2 CYBERSECURITY TRENDS

De wereld om ons heen is toenemend aan het digitaliseren. Dit brengt vele gemakken met zich mee, niet alleen voor de gebruikers van online services, ook voor kwaadwillenden. Cybercriminelen weten op afstand schade toe te richten aan nietsvermoedende personen en worden hierbij steeds creatiever in hun aanpak. Vooral op het gebied van machtigingen, waar mensen toegang verleend worden tot persoonlijke zaken van anderen, dienen er preventief maatregelen genomen te worden om gebruikers te beschermen. Er zal daarom onderzoek worden gedaan naar de laatste trends op cybersecurity gebied, om de veiligheid te kunnen waarborgen.

Naam Jens van Lierop
Datum 09-03-21

Versie 1.3

DOELEN

Wat moet er met dit onderzoek bereikt worden?

Richtlijnen

Meer informatie opdoen over cybersecurity en de daarbij algemeen gelded richtlijnen

Deze kunnen mogelijk invloed hebben op de uitwerking van he t concept.

Preventie

Aan de hand van de trends kunnen er preventieve maatregelen worden geïmplementeerd tijdens de design– en ontwikkelfase van het project.

Op deze manier kunnen problemen voorkomen worden

ONDERZOEKSVRAAG

Wat wordt er onderzocht?

Wat zijn de huidige trends op het gebied van cybersecurity?

- Wat zijn de meest voorkomende en groeiende vormen van cybercriminaliteit?
- Welk van deze ontwikkelingen vormt het grootste gevaar voor de doelgroep?
- Welk van deze ontwikkelingen vormt het grootste gevaar binnen de context van machtigen?
- Welke nieuwe maatregelen worden er genomen?
- Kunnen deze ingezet worden bij onze doelgroep?

METHODIEK

Welke onderzoeksmethode wordt er toegepast?

Trend onderzoek (Meta-analyse)

Net als bij het voorgaande onderzoek is het grootste deel van de informatie op het internet te vinden. Dit zal dan ook als primaire bron gebruikt worden.

Omdat cybersecurity op het moment een hot topic is, zijn er veel opsommingen van huidige trends beschikbaar. Door middel van een meta-analyse, waarbij deze lijsten van trends naast elkaar worden gelegd, kunnen we ontdekken waar de daadwerkelijke zwaartepunten op cybersecurity vlak.

"You can make use of reports of trend watchers who summarize major trends in almost any area. Some trends may be short term (a hype), while others are much more stable over time. Make sense of trends based on their underlying data.. Relate these trends to your own design challenge."

(HAN University of Applied Sciences, z.d.-c)

Aanpak

1. In de Google zoekmachine wordt de term: "Cybersecurity Trends" of gelijksoortige termen ingevoerd (afhankelijk van de resultaten). Er wordt vooral gezocht naar opsommingen van trends of bij voorkeur eerdere onderzoeksrapporten. De artikelen dienen afkomstig te zijn van een organisatie die zich in het ICT werkveld bevind, of een grote aanwezigheid op dit gebied. (Bijvoorbeeld Forbes).
2. De resultaten worden in bulk verzameld in een Excel sheet. De bronnen (+ jaartal) worden in de kolommen geplaatst, de verschillende trends in de rijen en als waarde wordt de positie van het item op de lijst uit de desbetreffende bron neergezet (zie figuur 1). In een apart Word bestand worden de belangrijke steekpunten van de artikelen opgesomd als naslagwerk.
3. De verschillende trends worden gecatagoriseerd naar thema, waarbij de waardes voor alle trends per thema worden gemiddeld, lege waardes worden vervangen met de waarde 10 (omdat dit de hoogst mogelijke waarde is in een trendlijst). Hierna zullen de waardes uit het Excel sheet worden verwerkt in een lijngrafiek die de gemiddelde positie per trend per jaartal weergeeft. Een lagere waarde betekent dus een hogere positie en dus dat het een belangrijkere trend is.

