Auteur: Chris de Vries is redacteur van iB-magazine. Hij werkt als zelfstandige professional werkzaam onder de naam De Vries Impuls Management. Chris is bereikbaar via e-mail: impuls@euronet.nl. Het artikel is op persoonlijke titel geschreven.

Afbeelding 1 - De setting van de cyberoefening.

Overheidsbrede cyberoefening

Het is 1 november, het weer is redelijk en de A1 weer jammer genoeg vertrouwd druk. Het zou een dag als zoveel andere kunnen zijn, ware het niet dat het fictieve Sociaal Werkbedrijf Bison juist vandaag erachter komt dat zij gehackt zijn. Bison vertegenwoordigt zeven gemeenten met 300.000 inwoners en draagt o.a. de verantwoordelijkheid voor 4.500 uitkeringen en de salarisadministratie rondom detacheringen. Een crisis van de eerste orde dus.

Met deze uitdaging wordt een crisisteam geconfronteerd bestaande uit de bekende C-managers, nu voor deze gelegenheid gerekruteerd uit het Nederlandse bedrijfsleven, de overheid en security-specialisten. Ze zijn allen naar Amersfoort gekomen om dit avontuur voor de camera te spelen. Thuis of op het werk zitten ruim 320 publieksdeelnemers en in de zaal circa 40 genodigden. Ikzelf observeer de oefening om van te leren en om een verslag met de lezers van dit magazine te delen.

De casus is realistisch. Het werkbedrijf zit midden in een transitieperiode waarbij de 'switch' naar de cloud wordt gemaakt, maar men is nog niet klaar (50% gereed) en ook zijn net niet alle kwetsbaarheden op tijd gepatcht. De eerste stap was van de CISO dan ook om alle systemen uit te zetten. Dat brengt mij meteen tot dilemma 1 in een dergelijke situatie: 'zet je de systemen uit of houd je ze actief?'. De overwegingen: moet je als CISO dat besluit zelfstandig nemen of overleg je daarover? Verder, is het belang van een justitieel opsporingsapparaat hoger dan het belang van het werkbedrijf om verdere hack-activiteiten te blokkeren?
Het crisisteam begint vervolgens met een inventarisatie van de risico's. In dit scenario moet men ervan uitgaan dat persoonlijke data (BSN) is buitgemaakt, dat uitkeringen geblokkeerd zijn (net de dag voor de uitkeringsdatum), dat ook de gedetacheerden de hack zullen ervaren en erger nog dat men niet meer beschikt over actuele data! Ook wordt meteen aangekaart dat er een 'ransomware note' met de eis van € 300.000,00 is gevonden en of men in onderhandeling met de dader(s) moet treden. De crisisteamleider sprak daarbij de verschillende teamleden afzonderlijk aan en vroeg elk van hen dienaangaande te adviseren. Het gesprek verliep daardoor civiel en geordend. Opvallend was ook dat de crisisteam spelers een goede balans wisten te vinden in de interne en externe communicatie. Wat ik wel miste was het fictief op tafel leggen van een crisisplan en het werken vanuit een dergelijk plan. In de spelpraktijk leek men een

dergelijke route wel te volgen.
In een verdere fase van het spel kwam de keten aan bod. Er werd bediscussieerd de ketenpartners te informeren, na te gaan in hoeverre zij getroffen waren door deze hack en af te stemmen of een gezamenlijke actie nodig c.q. mogelijk is.
Aardig feitje tussendoor; het PvIB is enige jaren terug intensief bezig geweest de ketenrisico's in beeld te brengen en te zien of er coördinatie mogelijk zou zijn tussen de diverse 'stakeholders'. De noodzaak wordt alom onderkend, maar de uitvoering is een zaak apart. Benieuwd hoe de stand van zaken nu is. Een ludieke reactie vanuit de toeschouwers thuis was, om maar alvast Chinese maaltijden te bestellen, want het zal nog wel even duren. Na de pauze ging de casus verder. Nu was bekend dat zeker van 1.000 inwoners data was gestolen, waaronder naam, geboortedatum en BSN. De 'deadline' van de melding aan de Autoriteit Persoonsgegevens (AP) kwam aan de orde alsook dat men onderhandelde met de aanvaller en het losgeld had weten terug te dringen tot € 200.000,00 De vraag werd door de spelers gesteld of de gemeenten zouden instemmen met betaling. Hier komt voor mij dilemma 2 aan de orde. De politie dringt bij bedrijven erop aan nooit losgeld te betalen. Binnen de overheid wordt er verder over nagedacht om betaling van losgeld vanuit verzekeringsmaatschappijen (verzekerde gebeurtenissen) te verbieden. Consequentie: bedrijven dragen alle kosten en de reputatieschade; zij kunnen die niet verhalen. Wat nu bij overheidsinstellingen? Als zij zouden betalen dan zou voor de overheid blijkbaar andere regels gelden en alle schade die zij oplopen (behalve de reputatieschade) verrekenen zij via belastingen, retributies en toeslagen aan de burger door. Dit lijkt mij zeer onredelijk en dus een moreel dilemma.

