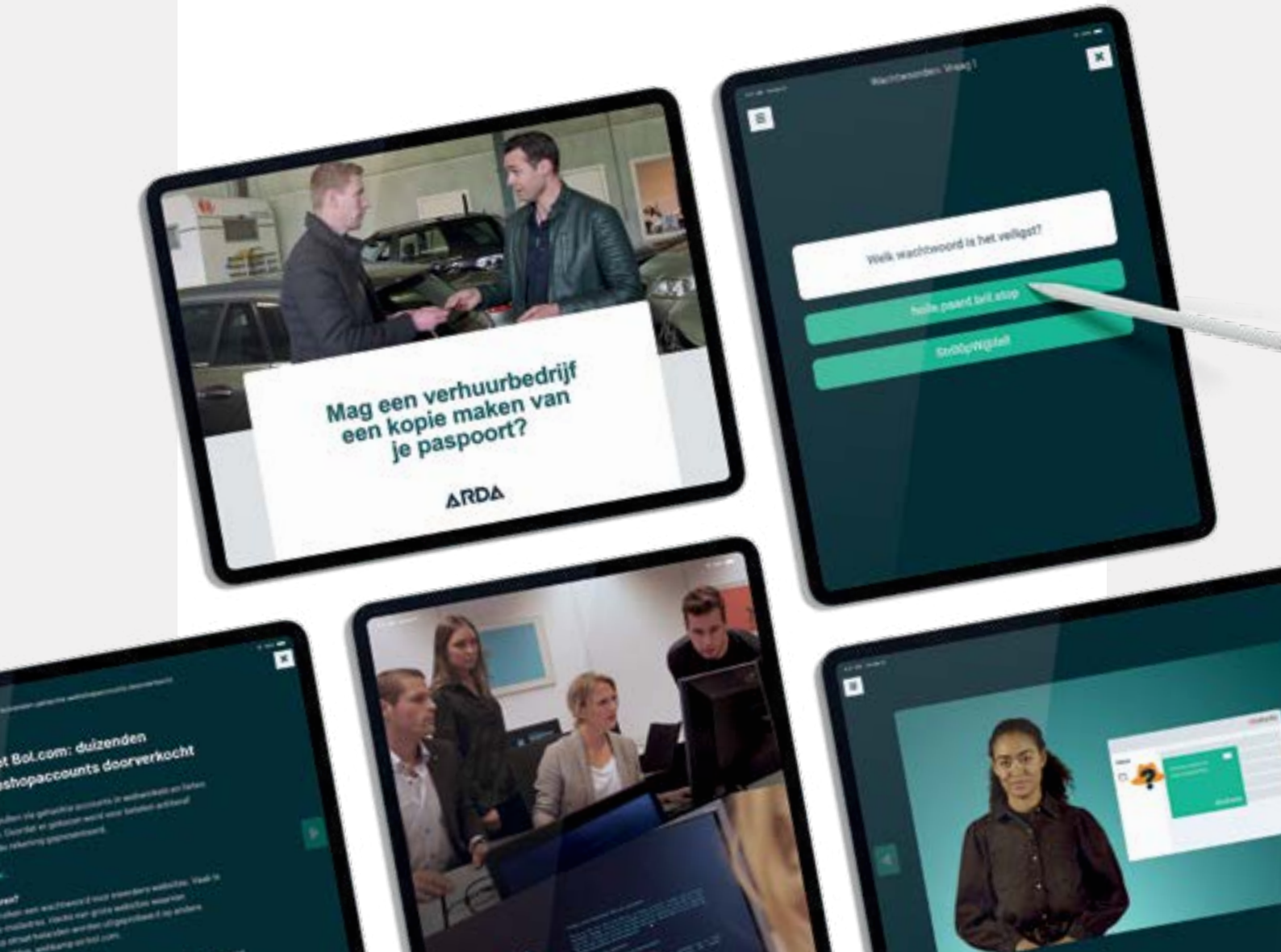
centric
connect.engage.succeed.

