Tekst & fotografie: Aart van der Haagen

THE S-UNIT: PENTESTEN MET NADRUK OP MENSELIJK INZICHT

MAATPAK IN HACKEN

De invloed van dataverkeer blijft onophoudelijk toenemen en vraagt om een navenante ontwikkeling in digitale beveiliging. Dagelijkse kost voor The S-Unit, een bedrijf dat penetratietesten uitvoert om kwetsbaarheden naar boven te halen. Het ethisch hacken gebeurt geautomatiseerd, maar vooral ook handmatig, omdat het beschermen van de 'kroonjuwelen' van een onderneming altijd maatwerk vormt.

'To defend against an attacker, you must know how to think like one', valt te lezen op het visitekaartje van Dirk van Veen, die vier jaar geleden samen met collega's Sjoerd Versteeg en Barry van Kampen de afdeling 'The S-Unit' van hun voormalige werkgever verzelfstandigde. Het formuleert precies de gedachte achter ethisch hacken: zwakke plekken in de IT van een bedrijf opsporen en daarmee de klant handvatten geven om beveiligingsmaatregelen te (laten) treffen. "Je voert dus aanvallen uit, binnen de ICT-sector beter bekend als penetratietesten, kortweg pentesten," legt Van Veen uit. "Wij doen dat binnen ons team van tien experts, die vrijwel altijd op afstand werken en zich in de dagelijkse praktijk continu ontwikkelen. In bijna elke case komt wel weer iets nieuws naar voren, dat de tester vervolgens deelt met zijn collega's." The S-Unit werkt met een multidisciplinair team dat veel menselijke inbreng in plaats van alleen scripting toevoegt, aanbevelingen op technische en diverse procesniveaus doet, onzekerheid wegneemt, inzicht geeft in de beveiligingsstatus van de IT-omgeving en veel kennis heeft van mobiele applicaties.

CONTRACTAFSPRAKEN

Welke zaken kunnen aanleiding geven om een specialist als The S-Unit in te schakelen? "In het bedrijfsleven ontstaat steeds meer bewustzijn omtrent digitale

beveiliging, mede door de invoering van de AVG. Soms leeft dat besef meer bij medewerkers - vaak op een specifieke afdeling - dan bij het management. Aandringen op het investeren in betere security heeft niet altijd effect, maar het laten uitvoeren van een penetratietest die aantoont hoe makkelijk gevoelige gegevens op straat komen liggen maakt wél indruk. Verder ontstaat er steeds meer wettelijke regelgeving en maken leveranciers en afnemers contractafspraken met elkaar die beveiligingseisen bevatten, waaronder het periodiek laten uitvoeren van een pentest. Dat komt met name voor in bedrijfskolommen waar betaalsystemen of - zoals bij medische zaken - persoonsgegevens van toepassing zijn. Steeds vaker moeten partijen die zich bezighouden met ontwikkeling, bijvoorbeeld van webwinkels, zorgplatformen, klantportalen, infraoplossingen of kantooromgevingen, hun producten laten testen om de veiligheid ervan te kunnen aantonen. Meestal blijft niet bij een eenmalige exercitie; het betreft immers altijd een momentopname."

AANVALSOPPERVLAK

The S-Unit besteedt veel aandacht aan de voorbereiding op een penetratietest. Van Veen: "We peilen zorgvuldig de behoefte van de klant en spreken op basis daarvan de scope met hem af, die we het aanvalsoppervlak noemen. Het is voor de onderneming belangrijk om zogezegd haar kroonjuwelen te beschermen, zoals financiële en persoonsgegevens, toegang tot een beveiligd netwerk of scheiding van klanten, met name bij het aanbieden van diensten in de cloud. Het aanvalsoppervlak kan zich beperken tot een website en/of mobiele applicaties, maar soms krijgen we carte blanche om alles wat onder de bedrijfsnaam valt in het trajectplan op te nemen. Daarbij richten wij ons niet zo zeer op social engineering, dus het testen van mensen, maar op de technische kant. Op die manier kunnen we heel gericht aantonen waar het fout gaat, tot welke consequenties dat leidt en welke acties je moet ondernemen om de kwetsbaarheden op te lossen."

