DIEPGAANDE KENNIS VAN SOFTWARE-ONTWIKKELING IS CRUCIAAL

INTERVIEW MET GARY McGRAW, door Lex Borger

Gary McGraw is de CTO van Cigital, Inc., een software security adviesbedrijf gevestigd in Dulles, Virginia, vlak bij Washington D.C. Cigital heeft ook een vestiging in Amsterdam aan de zuidas. Gary is de auteur van meerdere boeken over software security en heeft meer dan 100 wetenschappelijke artikelen op zijn naam staan. Hij is te bereiken via gem@cigital.com. Opmerkingen of vragen naar aanleiding van dit interview kunnen gestuurd worden naar lex.borger@domustechnica.com.

Op 8 mei had ik het genoegen om een gesprek te hebben met Gary McGraw. Hij was in Nederland voor een OWASP presentatie en de BSIMM European Community Conference, twee verschillende doelen dacht ik, maar in het gesprek kwamen die twee nader tot elkaar. Ik kwam er al snel achter dat Gary een drukke agenda heeft. Hij schrijft veel - boeken en artikelen. Soms komt het verzoek voor een artikel van ver buiten het securityveld. Ook dit overweegt hij altijd. "Het helpt om naar een nieuw publiek uit te reiken."

Gary reist ook veel. "Ik geef ongeveer 35 presentaties per jaar, waarvan 10 tot 15 keynotes zijn voor meer dan duizend mensen. Dat is gewoon een deel van wat ik doe. Maar weet je, ik kijk geen TV. Nooit." Verder woont hij landelijk en speelt in een band. Zijn bedrijf heeft hem al in bescherming genomen tegen een te druk schema. "Vier jaar geleden hebben ze tegen mij gezegd: Je bent jong, maar je kunt niet aan een stuk blijven reizen de komende 10 jaar, je put jezelf uit. Stel voor jezelf een leefpatroon in dat wél werkt, dat je vol kunt houden. Dat was een prachtadvies. Zo hebben we 'no-fly-July' ingesteld. In juli zit ik niet in een vliegtuig. Ik blijf thuis, zit op mijn steen in de rivier. Als mensen mij willen zien dan zitten ze bij mij op de steen in de rivier. Ik lees dan veel en denk na. Dat is zo'n waardevolle gewoonte voor mij geworden dat ik het nu ook in december toepas, 'no-fly-Noel'. Ik blokkeer een week per maand waarin ik niet op pad ga en ben ieder weekend thuis. In de overige tijd, wie weet waar ik ben… Mijn agenda is het komende jaar al gevuld."

Silver Bullet Security podcast

Ik luister veel naar podcasts en heb een abonnement op de podcast van Gary, de Silver Bullet Security podcast, maar ik hoor hem ook op andere podcasts langskomen als gast. Ik maakte de opmerking dat hij het in zijn eigen podcast nooit heeft over zaken als BSIMM. Gary is daar simpel en direct over: "Mijn podcast gaat niet over mijn werk."

