Vertrouw je op beveiliging of beveilig je vertrouwen?

Bedrijven, overheden, werkgevers en burgers hebben er allemaal baat bij dat we op IT-systemen kunnen vertrouwen voor administratie, financiële transacties, communicatie en vermaak. Steeds vaker wordt echter duidelijk dat IT-systemen niet zo veilig zijn als we denken. Cybercriminelen kunnen meekijken en zo gegevens buitmaken. Niet elk systeem is dus even veilig, even goed te vertrouwen. Waarom hebben we dan toch zo veel vertrouwen in IT-systemen? En hoe kun je weten wat wel en niet veilig is? Je bewust zijn van de risico's is op zichzelf niet voldoende. Dit artikel verkent de aard van vertrouwen in IT-systemen en manieren om daar gezond en cyberveilig mee om te gaan.

Dr. Heather Young
is trekker van het programma Human Factors in Cybersecurity bij TNO.
heather.young@tno.nl

Dr. Remco Wijn
is gedragsonderzoeker bij TNO.
remco.wijn@tno.nl

INLEIDING

Veel stakeholders hebben belang bij het laagdrempelig en toegankelijk houden van het internet en de digitale omgeving. Bedrijven hebben er economisch baat bij wanneer het vertrouwen van mensen in technologie en de veiligheid ervan groot is. Burgers hebben er baat bij wanneer ze snel en makkelijk online kunnen shoppen, internetbankieren of andere zaken regelen. Naarmate de samenleving, (kritieke) infrastructuren en bedrijvigheid echter meer afhankelijk worden van IT-systemen, worden ook de risico's groter. Denk bijvoorbeeld aan digitale criminaliteit of bedrijfsspionage: ransomware, DDOS-aanvallen of social engineering.

De baten en kosten van vertrouwen zijn niet gelijk verdeeld. Sociale netwerken, webwinkels en softwareontwikkelaars zijn typisch gebaat bij veel vertrouwen, om zo de drempel voor het delen, kopen en gebruiken ervan laag te houden. Hoewel gebruikers van digitale platforms of software (zowel individuen als bedrijven) ook baten hebben, zoals het gemak van internetbankieren, komen daar ook veel nadelige consequenties bij. Denk bijvoorbeeld aan identiteitsfraude op basis van gegevens die van sociale media of gehackte websites worden geplukt, en vervolgens aanleiding zijn voor illegale praktijken. Bovendien zijn het, door de interconnectiviteit, in toenemende mate derden (zowel bedrijven als individuen) die problemen ondervinden als gevolg van risico's op andere plekken. Zo zijn het bijvoorbeeld slachtoffers zelf, maar ook banken, verhuurders en anderen die de kosten dragen van te open gebruik van sociale media.

De oplossing hiervoor is niet eenduidig en zeker niet eenvoudig. In ieder geval zou een beetje gezond wantrouwen in IT, of een slimmere taakverdeling tussen mens en IT om systemen te beveiligen, op zijn plaats zijn.

Het is echter niet wenselijk dat mensen *wantrouwig* worden ten opzichte van IT. Beter zou zijn dat mensen er niet blind op vertrouwen, in staat zijn de risico's effectief in te schatten en vervolgens verstandig te kunnen handelen. Helaas kunnen mensen niet bij iedere beslissing bewust nadenken, alle opties overwegen, risico's afwegen, et cetera. Enerzijds omdat we simpelweg niet de tijd hebben om alles wat we dagelijks tegenkomen grondig te overdenken, anderzijds doordat de meeste mensen niet voldoende kennis van IT hebben om het risico, de consequenties ervan en mogelijke mitigatiestrategieën te beoordelen. De behoefte is dus tweeledig:

1. dat mensen zich bewuster zijn van de risico's en dat ze niet zomaar alles moeten vertrouwen (lees: een gezond wantrouwen in IT hebben);
2. omdat bewustzijn alleen niet het gewenste resultaat zal geven, is het nodig dat ondersteuning voor handen is om mensen te helpen risico's, consequenties en alternatieven in te schatten en daarin keuzes te maken.

