DESIGN – WEEK 4

Opstellen van een verhaal die ondersteund wordt door de sketches uit week 3.

CYBER ATTACK TRENDS

“Storytelling/Narrative”

Deze week is er nagedacht over welk verhaal er verteld gaat worden bij de opgemaakte schetsen.

Titel:

Cyber Attacks: A freely available weapon that affects everybody

Opening:

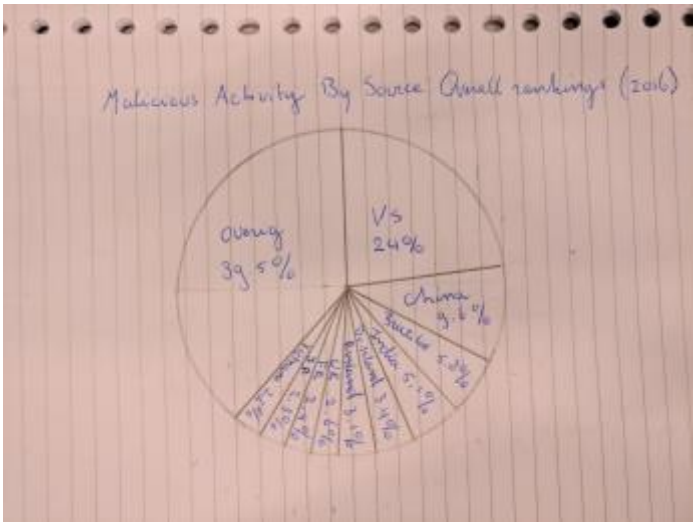
Wat als iemand met een enkele druk op de knop het elektriciteitsnet van een compleet land kan uitschakelen?

Wat als alle digitale systemen in een ziekenhuis worden gegijzeld?

Wat als de verkiezingsuitslag beïnvloed wordt door andere overheden?

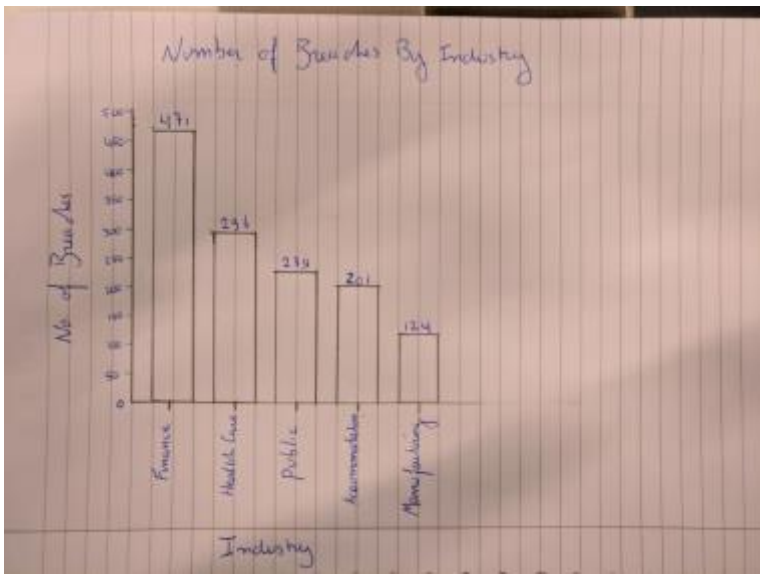
Het internet is over de jaren heen enorm gegroeid en is niet meer weg te denken uit de samenleving, tegelijkertijd wordt het ook vaker ingezet met kwade bedoelingen. Laten we eens kijken wie verantwoordelijk zijn voor deze Cyber attacks en wat deze voor gevolgen met zich meebrengen.