ARDA

Bescherm uw gemeente tegen cybercrime



Ook uw gemeente loopt gevaar

Online een rijbewijs verlengen, een vergunning aanvragen voor een dakkapel of een melding maken van overlast. Het gebeurt steeds vaker geheel digitaal. Maar wat als al deze processen van het ene op het andere moment stilstaan? Of misschien nog wel erger: wat als deze data zomaar op straat ligt?

Cybercriminelen beperken zich niet tot het bedrijfsleven, ze slaan steeds vaker toe bij gemeenten. Gemeenten zijn namelijk afhankelijk van digitale systemen én bewaren een enorme hoeveelheid data. Bescherming tegen cybercrime zou dus vanzelfsprekend moeten zijn. Maar dat is het nog niet. Het gaat nog veel te vaak mis. Regelmatig verschijnt in het nieuws dat een gemeente is gehackt. En dat terwijl alle inwoners en ondernemers erop vertrouwen dat hun informatie in goede handen is.

Het belangrijkste ingrediënt om de risico's van een cyberaanval te voorkomen, is kennis. Bij een cyberaanval is de medewerker namelijk vaak de zwakke schakel.

Hoe complex het beveiligingssysteem of IT-afdeling ook is, een cyberaanval komt door menselijk falen. Een te makkelijk wachtwoord, onveilig online gedrag of ondoordacht klikken op een link. Eén verkeerde handeling en de hacker is binnen. En die kans is groter dan u denkt.

Het geheim van cybersecurity is simpel

Wist u dat 90 procent van alle cyberaanvallen begint met een nepmailtje?

Het overkwam bijvoorbeeld gemeente Bergen op Zoom in 2020. Van negen medewerkers is via phishing de mailbox gehackt. Daarin zaten gegevens van vierhonderd inwoners. Ook gemeente Nuenen werd de dupe van een phishingmail. Het account werd gehackt en vervolgens misbruikt voor duizenden nepmails. En een onderzoek uit de Rekenkamercommissie bij de drie A2-gemeenten liet bovendien zien dat wachtwoorden van medewerkers makkelijk achterhaald konden worden.

Het is dus cruciaal om het bewustzijn op het gebied van digitale veiligheid te vergroten. Het begint met medewerkers bekend te maken met veilig online gedrag. Ze moeten de risico's leren herkennen van cybercrime en alert zijn op eventuele verstoringen. De vraag is natuurlijk: hoe doe je dat?

Arda leert medewerkers online gevaar herkennen

Cybersecurity is niet de verantwoordelijkheid van één persoon of afdeling. Het is voor iedereen van groot belang. Gemeenten zijn afhankelijk van digitale systemen en beheren een grote hoeveelheid (gevoelige) data van inwoners en ondernemers. Het is dus cruciaal dat álle medewerkers van de gemeente zich bewust zijn van de kenmerken en risico's van cybercrime. Met Arda lukt dat.

Speciaal om het kennisniveau over cybersecurity binnen gemeenten te vergroten, hebben wij een programma ontwikkeld. Geen eenmalige training, wel een awarenessprogramma dat communiceert, uitlegt en aandacht vraagt over online dreigingen. Een programma dat naadloos aansluit bij de wensen en behoeften van gemeenten over cybersecurity. Het combineert online leren met serious gaming. Al spelend ontdekken de deelnemers uiteenlopende vormen van cybercrime, en vooral: hoe ze zich ertegen kunnen wapenen.

Hier doen we het voor:

Recente cyberaanvallen in het nieuws die we voor uw gemeente willen voorkomen.

