Interview met Pieter Lacroix, Director Security van Sogeti

Zo weet je hoe veilig jouw organisatie is

Het valt niet altijd mee om security-budget te rechtvaardigen. Zeker omdat inzicht geven in de ROI een flinke uitdaging is. Inmiddels zijn de meeste bestuurders zich bewust van de toenemende cybercriminaliteit en strenge wet- en regelgeving rondom gegevensbescherming en datalekken. Dat zijn - kort door de bocht - de belangrijkste drijfveren voor het geld dat wordt besteed aan het beschermen van de digitale veiligheid van de organisatie. Maar wanneer weet je of je na die investeringen ook veilig bent?

Het merendeel van de Chief Information Officers geeft aan dat cyberaanvallen helaas onvermijdelijk zijn. Nodeloos blijven investeren in security heeft dus geen zin. Maar het is wel prettig om te weten waar je staat. Pieter Lacroix, Director Security bij ICT-dienstverlener Sogeti, vertelt wat in zijn ogen de beste aanpak daarvoor is. Over het hoe, wat en waarom van 'redteaming'.

Hoe is het volgens jou gesteld met de security-status van Nederlandse Top 500-bedrijven? "Het belang van een digitaal veilige organisatie is inmiddels onderwerp van gesprek in bestuurskamers. Dat was een aantal jaren geleden nog niet zo vanzelfsprekend. Het was vooral een uitdaging voor IT-afdelingen. Inmiddels is de veiligheid van een digitaal gedreven organisatie van zo'n groot belang, dat gealloceerde budgetten niet langer als kosten moeten worden beschouwd, maar als investeringen die direct bijdragen aan reputatiebeheer, vertrouwen van stakeholders en zelfs continuïteit van de organisatie."

Wat is er nodig voor een digitaal veilige organisatie? "Uiteraard moet een aantal fundamentele zaken op orde zijn ter verdediging van

cyberdreigingen. Een veilige infrastructuur, applicaties en processen zijn daarvoor de uitgangspunten. De meeste grote organisaties hebben dat inmiddels wel op orde. Echter, veiligheid is een dynamisch proces. Vandaag kun je bestand zijn tegen cyberinbraken, en morgen misschien niet meer."

Wanneer weet je of je je zaken op orde hebt? "Het treurige antwoord is eigenlijk dat je dat nooit 100% kan garanderen. Er zijn wel manieren om de veiligheid van een organisatie voortdurend te toetsen. Daarvoor hebben we bij Sogeti onze redteaming diensten opgetuigd."

Hoe profiteert een organisatie van Sogeti redteaming-expertise? "De meeste bedrijven hebben eigen security teams in dienst. Daarnaast doen ze vaak een beroep op externe expertise voor het testen van specifieke applicaties op zwakheden. Maar de uitdaging zit hem veelal in het holistische beeld en het kwaliteitsniveau van de veiligheid in brede zin. Security professionals zijn geen (ethische) hackers. Deze digitale inbrekers handelen anders. Die denken niet vanuit één bepaalde afdeling, applicatie, infrastructuur of proces. Bovendien kan een organisatie onbewust ook bedrijfsblind zijn. Dan kan een red team dat van buitenaf komt, uitkomst bieden. Zij zoeken als hackers naar allerlei manieren om zowel digitaal als fysiek in te breken."

Vertel eens hoe dat in de praktijk in zijn werk gaat? "Onze red team professionals gaan op zoek naar zwakheden op drie verschillende niveaus; de infrastructuur, applicaties plus mensen en processen. Voordat we werkelijk van start gaan, doen we in overleg met de klant een intake. Tijdens dit gesprek stemmen we bijvoorbeeld af welke informatie vooraf gedeeld wordt. Afhankelijk van de gegevens die het bedrijf wil prijsgeven, kiezen we voor een zogeheten white, grey of blackbox aanpak. Hoe meer informatie we vooraf krijgen, hoe efficiënter we ons werk kunnen doen. Zo kunnen we zoveel mogelijk doen in beperkte tijd. Uiteraard kan de klant ook kiezen voor een blackbox scenario. Dan gaan we zonder voorinformatie aan de slag. Na overeenkomst over de aanpak spreken we een window af waarbinnen ons red team actief zal zijn. Dat kan een specifiek moment zijn maar meestal komen we een termijn van twee tot drie maanden overeen. Zo weet de klant niet wanneer we toeslaan. Dat is natuurlijk ook de realiteit bij echte cyberaanvallen. Daarmee zijn onze bevindingen ook het meest waardevol."

