AUDIT
MAGAZINE

INTERVIEWS | 21 DECEMBER 2022

EEN WACHTWOORD WIJZIGEN DAT NOOIT GELEKT IS? NIET NODIG!

Auteur: Bas de Jong MSc RA
Beeld: NFP Photography
Leestijd: 10 min

Hoe veilig zijn onze data en systemen eigenlijk? Prijswinnende hackers Thijs Alkemade en Daan Keuper van Computest geven het antwoord.

Wat doet Computest eigenlijk?

Daan Keuper (DK): “Computest heeft meerdere disciplines, maar vanuit Computest Security helpen wij klanten van begin tot eind. Wij hebben een preventieve cybersecurityafdeling waar wij kwetsbaarheden en risico’s beoordelen en trainingen verzorgen. Verder hebben wij een detectieafdeling waar wij de systemen van klanten kunnen monitoren om te beoordelen of er verdachte activiteiten zijn, en een incident-responseafdeling die komt invliegen als het toch een keer misgaat, bijvoorbeeld bij een ransomware-incident. Tot slot hebben we een governancetak waarbij we het beleidsmatige stuk als service aanbieden.”

En Sector 7?

DK: “Sector 7 is onze researchafdeling. Met Sector 7 werken wij niet voor klanten. Wij hebben ook geen winstoogmerk, maar doen securityonderzoek naar zaken die wij maatschappelijk relevant achten. Dat is ooit begonnen met auto’s, waarbij wij kwetsbaarheden vonden in de auto’s uit de Volkswagengroep. Wij hadden een visie op security van IoT-items (Internet of Things, apparaten die verbonden zijn met internet – red.) en hebben onderzoek gepubliceerd over een van de meest voorkomende apparaten waar wij op dat moment aan konden komen, een auto uit de Volkswagengroep dus. Door dit onderzoek werd er naar ons geluisterd. Sindsdien pakken wij producten en zaken op die maatschappelijk relevant zijn.”

Hoe komen jullie aan jullie expertise?

Thijs Alkemade (TA): “Ik heb wiskunde en informatica gestudeerd en had veel interesse in het ontwerpen van programmeertaal tijdens mijn studie. Na mijn studie ben ik de security ingerold.”

DK: “Ik ben hier eigenlijk altijd al mee bezig geweest. Op jonge leeftijd wist ik al dat ik de IT in wilde, ik ben ook vrij jong begonnen met security. Ik was vrij slecht in gamen en wilde liever weten hoe het werkte, daarna wilde ik weten hoe je het ‘kapot’ kon maken. Ik heb een master IT-security gedaan, maar daar leer je meer de theoretische kant en het echt praktische, dat komt daarbuiten. Ik ging als PEN-tester (penetratietester – red.) aan de slag en via wat omwegen kwam ik uiteindelijk hier terecht.”

Daan Keuper, Computest: “We kijken naar wat er speelt in de markt of de samenleving en wat we leuk vinden om te onderzoeken”

Nooit ergens voor vastgezeten? Ik vraag het maar even

DK: “Ha, nee zeker niet. Je hebt in deze sector een Verklaring Omtrent Gedrag (VOG) nodig en een strafblad kan je dan goed in de weg staan.”

Wat hebben jullie recentelijk bekeken?

DK: “Vorig jaar hebben wij gekeken naar de beveiliging van Zoom, wat natuurlijk ineens door de pandemie op grote schaal werd gebruikt. Maar we hebben ook naar de CoronaCheck-app gekeken en de examenmonitoringssoftware die studenten verplicht moesten installeren om thuis examens te kunnen maken. Dit jaar hebben we ons gericht op industriesoftware, zoals software die wordt gebruikt in fabriekshallen, kerncentrales en sluizen. Daar speelt een grote IT-securitybehoefte. Deze operationele technologie (OT) is heel anders dan een standaard IT-landschap.”

Doen jullie onderzoek op aanvraag of op eigen initiatief?

DK: “Dat kan allebei, maar vooral op eigen initiatief. We kijken naar wat er speelt in de markt of de samenleving en wat we leuk vinden om te onderzoeken. Maar het kan ook op verzoek en dat verzoek komt dan vaak van een van de afdelingen van Computest. Het zou bijvoorbeeld kunnen dat het incident responseteam nieuwe malware tegenkomt of een van de andere teams heeft een klant die nieuwe technologie heeft waar weinig over bekend is. Dat zijn zaken waar wij op aanvraag onderzoek naar kunnen doen.”

Wat levert jullie onderzoek op?

DK: “Het doel is dat we kwetsbaarheden die wij zien rapporteren, zodat deze dichtgezet kunnen worden voordat de buitenwereld daar lucht van krijgt. Maar wij publiceren ook technische details van kwetsbaarheden – nadat deze zijn verholpen – zodat andere securityonderzoekers daarvan kunnen leren en eventueel op kunnen voortbouwen. We proberen de wereld een stukje veiliger te maken.”