BSIMM is organisch gegroeid

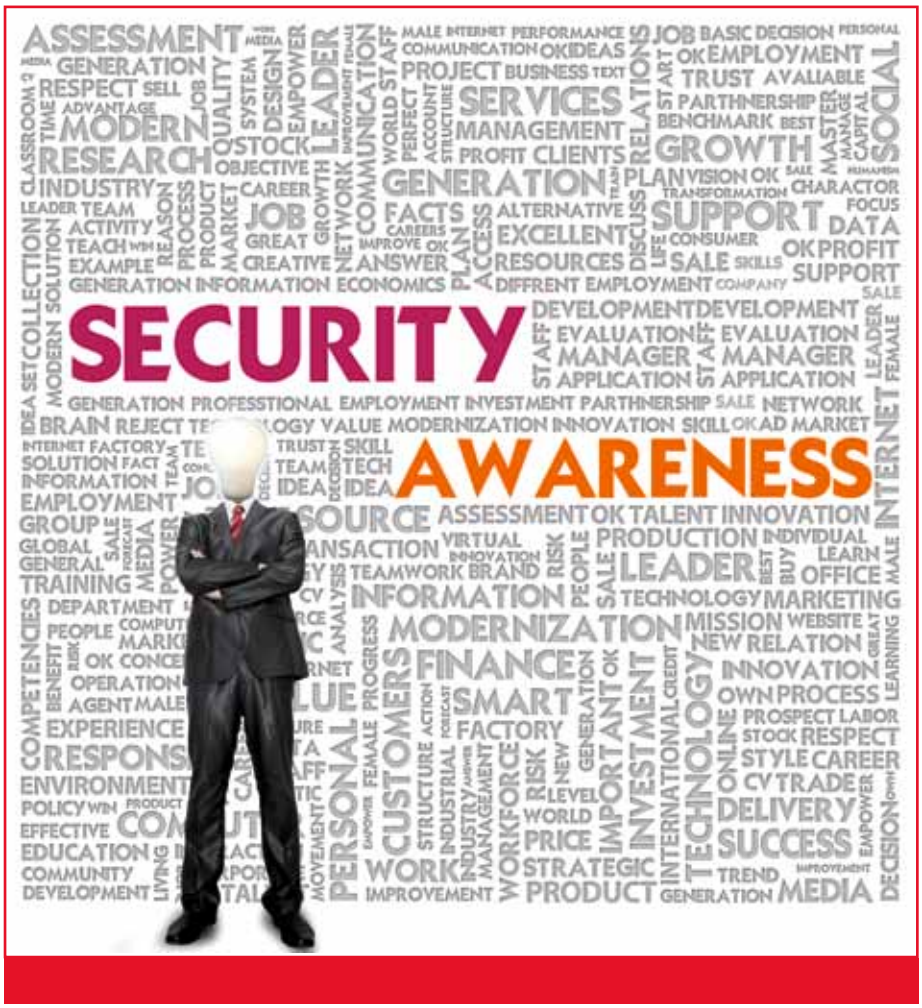
Harde gegevens verzamelen

Zo gaan we naadloos over in het ontstaan van BSIMM. "Het is organisch gegroeid. Er zit een leuk verhaal achter. Toen ik voorzitter was van de technical advisory board bij Fortify hadden ze een jonge ingenieur de opdracht gegeven een software security methode te ontwikkelen. Hij presenteerde deze methode aan de directie en hij werd aan stukken gereten. Ze vroegen waarom er een nieuwe methode nodig was, "we hebben de zeven Touchpoints, Microsoft's SDL, OWASP CLASP en hier voeg jij er wéér een aan toe!" We hadden hier een discussie over en ik kreeg de ingeving om eens in de buitenwereld echte gegevens te verzamelen en dáár een model omheen te bouwen dat de data beschrijft. Ik heb negen vrienden gebeld bij bedrijven en ze gevraagd of ze mee wilden doen aan wetenschappelijk onderzoek voor software security. We verzamelden een heleboel gegevens en Brian Chess, Sammy Migues en ik hebben drie dagen bij mij thuis doorgebracht met ploeteren door de gegevens, argumenteren over wat er gezegd was, structureren van de informatie, samenstellen van het raamwerk en alle activiteiten benoemen. Het was een zeer creatieve bezigheid, inmiddels drie jaar geleden. Nu hebben we het aantal bedrijven in

BSIMM

BSIMM (spreek uit als "biesim") staat voor "Building Security In Maturity Model". Het BSIMM is opgezet om een software security programma binnen een bedrijf begrijpelijk en meetbaar te maken. Het model kan gebruikt worden als uitgangspunt bij het opzetten of evalueren van zo'n programma. Het BSIMM is het resultaat van observatie en analyse van bestaande software security programma's bij meer dan 50 vooraanstaande bedrijven. In September 2012 is BSIMM versie 4 gepubliceerd.

de dataset vervijfvoudigd en de data zelf vertienvoudigd. Er zijn bedrijven die meerdere malen gemeten zijn, sommige bedrijven hebben deelmetingen gedaan. Wij publiceren alleen de globale resultaten, maar de hele dataset bevat een verbazingwekkende hoeveelheid informatie."



