14-04-2025

BOP ADVIESOPDRACHT

KlikKlak Klaar
CYBERSECURITY

AAN:
UNIVERSITEIT UTRECHT
MARTIJN VAN DER MEULEN

GESCHREVEN DOOR:
EVA VAN JAARSVELD, THOMAS KLOK
LLOYD-LEONARD OPDAM & ANISA SUHERLI

Aanleiding

Op 12 januari 2025 werd de Technische Universiteit Eindhoven (hierna: TU/e) getroffen door een cyberaanval. Hierdoor werden de systemen offline gehaald en kon er een week geen onderwijs plaatsvinden. TU/e werd gedurende het weekend getroffen door de cyberaanval. Hackers gebruikten gegevens van een medewerker en een student om toegang te krijgen. Ze zijn op heterdaad betrapt, toen er een significante piek in datastromen werd opgemerkt door monitoringsoftware. De universiteit onderzocht meerdere use cases en signalen van compromittering. De aanval leidde tot inzicht in kwetsbaarheden en de effectiviteit van bestaande beveiligingsmaatregelen. Hoewel er geen directe aanwijzingen zijn dat data is buitgemaakt, werd de situatie nauwlettend geanalyseerd.

Omdat uit een recent artikel van het AD blijkt dat de hogescholen in Utrecht ook een aantrekkelijk doelwit zijn voor cyberaanvallen, is binnen de Universiteit Utrecht de vraag gaan spelen hoe het is gesteld met hun digitale weerbaarheid tegen cyberaanvallen en wat aandachts- en verbeterpunten zijn. Voor de Universiteit Utrecht is het hierbij vooral relevant hoe zij er als organisatie voorstaan in het licht van hun digitale weerbaarheid en wat hierbij aandachts- en verbeterpunten kunnen zijn.

Vraagstelling

Op basis van hetgeen hierboven is geschreven, is het College van Bestuur van Universiteit Utrecht gekomen met de volgende vraag, dit wij uiteen zullen zetten in dit adviesrapport:

"*Hoe is het, gezien in het licht van de cyberaanval op de TU/e, gesteld met onze digitale weerbaarheid tegen cyberaanvallen en wat zijn aandachts- en verbeterpunten?*"

Wie zijn wij?

Als we spreken van *wij*, dan bedoelen we het cyberbeveiligingsadviesteam **KlikKlakKlaar**. Een team dat zich met volle overtuiging inzet voor één missie: *het versterken van de digitale weerbaarheid van Nederland.* Wij geloven dat effectieve cyberbeveiliging begint bij helderheid. Daarom werken we met een eenvoudige en doeltreffende drieslag, gewoonweg: **klik, klak, klaar**. We vertalen complexe risico's en vraagstukken naar concrete stappen die u snel kunt implementeren binnen uw organisatie.