Met alles wat jullie zien, waar verbaas je je het meest over?

TA: “Soms vraag je je af hoe dingen in elkaar zitten en waarom dat zo is. En als je dan goed kijkt, blijkt het niet zo robuust te zijn ontworpen als je eigenlijk zou verwachten.”

DK: “Soms ziet iets er op het eerste gezicht heel complex uit, maar blijkt het niet zo moeilijk als ik op voorhand had verwacht. Software blijft uiteindelijk mensenwerk. Mensen programmeren en mensen maken fouten.”

Daan Keuper: “Het doel is dat we kwetsbaarheden die wij zien rapporteren, zodat deze dichtgezet kunnen worden voordat de buitenwereld daar lucht van krijgt”

Jullie hebben prijzen gewonnen

TA: “We hebben twee keer meegedaan aan de internationale competitie Pwn2Own. Dat is een hackwedstrijd waarbij van tevoren een aantal targets bekend wordt gemaakt. Vorig jaar was dat bijvoorbeeld Zoom. We hebben die wedstrijd beide keren gewonnen.”

DK: “Je moet dan binnenkomen in de applicatie via tot dan toe onbekende kwetsbaarheden en vervolgens het systeem volledig overnemen. We zijn ontzettend blij dat we die wedstrijd nu twee keer achter elkaar hebben gewonnen.”

Waren ze bij Zoom ook blij?

DK: “Jazeker, de kwetsbaarheid die in de software zat, zat er sowieso in. Wij hebben die aangetoond, zodat ze in staat zijn deze te verhelpen.”

TA: “Die kwetsbaarheid is daarna ook snel opgelost. Het idee van die competitie is dat je na het vinden van het probleem in contact komt met de organisatie om details uit te wisselen, zodat ze het kunnen herstellen. Pas nadat het opgelost is mogen wij erover praten.”

Onlangs waren jullie in Las Vegas. Wat hebben jullie daar gedaan?

TA: “Ik heb in augustus 2022 een presentatie gegeven op het hackerscongres Def Con in Las Vegas over kwetsbaarheden in macOS. Dat was een grote vondst met best verstrekkende gevolgen. Het heeft geleid tot een wereldwijde update van de systeemsoftware van Macs en aanpassingen in applicaties die op macOS draaien.”

Als je dan toch gehackt wordt, wat doe je dan?

DK: “Een responseteam komt naar je toe om je te ondersteunen. Zij onderzoeken wat er precies is gebeurd, hoe ze zijn binnengekomen en welke systemen er precies zijn geraakt. Ze proberen een totaalbeeld te krijgen van het incident en de impact daarvan. Vervolgens wordt er gekeken naar de herstelopties, omdat de klant zo snel mogelijk terug wil naar een normale situatie, of in ieder geval naar een situatie dat de meest kritieke systemen weer operationeel zijn. Wij onderzoeken hoe de aanvallers zijn binnengekomen, wat er is gestolen en wat je herstelopties zijn.”

Thijs Alkemade: “Houd bij technische maatregelen rekening met hoe je mensen werken en dat het werkbaar blijft”

Back-up herstellen en weer door?

DK: “Het herstellen van back-ups is een mogelijke oplossing als je niet bij je data kunt (mits de back-up niet ook versleuteld is door de hacker), maar niet als je data gestolen is. Ook kan het een probleem zijn als de back-up verouderd is of niet snel genoeg te herstellen valt.”

TA: “Als je nooit getest hebt je hele netwerk te herstellen vanaf een back-up kan het best dat dit twee weken duurt of helemaal niet lukt. Dan is je back-up dus niets waard.”

Hoe ga je om met gestolen of geblokkeerde data?

DK: “Wij nemen contact op met de criminelen en openen het contact voor onderhandelingen over het losgeld. Maar er moet van alles geregeld worden op zo’n moment. De medewerkers moeten worden ingelicht, de belangrijkste partners moeten op de hoogte worden gesteld en mogelijk moeten getroffen personen worden geïnformeerd of gemeld worden

bij de Autoriteit Perspoonsgegevens. Er komt heel wat op je af, mensen verkijken zich vaak op hoeveel impact zoiets heeft op je bedrijfsvoering en op je medewerkers."

Onderhandelen met criminelen?

DK: "Het hele businessmodel van de hacker is erop gericht dat jij betaalt en dat jouw problemen daarna zijn opgelost. Als dat niet zo is, dan betaalt niemand meer. Dus hoe gek het ook klinkt, zij zijn erbij gebaat dat hun 'klant' enigszins tevreden blijft. Maar ze zitten er wel voor het geld. Men heeft dus geen zin in ellenlange onderhandelingen. Ze draaien op snelheid en volume. Niet betalen is ook prima, maar dan ben jij alles kwijt en gaan zij door naar de volgende."