Dingen die iedereen doet

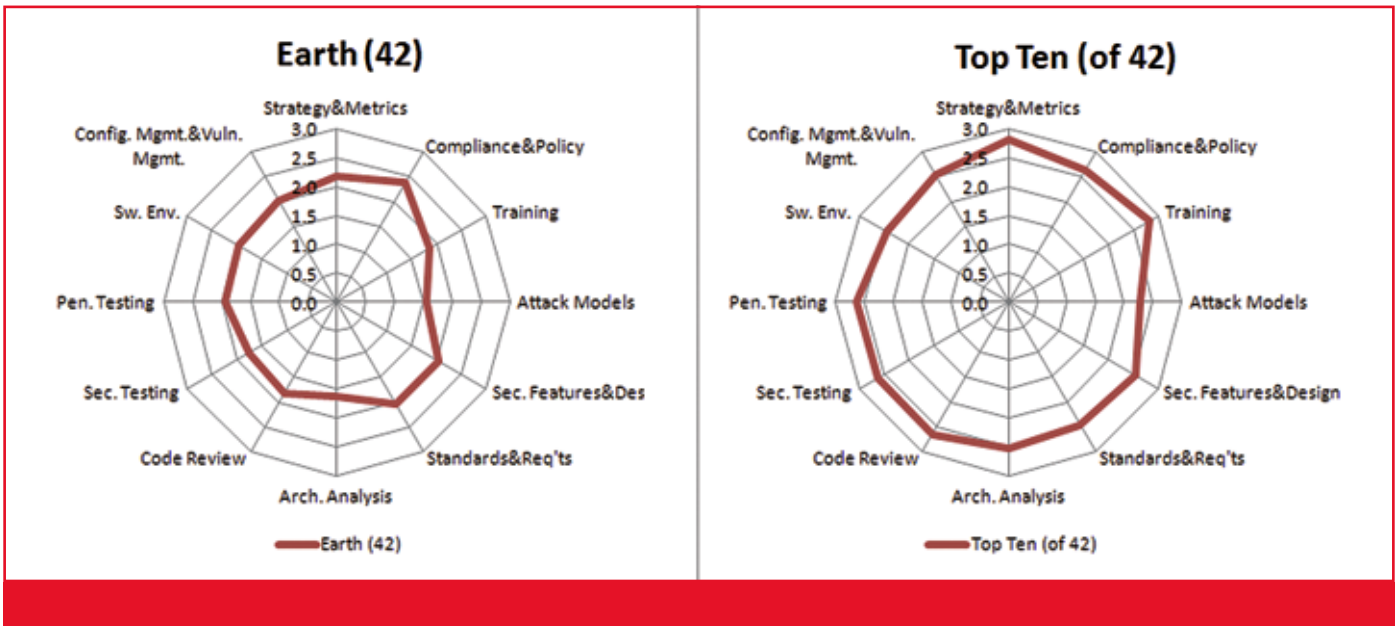
Ik had als voorbereiding uiteraard BSIMM versie drie doorgenomen en ik maakte de opmerking dat het softwareproject waar ik in zat niet alles deed uit de lijst 'Stuff everybody does'. "Er is een voorbehoud: 'iedereen' slaat maar op 67% van de bedrijven. Soms zijn activiteiten niet zinvol in de (bedrijfs)cultuur of de organisatie en dat is OK. We zijn daarom ook erg voorzichtig in onze presentatie van de BSIMM activiteiten en geven duidelijk aan dat dit is wat andere bedrijven doen. Je kunt hier naar kijken en beoordelen of het voor jou zinvol is. Wij zeggen niet dat je dit moet doen. BSIMM is een beschrijvend model. Er zijn critici die vinden dat bepaalde activiteiten niet thuishoren in het model en kraken het daarom af. Voor hen heb ik het advies: Lees het document, dat is niet wat we gezegd hebben. Ga de bron, bijvoorbeeld Microsoft, vertellen dat ze activiteit X niet moeten doen en kijk of ze naar je willen luisteren." "Een probleem wat we hadden in het werkveld van software security is dat er een aantal mensen werken die een opinie hebben die niet gebaseerd is op feitelijke gegevens.

Security team

Nu hebben we een hoop informatie waar we naar kunnen verwijzen. Bijvoorbeeld, ik heb in een blog geschreven dat je een software security team moest hebben in je organisatie. Want als je dat niet hebt, hoe weet je dan wie hiervoor verantwoordelijk is? Dus, richt een security team in. En ik kreeg commentaar op mijn blogpost van mensen die aangaven in hun IT-afdeling van zeven man alle security erbij te doen. Een discussie volgde. Nu kan ik uit de BSIMM-data zeggen dat ieder bedrijf uit de BSIMM-dataset een bestuurder heeft die verantwoordelijk is voor software security en er is ongeveer één software security teamlid per vijftig ontwikkelaars."

Security is veranderd

Al filosoferend komen we op de veranderingen in het vakgebied. "De top-level security managers van nu sturen informatiebeveiliging totaal anders aan dan tien jaar geleden. En dat is goed. Ze vragen om meer informatie, ze eisen een meetbaar



resultaat, ze besturen het meer als een bedrijf. Die managers zijn voor ons fijn om mee te werken.
Bij Cigital proberen we niet security budget af te snoepen van een grote hoop. In plaats daarvan benoemen we problemen die opgelost moeten worden en wijzen daar budget aan toe. Een strategische aanpak vanuit de top is te verkiezen boven het veranderen van IT-systemen aan de onderkant. Je moet wel je zaak bepleiten met gegevens die dat ondersteunen. Wanneer je een spider-chart maakt voor een bank, waarbij je het bedrijf vergelijkt met alle andere banken, geeft het voldoening wanneer je het laat zien aan de CIO, een machtige man binnen de bank. Hij vraagt dan gelijk door over de aspecten in de tabel waarbij ze achterblijven ten opzichte van de concurrentie. Ze willen weten of dat een slecht teken is en wat ze in dat geval eraan kunnen doen. "Het werken aan BSIMM is een plezier. We hopen nu dat we in Europa ook een gemeenschap kunnen opzetten die even sterk is als in de VS. Een gemeenschap van mensen die informatie uitwisselen en samen willen werken. Over drie dagen weet ik het." Gary doelt hierbij op de BSIMM European Community Conference, die ten tijde van het gesprek nog moest plaatsvinden. "We hebben twaalf grote bedrijven doorgelicht in Europa. Ik zou graag zien dat dit doorgroeit naar dertig in de komende twee jaar. Als we in London kunnen doorbreken zoals we in New York hebben gedaan, dan zal dit zo bereikt zijn. En veel bedrijven in London hebben ook een kantoor in New York…"