KlikKlak Klaar
CYBERSECURITY

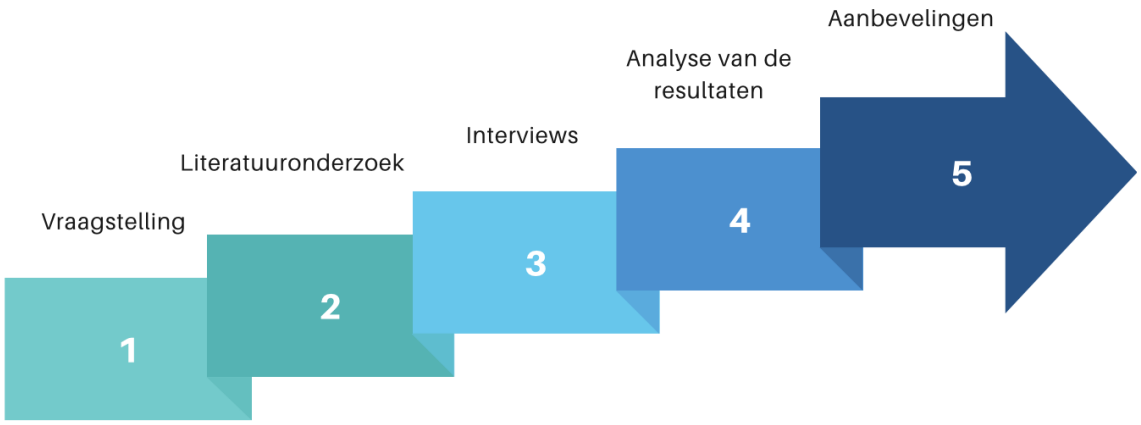
Aanpak

Dit adviespaper is tot stand gekomen door een combinatie van literatuuronderzoek en kwalitatief onderzoek. In eerste instantie hebben we relevante wetenschappelijke literatuur bestudeerd om een theoretisch kader te vormen voor de verdere analyse. Digitale weerbaarheid wordt niet alleen bepaald door technologische maatregelen, maar ook door het gedrag van gebruikers. Wanneer medewerkers en studenten zich niet bewust zijn van cyberdreigingen, vergroot dit de kwetsbaarheid van onderwijsinstellingen. Daarom hebben we zowel aandacht voor de verspreiding van innovaties om de digitale weerbaarheid te vergroten, als voor het individu.

Om tot concrete aanbevelingen te komen, is kwalitatief onderzoek verricht door middel van interviews. In totaal zijn twee interviews afgenomen met experts op het gebied van digitale weerbaarheid binnen onderwijsinstellingen. Deze interviews boden ons diepgaand inzicht in ervaringen, percepties en uitdagingen met betrekking tot digitale weerbaarheid tegen cyberdreigingen op onderwijsinstellingen. De interviewvragen, die online zijn afgenomen, richtten zich op het beoordelen van de huidige digitale weerbaarheid, het leren van eerdere cyberincidenten en het identificeren van verbeterpunten. Eerst keken we naar de kwetsbaarheden en bewustwording binnen de organisatie. Vervolgens bespraken we de lessen die uit de TU/e-hack konden worden getrokken. Tot slot vroegen we naar concrete aanbevelingen om de digitale weerbaarheid op onderwijsinstellingen te vergroten.

De respondenten zijn geselecteerd op basis van hun expertise en ervaring met digitale veiligheid binnen onderwijsinstellingen. Onder hen is Maarten Goldberg, specialist in privacy en security voor onderzoek aan de Universiteit van Groningen, en David de Boer, de Chief Information Security Officer (CISO) van de Universiteit Utrecht. Beide respondenten hebben ruime kennis van en ervaring met de digitale risico's en uitdagingen waarmee onderwijsinstellingen worden geconfronteerd. Bovendien is David de Boer op de hoogte van de huidige situatie van de digitale weerbaarheid van de Universiteit Utrecht.

De verzamelde data uit de interviews hebben we vervolgens geanalyseerd om terugkerende problemen en overeenkomsten te identificeren. De belangrijkste patronen die uit deze analyse naar voren kwamen, vormen de basis voor onze adviezen.

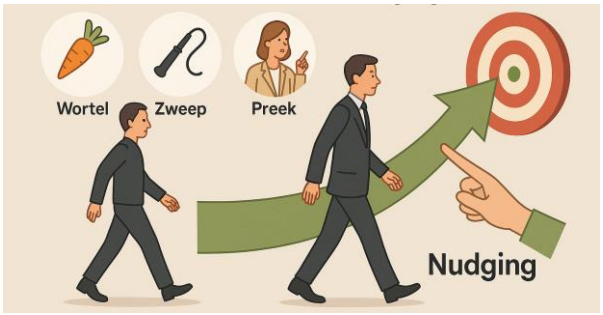


Theorie

Weerbaarheid is een concept dat aangeeft wat het vermogen van een systeem is om verstoringen te absorberen en zichzelf opnieuw te organiseren terwijl het zijn kernfuncties behoudt (Weller & Anderson, 2013, p. 54). In de context van digitale systemen, zoals in het hoger onderwijs, betekent dit dat organisaties en individuen in staat moeten zijn om zich aan te passen aan en te herstellen van digitale verstoringen in de vorm van cyberaanvallen. Digitale middelen kunnen hierbij een cruciale rol spelen, bijvoorbeeld door goede systemen te hebben die in staat zijn om storingen te weerstaan en zich aan te passen aan veranderingen.