Sketch 1



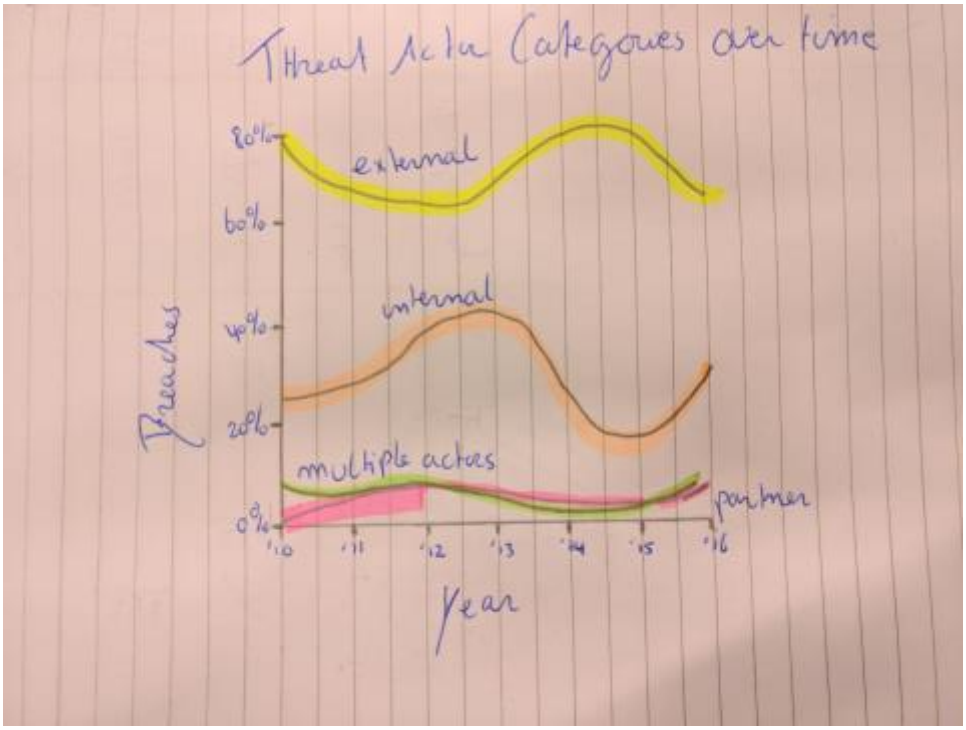
Actoren uit de Verenigde Staten waren in 2016 voor bijna een kwart van alle digitale kwaadaardige activiteiten verantwoordelijk, gevolgd door China en Brazilië.

Sketch 2



Uit een overzicht van alle datalekken in 2016, kan opgemaakt worden dat de financiële-, gezondheids- en publieke sector het vaakst doelwit zijn van dergelijke Cyber Attacks. Een datalek is een gebeurtenis waarbij persoonlijke en/of vertrouwelijke informatie zonder toestemming wordt buitgemaakt of vrijgegeven.

Sketch 3

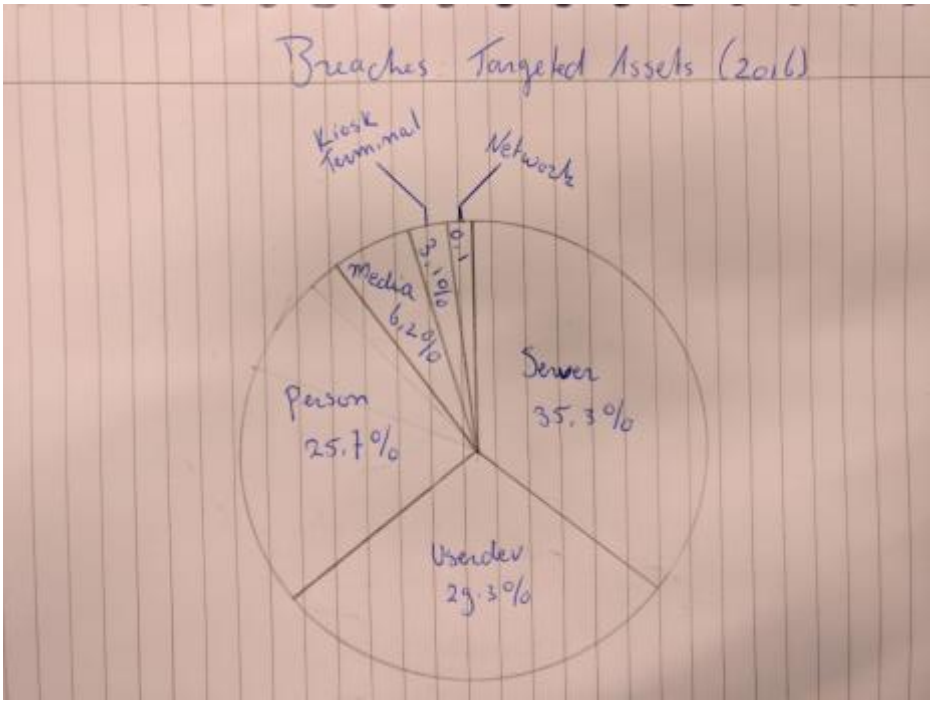


Actoren kunnen we onderverdelen in een aantal categorieën, zo onderscheiden we:

- Externe actoren zoals hackers, overheden en amateurs. Zij hebben profijt bij het lekken van data en handelen vaak met kwade bedoelingen.
- Interne actoren zoals medewerkers waaronder de receptionist, het ICT-personeel of de directie. Datalekken door medewerkers zijn vaak onbewust en niet georganiseerd.
- Meerdere actoren zijn een combinatie van interne en externe actoren
- Partners zijn derde partijen die een organisatie in dienst heeft.

