U denkt dat uw organisatie goed beveiligd is?

Laat ons u zekerheid geven!

RED TEAM

Wij tonen u waar het mis kan gaan!

Uit onze lange ervaring blijkt dat wij van Cocoon risk management bij 85 procent van de bedrijven en instellingen kunnen binnendringen en kwaad kunnen aanrichten. De kans is dus reëel dat dit ons of een echte kwaadwillende ook bij u zal lukken. Vrijwel elke organisatie heeft wel zwakke schakels in de beveiliging. En die zijn door een buitenstaander makkelijker te ontdekken dan door uzelf. Vooral als deze, zoals wij, ervaring heeft in het op honderden manieren omzeilen van beveiligingsmaatregelen. Helaas zijn kwetsbaarheden niet altijd te vermijden. Dat hoeft ook niet. Als u ze kent, kunt u zich voorbereiden op de gevolgen en zo uw continuïteit verzekeren. En wij leren u ze kennen door zonder schade aan te richten en zonder uw proces noemenswaardig te verstoren uw organisatie in korte tijd op verschillende manieren aan te vallen. Dat is de meerwaarde van Red Teaming. *Expect the Unexpected!*

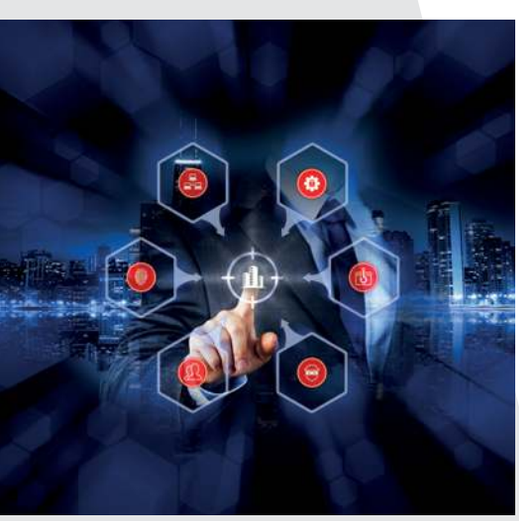
Misverstanden over veiligheid

‘Ernstige incidenten komen in onze organisatie niet voor!’
Weet u dat zeker? Kwaadwillende derden kunnen al geruime tijd toegang hebben tot uw vitale processen en data, zonder dat u dat direct merkt!

‘Onze medewerkers zijn gescreend en voor 100% te vertrouwen.’
Toch zijn uw medewerkers de zwakste schakel. Niet altijd bewust. Het kan slordigheid zijn, of een vals gevoel van veiligheid. Daarom geldt altijd: waar gelegenheid is, kan het misgaan! Alleen een test geeft zekerheid.

‘Onze beveiliging voldoet aan alle eisen.’
Dat is heel goed. Maar wie stelt die eisen? En wat is het belang van die partij? Is dat ook uw belang? Onderschat niet de creativiteit van uw aanvaller. Ook die kent de eisen en heeft geen boodschap aan regels en protocollen.

‘Iemand die per se kwaad wil, houd je toch niet tegen!’
Dat klopt. Maar dat geeft pas echt problemen als u niet weet wat er zou kunnen gebeuren, zodat u zich daar ook niet op kan voorbereiden.



Wat maakt het verschil?

Beveiligingsexperts gaan meestal, afhankelijk van hun specialisme, uit van bepaalde dreigingen. Cocoon risk management pakt het anders aan. Bij ons staat de continuïteit van uw proces centraal. Ons doel is niet het verkopen van producten, maar het weerbaar en veerkrachtig maken van uw proces. Wij onderzoeken de effectiviteit van bestaande beveiligingsmaatregelen, onder andere door deze van binnenuit aan te vallen. Bedenk hoe u zelf schade zou kunnen aanrichten en neem van ons aan dat criminelen dat op vrijwel dezelfde manier kunnen doen. Denk daarbij niet alleen aan inbrekers. Iemand die overdag in een keurig pak naar binnen glipt, kan nog veel grotere schade aanrichten.