Echter, zoals onderzoek van Jansen (2023) aangeeft, is digitale weerbaarheid niet alleen afhankelijk van technologie, maar ook van de organisatorische en menselijke capaciteiten om digitale verstoringen effectief op te vangen. Het individu is dus belangrijk binnen het concept digitale weerbaarheid. Dit omvat het trainen van mensen om digitale dreigingen te herkennen en snel en effectief te reageren (Boh et al., 2022).

Maar ook is de wil van het individu om in actie te komen van belang. Traditionele beleidsinstrumenten om individueel gedrag te beïnvloeden zoals: de wortel (beloningen), de zweep (verboden) en de preek (voorlichting), veronderstellen een rationeel handelende individu (Tummers & De Ridder, 2019). Echter, inzichten uit de psychologie tonen aan dat menselijk gedrag vaak irrationeel en afhankelijk is van de context. De manier van het beïnvloeden van deze emotionele gedragsverandering heet nudging (Tummers & De Ridder, 2019). Dit concept is de manier om gedrag subtiel te beïnvloeden zonder iets te verbieden. Het werkt door de keuze-omgeving zo aan te passen dat mensen vanzelf eerder de gewenste keuze maken.

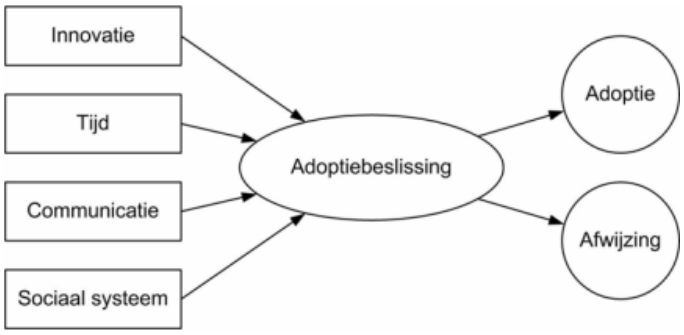


Diffusion of Innovation Theory (Rogers, 1983)

Een reden waarom er zoveel aandacht is voor de verspreiding van innovaties is dat het vaak erg moeilijk is om een nieuw idee ingang te doen vinden in organisaties, zelfs als het idee duidelijke voordelen heeft. Veel innovaties vergen een lange periode, vaak enkele jaren, vanaf het moment dat ze beschikbaar komen tot het moment dat ze algemeen worden toegepast. Daarom is een veelvoorkomend probleem voor veel individuen en organisaties hoe het proces van de verspreiding van een innovatie kan worden versneld (Rogers, 1983, p. 1), zo ook bij de Universiteit Utrecht. Om deze reden gebruiken we de Diffusion of Innovation Theory van Rogers (1983).

Deze theorie is relevant voor de analyse van digitale weerbaarheid binnen de Universiteit Utrecht omdat het inzicht biedt in hoe nieuwe ideeën en gedragingen, zoals veilig digitaal handelen, zich verspreiden binnen een organisatie. De theorie benadrukt dat succesvolle verspreiding van innovaties afhankelijk is van vier factoren: de innovatie zelf, de communicatiekanalen, de tijd en het sociale systeem (Rogers, 1983,

p. 10). Dit helpt verklaren waarom gedragsverandering rondom digitale veiligheid vaak langzaam verloopt.



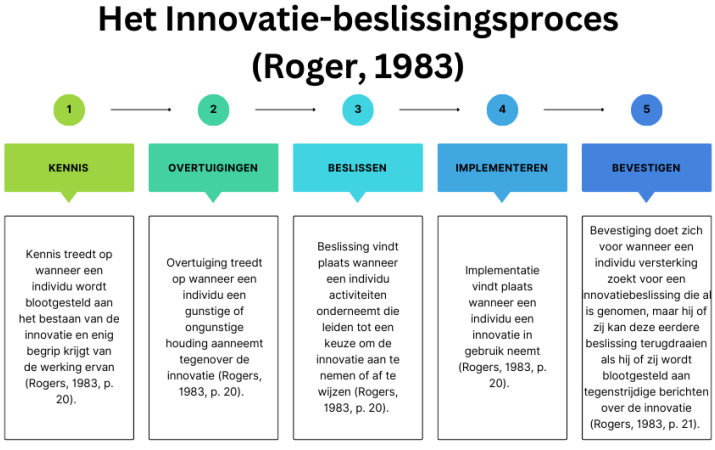
In dit theoretisch kader gaan we verder in op de communicatiekanalen, omdat deze een belangrijke rol spelen in hoe informatie over digitale veiligheid effectief kan worden overgebracht, begrepen en uiteindelijk toegepast binnen de universiteit. Een communicatiekanaal is het *middel* waarmee berichten van de ene persoon naar de andere worden overgebracht. De manier waarop deze informatie-uitwisseling plaatsvindt, bepaalt niet alleen of de innovatie wordt doorgegeven, maar ook hoe deze wordt ontvangen en geïnterpreteerd (Rogers, 1983, p. 17).