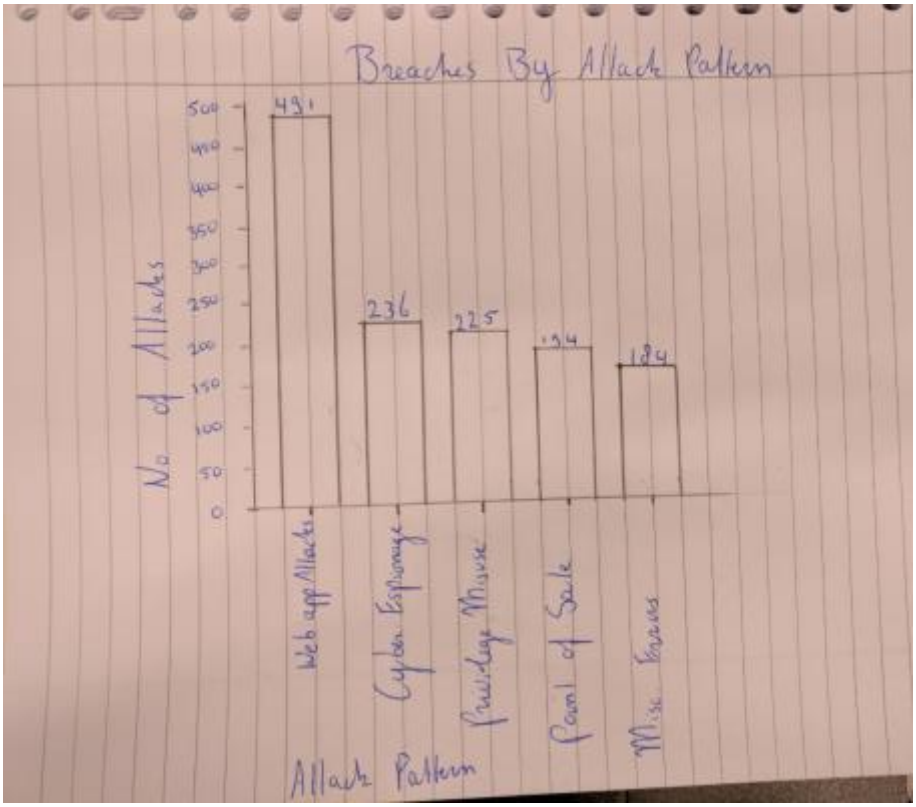
Duidelijk is geworden dat over de jaren heen de externe en interne actor de overhand heeft bij het lekken van data.

Sketch 4



Het blijkt dat servers het vaakst doelwit zijn van aanvallen, opvolgend door gebruikersapparaten. Opvallend is dat personen vlak daarachter volgen, dat wil zeggen datalekken die tot stond komen door het manipuleren van personen binnen een organisatie. Denk bijvoorbeeld aan iemand die zich voordoet als een medewerker van het bedrijf, en daardoor toegang krijgt tot gevoelige informatie. Cyberaanvallen hoeven dus niet per se over het internet te gebeuren, maar dit gebeurt ook veel door in de ‘echte’ wereld slimme trucs toe te passen.

Sketch 5



Er zijn veel verschillende soorten aanvallen te onderscheiden. Degene die er vooral bovenuit springt is de webapplicatie-aanval. Dit is wel een hele brede categorie; hieronder valt bijvoorbeeld een aangepaste bankoverboeking, waardoor je in plaats van 300 euro 3000 euro overmaakt, maar ook het uitschakelen van de beveiliging op een bank-app.

Cyberspionage staat op een opvallende tweede plek. Dit zijn vaak overheden die elkaars staatsgeheimen proberen te verkrijgen door middel van hacking, met vaak politieke of militaire doeleinden.

Conclusie:

Wat voor gevolgen hebben deze cyberattacks nu voor jou? We zien steeds meer dat cyberattacks zich richten op de maatschappij, bijvoorbeeld de publieke sector of ziekenhuizen. Zo was er dit jaar nog een grootschalige ransomware-aanval genaamd Wannacry, die een grote impact had op digitale systemen in de hele wereld - het besmette meer dan 230.000 computers. Onder andere ziekenhuizen in het Verenigd Koninkrijk werden platgelegd, en de complete bedrijfsvoering van de Rotterdamse haven werd stilgelegd. De schade van dat laatste incident bedroeg tientallen miljoenen euro's.

Ook een aanval op Oekraïense infrastructuur had verregaande gevolgen. De aanval zorgde ervoor dat 230.000 mensen een dagdeel zonder stroom zaten. Deze aanval is hoogstwaarschijnlijk door statelijke actoren uitgevoerd.

Bij de laatste Nederlandse verkiezingen is besloten om geen software te gebruiken om stemmen te tellen, vanwege de angst dat deze gehackt zou kunnen worden.

Uit deze incidenten blijkt dat aanvallen geen abstracte gevolgen hebben voor jou als burger, maar wel degelijk invloed hebben op de maatschappij en daarmee iedereen als persoon.