Thijs Alkemade: "Als je nooit getest hebt je hele netwerk te herstellen vanaf een back-up kan het best dat dit twee weken duurt of helemaal niet lukt. Dan is je back-up dus niets waard"

Kun je iets zeggen over de oorzaak van hacks?

DK: "Vaak zijn het updates die niet worden gedraaid, wachtwoorden die worden hergebruikt of phishing. Mensen hebben de neiging wachtwoorden op meer dan een plek te gebruiken en als een van die plekken gehackt wordt ligt je wachtwoord dus op straat. Je moet een wachtwoord zien als een geheim tussen jou en de partij aan wie je dat wachtwoord geeft. Met hoe meer partijen je dat deelt, hoe groter het risico dat het geheim een keer verklapt wordt."

En het beheer van rechten binnen de organisatie zelf?

DK: "Wij testen veel op toegangsrechten in interne netwerken en, los van dat gebruikers soms te veel rechten krijgen, zijn er veel trucjes om van lage rechten naar volledige rechten te gaan. Dat lukt tot nu toe eigenlijk altijd wel. De partij die die initiële rechten heeft, is vaak een andere partij dan de uiteindelijke aanvaller die de ransomware installeert. De eerste groep noemen we de Initial Access Group en het enige wat zij doen, is bij bedrijven binnenkomen. Zij verkopen die toegang vervolgens op allerlei online forums, gesorteerd per sector, grootte van bedrijf en jaaromzet. Groeperingen die die toegang kopen proberen vervolgens de rechten om te zetten naar een systeembeheeraccount, zodat ze data naar buiten kunnen kopiëren, virusscanners kunnen uitzetten en ransomeware in het hele netwerk kunnen plaatsen. Vaak onderzoeken ze die data ook en weten ze bijvoorbeeld of je een cybersecurityverzekering hebt en tot welk bedrag je verzekerd bent. Hackers zijn soms een paar maanden binnen voordat ze toeslaan."

Is het een balans tussen gemak en beveiliging?

DK: "Bij security is het een beetje een ongelijke race, omdat de verdediging alles goed geregeld moet hebben terwijl de aanvaller maar één manier hoeft te vinden. Maar je kunt het ook omdraaien. Als die aanvaller eenmaal binnen is, zijn er veel manieren om de aanvaller te detecteren. Dan hoeft de aanvaller maar één keer verkeerd te klikken en dan weet je dat hij er zit. En dan kun je er wat mee. Maar de meeste klanten investeren wel in de preventieve kant, maar niet of nauwelijks in het detecteren van aanvallen. Partijen kunnen veel winnen door meer te investeren in detectie."

Zit het ook voor een deel in het bewustzijn van mensen?

DK: "Ik vind zelf dat we de schuld niet bij de gebruikers moeten leggen, maar dat we technische oplossingen moeten ontwerpen waarmee we de gebruiker van minder groot belang kunnen maken. Gedrag zou er idealiter niet toe moeten doen. Als je nu veilig wilt werken vraag je heel veel van je medewerkers. Zij moeten allerlei dingen nalaten of juist wel doen om op een veilige manier te kunnen werken. In de praktijk werkt dat niet. Een gebruiker wil gewoon zijn werk doen en wil helemaal niet bezig zijn met security. Dat is ook niet zijn expertise. Ik zie veel bedrijven die investeren in phishingsimulaties, maar als ik kijk naar de incidenten die we zien dan zijn moderne phishing mails niet van echt te onderscheiden. We moeten naar een wereld toe waarin IT-security het echte werk niet in de weg staat."

Zeg je dat awareness niet belangrijk is?

DK: “In bepaalde mate niet nee. Je hebt wel iets van awareness nodig, maar ik zou liever zien dat we naar technische maatregelen gaan die ervoor zorgen dat we minder van gebruikers vragen. Of, wanneer een gebruiker toch op een phising mail klikt, het effect hiervan beperkt is tot alleen die gebruiker en zijn systeem. Eén groot securityincident is niet hetzelfde als twintig kleintjes die in een half uur per keer zijn opgelost. Daar moeten we naartoe. Als je ervan uitgaat dat je je bedrijf kunt beschermen door ervoor te zorgen dat gebruikers niet op linkjes klikken, dan kom je van een koude kermis thuis. Een awarenesstraining is een relatief goedkope oplossing, maar biedt misschien meer schijnzekerheid dan echte security.”

En de combinatie van techniek en gedrag?