Het innovatie-beslissingsproces

Daarnaast biedt het innovatie-besluitvormingsproces van Roger (1983) concrete handvatten voor het strategisch sturen van gedragsverandering, door bijvoorbeeld eerst kennis te creëren, vervolgens overtuiging te stimuleren en daarna implementatie en bevestiging te faciliteren bij medewerkers en studenten van de universiteit.

Het innovatie-besluitvormingsproces is het proces dat een individu (of een andere besluitvormende eenheid) doorloopt vanaf de eerste kennis van een innovatie tot het vormen van een houding ten opzichte van de innovatie, tot een besluit om het idee aan te nemen of af te wijzen, tot de uitvoering van het nieuwe idee, en tot de bevestiging van dit besluit (Rogers, 1983, p. 20).

We conceptualiseren vijf hoofdstappen in het proces: (1) kennis, (2) overtuigen, (3) beslissen, (4) implementeren en (5) bevestigen. Deze zijn beschreven in de flowchart hieronder.

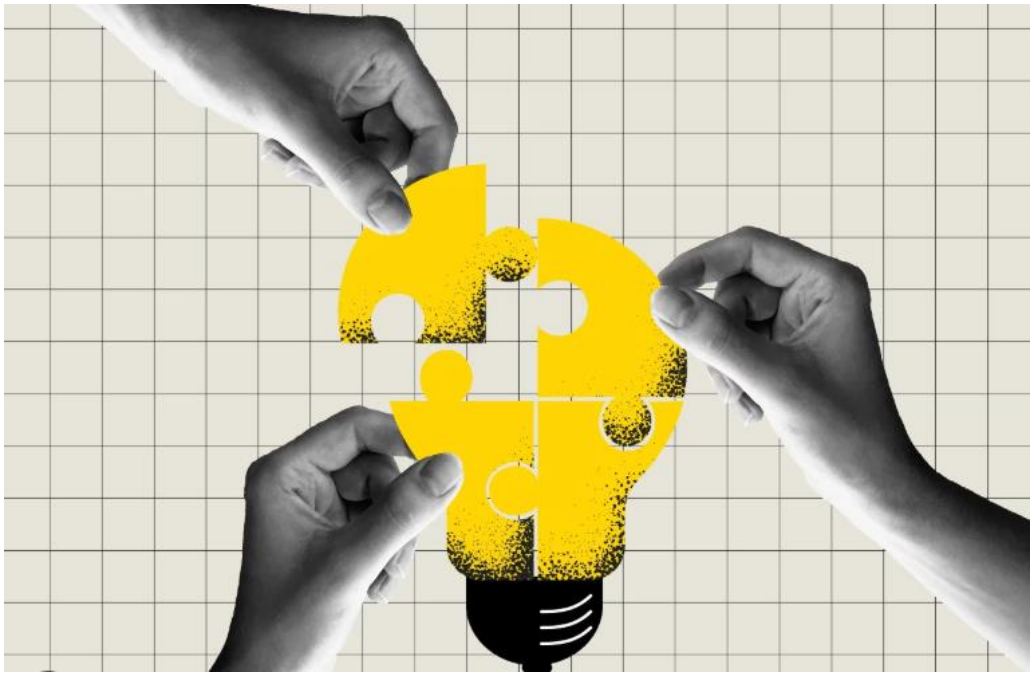


Analyse

Een kritische blik op de UU

Zoals eerder benoemd is het kenmerkend voor een innovatie dat het idee of plan als nieuw wordt gepercipieerd. Door de technologische en digitale ontwikkelingen van de afgelopen jaren, is digitale weerbaarheid een relatief nieuw idee voor individuen. Ondanks dat er tal van investeringen zijn gedaan in het creëren van bewustzijn, blijft dit een lastige opgave voor de UU. Nu wordt er met name gecommuniceerd naar de medewerkers via nieuwsbrieven, het medewerkersplatform ‘Intranet’ en de zogeheten ‘security parade’ waar lezingen worden gegeven. Het bereik van deze kanalen is zeer beperkt. Bovendien is de communicatie top-down en nauwelijks geïmplementeerd in de dagelijkse routines van medewerkers. Hierdoor ontbreekt het aan structurele, herhaalde en sociale interactie rondom het thema. Dit sluit nauw aan bij het diffusieperspectief van Rogers (1983), waarbij innovatieverspreiding herhaling en aansluiting vereist bij het sociale systeem waarin zij plaatsvindt. We zien hierbij dat de UU als onderwijsinstelling veel (eigenwijze) professionals huist, die veel waarde hechten aan academische vrijheid. De discretionaire ruimte die de medewerkers hierbij hebben maakt top-down sturing moeizaam.

Tot slot blijkt uit de interviews met onder andere David de Boer dat digitale weerbaarheid zich stap voor stap ontwikkelt. Tijd (Rogers, 1983) speelt hierbij een cruciale rol: van bewustwording tot gedragsverandering verloopt het proces geleidelijk en verschilt het per individu of groep. Dit benadrukt dat digitale weerbaarheid geen eindpunt is, maar een ontwikkeling die tijd, herhaling en contextuele ondersteuning vereist.