Gemeente	Wat
Gemeente Lochem	Hackers weten binnen te dringen in het ICT-systeem van de gemeente. De aanval was erop gericht om de administratie te versleutelen en losgeld te eisen. Er is sprake van een datalek. De aanvaller(s) hebben waarschijnlijk toegang gehad tot (gebruikers)namen en e-mailadressen van medewerkers en raadsleden.
Gemeente Hof van Twente	Mede door de goedgelovigheid van medewerkers weten hackers de systemen van de gemeente binnen te komen en plat te leggen. Data worden vernield, gewist, versleuteld en gestolen. Herstel van de systemen en hardware kost rond de acht ton. Daar komen de kosten voor onderzoek en dataherstel nog bij.
Gemeente Ede	Een medewerker trapt in een phishingmail en geeft onbewust de hacker toegang tot het e-mailaccount. Er worden in zes uur tijd meer dan 43.000 nieuwe phishingmails verstuurd naar willekeurige adressen. Waarschijnlijk heeft de hacker geen toegang gehad tot privacygevoelige bestanden, maar er is wel sprake van een datalek.
Gemeente Bergen op Zoom	Cybercriminelen slaan toe op het stadskantoor in Bergen op zoom. Negen medewerkers klikken op een phishingmail waardoor hackers toegang krijgen tot gegevens van vierhonderd inwoners. Het gaat om bestanden met persoonsgegevens waaronder naam, adres en BSN-nummers van Bergenaren.
Gemeente Dronten	Dankzij een phisingmail dringen hackers het computersysteem van gemeente Dronten binnen en gijzelen data. Een jaar eerder gebeurde dat ook. Bij de eerste aanval kon het personeel een dag niet werken. Bij de laatste lag het systeem twee uur plat. De gemeente weigerde het losgeld van tienduizenden euro's te betalen.

Gemeente Ede waarschuwt voor phishingmail

woensdag 17 november 2021

De gemeente Ede waarschuwt voor een phishingmail die vanuit een @ede.nl e-mailadres is verzonden. Het lukte hackers onlangs om met een nepmail de inloggegevens van een medewerker van de gemeente te pakken te krijgen. Vanuit het mailadres van deze medewerker zijn vervolgens grote hoeveelheden nieuwe phishingmails naar willekeurige emailadressen verzonden, zowel binnen als buiten de gemeente.

ede.nl

Het Arda-programma in het kort

Zoals gezegd wordt het programma verspreid over meerdere jaren.
Op regelmatige basis leren de deelnemers steeds een ander onderwerp kennen dat te maken heeft met cybercrime. Hierbij wordt altijd een verband gelegd tussen het gevaar en de werkvloer. Zo worden de risico's herkenbaar, voorkomen we verveling bij de deelnemers en wordt de theorie onmiddellijk toepasbaar in de praktijk.

We zijn het meest trots op de zogeheten Steinitz -reeks (vernoemd naar de grote schaker Wilhelm Steinitz). Dit zijn afleveringen van een spannende serie met scènes die worden gespeeld door Nederlandse acteurs. Zo krijgen de deelnemers te zien hoe een medewerker per ongeluk belangrijke data lekt, of hoe een CEO en zijn bedrijf slachtoffer worden van het fenomeen social engineering (wat dat precies is, wordt uiteraard uitgelegd).

Tijdens korte **e-learning** modules worden filmpjes afgewisseld met vragen. Zo worden deelnemers automatisch meegezogen in lessen over cybercrime. Ze krijgen onder andere te zien waarom tweestapsverificatie zo belangrijk is en hoe je dat instelt. Ook leren ze wachtwoordmanagers gebruiken.

Om de zoveel tijd worden de deelnemers onderworpen aan een **challenge.** Hierdoor wordt de kennis die tijdens de e-learnings is opgedaan opgefrist.