Persoonlijke mening: conform het principe van 'gelijke monniken, gelijke kappen' zou ook de overheid de pijn zelf echt moeten voelen en dat zou alleen zo zijn als de getroffen overheden gekort worden op hun budgetten zonder het recht tot herbestemming van budgetten of het aanvullen uit andere bronnen. Dit zou dan door de Rekenkamer gecontroleerd moeten worden.
Voordeel: de overheid voelt de pijn en zal alles op alles zetten om de keten te versterken en dus professionele steun te gaan bieden aan de zwaksten in de keten, t.w.: slecht functionerende overheden, maar ook hun toeleveranciers zoals het Midden- en Kleinbedrijf, die te klein zijn of niet beschikken over de professionaliteit om zich te wapenen tegen superieure hackers (waaronder statelijke actoren) met grote buidels.

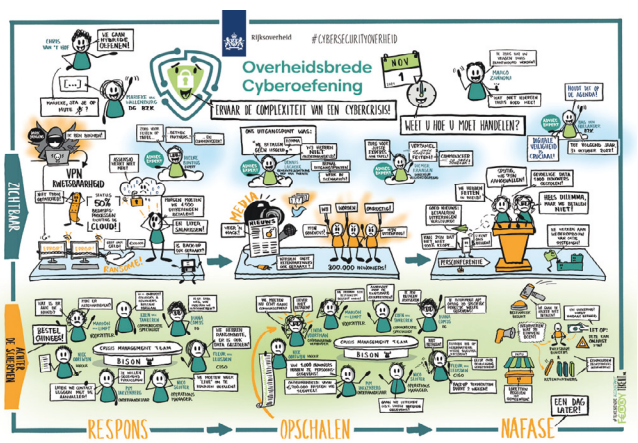
Boeiend was dat tijdens een pauze in het spel de heer Dennis Lacroix van de gemeente Hof van Twente openhartig verhaalt van zijn ervaringen met de hack bij hen. Zij hebben niet onderhandeld met de aanvaller en zij hebben bedrijfsmatige – en risico afwegingen gemaakt. Hun uitgangspunten: 1. wat zijn de belangrijkste pijnpunten; 2. wees transparant en 3. werk in scenario's en volg ze (ijk ze meteen). Inschakeling van de politie zagen zij als een moreel besluit. In deze spelcasus kwamen ook de gemeenten tot het besluit om niet te betalen. Gezien de diefstal van persoonlijke gegevens moest men de burger daarop attenderen en zeker de kwetsbare mensen daaronder. Vandaar dat besloten werd tot een getrapte aanpak en het rechtstreeks bereikbaar zijn voor deze burgers. Men formuleerden toen samen op welke wijze men naar buiten zouden treden – door middel van een persconferentie – en wat men zou mededelen. Ook dat het gebrek aan actuele data ertoe zou kunnen leiden dat uitgevoerde betalingen onjuist zouden zijn. Zo dat het geval dan zou laagdrempelig en opgeschaalde toegang tot gemeente en werkbedrijf geborgd zijn.

Aan het einde van deze oefening werden de deelnemers naar hun bevindingen gevraagd. De belangrijkste constateringen:

- Houd elkaar vast/ steun elkaar;
- Oefen het teamwerk;
- Zorg dat er ook van buiten naar binnen wordt gekeken;
- Focus op alle burgers, persoonlijke focus daar waar het verkeerd gaat;
- Luister naar de experts en
- Oefen, oefen en oefen.

Alles bij elkaar een leuke en leerzame middag en in vergelijking met andere oefeningen (vanuit het bedrijfsleven en de beveiligingssector) een verrijkende blik in de keuken van onze overheid. Goed om het denken ook van die kant te leren kennen.

Voor een visuele notulering zie navolgende tekening:



Afbeelding 2 - Visuele notulering Overheidsbrede Cyberoefening.

Laatste weetjes:

-de vierde Overheidsbrede Cyberoefening vindt plaats op 31.10.2022
-voor wie de training wil terugzien:
https://www.weerbaredigitaleoverheid.nl/inloggen/ (wachtwoord vereist!)