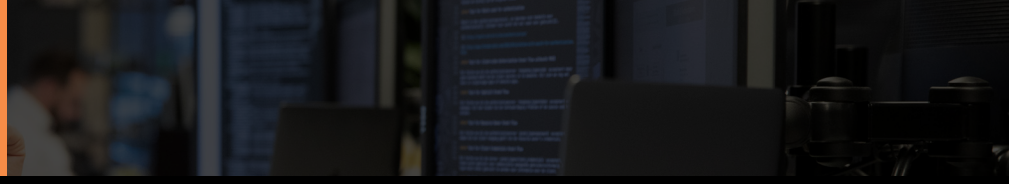
Computest
always on.



Red Teaming voorbeeldcase

Het simuleren van een echte cyberaanval

Organisatie ACME wil graag weten of het mogelijk zou zijn voor een kwaadwillende om de blauwafdrukken van hun gepatenteerde productieproces te verkrijgen. ACME heeft al verschillende securitymaatregelen (zoals pentesting en vulnerability assessments) genomen en werkt sinds een jaar met een securitybeleid en een SOC. Zouden deze maatregelen voldoende bescherming bieden in een realistische situatie waarbij een concurrent probeert de bedrijfsgevoelige informatie te bemachtigen?

Wij spraken met ACME af om een Red Teaming-opdracht uit te voeren gedurende een maand. In de kick-off van de opdracht werden de rules of engagement bepaald:

- We mogen gebruikmaken van alle beschikbare middelen; enkel aanvallen tegen het OT-domein zijn uitgesloten, om het productieproces niet te verstoren.
- Alleen de CEO en CTO zijn op de hoogte van de Red Teaming-opdracht, zodat de aanval een zo realistisch mogelijk beeld gaat opleveren.

Het pand fysiek binnendringen

We startten met externe aanvallen tegen de IT-infrastructuur van ACME, maar dit leverde niets op. Daarop besloten onze ethical hackers te proberen het pand van ACME fysiek binnen te dringen. Door bij de rokersingang aan de achterkant van het pand achter een medewerker aan te lopen kwam een van de hackers binnen. Eenmaal in het pand sloot hij een apparaatje aan op een netwerkpoort in de vergaderruimte. Het apparaatje had zijn eigen internetverbinding via 4G, waardoor je vanaf buitenaf toegang kan krijgen tot het interne netwerk.

Toegang tot het HR-systeem

Het was op deze manier eenvoudig om op het interne netwerk van ACME te komen, maar hoe ver zouden we nu kunnen komen? Via het interne netwerk kregen we toegang tot het interne HR-systeem, omdat één van de medewerkers, gevonden via LinkedIn, een wachtwoord had hergebruikt dat eerder in een datalek was beland. Middels kwetsbaarheden in het HR-systeem waren we in staat om onszelf op te voeren als medewerker van ACME. We vinkten ook de optie BHV'er aan.

Opnieuw het bedrijfspand betreden

Gewapend met een eigen geknutselde toegangspas liep een van onze hackers -dit keer via de voorkant- door de hoofdingang naar de balie van ACME. Hij vertelde aan de baliemedewerkster dat zijn pas niet werkte. Omdat hij inmiddels als medewerker geregistreerd stond, kreeg hij een tijdelijke toegangspas. Eenmaal bij de IT-afdeling heeft onze hacker om een nieuwe pas gevraagd en dit was geen probleem. Omdat hij in het HR-systeem gekenmerkt was als BHV'er heeft hij zelfs een persoonlijke pas gekregen die toegang geeft tot alle ruimtes in het pand. Nadat hij een praatje bij het koffiezetapparaat had gemaakt, vervolgde hij zijn weg naar de serverruimte. Het slot accepteerde direct de nieuwe toegangspas. Ons doel was om het wachtwoord van de beheerder te achterhalen.

Wachtwoord van de systeembeheerder achterhalen

De CTO van ACME had eerder aangegeven dat enige downtime bij een bepaalde server acceptabel zou zijn. De hacker plaatste daarom een klein apparaatje tussen het toetsenbord en de server, die alle toetsaanslagen opneemt. Daarna schakelde hij de server uit en verliet snel de serverruimte. Vanaf dat moment hoefden we alleen maar te wachten totdat een systeembeheerder de server weer aanzette en zijn wachtwoord invoerde. Binnen 15 minuten hadden we beet! Oeh, het wachtwoord bleek een combinatie te zijn van zijn favoriete voetbalclub met een jaartal. Met het wachtwoord van de systeembeheerder op zak konden we eenvoudig vanaf kantoor inloggen op de bestandsserver om zo de blauwafdrukken van ACME te downloaden. Operatie geslaagd.

Cyberaanval: blauwdrukken gestolen van gepatenteerd productieproces van ACME

Totaal geschatte financiële schade is 50,5 miljoen euro, bestaande uit:

- Internationaal patent waardeverlies: 50 duizend euro
- R&D kosten verlies: 450 duizend euro
- Gederfde omzet door verhoogde concurrentie: 50 miljoen euro

info@computest.nl
www.computest.nl
+31(0)88 733 13 37