Mijn podcasts gaan niet over mijn werk

Wie moet software security leiden?
"Over het algemeen komen mensen in IT security uit operationeel beheer, netwerkbeheer of systeembeheer en ze weten veel van de infrastructuur van security. Ze weten wat een SOC (security operations center) is en hoe dat werkt. Maar het zijn niet de beste mensen om met software security bezig te gaan. Zo iemand met ontwikkelaars laten werken om ze software security bij te brengen is als een hond voor de wolven gooien. De hond overleeft het niet." "Mijn indruk is - en ik heb geen wetenschappelijke onderbouwing hiervoor - dat in Europa de eerste generatie software security professionals operationele security mensen waren. Ze liepen tegen de ontwikkelaars en de top-managers op zonder voortgang te boeken. Dus we hebben nu mensen nodig met een gedegen software ontwikkelingsachtergrond die de strekking van het verhaal kunnen bijsturen. Penetration testing is alsof je stenen gooit naar je vrienden.
De software ontwikkelaars willen niet

Bugs

geraakt worden door stenen. Je maakt op die manier geen vrienden."

Vooruitgang…

"Er zijn mensen die zeggen dat software security helemaal geen vooruitgang boekt. We hebben nu vijf, tien jaar gewerkt aan beveiliging en de software ziet er nog steeds problematisch uit. Waarom moeten we nog geld spenderen aan software security? Het antwoord is complex. Eigenlijk boeken we goede vooruitgang, de defect-density-ratio (het aantal problemen per regel code) daalt. De trend gaat de goede kant op. Het lijkt alsof we geen vooruitgang boeken omdat de hoeveelheid software nog sneller groeit. De hoeveelheid bugs groeit dus, ondanks de vooruitgang. Als we stoppen krijgen we een exponentiële explosie van bugs. Je moet daarom door blijven gaan."

"Ik houd er niet van om incidenten hiervoor te gebruiken. BSIMM geeft me de mogelijkheden om een manager te overtuigen zonder incidenten te gebruiken. Zijn concurrenten hebben we al geanalyseerd. Nu kun je hem gelijk laten zien hoe hij daarmee verschilt, dat hij de langzaamste zebra in de kudde is. Je wilt die zebra niet zijn, want de cheeta's jagen al op je. Dat is veel beter dan stenen laten gooien door pen-testers. Pen-testing is nodig, maar gebruik het niet om de aandacht van het management te trekken."

Where's Aubrey?

Aan het eind van het gesprek vraag ik Gary nog iets wat hij zijn gasten ook vaak vraagt, ik vraag hem om zijn muzikale voorkeuren en activiteiten.

"Ik speel in meerdere bands. De belangrijkste band waar ik in speel is 'Where's Aubrey', al onze muziek is online te krijgen en we hebben 6 CD's uitgebracht. 'Luminous' is de meest recente, uitgekomen in december 2011. Ik speel al viool sinds ik drie jaar oud ben. Een andere band waar ik net mee begonnen ben is 'The Bitter Liberals'. Daar zal je binnenkort meer over horen. Een derde band is een Django Reinhardt coverband, 'Hot Club Millwood'. Muziek is belangrijk voor mij. Toen ik er voor koos om naar de universiteit te gaan en niet naar het conservatorium, kwam ik er achter dat ik moeilijker in het leven stond omdat ik geen muziek meer speelde…"

Security wordt nu anders aangestuurd dan 10 jaar geleden

Gary is een expert met enthousiasme en passie. Experts hebben we genoeg, maar in ons vakgebied wordt het nogal snel mat en droog. Ik bewonder zijn energieke enthousiasme en passie. Die werken om management te overtuigen. En voeg daar een instrument als BSIMM bij om het inhoudelijk af te maken. ●

Gary on stage

Links

OWASP: https://www.owasp.org/

BSIMM: http://bsimm.com

Gary McGraw: http://www.cigital.com/~gem/

Silver Bullet Security podcast feed: http://feeds.feedburner.com/silverbulletsecurity

7 Touchpoints: http://www.buildingsecurityin.com/concepts/touchpoints/

Microsoft SDL: http://www.microsoft.com/security/sdl/default.aspx

OWASP CLASP: https://www.owasp.org/index.php/Category:OWASP_CLASP_Project

Where's Aubrey: http://www.wheresaubrey.com/