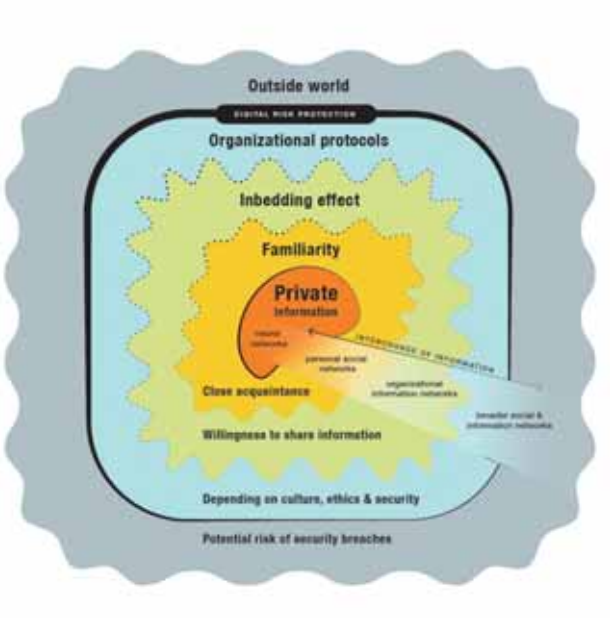
Erik Schoppen is merkexpert, neurowetenschapper, gedragsonderzoeker, innovator, designer, auteur en een veelgevraagd internationaal spreker over vertrouwen en (merk)leiderschap. Erik is bereikbaar via info@erikschoppen.com.

Vertrouwen gaat niet over veiligheid maar over vrijheid

Vertrouwen is een vraagstuk dat vooral ter tafel komt bij de inbedding binnen kwetsbare veiligheidssystemen. Hoe kunnen we het vertrouwen in een systeem vergroten zonder dat de integriteit en veiligheid binnen zo'n systeem schade wordt aangedaan? Aan de ene kant wil je een systeem zo veilig en beregeld mogelijk houden, aan de andere kant geef je gebruikers de vrijheid en autonomie om hier zelfstandig mee om te gaan. Dat vraagt om vertrouwen.



Figuur 1 - From neural networks to digital information networks.

Zonder vertrouwen in gebruikers worden systemen onbruikbaar, mede door de eindeloze protocollen die dan gevolgd moeten worden om informatie te ontsluiten binnen en buiten een systeem. Gebruikersgemak en vertrouwen gaan daarom hand in hand. Een eerste voorbeeld hiervan is de 'single sign-on', een inlogmethode waarmee gebruikers met één ID en wachtwoord toegang krijgen tot verschillende, al dan niet verbonden, systemen binnen een organisatie. Als deze inlog gehackt wordt, liggen alle aangesloten applicaties binnen de organisatie open. Het is vaak niet praktisch en zeker niet gebruiksvriendelijk om voor alles aparte inloggegevens aan te maken. Ons brein is 'cognitief lui' en kiest voor de makkelijkste weg - dus gebruiken mensen vaak dezelfde wachtwoorden. Volgens recent onderzoek van SplashData (2019) was het meest gebruikte wachtwoord nog steeds '123456.' Twee-staps-verificatie verdient daarom de voorkeur, ook omdat er dan ook een bewuste cognitieve handeling tussen zit die routinegedrag of fraude voorkomt. Als je persoonlijk je smartphone moet pakken om een code te activeren, is dit ook een bevestiging die je erop attendeert dat je op dat moment inlogt in een mogelijk kwetsbaar systeem – moeilijker te hacken dus.

Veiligheid begint in ons brein

Het is de uitdaging om in een digitale architectuur een zodanig systeem te ontwerpen dat zowel veilig en betrouwbaar als toegankelijk en gebruiksvriendelijk is. Maar hiervoor moeten we wel eerst begrijpen hoe vertrouwen als mentaal mechanisme een rol speelt in onze besluitvorming. Op basis waarvan nemen mensen hun beslissingen en besluiten ze vervolgens wel of geen informatie te delen? Daarom eerst een introductie over hoe vertrouwen werkt in ons brein.