Bron →	Gartner			
Trend ↓	2017	2018	2019	2020
Brute force attacks -> Extended detection and response (XDR) solutions				
Continuous adaptive risk and trust assessment (CARTA)	3	10	7	1
AI/machine learning (ML), Deep fake attacks	10	4	10	2.5
Enterprise-level chief security officers (CSOs)				
Security operations centers (SOCs)	10	10	2	4
Safety, reliability and privacy -> Privacy becoming its own thing	5	10	10	5
Decentralization				
Cross-functional trust and safety teams				
Application and data security are led by development operations center	4	6	10	6
Cloud security	2	3	6	7.5
Zero-trust network access (ZTNA)	10	10	10	9
Leading SRM leaders are creating pragmatic risk appetite statements				
PROMOTING COMMUNICATION BETWEEN EXPERTS AND EXECUTIVES	10	1	1	10
"Passwordless" authentication/MFA	10	10	4	10
Shortage Security staff	1	10	5	10
Regulations (for example GDPR)	10	2	10	10
Origin beats pricing				
Third party supplier issues	10	5	10	10

Figuur 1: Opstelling Excel bestand

15 trends

Op het gebied van machtigen

5 jaar

Aan ontwikkelingen

100%

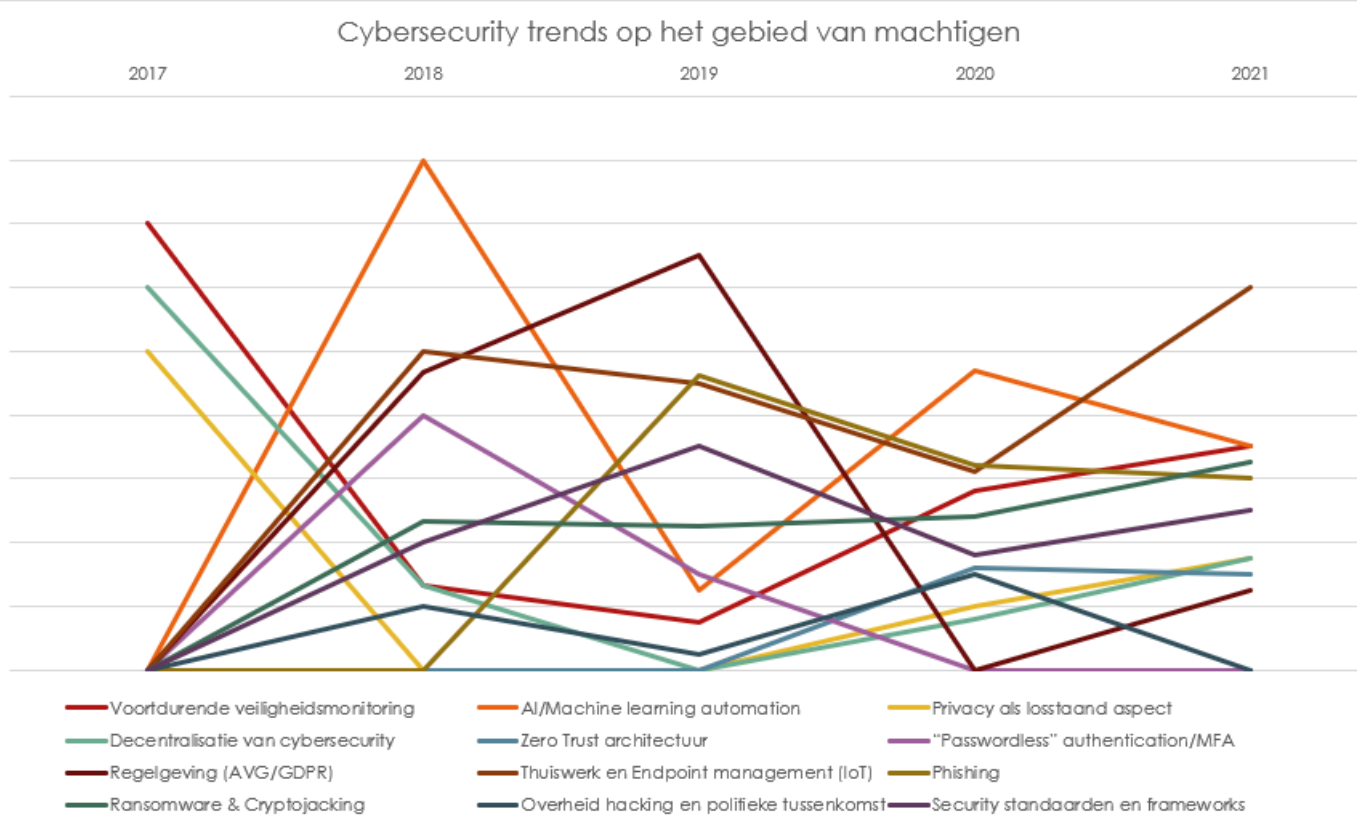
Komt meer dan 1x terug

RESULTATEN

Wat zijn de uitkomsten van het onderzoek?