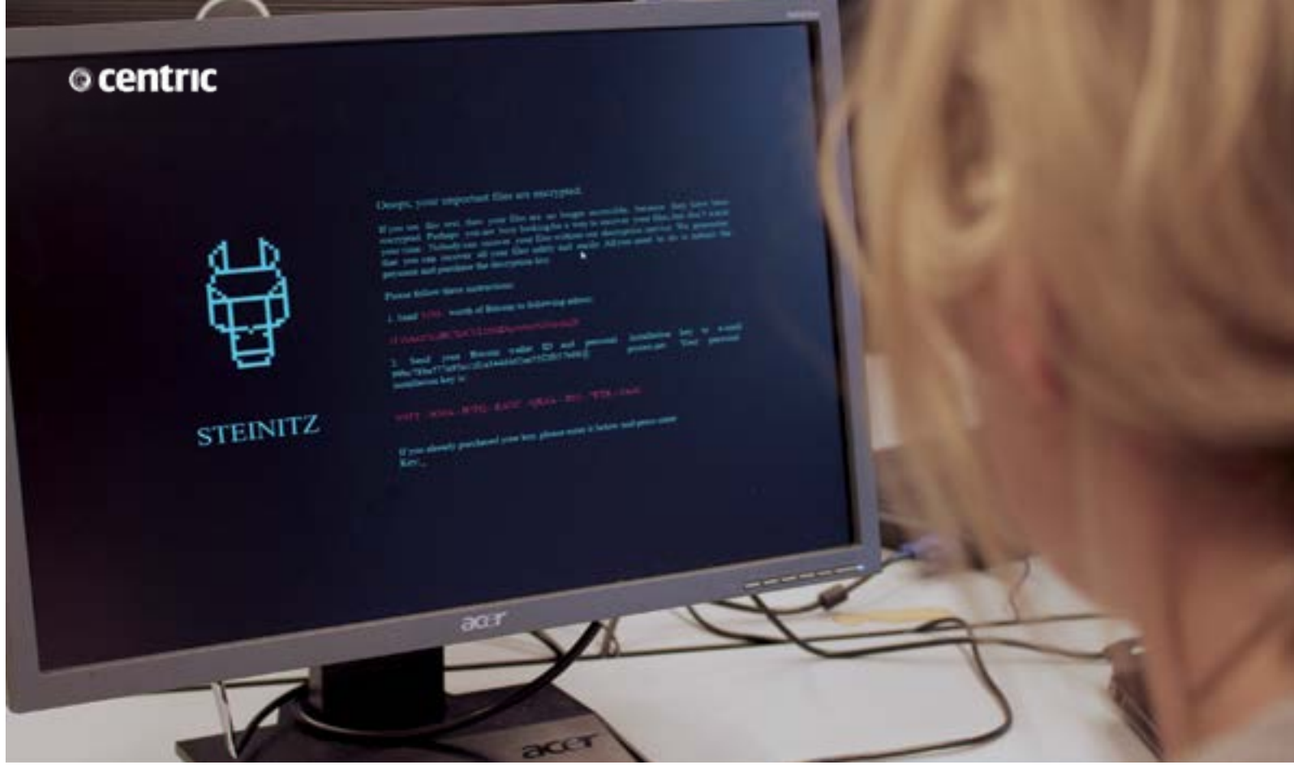
Daarnaast bekijken de deelnemers **interviews met experts en ervaringsdeskundigen.** Er komt onder meer een slachtoffer aan het woord die door hackers om de tuin is geleid en die zijn hele familie daardoor in de problemen heeft gebracht. Ook vertelt een journalist over het belang van cybersecurity, en legt een hacker zelf uit wat zijn manier van denken is.

Een ander belangrijk onderdeel van ons programma is de **phishingcampagne**. Phishing is een van de grootste gevaren voor alle organisaties. We leren de deelnemers nepmails herkennen en hoe te handelen. Deze kennis toetsen we vervolgens door een zogenaamde phishingmail naar ze te sturen.

Gedurende het hele programma houden we de resultaten bij, zodat we kunnen beoordelen hoe de medewerkers scoren. En of ze het beter doen naarmate het programma van Arda vordert. Want daar draait het om.

Wat Arda uiteindelijk oplevert:

- Medewerkers die bewust zijn van mogelijke digitale gevaren en zichzelf kunnen beschermen tegen cybercriminelen.
- Dit levert uiteindelijk een verlaging van het risico op een succesvolle cyberaanval op.