> 'Het komt helaas voor dat een red team na een jaar opnieuw dezelfde zwakheden vindt'

Waar moet een goed red team aan voldoen? "Het is van groot belang dat het een multidisciplinair team is. De ethische hackers moeten thuis zijn in de wereld van applicaties en infrastructuur maar beschikken ook over psychologische en communicatieve vaardigheden. Bovendien moeten ze inzicht hebben in de fysieke processen van een organisatie. Inbreken hoeft niet altijd digitaal te gaan."

En wat levert zo'n red team dan op? "Het red team geeft inzicht in de zwakheden van de organisatie. De zogenaamde blinde vlekken. En daarmee krijg je eigenlijk antwoord op de vraag hoe veilig je organisatie nu echt is. De inzichten geven eveneens een gerichte aanleiding voor het nemen van maatregelen of het aangaan van dialoog met het management voor meer budget. Verder leert onze ervaring dat de opgedane kennis blue teams ook dwingt beter of anders te gaan samenwerken."

Hoe confronterend zijn de red team uitkomsten voor de interne security professionals? "Wat mij betreft helemaal niet. Als er nauwelijks zwakheden zijn gevonden, hebben de security experts het gewoon goed op orde. En als er wel zwakheden worden gevonden, is er aanleiding voor gesprek en verbetering. Dus ja, volgens mij heb je niks te verliezen. Natuurlijk moet een organisatie open staan voor kritiek en bereid zijn om vervolgens ook echt maatregelen te nemen. Het komt helaas voor dat een red team na een jaar opnieuw dezelfde zwakheden vindt."

Serieus!? "Dat gebeurt wel. Eigenlijk hoeft dat niet per definitie een drama te zijn. Het kan ook een bewuste keuze zijn om bepaalde risico's te accepteren. Het bedrijf weet zelf vaak beter dan wij wat de mogelijke impact is van bepaalde risico's."

Is jouw advies om zo'n red team regelmatig aan de slag te laten gaan? "Veilig zijn is dus een dynamisch proces. Iedereen weet dat security-ontwikkelingen razendsnel gaan. Extra uitdagend in deze tijd waarin organisaties volop in hun digitale transformatie zitten. Dan kan het heel nuttig zijn regelmatig van buitenaf te laten toetsen hoe je ervoor staat. Een periodieke red team-actie geeft je structureel inzicht in de status van je veiligheid."

Waarom zouden organisaties voor een Sogeti red team moeten kiezen? "In tegenstelling tot niche spelers hebben wij als ICT-dienstverlener ervaren experts in huis die ook de taal van de business spreken. Dat is van groot belang, want ook de niet-IT-afdelingen moeten snappen wat nodig is voor hun (digitale) veiligheid. Wij hebben hackingdiensten gebundeld met een breed scala aan security-expertise en adviseurs. Zo zorgen we ervoor, dat gevonden zwakheden direct aangepakt kunnen worden en helpen we met het mitigeren van risico's. Dit in tegenstelling tot de grote consultancy bedrijven, die vaak met dikke rapporten binnenkomen zonder concrete technische oplossingen. Ik zou haast zeggen dat het testen van veiligheid in onze genen zit. We zijn niet voor niks groot geworden met het testen van software op functionaliteit, prestaties, snelheid, betrouwbaarheid èn veiligheid."

VAN DE REDACTIE

CyberSecurity Specialist? Hack your career at Sogeti.

De top van het Nederlandse bedrijfsleven én de overheid kiest voor Sogeti en haar cybersecurity expertise. Alle reden voor jou om hetzelfde te doen. Als CyberSecurity Specialist wil je immers niets liever dan opereren in de frontlinie van de ontwikkelingen en voorop lopen bij toporganisaties. En daar krijg je bij Sogeti alle ruimte voor. Naast een breed aanbod van trainingen, cursussen en certificeringstrajecten vind je bij ons de gaafste projecten. In uiteenlopende sectoren. Waar je ook aan de slag gaat, als CyberSecurity Specialist laat jij klanten zien dat cybercriminaliteit bij Sogeti geen kans heeft! Is cybersecurity jouw passie en wil jij onze klanten beveiligen? Hack your career! Kijk voor onze vacatures op **www.sogeti.nl/cybersecurityspecialist**

sogeti
Part of Capgemini