Samenvatting

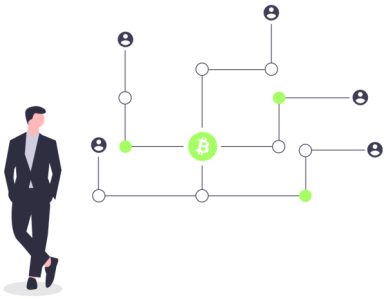
Onderstaande grafiek geeft de gemiddelde positie van de cybersecurity trends per jaar weer. Een van de belangrijkste ontwikkelingen is het gebruik van Artificial Intelligence/ Machine learning door zowel cybersecurity specialisten als cybercriminelen. Een aanhoudende trend zijn cyberaanvallen op basis van Phishing. Daarnaast is endpoint management een groeiende trend door de opkomst van Internet of Things aparaten en thuiswerken.



Figuur 2: Cybersecurity Trends grafiek

Toelichting

Bovenstaande grafiek geeft de trends van de afgelopen 4 jaar weer. Een aantal van deze trends, lijken tijdelijk popular te zijn zoals AVG en MFA. Andere trends daarentegen lijken zich elk jaar weer te herhalen. Problemen zoals phishing en ransomware, de interesse in AI en algemene veiligheidsstandaarden. In het 2021 lijkt vooral de focus te liggen op thuiswerken en de risico's dat dit met zich meebrengt. Op de volgende pagina's wordt iets dieper ingegaan op elk van deze aspecten.

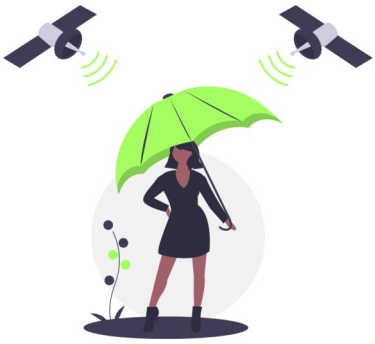


Decentralisatie van cybersecurity

Om te beginnen is dit misschien een van de belangrijkste redenen om het cybersecurity aspect mee te nemen in de ontwerp en ontwikkelfase van dit project. Veel bedrijven kiezen er vaak voor om ontwikkelaars op te leiden tot security specialisten in plaats van één afdeling verantwoordelijk te stellen voor de veiligheid van digitale omgevingen en producten. Zodoende kunnen veiligheidsaspecten kunnen implementeren in het ontwikkelproces.

Regelgeving - AVG/GDPR

Het tweede aspect om even uit de weg te werken gaat over regelgeving. Sinds de introductie van Algemene verordening gegevensbescherming (AVG) in 2018 is er binnen bedrijven een verhoogde focus op het veilig opslaan en verwerken van persoonsgegevens om boetes te voorkomen. (Dit blijkt ook uit de piek in 2019). Dit aspect is voor elke context van belang en uiteraard erg belangrijk voor ons project omdat het gevoelige data betreft.



Privacy als losstaande discipline

Een trend die laatste tijd steeds meer relevant aan het worden is, is privacy.
Niet langer is het slechts een onderdeel van het cybersecurity, auditing of juridische beleid, het is een groeiend onderdeel die alle taken van een bedrijf beïnvloed. Met onduidelijkheid over hoe gebruikersdata wordt gebruikt en verwerkt, wordt de vraag naar online privacy dan ook steeds groter.

Phishing

Phishing is en blijft een van de meest voorkomende vormen van cybercriminaliteit en zal niet verdwijnen. De reden is simpel, het is heel effectief en relatief eenvoudig: Criminelen maken gebruik van de zwakste schakel in een IT system: De mens. Door in te spelen op specifieke onzekerheden van een gebruiker, ook wel Social engineering genoemd, weten ze via deze gebruiker toegang te krijgen tot een IT systeem.

Ransomware & Cryptojacking

Wanneer een cybercrimineel toegang heeft tot een systeem, zijn er allerlei manieren waarop deze persoon schade aan kan richten. Tegenwoordig zijn Ransomware en Cryptojacking de grootste dreigingen. Ransomware gijzelt een IT systeem, waardoor deze compleet niet meer functioneert, tenzij er een borgsom wordt betaald aan de crimineel. Bij cryptojacking wordt het systeem stiekem door criminelen benut voor het genereren van cryptocurrency (ook wel ‘mining’ genoemd)

AI/Machine Learning Automation

AI is een van de meest veelbelovende trends op digitaal gebied. In de cybersecurity wereld, waar het tekort aan personeel alsmaar stijgt, is de inzet van AI onvermijdelijk. Ze bieden een manier om cybersecurity op een betrouwbare manier te automatiseren. Echter wordt AI niet alleen voor goede doeleiden gebruikt. Ook cybercriminelen maken er maar al te graag gebruik van. Ze gebruiken AI om de efficientie van hun aanvallen te verhogen.