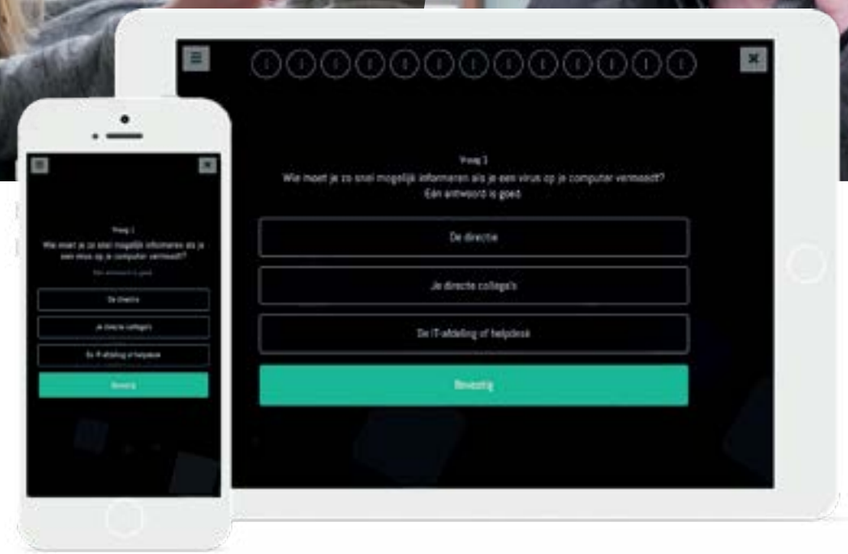


UITGELICHT

De unieke interactieve filmreeks: Steinitz

In aflevering 1 van Steinitz begint Ellis, de hoofdpersoon, nietsvermoedend aan haar werkdag. Ze ziet haar scherm zwart worden met een nogal vreemde tekst. Ellis kijkt geschrokken rond. Dan ziet ze dat haar collega's ook zo'n zwart scherm hebben gekregen. We zijn gehackt, beseft ze, en het is mijn schuld.

Om erachter te komen wat er is gebeurd, wordt Ellis ondervraagd. Men gaat na wat ze de afgelopen week heeft gedaan en waar ze allemaal is geweest. Zo zien we stap voor stap hoe een hacker via het account van Ellis uiteindelijk in het systeem van haar werkgever is gekomen.



Stopmomenten

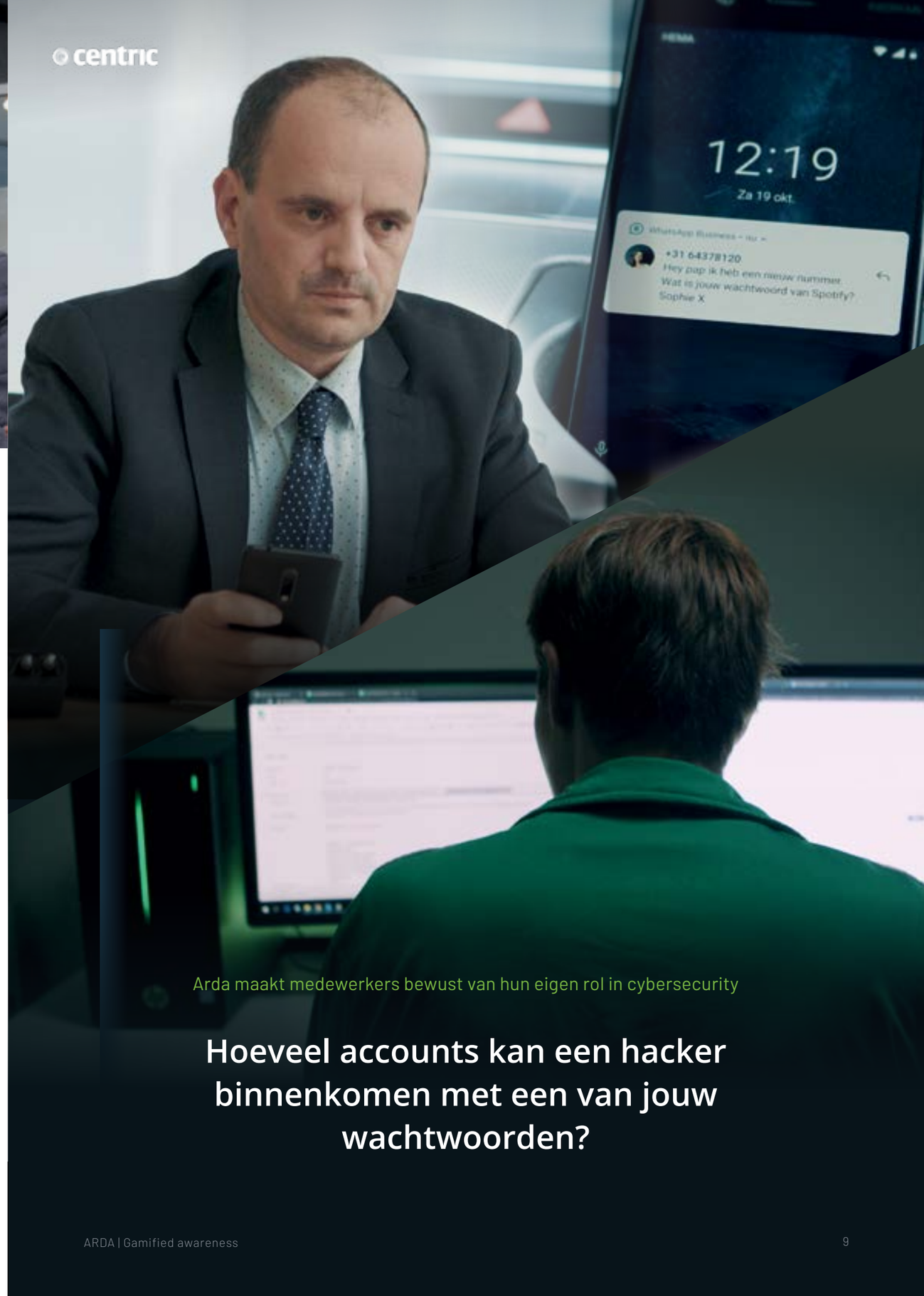
Uiteraard bestaat Steinitz niet alleen uit filmpjes. De deelnemers worden ook aan het werk gezet. Tijdens de stopmomenten worden vragen gesteld, onder meer over het drama dat Ellis doormaakt. Dit noemen we een immersive leervaring. De deelnemers worden geconfronteerd met de noodzaak van cybersecurity door een schrijnend voorbeeld, beantwoorden daar vervolgens vragen over en krijgen meteen te zien of ze goed zitten.