DK: “Ja, als we het hebben over awareness hebben we eigenlijk al een beetje verloren. Het zit in meer dan alleen het gedrag van mensen. De techniek kan ervoor zorgen dat dingen simpelweg niet mogelijk zijn, het gedrag moet ervoor zorgen dat die techniek goed wordt toegepast. En gedrag raakt aan cultuur, dat is moeilijk snel te veranderen, maar in

sommige gevallen heel relevant. Als je gedragsverandering wilt, moet je dat vanaf het bestuur/de directie uitrollen en afdwingen. Maar ja, hoeveel board members ken jij die fanatiek met een wachtwoordmanager aan de slag gaan? Daar zit een uitdaging."

Welke ontwikkelingen zien jullie op dit moment?

DK: "We zien dat via sociale platformen mensen worden benaderd om een deel van hun zakelijke accountgegevens te verkopen. Maar ook dat inloggegevens actief worden verhandeld."

Thijs Alkemade: "Je wilt security die voor mensen werkt en niet tegen ze"

TA: "Er is een zeer actieve handel in inloggegevens. Dat maakt het risico van het hergebruiken van wachtwoorden of het gebruiken van dezelfde wachtwoorden bij verschillende accounts erg groot."

DK: "We zien ook een trend dat multifactor authenticatie wordt gecombineerd met phising mails of notificaties via apps. Aanvallers loggen honderd keer in en er is altijd wel een gebruiker die op de mail klikt ter bevestiging. Dan zijn ze ook binnen. Dus multifactor is absoluut goed voor de beveiliging, maar het is niet zo dat je daardoor 100% veilig bent."

Geldt dit alleen voor zakelijke gebruikers of ook voor particulieren?

DK: "Voor particulieren geldt dat ze hun IT eigenlijk volledig hebben uitbesteed en niet in eigen beheer hebben. Wat je als particulier moet doen is 1) installeer updates tijdig; 2) gebruik een wachtwoordmanager; 3) zet multifactor authentication aan waar mogelijk. En met betrekking tot detectie: schaf een virusscanner aan."

Is een wachtwoordmanager niet een groot risico?

DK: "Als een hacker daar toegang toe krijgt ligt alles op straat. Maar als je een wachtwoordmanager hebt die wachtwoorden alleen op je computer opslaat, dan kan het goed werken. Heeft een aanvaller toegang tot die computer, dan is het sowieso al game over, los van de wachtwoordmanager. Een wachtwoordmanager gebruiken is beter dan hetzelfde wachtwoord hanteren bij verschillende accounts, want je kunt niet honderd verschillende wachtwoorden onthouden. De kans dat een webshop waar jij je gegevens hebt achtergelaten wordt gehackt is groter dan een wachtwoordmanager die zijn businessmodel hiervan heeft gemaakt."

Daan Keuper: "Ik ben geen fan van phisingsimulaties. Wat mij betreft heb je dan sowieso al verloren"

Nog tips voor bedrijven?

DK: "Eerste tip: zoek naar technische maatregelen om de impact van aanvallen te beperken en zorg dat je minder afhankelijk bent van gedrag. Een tweede tip is dat je een incident oefent. Als het gebeurt is namelijk iedereen in rep en roer en komt er veel op je af. En als derde: maak een business continuity plan en vergeet daarbij je leveranciers niet."

TA: "Ik wil bij de technische maatregelen toevoegen dat je rekening houdt met hoe je mensen werken en dat het werkbaar blijft. Je wilt security die voor mensen werkt en niet tegen ze. Als bijvoorbeeld attachments standaard worden verwijderd gaat men actief op zoek naar manieren om dat te omzeilen."

Nog meer wat je juist niet moet doen?

DK: "Ik ben geen fan van phishingsimulaties. Wat mij betreft heb je dan sowieso al verloren. En een wachtwoordpolicy dat een minimumlengte, hoofdletter, speciaal teken en iedere-dertig-dagen-wijzigenregels oplegt: stop daarmee."

TA: "Ja, wij zien dan dat het vorige keer op 03 eindigden dus laten we nu eens 04 proberen. Het maakt wachtwoorden onveiliger, omdat het niet past in de praktijk van de gebruiker. Waarom zou je een wachtwoord dat nooit gelekt is

moeten wijzigen?”

DK: “Gebruik desnoods een wachtwoordmanager of neem een zin in plaats van een woord, maar laat de vrijheid bij de gebruiker en zet het niet vast in een beleid.”

Over
Daan Keuper is hoofd van de securityresearchafdeling bij Computest. Deze afdeling is verantwoordelijk voor diepgaande security research op veelgebruikte systemen en IT-omgevingen.

Thijs Alkemade studeerde wiskunde en informatica. Hij werkt op de securityresearchafdeling bij Computest. Alkemade won twee keer de Pwn2Own-competitie, onder meer door kwetsbaarheden in Zoom aan te tonen.

Tags: Cyber resilience

Bron url: https://auditmagazine.nl/interviews/een-wachtwoord-wijzigen-dat-nooit-gelekt-is-niet-nodig/