INTERVIEW PAUL DERKSEN EN RONALD VAN DER WESTEN, ETHICAL HACKERS VAN MOTIV

AANVAL

'HET MOOIE IS DAT EEN BEVEILIGINGS-ONDERZOEK EIGENLIJK NOOIT HETZELFDE IS'

Ronald van der Westen - Security Consultant bij Motiv

'IK WALSTE HIER ALS HET WARE DWARS DOOR DE VOORDEUR NAAR BINNEN'

Paul Derksen - Security Consultant bij Motiv

Fotografie: ??????????

Recente berichtgeving over grootschalige hacks heeft gezorgd voor 'een run op beveiligingsonderzoeken', zo signaleren security-consultants Paul Derksen en Ronald van der Westen van Motiv. "Door de berichtgeving gaat bij veel bedrijven toch de vraag leven of zij misschien ook kwetsbaar zijn", zegt Van der Westen. Motivator sprak met de ethical hackers van Motiv over de schoonheid en de noodzaak van (ethisch) hacken.

IS DE BESTE VERDEDIGING

Paul Derksen en Ronald van der Westen kwamen respectievelijk in 2006 en 2007 in dienst van Motiv. Van der Westen: "Tijdens mijn eerste beveiligingsonderzoek voerde ik samen met Paul een social engineering-aanval uit waarbij we via twee verschillende ingangen tegelijkertijd het gebouw probeerden binnen te komen. Ik had mezelf voorgedaan als een engineer van een andere partij die zogenaamd een storing kwam verhelpen en binnen twee minuten stond ik in de serverruimte en kon ik letterlijk mijn gang gaan. En het was nota bene de opdrachtgever voor het beveiligingsonderzoek die me had binnengelaten!"

Ook Derksen was er kinderlijk eenvoudig in geslaagd om het gebouw binnen te komen. "Ik walste als het ware dwars door de voordeur naar binnen. Vervolgens kreeg ik zelfs een rondleiding door de catacomben en werden alle kasten en deuren opengetrokken. Toen ik buiten stond dacht ik: wat gebeurde me nu? Dan blijkt later ook op netwerkgebied het nodige niet op orde te zijn. Zo was de dataversleuteling met name op authenticatiepunten niet consequent en vanuit de werkplekomgeving kon je rechtstreeks naar het servergebied. Ook de applicaties waren niet bijgewerkt. Eigenlijk allemaal standaardzaken die je bij bijna iedere organisatie aantreft."

Terugkerende problemen

Volgens Derksen is en blijft patchmanagement een probleem. "En dan met name het niet tijdig bijwerken van de software op de desktop, zoals Adobe, Flash en Java." Onder andere de lekken die enkele maanden geleden werden blootgelegd in een groot aantal overheidssites tonen volgens Van der Westen en Derksen de risico's van het niet goed bijwerken van software.

Een ander punt waar het volgens de ethical hackers van Motiv regelmatig fout gaat, is de inrichting van Intrusion Detection and Prevention. Van der Westen: "Vaak zie je dat IDP alleen goed is ingeregeld voor het verkeer van buiten naar binnen. Eenmaal op het netwerk vindt er vaak helemaal geen detectie plaats en kun je vrijwel alles benaderen." Een goed voorbeeld van 'hard on the outside, soft on the inside', meent Derksen. "Van oudsher zijn we gericht op die stenen muur die om de organisatie heen staat, maar als je daar doorheen bent heb je vrij spel."

Beveiligingsonderzoek in trek

Derksen en Van der Westen signaleren beiden een toenemende belangstelling voor het beveiligingsonderzoek als middel om de weerbaarheid van organisaties tegen bijvoorbeeld cybercrime te meten. Volgens de securityconsultants is dat mede te danken aan de media-aandacht die hacks op bijvoorbeeld DigiNotar en overheidssites hebben gegenereerd. "Het beveiligingsonderzoek maakt momenteel zo'n zeventig procent van mijn werkzaamheden uit", geeft Van der Westen ter indicatie aan. Ook bedrijven die zelf problemen hebben ondervonden – en hardhandig zijn gewezen op de risico's – wenden zich vaak tot de ethical hackers van Motiv. Derksen: "Bedrijven zijn vaak heel erg gericht op de defensieve kant van beveiliging, maar de aanval is de beste verdediging. Een offensievere opstelling brengt vaak veel meer aan het licht."

Verloop onderzoek

Een beveiligingsonderzoek begint altijd met een intakegesprek bij de klant, zo schetsen Van der Westen en Derksen. Tijdens dit gesprek worden onder andere de doelstellingen besproken, de beveiligingspostuur van de klant bepaald en besproken hoe wordt getest. "Als ethical hacker heb je nu eenmaal niet altijd carte blanche", stelt Derksen. Van der Westen: "Sommige klanten geven aan een black box-test te willen en dan gaan wij zonder informatie aan de slag; dat kost altijd veel meer tijd. In de meeste gevallen gaat het toch om een white box-test waarbij de klant informatie zoals netwerktekeningen aanlevert."

Een vrijwaringsverklaring is altijd een voorwaarde om te beginnen met testen. Middels een eerste scan proberen de ethical hackers zicht te krijgen in wat er leeft binnen een organisatie. Derksen: "Uit publieke bronnen zoals Facebook en LinkedIn valt al enorm veel informatie los te weken. Als je die informatie een beetje handig in kaart brengt en met elkaar linkt, krijg je al een goed profiel van je target zonder dat je een pakketje op je doelwit hebt afgevuurd." Daarna wordt onderzocht welke poorten beschikbaar zijn om een aanval uit te voeren. Van der Westen: "Op basis van die informatie gaan we verder en vanaf dat punt is het echt handwerk."

Het onderzoek wordt afgesloten met een rapportage waarin de plus- en verbeterpunten staan vermeld en op welke manier verbeteringen kunnen worden doorgevoerd. In veel gevallen verzorgen de security-consultants die betrokken zijn bij het onderzoek een presentatie bij de opdrachtgever. Hoeveel tijd een compleet onderzoek in beslag neemt, is volgens Van der Westen en Derksen moeilijk aan te geven; dat is volledig afhankelijk van de scope van het onderzoek.

Creativiteit

"Het mooie is dat een beveiligingsonderzoek eigenlijk nooit hetzelfde is; je kunt altijd je creativiteit kwijt", besluit Van der Westen. "Je doet dingen die eigenlijk niet mogen en dat maakt het interessant." Derksen: "Je blijft prikken om te kijken of het echt geen krak zegt. Soms is het heerlijk om dingen onderuit te halen in plaats van op te bouwen." ●●