Recap

Mocht een deelnemer na een aflevering van Steinitz nog met vragen zitten, dan is er de mogelijkheid tot verdieping. De deelnemer kan een recapvideo aanklikken waar cruciale situaties uit de film nog eens worden toegelicht.

Bekijk de trailer

Klik mij



Arda maakt medewerkers bewust van hun eigen rol in cybersecurity

Hoeveel accounts kan een hacker binnenkomen met een van jouw wachtwoorden?

SERIOUS GAMES

Cybercrime zelf ervaren

Wat ons betreft is een game de beste manier om Arda te leren kennen. Daarom raden wij organisaties aan om een van onze serious games te spelen.

Serious games zijn vermakelijke spellen, uiteraard met een serieus, leerzaam tintje. Zo kunt u in een van de games bijvoorbeeld ontdekken wie achter een datalek zit. Een serious game maakt aan uw hele organisatie onmiddellijk duidelijk wat Arda inhoudt, waarom het programma zo belangrijk is, en wat uw medewerkers ervan kunnen verwachten. Zet bijvoorbeeld Deception in om de lancering van het programma te vieren.

STEINITZ
MINI

Een verkorte versie van de derde episode. Behandel kort een paar cruciale lessen en zie wie er de meeste kennis heeft.

15 m

Reigersdael
1863 UNIVERSITEIT

Een verkorte versie van de derde episode. Behandel kort een paar cruciale lessen en zie wie er de meeste kennis heeft.

30 m

DECEPTION

Door een datalek staat de reputatie van Delta Industries op het spel! Lukt het jullie de juiste dader, motief en het middel aan te wijzen?

Voor het gehele bedrijf of als teambuilding oefening. Deception is beschikbaar in het Nederlands & in het Engels.

50 m

Meer over deze games is te vinden op **arda.nl/serious_games**

Wat zit er in het programma?

Kennis van morgen is gisteren al verouderd, luidt een bekend gezegde.
Dat geldt al helemaal voor cybercrime. Daarom vernieuwen wij ons programma voortdurend. Toch kunnen we in grote lijnen een goed beeld geven.