De mens als sleutel (én risico) voor digitale veiligheid

Zoals eerder benoemd is de individuele medewerker/student van groot belang bij het versterken van de digitale weerbaarheid. Het is dan ook relevant om verder in te gaan op het innovatie-beslissingsproces dat het individu doorloopt ten aanzien van de innovatie, omdat op deze manier duidelijk kan worden gemaakt waar en hoe het bij de Universiteit Utrecht verkeerd gaat.

Rogers (1983) onderscheidt in het innovatie-beslissingsproces vijf (hoofd)stappen. De eerste stap heeft betrekking op de kennis die het individu heeft over de innovatie. Op basis van de interviews gesteld worden dat er in het algemeen, maar ook specifiek bij de Universiteit Utrecht te weinig kennis/bewustzijn is over de digitale weerbaarheid (de innovatie). Het is dan ook niet voor niets dat de experts die wij hebben geïnterviewd dit als het pijnpunt zagen. Wanneer het namelijk al bij de eerste stap van het innovatieproces fout gaat, heeft dit verstrekkende gevolgen voor de andere stappen uit het innovatie-beslissingsproces.

Zonder kennis over de innovatie – de eerste stap – zal de individuele medewerker en/of student nooit komen bij de tweede stap, het aannemen van een gunstige of ongunstige houding tegenover de innovatie. Nu is het natuurlijk niet zo dat geen enkele medewerker of student kennis/bewustzijn heeft over digitale weerbaarheid. Door veel studenten en medewerkers wordt dan ook wel een houding aangenomen ten aanzien van de innovatie. In het algemeen kan gesteld worden dat de meeste studenten en medewerkers een ‘gunstige’ houding hebben tegenover het verbeteren van de digitale weerbaarheid.

Wanneer bij een individu een bepaalde overtuiging optreedt, wordt overgegaan tot de derde stap in het innovatie-beslissingsproces; het ondernemen van activiteiten die leiden tot de keuze om de innovatie aan te nemen of af te wijzen. In deze fase – en deels in de tweede fase – onderzoekt het individu de voordelen en nadelen van de innovatie, toegespitst op zijn persoonlijke situatie (Rogers, 1983, p. 21). Uit de interviews kwam hierbij een interessante bevinding naar boven. Hoewel medewerkers en studenten een gunstige houding hebben tegenover digitale weerbaarheid in het algemeen, zijn de nadelen voor hen vaak groter dan de gepercipieerde voordelen. Volgens hen is het vervelend en ‘tijdrovend’ om allerlei extra beveiligingsstappen te nemen.

