het Red Team volledig onafhankelijk.

Red Teaming Pro is de meest realistische simulatie van aanvallen door Advanced Persistent Threats (APT's) tegen uw organisatie.

ZORRO

ZORRO staat voor "ZOrg Red teaming Resilience Oefeningen". Dit raamwerk, ontwikkeld door Z-CERT, is gericht op het structureel **verbeteren van de cyberweerbaarheid van zorgaanbieders en de zorgsector als geheel.** Secura biedt een kosteneffectief testprogramma dat voldoet aan de eisen van de ZORRO-methodiek.

RT in OT

Deze service is specifiek **gericht op organisaties die OT-assets als kroonjuwelen hebben.** Secura hanteert een gelaagde aanpak. Eerst zal het Red Team proberen informatie te verkrijgen die cruciaal is voor het doorgronden van uw OT-processen. Daarna probeert het team strategische toegang tot uw OT-netwerken te verkrijgen. Wij gebruiken een op maat gemaakt proces om eventuele risico's voor uw industriële bedrijfsvoering te beperken.

TIBER

TIBER staat voor Threat Intelligence Based Ethical Red Teaming. Hiermee wil de **financiële sector* de cyberweerbaarheid verbeteren, onder begeleiding van De Nederlandsche Bank.** Ook andere cyberbeveiligingskaders en -regelgeving noemen TIBER-achtige tests. Secura werkt met u samen om ervoor te zorgen dat uw organisatie volgens de juiste eisen wordt getoetst.

*Voor Europese organisaties in de financiële dienstverlening werkt Secura ook met u samen om u voor te bereiden op de komende **DORA regelgeving (Digital Operational Resilience Act)** en de bijbehorende **Advanced Red Teaming (ART).**

Succes van Red Teaming

Wanneer is een Red Teaming oefening een succes? Sommige mensen zeggen 'als de kroonjuwelen of vlaggen zijn bereikt zonder dat het Blue Team dat heeft gemerkt.' Deze definitie impliceert alleen dat het Blue Team er weinig van opsteekt. Aan de andere kant betekent het wel dat er een realistisch aanvalspad is blootgelegd, dat nu kan worden gesloten of beperkt. Wij beschouwen een oefening als een succes als het Red Team een behoorlijke uitdaging heeft gehad, maar ook veel nieuwe aanvalspaden of onbekende kwetsbaarheden heeft geïdentificeerd die oplossingen vereisen. Na de oefening kent u uw cyberrisico's en kunt u deze beperken. Dit is het uiteindelijke doel van Red Teaming.

Red Teaming is iets anders dan een traditionele penetratietest. Een Red Team kan kwetsbaarheden van verschillende aanvalsklassen combineren, bijvoorbeeld social engineering en aanvallen op de externe infrastructuur, om zo onbekende zwakheden te vinden. Dit is anders dan bij een pentest, waarbij de scope beperkt is tot één netwerk of applicatie.

Red Teaming test het vermogen van verdedigers om aanvallen te detecteren, daarop te reageren en ze af te slaan, in een realistische omgeving. Het traint ze om te reageren tijdens een echte aanval en laat zien waar de detectiemogelijkheden beter kunnen. Secura heeft veel ervaring in Red Teaming, we hebben de juiste capaciteiten, passie en sectorspecifieke ervaring. Die bieden tezamen onze klanten de best mogelijke basis voor de solide uitvoering en management van Red Teaming-opdrachten.

Gerelateerde diensten

Secura biedt een volledig spectrum aan beveiligingsdiensten. Doorgaans hebben onze klanten niet alleen Red Teaming-services nodig. Gerelateerde diensten die Secura aanbiedt zijn bijvoorbeeld:

VULNERABILITY ASSESSMENT EN PENTESTEN

Tijdens een veiligheidstest onderzoekt Secura specifieke applicaties, infrastructuren en netwerken onderzoeken. We gebruiken de mindset van een hacker om kwetsbaarheden te identificeren we geven advies voor verbetering.

TABLE TOP CRISIS MANAGEMENT

Secura legt uw crisismanagementteam een uitdagend maar realistisch cyberdreigings- incident voor, om samenwerking en coördinatie op de proef te stellen. Tijdens een eendaagse tabletop-sessie ontvangt uw team zogenoemde injects, die een realistisch gevoel geven in een gecontroleerde omgeving. Een tabletop-sessie ontwikkelt uw vaardigheden op het gebied van cybercrisisbeheer en bereidt het team voor op incidenten die grote impact hebben.

Secura
A BUREAU VERITAS COMPANY

Waarom Secura?

Een aanvaller gebruikt allerlei middelen om uw beveiliging, zowel digitaal als fysiek, uw technologie, en uw mensen te omzeilen. Het doel: toegang krijgen tot uw belangrijkste kroonjuwelen. Om dit type aanval na te bootsen heeft u een team van ervaren hackers en social engineers nodig, met de juiste kennis, ervaring en specialiteiten. Secura heeft deze de afgelopen twintig jaar opgebouwd. Ons multidisciplinaire team bestaat uit topspecialisten met kennis en ervaring in de drie beveiligingsdomeinen: techniek, fysieke beveiliging en menselijk gedrag.

Onze Red Teamers bezitten relevante certificeringen, zoals Certified Red Team Professional (CRTP), Certified Red Team Operator (CRTO), Certified Red Team Expert (CRTE), Master Level Social Engineer (MLSE) en vele anderen.

Secura's ervaring in Red Teaming, onze capaciteiten, passie en sectorspecifieke ervaring, bieden onze klanten de best mogelijke basis voor solide uitvoering en management van Red Teaming-opdrachten.

Secura
A BUREAU VERITAS COMPANY

Interesse?

Neem vandaag contact op:

Volg ons:

+31 88 888 31 00

info@secura.com

secura.com

BUREAU VERITAS 1828

Shaping a World of Trust