Momenteel ziet het 1ste jaar Arda er als volgt uit:

Onderdeel	Thema
Arda Basics	Introductie van Arda: uitleg over het programma
Phishingcampagne	Een nep-phishingmailing als 0-meting
Brenno de Winter, expert informatiebeveiliging, privacy en ICT	Over digitale veiligheid en de verantwoordelijkheid om hier zelf actief keuzes in te maken
Steinitz 1	Een grootschalige hack: hoe begint het en wat zijn de gevolgen
Wachtwoorden	Alles over veilige en onveilige wachtwoorden
Phishing	Wat is het, en wat is het gevaar?
Maria Genova, schrijver van o.a. ‘Komt een vrouw bij de h@cker’, spreker over cybersecurity	Over online privacy en cybersecurity: waarom ook jij interessant bent voor hackers en hoe je jezelf hiertegen kunt beschermen
De AVG	Wat is de Algemene Verordening Gegevensbescherming?
Phishingcampagne	2e nep-phishingmailing
Steinitz 2	Oplichting en identiteitsfraude
Fysieke veiligheid	Hoe ga je in praktijk veilig om met informatie, en wat zijn de risico’s
Tweestapsverificatie	Waarom is het belangrijk? En hoe stel je het in?

Onderdeel	Thema
Phishingcampagne	3e nep-phishingmailing
Wachtwoordmanager	Hoe een wachtwoordmanager je kan helpen om je accounts veilig te houden
Steinitz 3	CEO-fraude
Inge Wetzer, sociaal psycholoog cybersecurity	Over wat er nodig is om mensen cyber-veilig gedrag te laten vertonen
Social engineering	Wat is het, en hoe herken je het?
Phishingcampagne	4e nep-phishingmailing
Dave Maasland, CEO Eset Nederland (leverancier van beveiligingssoftware)	Over DHV-ers: wat zijn het, en hoe kun je er als organisatie je voordeel mee doen
Mobiel en onderweg	Hoe zorg je ervoor dat hackers geen kans krijgen als je onderweg bent.
AVG extra	Een verdieping op de Algemene Verordening Gegevensbescherming
Steinitz 4	Vervolg CEO fraude
Elsine van Os, CEO Signpost Six Insider Risk Management	Hoe wordt iemand een ‘insider risk’, en hoe ga je daar als organisatie mee om
Afronding jaar 1	Bij het afronden van de training ontvangen de spelers een certificaat van voltooiing

Arda bevat de perfecte balans tussen entertainment en opleiding.
Geen droge betogen over technische details, of platte waarschuwingen waar uw medewerkers gek van worden – nee, het programma bestaat uit spannende, interactieve verhalen, glasheldere uitlegvideo’s en boeiende interviews met kenners en ervaringsdeskundigen.

Uw programma op maat

Ook gemeenten die hun eigen invulling willen geven aan voorlichting over cybercrime kunnen bij ons terecht. Wilt u bijvoorbeeld meer aandacht voor specifieke onderwerpen omdat die voor uw medewerkers relevanter zijn? Of wilt u misschien een eigen casus als voorbeeld aandienen waar uw medewerkers van kunnen leren? Dat kan.

Zo kunt u van die sterke inhoudelijke presentatie die uw medewerkers al een keer hebben gezien, een e-learning maken. Of zet een stapje extra en regisseer een film die naadloos aansluit op de risico’s voor uw gemeente. De opnames kunnen plaatsvinden in onze studio of op locatie.