Is het legaal wat jullie doen?

Met Red Teaming zoeken wij met toestemming van u als opdrachtgever de grenzen van het toelaatbare op. Vergeet niet dat de aanvaller er vaak heel onorthodoxe principes op na houdt. Wij benaderen die zo dicht mogelijk, zonder de wet te overtreden of uw organisatie, proces en medewerkers schade te berokkenen. Heel belangrijk is het om rekening te houden met het volgende: Red Teaming is zeker niet bedoeld om het functioneren van medewerkers of (beveiligings)leveranciers te bekritiseren. Het gaat om het geheel. Een medewerker kan fouten maken of bewust kwaad aanrichten, maar als dat tot grote schade leidt, is vaak niet de medewerker, maar diens authorisatie de zwakke schakel. Wij kennen de wet en zorgen ervoor dat u die als onze opdrachtgever niet overtreedt. Denk bijvoorbeeld aan het risico dat u de persoonlijke levenssfeer van uw medewerkers schendt. Wij zoeken de randen op, maar wel met de grootst mogelijke zorgvuldigheid, deskundigheid en vertrouwelijkheid.

Heeft het wel zin om zo ver te gaan?

Als u ons werk aan criminelen overlaat, kunt u door schade en schande wijzer worden. Wij hebben het dan dus niet alleen over inbrekers of hackers. Zelfs uw meest vertrouwde medewerker kan door een fout, of misschien zelfs onder bedreiging de kroonjuwelen van uw organisatie afstaan. Als dit data betreft, merkt u dat pas als bijvoorbeeld uw concurrent ineens de ene na de andere opdracht voor uw neus wegkaapt. De schade van één zo'n incident kan een veelvoud zijn van wat wij u in rekening brengen. Bovendien is de kans klein dat het bij één incident blijft. Als u het risico niet kent, kunt u zich ook niet voorbereiden op de gevolgen en zal de schade des te erger zijn.

En wat levert het mij op?

100% veiligheid kan niemand u garanderen. Wel kunnen wij u helpen zwakke schakels in uw beveiliging te identificeren en te versterken. Zo komt u te weten wat uw kwetsbaarheden zijn en welke mogelijke incidenten u kunt verwachten, zodat u zich daarop kunt voorbereiden. Ook bij dat laatste bieden wij de helpende hand. Bij 85 procent van onze opdrachtgevers lukt het ons om zonder veel moeite binnen te komen en invloed te krijgen op vitale processen. 98 procent heeft na ons onderzoek kwetsbaarheden in de beveiliging kunnen verhelpen. Nog niet overtuigd? Bel vandaag nog voor een vrijblijvend kennismakingsgesprek!

Bereid u voor op wat u niet wilt meemaken!

Bel: +31(0)79 320 31 50

cocoon
risk management

Wat houdt Red Teaming in?

In goed overleg met u als opdrachtgever, maar zonder dat uw medewerkers dit weten, vallen wij uw organisatie aan met één of meerdere of combinaties van de volgende methodes:

Physical Pentesting
Wij dringen uw gebouw binnen en kijken hoe dicht wij bij uw vitale processen kunnen komen.

Identification Testing
Door middel van valse ID's en identiteitsfraude proberen wij uw organisatie binnen te dringen.

On-Site Network Infiltration
Ethische hackers proberen van binnenuit in te breken op uw netwerk.

Security Application Testing
Beveiligingssystemen worden onderzocht op digitale kwetsbaarheden.

(Spear) Phishing
Een medewerker ontvangt een gepersonaliseerde phishingmail om gevoelige gegevens te ontfutselen.

Social Engineering
We kneden en beïnvloeden uw medewerkers om hen onbedoeld 'medeplichtig' te maken.

Kijk voor meer informatie op www.redteam-experts.com

Cocoon risk management, Koraalrood 153, Postbus 7318, 2701 AH Zoetermeer
www.cocoon.nl, 079-3203150 / Rob van Dijk: r.v.dijk@cocoon.nl