Veel medewerkers en studenten komen dan ook niet tot de vierde stap van het innovatie-beslissingsproces; het in gebruik nemen van de innovatie.

Voor de medewerkers en studenten die de innovatie wel in gebruik nemen betekent dit niet het einde van het proces. De vijfde stap van het innovatie-beslissingsproces verklaart namelijk waarom individuen eerder genomen beslissingen kunnen terugdraaien. Wanneer slechts een enkeling de innovatie in gebruik neemt en anderen een ongunstige houding hebben tegenover deze innovatie, kunnen zij deze houding overnemen.

Wat we kunnen leren van TU/e's fout

Uit de interviews valt te halen dat de punten waarop het bij de cyberaanval op de TU/e fout ging, goed te koppelen zijn aan de hierboven gegeven analyse. De reden waarom de hackers succesvol waren in hun aanval op de TU/e was de afwezigheid van MFA op gedeelde accounts. De afwezigheid van MFA kan geduid worden als een gebrek aan bewustzijn/kennis over de gevaren van cyberaanvallen, maar ook als het resultaat van de afweging van medewerkers dat de voordelen van het niet gebruiken van MFA groter zouden zijn dan de mogelijke nadelen.

Deze twee pijnpunten sluiten haarfijn aan op de verschillende stappen van het innovatie-beslissingsmodel. Zo komt de 1e stap van het innovatie-beslissingsmodel, het creëren van kennis over de innovatie, overeen met de eerste reden waarom geen MFA werd gebruikt op gedeelde accounts; medewerkers hadden te weinig of geen kennis over cyberveiligheid.

Een gebrek aan kennis/bewustzijn verklaart een deel van het voorval dat zich heeft voorgedaan bij de TU/e, maar zo mogelijk nog belangrijker is de belangenafweging van de medewerkers die ertoe leidde dat ze onveilig handelde, de 3e stap van het innovatie-beslissingsmodel. Beslissend hierin was het idee dat MFA 'vervelend' is en dat 'het allemaal wel los zou lopen' met mogelijke cyberaanvallen.

Aanbevelingen

De 3 C's van Cyberbewustzijn

Op basis van de analyse kunnen we stellen dat het vergroten van digitale weerbaarheid binnen de onderwijsinstelling niet slechts een technische uitdaging is. Het is van belang dat ook wordt gekeken naar motivatie en gedragswetenschap. Medewerkers en studenten staan namelijk over het algemeen positief tegenover het vergroten van de digitale weerbaarheid, maar daadwerkelijke gedragsverandering blijft uit doordat kennis/bewustzijn ontbreekt en het gebruik van nieuwe beveiligingsmaatregelen als tijd belastend of lastig wordt gezien. Daarbovenop kan de afwezigheid van een breed gedragen sociale norm ertoe leiden dat maatregelen niet worden nageleefd. Tot slot staat vast dat digitale weerbaarheid geen eindpunt is, maar een ontwikkeling die tijd, herhaling en contextuele ondersteuning vereist.

Deze resultaten laten het belang zien van oplossingen die niet alleen gericht zijn op het informeren van medewerkers, maar vooral op het creëren van draagvlak en het verlagen van sociale drempels om innovaties in gebruik te nemen. De adviezen richten zich daarom op herhaling, sociale verankering en herkenbare momenten van bewustwording, in tegenstellig tot de top-down benadering die nu wordt gehanteerd. Op basis hiervan zijn de volgende aanbevelingen geformuleerd: *Click*, *Chat* en *Commit*. De drie C's vormen samen een pakket dat het CvB direct kan in gebruik kan nemen.

Click

Het organiseren van maandelijkse simulaties van phishingmails, gekoppeld aan tijdelijke beperkingen (bijvoorbeeld een zwart scherm van 10 minuten), is een doeltreffende methode om medewerkers bewust te maken van cyberdreigingen. Door herhaling ontwikkelen zij routine in het herkennen van phishingpogingen (de eerste stap van het innovatie-beslissingsproces) en dit stimuleert overtuiging om de innovatie in gebruik te nemen. Deze aanpak verlaagt de sociale drempel om het onderwerp bespreekbaar te maken, aangezien elke medewerker ermee wordt geconfronteerd. Dit werkt collectieve betrokkenheid in de hand. Hierdoor ontstaat een verandering binnen de organisatiecultuur, waarbij het thema digitale weerbaarheid structureel belangrijk wordt geacht binnen de Universiteit Utrecht. Deze maatregel stimuleert daarmee een snelle verspreiding van kennis binnen het sociale systeem van de organisatie, doordat medewerkers elkaar willen beschermen tegen de mogelijke gevolgen. Dit draagt bij aan het versterken van de overtuiging om een positieve houding aan te nemen ten opzichte van het implementeren van digitale weerbaarheidsmaatregelen.