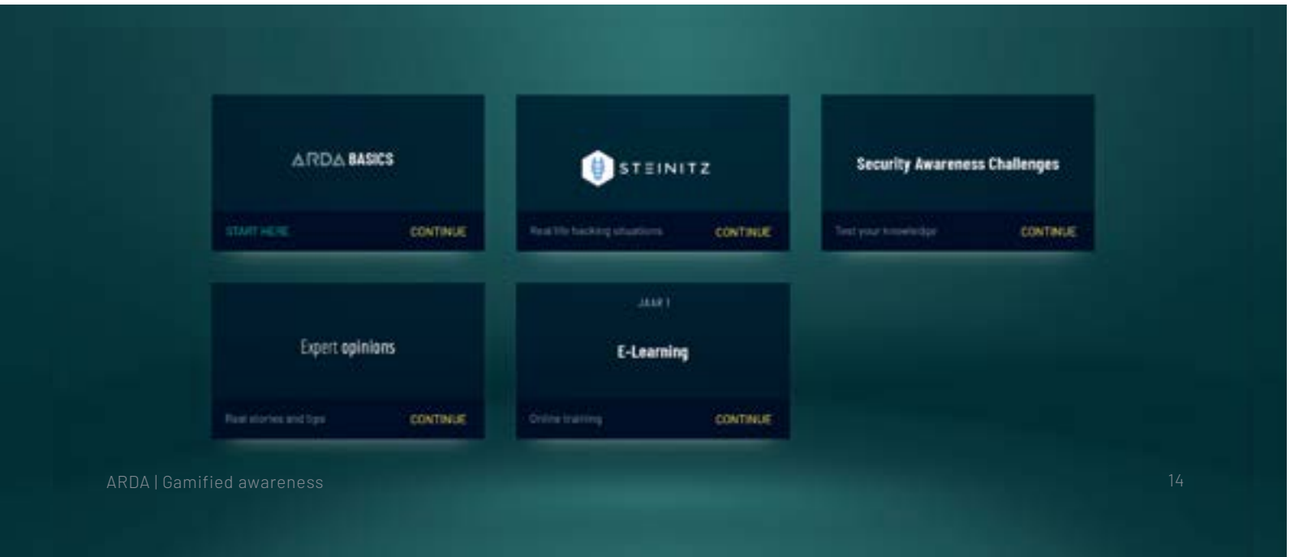
Een tempo dat bij uw medewerkers past
Het programma van Arda kan op ieder moment starten. Misschien vindt u het verstandig om uw medewerkers meerdere onderdelen tegelijkertijd te laten doorlopen, of wilt u ze juist een periode rust geven. We kunnen rekening houden met schoolvakanties, met examenperioden – alles is mogelijk.

Altijd een schuin oog op de resultaten
Voor welk programma u ook kiest, als ‘administrator’ heeft u altijd inzicht in de voortgang van uw medewerkers. Deze rapportages kunt u zelf in Arda opvragen.

Arda in de praktijk: zo gaan we te werk

- De medewerkers die zijn aangemeld voor Arda ontvangen een mail zodra er een onderdeel klaarstaat. Met één klik op de link doorlopen ze zo stap voor stap het programma.
- Arda werkt met licenties vanaf 100 gebruikers. Elke licentie is één jaar geldig vanaf een startdatum die door u is gekozen.
- Een meevaller: licenties zijn overdraagbaar. Als medewerkers uit dienst gaan, kunnen nieuwe medewerkers die plekken dus gewoon innemen.
- Het programma van Arda draait op een zogeheten learning management system (LMS). Dit systeem werkt op alle soorten apparaten en browsers. Toch raden we Internet Explorer 11 en lager af. Voor technische vragen kun je altijd terecht bij onze supportafdeling.
- Na afronding van ieder jaarprogramma ontvangen de deelnemers een certificaat.

Na elk jaar nemen we tevens de balans op. U besluit zelf of u het programma ook voor de daaropvolgende jaren wilt afnemen. (Spoiler alert: tot nu toe gaan ál onze klanten na het eerste jaar door voor de rest van het programma. Ja, daar zijn we best trots op!)



ARDA

Cybercrime kan iedereen overkomen

Maar wie het herkent en weet wat te doen, verlaagt het risico op een succesvolle aanval aanzienlijk. Arda maakt cybersecurity-awareness toegankelijk en betaalbaar.

Bent u inmiddels benieuwd geworden naar Arda?
Goed om te horen! Ga naar **Centric.eu/arda** voor meer informatie. U kunt daar ook filmpjes bekijken die een goede indruk geven van het programma. En als kers op de taart hebben we een demo in de aanbieding waarmee u het programma zelf kunt proberen. Vooral dat laatste is een enorme aanrader.

Uiteraard is het ook mogelijk om meteen contact met ons op te nemen.
Ons team staat voor je klaar!

Neem voor meer informatie contact op met Serano van der Hurk via serano.van.der.hurk@centric.eu of bel +31 6 1195 8795.
Of met Derek Hillenaar via derek.hillenaar@centric.eu of bel +31 6 10590189

centric

ARDA

Cybercrime kan iedereen overkomen