Evolutionair vertrouwen

Vertrouwen ontstaat in ons brein op moleculair niveau in onze zenuwcellen. Boodschappers in deze cellen zorgen voor informatieoverdracht naar andere cellen die gezamenlijk weer neurale netwerken vormen. Door deze netwerken kunnen we informatie verwerken, onthouden en opslaan. Hoe sneller we toegang krijgen tot bepaalde informatie in deze netwerken - die bijvoorbeeld een aanname bevestigen - des te sneller ontstaat er vertrouwen. Deze neurale 'snelwegen' vormen het fundament voor ons vertrouwen. Ze spelen een rol bij 'familiarity' (het snel kunnen herkennen van informatie waarmee we goed

Digitaal vertrouwen stelt je in staat het gedrag van anderen te voorspellen

bekend zijn of personen die we vertrouwen) en het `inbedding-effect' (de omgeving waarin informatie wordt aangeboden is bepalend of we deze informatie vertrouwen en of we bereid zijn informatie uit te wisselen), zie ook figuur 1. Hierdoor kunnen we snel beoordelen of we op onszelf moeten vertrouwen of juist iemand anders kunnen vertrouwen. Dit miljoenen jaren oude systeem is niet perfect, maar werkt in de meeste gevallen prima, mede omdat het snel is. Denk aan de eerste indruk die we van een persoon kunnen hebben. We vertrouwen dan op wat we soms al in 200 milliseconden kunnen waarnemen. Hoewel deze beoordeling niet altijd correct is, is deze vorm van (patroon)herkenning vanuit de evolutie goed verklaarbaar. Als er een kwaadwillend persoon op je afkomt, is snel kunnen beslissen van levensbelang. Vaak speelt de omgeving hierin ook een rol – een donker steegje met daarin een verdacht opgesteld individu loop je `s avonds ook niet in. Maar in onze digitale wereld bestaan helaas geen donkere straatjes; we krijgen constant de illusie van verlichting en veiligheid voorgeschoteld. De digitale industrie draait primair om het creëren van virtuele veiligheid, maar cybersecurity en het begrijpen van menselijk gedrag blijft noodzakelijk. Een onbedachtzame handeling is online snel gedaan, vooral omdat één klik al grote consequenties kan hebben en authenticatie zo lastig valt te verifiëren. De tijd die betrouwbare identificatie kost op de digitale snelweg is veelal langer en ingewikkelder dan de kwart seconde die ons brein gemiddeld nodig heeft voor (h)erkenning in de reële wereld.

Netwerkvertrouwen

Vertrouwen in jezelf of in de ander draait er vooral om of je jezelf kwetsbaar durft op te stellen. Deze vorm van sociaal vertrouwen zorgt er van oudsher voor dat we kunnen samenwerken en taken kunnen verdelen. Het uitwisselen van gevoelige informatie binnen digitale netwerksystemen werkt tegenwoordig op exact dezelfde wijze. Weten wat mensen denken en voelen, maar vooral waarop ze vertrouwen, is de sleutel tot het begrijpen van hun huidige gedrag en het voorspellen van hun toekomstige gedrag binnen virtuele omgevingen. Ook omdat deze omgevingen vaak een afspiegeling zijn van de organisatie in de reële wereld. Hoe meer ze hierop lijken, des te sneller ze erop vertrouwen. Vertrouwen ontstaat hier vooral door bekendheid van omgeving en het secuur omgaan met (privacy)gevoelige data en het delen van elkaars waarden en kennis binnen deze netwerken. Als dit overeenstemt, voelt een relatie binnen zo'n systeem vertrouwd en motiveert het mensen om meer informatie over zichzelf te delen. Er is dus sprake van zowel familiarity als een positief inbeddingeffect. Zowel de beveiligde netwerkomgeving als de betrouwbaarheid van anderen in dit netwerk leidt dan tot netwerkvertrouwen. Dit is het vertrouwen dat we in elkaar stellen binnen grotere netwerken waarbij mensen kennisdelende schakels vormen in het netwerk. Elke schakel is belangrijk om interpersoonlijk vertrouwen tot stand te brengen. Daarom is toegang tot goede toegangsprotocollen en een gezamenlijk gedeelde bedrijfsbeveiligingscultuur zo belangrijk. We delen letterlijk elkaars (neurale en sociale) netwerken. Hoe sterker de organisatiecultuur, des te sterker het vertrouwen in de organisatie en daarmee vaak samenhangend het beveiligingsniveau.