OUT-OF-THE BOX DENKEN

Na het in overleg bepalen van de scope treedt het testtraject in werking, op iteratieve wijze, dat wil zeggen het doorlopen van een cyclus. "Wat zien we aan zwakke plekken binnen het aanvalsoppervlak, kunnen we ze daadwerkelijk misbruiken - soms zit er toch een bepaalde mate van beveiliging achter - en zijn we vervolgens in staat om dieper binnen te dringen? We gebruiken geautomatiseerde scantools, maar die herkennen over het algemeen alleen bekende en gepubliceerde kwetsbaarheden, zoals updates van Windows en webservers. De bevindingen doorgronden en correleren tussen applicaties en zwakke plekken, daar zijn deze tools vaak weer niet zo sterk in, dus gaan we ook handmatig dingen interpreteren en manipuleren. Dat betekent out-of-the-box denken en er een creatieve blik op loslaten. Maatwerk, dus." Als voorbeeld noemt Van Veen een webformulier. "Daar vullen we alle mogelijke waardes in, ook heel rare, om te zien of de applicatie ze op een veilige manier verwerkt. Stel je voor dat het mogelijk blijkt om de database binnen te komen en daar commando's in te voeren. Een ander voorbeeld is de gevoeligheid voor onveilig uploaden: dat je niet een plaatje verzendt, maar een bestandje met een code om de volledige webserver over te nemen."

WANNACRY-VIRUS

Waar liggen zoal de kwetsbaarheden in het bedrijfsleven? "Er valt veel te winnen in grote kantoornetwerken," zegt Van Veen, zelf veelvuldig actief als pentester. "Bij de meeste die wij onder de loep nemen lukt het ons om binnen één à twee dagen volledig beheerder te worden. Standaard wachtwoorden, slecht geconfigureerde netwerkschijven, de logingegevens van beheerders in scripts opslaan, we komen het heel vaak tegen. Rondom webapplicaties gaat het veelal om programmeerfouten, die een hacker toegang geven tot de database of het besturingssysteem van de server. Deze zijn vaak te herleiden tot de toptien van kwetsbaarheden, zoals gepubliceerd door de wereldwijde organisatie OWASP. Verder stuiten we regelmatig op verouderde versies van besturingssystemen, webservers en applicaties die erop draaien. Een tijdje geleden stelde een medewerker van ons binnen een bepaalde organisatie vast dat honderd werkstations kwetsbaar waren voor het WannaCry-virus: één druk op de knop en ze werden allemaal overgenomen."

HACKWEDSTRIJDEN

Heeft The S-Unit het traject van penetratietesten binnen een bepaalde tijdspanne afgerond, dan volgt een rapportage met de kwetsbaarheden, analyse van incidentele en structurele oorzaken, het gevolg voor de kroonjuwelen en advies over oplossingen. Van Veen: "Op verzoek bieden we ook nazorg, zoals het reviewen van maatregelen in de ontwerpfase en het periodiek opnieuw testen van bestaande of wisselende onderdelen. Verder organiseren we hackwedstrijden en workshops voor medewerkers van klanten, waaraan een toenemende behoefte bestaat. Op maatschappelijk vlak stellen we onze kennis beschikbaar aan een nieuwe generatie in het mede door ons geïnitieerde project 'Hack in the Class', waarmee leerlingen van basisscholen en het voortgezet onderwijs kennismaken met de goede kant van het fenomeen hacken. Een stukje bewustwording voor de toekomst, dus. Digitale beveiliging wordt immers alleen maar belangrijker."

Meer informatie: www.the-s-unit.nl

'IN HET BEDRIJFSLEVEN ONTSTAAT STEEDS MEER BEWUSTZIJN OMTRENT DIGITALE BEVEILIGING, MEDE DOOR DE INVOERING VAN DE AVG.'