Thuiswerk en Endpoint Management (IOT)

De COVID19 pandemie zag een groei aan mensen die remote vanuit thuis werken. Als gevolg van deze groei is het aantal externe apparaten dat verbonden is met een bedrijfsnetwerk is toegenomen (Bijvoorbeeld persoonlijke computers of smartphones). Deze zogenoemde 'endpoints' vormen een mogelijk infectiegevaar voor een bedrijfsnetwerk en daarom is het ook belangrijk dat deze zorgvuldig gemanaged worden. Ook smarthome apparten (ook wel bekend als IoT, of Internet of Things) die verbonden zijn met het internet vormen grote risico's

Zero Trust Architectuur

Een van de maatregelen die hiervoor worden toegepast is een Zero Trust Network/Architectuur. Dit type netwerk gaat uit van het principe dat geen enkel apparaat te vertrouwen is, onafhankelijk van locatie, verbinding of eerdere interacties. Pas na auditing van het apparaat en goedkeuring vanuit beide richtingen kan er toegang worden verschaft.

'Passwordless' Authentication/MFA

Ook authenticatie methodes veranderen langzaamaan. Wachtwoorden zijn niet meer van deze tijd en in veel gevallen niet veilig. Om inloggen soepeler en veiliger laten te verlopen worden vormen van Multifactor Authenticatie (MFA) ingezet, waarbij de gebruiker aanvullend op een wachtwoord ook een persoonsgebonden code moet aanleveren. Ook worden er steeds vaker manieren toegepast waarbij wachtwoorden niet eens nodig zijn zoals facial recognition of fingerprint scanners.

Security standaarden en frameworks

Tenslotte is het belangrijk dat je, ondanks de gevaren die je loopt in jouw specifieke werkveld, je altijd bewust bent van de standaardrichtlijnen van cyberveiligheid. Hieronder vallen zaken zoals toegangsbeheer en versleutelingvan gegevens. Er zijn verschillende standaarden en frameworks om dit toegankelijker te maken en deze dienen nageleeft te worden, anders is een incident onvermijdelijk.

CONCLUSIE

Wat kan er uit de resultaten geconcludeerd worden?

De belangrijkste trends op dit moment zijn AI, Phishing, Endpoint Management en AVG/Privacy

Vooral phishing zal mogelijk een problem vormen voor de doelgroep, omdat deze trend inspeeld op de zwakte van de mens en omdat ouderen en digibeten, vaak minder bekwaam zijn in het herkennen van dit soort valstrikken.
Omdat het bij machtigen vaak gevoelige informatie betreft zal er rekening moeten gehouden worden met zowel de privacy van de gebruiker als de wetgeving. Daarom zal er op een veilige en vertrouwelijke manier moeten omgegaan met de data en authenticatie op een goede manier moeten verlopen.

DISCUSSIE

Welke factoren kunnen invloed hebben gehad op de resultaten?

- De posities van de verschillende trends in elk artikel kunnen willekeurig zijn, zonder dat dit staat vermeld. Hierdoor zou de score per item kunnen afwijken van het resultaat.
- Het resultaat is een samenvatting van andere onderzoeken. De auteurs van de geraadpleegde bronnen kunnen de focus hebben liggen op het werkveld waarin ze actief zijn. Het aantal gebruikte bronnen ligt relatief laag en niet elke bron heeft voor ieder jaar een publicatie, waardoor het balans tussen de inbreng van elke bron per jaar verschillend is.

AANBEVELINGEN

Wat zijn de vervolgacties aan de hand van het resultaat?

Scope

Er moet bepaald worden welk van deze aspecten binnen onze scope vallen en welke buiten.

Hiervoor zal de opdrachtgever worden geraadpleegd.

Standaarden

Een van de actiepunten die direct opgepakt kan worden is het inlezen op standaarden over cyberveiligheid en deze toepassen binnen het project.

Phishing onderzoek

Gebruikerstests doen om te ontdekken voor welke vormen van phishing de gebruiker het meest vatbaar is en onderzoeken op welke manier we dit kunnen voorkomen