Systeemvertrouwen

Ook zijn organisaties en samenwerkingsverbanden in het digitale tijdperk steeds groter en complexer geworden - resulterend in steeds grotere systemen en bijbehorende architectuur. Dit vraagt om vertrouwen in iets wat ons

menselijk brein niet meer kan overzien. Mensen denken het liefst in voorspelbare factoren en nabijheid. Hoe dichter iets mentaal of fysiek bij ons staat, des te meer aandacht we hieraan schenken en hoe sterker het vertrouwen is. Hier maken hackers gebruik van middels familiarity en inbedding. Maar hoe werkt dit in de onlinewereld waarin via globale netwerkstructuren alles met alles aan elkaar verbonden is? In digitale onlinesystemen ben je altijd en overal kwetsbaar voor aanvallen. Dit vereist een ander veiligheidsniveau. Vertrouwen in een systeem kan namelijk uitgroeien tot een wereldwijd niveau bij miljarden mensen.

Systeemvertrouwen draait dan om de kredietwaardigheid en reputatie van allerlei digitale netwerken die gezamenlijk met elkaar verbonden zijn tot één herkenbare entiteit die qua gevoel weer dicht bij mensen staat of hun zorgen wegneemt. Een voorbeeld van dit systeemvertrouwen is als je bijvoorbeeld een volledig verzorgde vakantie boekt. De aanbieder (de entiteit waarop je vertrouwt) boekt voor jou de tickets bij een internationale vliegmaatschappij (die weer afspraken heeft met vliegvelden in verschillende landen), de huurauto bij een verhuurbedrijf in het land van bestemming en het huisje en restaurant op het vakantiepark (die ook weer afspraken hebben met lokale leveranciers). Hier zijn dus allerlei partijen bij betrokken waarmee je geen rechtstreeks contact meer hebt als klant. Je vertrouwt er dan op dat al deze samenwerkende organisaties, die op een of andere manier met elkaar verbonden zijn, de juiste informatie veilig met elkaar delen om jou zorgeloos de dienst te kunnen leveren. Al die partijen vertrouwen erop dat zij beveiligde toegang krijgen tot (delen van) elkaars informatie, want voor alle betrokken partijen in dit systeem geldt: geen veilige en betrouwbare informatie betekent geen vertrouwen en geen transactie. Net zoals dat op microschaal in de neurale netwerken binnen in je brein gebeurt, gebeurt dit op grotere schaal in de wereld daarbuiten. Hoe houd je hier als security officer het overzicht? De principes van familiarity en inbedding gaan hier immers niet meer op. Evenmin de controleerbare identificatieprotocollen binnen een organisatie.

Vertrouwen in (cyber)security

Waar bedrijven ooit zijn begonnen om hun interne netwerken binnen de organisatie te beschermen middels Digital Risk Protection-programma's (denk aan firewalls en identification authentication and authorization) richten zij zich nu steeds vaker op de beveiliging van netwerken en systemen buiten de organisatie. Gezien de complexiteit en schaalgrootte is dit door mensen niet meer te doen. Mede hierdoor vertrouwen we in cybersecurity steeds vaker op kunstmatige intelligentie, simpelweg omdat AI-systemen afwijkingen sneller en beter kunnen herkennen. Maar om het vertrouwen van mensen te krijgen moeten deze systemen hen eerst beter leren begrijpen. Daarvoor bouwen ze dezelfde neurale netwerken na als in jouw hersenen, zodat ze niet alleen sneller patronen kunnen herkennen in je gedrag, maar tegelijkertijd ook dezelfde neurale paden kunnen aflopen. Hierdoor kunnen ze net wat sneller voorspellen wat de gedachten zijn van hacker en slachtoffer en kunnen deze systemen hier adequater op inspelen. In de toekomst zullen AI-systemen steeds beter in staat zijn om familiarity en inbedding te simuleren, wat niet alleen de veiligheid en regelgeving binnen netwerken van organisaties ten goede komt, maar ook de vrijheid en autonomie van hun gebruikers.

In digitale onlinesystemen ben je altijd kwetsbaar voor aanvallen