Dit alles moet op een manier gebeuren waarbij mensen gewoon kunnen blijven doen wat ze willen: e-mailen, online werken, foto's posten, surfen op het web, streamen, enzovoort.

In dit artikel bespreken wij ten eerste kort het verdelen van taken tussen mens en machine. Centraal daarin staat een analyse van het vertrouwen dat mensen hebben in IT-systemen. Vervolgens bespreken wij hoe *onveilig cybergedrag* tot stand komt, en waarom blind vertrouwen het vaak wint van cyberveiligheid. Ten slotte bespreken wij hoe een gezond wantrouwen in IT een handje kan helpen om de inschatting van risico's en alternatieven te verbeteren.

VERDELING VAN TAKEN

Hoe goed IT-systemen ook technisch beveiligd zijn, incidenten zijn niet uit te sluiten. Ten eerste omdat criminelen, hackers, enzovoorts zullen blijven zoeken naar gaten in de beveiliging, en ten tweede omdat cybercriminelen juist door de toegenomen technische beveiliging van IT hun aandacht lijken te verleggen naar de kwetsbaarheid van gebruikers van de systemen die ze willen compromitteren ([SECU12]). Gebruikers van software maken zichzelf van tijd tot tijd kwetsbaar door onveilige sites te bezoeken, mazen te zoeken om gemakkelijker hun doelen te bereiken, te verzuimen hun software te updaten, of zich direct of indirect te laten overreden om gevoelige, persoonlijke informatie te delen.

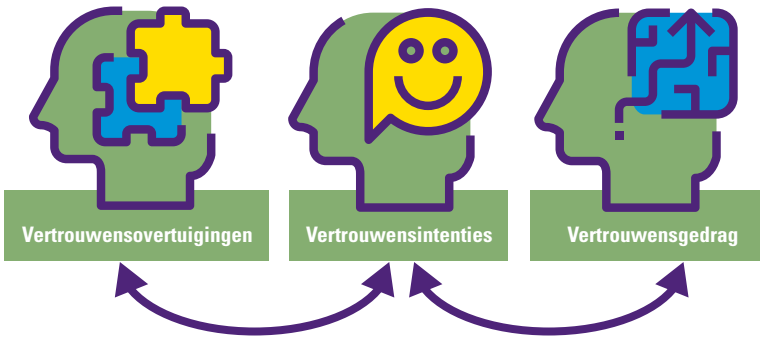
IT-systemen hebben geen eigen wil, en onder gelijkblijvende omstandigheden voeren IT-systemen iedere keer hun taken op precies dezelfde wijze uit. Mensen zijn gril-

liger: ze zijn snel afgeleid, weleens vermoeid en nemen zowel bewuste als onbewuste beslissingen. Dit leidt ertoe dat volgens sommige bronnen bij 95% van de beveiligingsincidenten menselijk handelen (een deel van) de oorzaak van het incident is ([IBM15]).

Mensen hebben echter ook hun sterke kanten. Ze zijn in staat creatief en kritisch na te denken, en kunnen daarom complexe informatie flexibel en dynamisch interpreteren ([Kame13]). Denk bijvoorbeeld aan het beoordelen van de veiligheid van een emailbijlage. Een IT-systeem kan zoeken naar kenmerken die wijzen op de betrouwbaarheid en veiligheid van een bijlage. Op basis daarvan kan het systeem een inschatting maken van het risico dat je loopt wanneer je deze opent, bijvoorbeeld wanneer er een virus in een bijlage lijkt schuil te gaan. Een mens is echter beter in staat om te bepalen wanneer er bij een ogenschijnlijk risico eigenlijk niets aan de hand is, bijvoorbeeld omdat je de bijlage verwachtte. Hiertoe is een IT-systeem op dit moment nog niet in staat.