Chat

Het strategisch plaatsen van cyberweetjes in informele omgevingen, zoals koffiehoeken, bevordert zowel gespreksstof als alertheid binnen het sociale systeem van de Universiteit Utrecht. Dit kunnen we herkennen in de theorie van Rogers, waarbij innovatie via communicatiekanalen kan worden verspreid. Voorbeeldweetje: *"Wist je dat een wachtwoord van meer dan 12 tekens 99% veiliger is dan één van 8?"* Door dergelijke visuele prikkels op strategische plekken te tonen op bijvoorbeeld koffiebekers en prikborden, ontstaat op natuurlijke wijze een sociale norm waarin cyberbewustzijn als belangrijk wordt beschouwd. Deze vorm van nudging beïnvloedt

gedrag subtiel, zonder dwang, en draagt bij aan de normalisering van digitale weerbaarheid binnen de organisatiecultuur. Hierdoor groeit de overtuiging om een positieve houding aan te nemen ten opzichte van digitale weerbaarheid en de latere implementatie van bijbehorende maatregelen.

Commit

De introductie van een jaarlijkse ‘Cyberweek’ biedt een gestructureerde en herhaalbare impuls voor bewustwording van cyberdreigingen. Tijdens deze week worden alle medewerkers actief betrokken bij de digitale weerbaarheid van de Universiteit Utrecht, onder meer door het verplicht wijzigen van wachtwoorden en het volgen van educatieve programma’s. Door deze week als een vast moment in het jaar te organiseren, ontstaat een voorspelbare tijdsstructuur. Dit bevordert kennisopbouw, gedragsverandering en de implementatie van digitale weerbaarheidsmaatregelen. Het terugkerende proces in de vorm van deze week, stimuleert de acceptatie van maatregelen en het bewustzijn van cyberdreigingen (dit reflecteert de laatste stap in het innovatie-beslissingsproces van Rogers).

Door het combineren van herhaling (Click), nudging (Chat) en een structureel moment in tijd (Commit), wordt bewustzijn op individueel, sociaal en organisatorisch niveau versterkt. Deze aanbevelingen vergroten de kans op blijvende gedragsverandering, borgen digitale weerbaarheid in de organisatiecultuur van de Universiteit Utrecht, en maken het aannemen van innovaties in de toekomst eenvoudiger.

Bronnenlijst

Boh, W., Constantinides, P., Padmanabhan, B., & Viswanathan, S. (2022). *Building Digital Resilience Against Major Shocks*. Nanyang Business School, Nanyang Technological University; Alliance Manchester Business School, University of Manchester; Muma College of Business, University of South Florida; University of Maryland. https://www.researchgate.net/publication/368469691_Building_Digital_Resilience_Against_Major_Shocks

Jansen, J. (2023, 30 mei). *Digitale weerbaarheid van mens en organisatie: De kracht van verbinding*. Politieacademie. https://www.researchgate.net/profile/Jurjen-Jansen/publication/371292484_Digitale_weerbaarheid_van_mens_en_organisatie_De_kracht_van_verbinding/links/647da470b3dfd73b77670557/Digitale-weerbaarheid-van-mens-en-organisatie-De-kracht-van-verbinding.pdf

Rogers, E. M. (1983). *Diffusion of Innovation (3rd edition).* Collier Macmillan Publishers.

Tummers, L., & De Ridder, D. (2019). *Nudging: Makkelijke oplossingen voor moeilijke keuzes*. Prometheus.

Weller, M., & Anderson, T. (2013). Digital resilience in higher education. *European Journal of Open, Distance and E-Learning, 16*(1), 53-66. https://files.eric.ed.gov/fulltext/EJ1017457.pdf