Verschillen tussen mensen en IT-systemen hebben consequenties voor de manier waarop je deze inzet bij het inschatten van de betrouwbaarheid van een IT-systeem, en vervolgens de risico's in de cyberketen verkleint. IT-systemen kunnen mensen helpen en ondersteunen, maar (nog) geen complexe informatie *interpreteren*, wat nodig is om een accuraat betrouwbaarheidsoordeel te vormen, zoals in het bijlagevoorbeeld van de vorige alinea. Om deze reden zijn mensen nog steeds onmisbaar in dit proces. Bovendien is het onder andere de creativiteit van mensen die juist op unieke wijze kan bijdragen aan onderdelen van het beveiligingsproces. Denk dan aan het kiezen van creatieve, persoonlijke en complexe wachtwoorden, die je ook nog kunt onthouden: dat is moeilijk voor een machine (met name dat een complex wachtwoord ook onthouden kan worden), maar met een beetje creativiteit is dit relatief gemakkelijk voor een mens.

Figuur 1. Relatie tussen drie soorten 'vertrouwen', volgens [Paul17].



VERTROUWEN

Vertrouwen is geen eenzijdig concept, maar kent verschillende facetten. [Paul17] identificeert drie concepten die invloed hebben op het vertrouwen in IT. Deze worden in figuur 1 weergegeven. Ten eerste: vertrouwensovertuigingen waarbij de gebruiker erin gelooft dat de ander – in dit geval een IT-systeem – positieve kenmerken heeft, zoals goedaardigheid, integriteit en competentie. Ten tweede gaat het om de vertrouwensintenties. Dit is de bereidheid om je afhankelijk of kwetsbaar op te stellen ten opzichte van het IT-systeem. Ten derde: vertrouwensgedrag, oftewel acties die overeenkomen met vertrouwensintenties, en die blijk geven van een afhankelijke relatie met de ander. Deze drie concepten zijn van toepassing op zowel de interactie tussen mensen onderling als de interactie tussen mens en machine.

Wanneer men herhalend ervaart dat het gebruik van IT-systemen tot de gewenste uitkomsten leidt en geen negatieve consequenties heeft, kan dit leiden tot een sterke koppeling tussen de IT en het vertrouwen daarin. Er ontstaat dan gewoontematig vertrouwen ([Pien16]), oftewel automatisch en onbewust vertrouwen in IT als een soort gewoonte.

Een voorbeeld hiervan is het gebruik van internetbankieren. Je gelooft erin dat je bank het beste met je voor heeft, en tevens haar eigen systemen en data veilig wil houden. De systemen die de bank heeft ontwikkeld voor internetbankieren zijn dus veilig, en ze zullen jouw gegevens nooit misbruiken of aan een ander prijsgeven (vertrouwensovertuiging). Je bent vervolgens bereid om naar dit vertrouwen te handelen en te internetbankieren (vertrouwensintentie). Je downloadt de app en neemt de sprong: een internetaccount, alle rekeningen zichtbaar, en met een vingerafdruk inloggen (vertrouwensgedrag).

Vertrouwen wordt verder versterkt door zogenaamd institutioneel vertrouwen ([Paul17]). Hierbij gaat het om het vertrouwen in de structuren en situationele factoren in onze omgeving die het vertrouwen bevorderen. In het kader van IT kun je denken aan technologische bescherming, contracten en wetgeving die bestaan om de gebruiker te beschermen tegen cyberdreigingen en -criminaliteit: mensen hebben meer vertrouwen in IT omdat deze beschermmaatregelen bestaan. Zo is de consument bijvoorbeeld beschermd bij internetshoppen, dankzij wetgeving dat een internetwinkel goederen verplicht moet terugnemen en geld restitueren, inclusief verzendkosten ([Quis18]).

Mens of machine

Er is een belangrijk verschil tussen het vertrouwen in machines en vertrouwen in mensen. Vertrouwen in mensen heeft vaak een emotionele component, zoals wanneer iemand vertrouwt op zijn beste vrienden. Vertrouwen in IT heeft echter meer het karakter van een transactie, waarbij het gaat om verwachtingen van het nut dat wordt waargemaakt ([HSBC17]): als ik een document in een tekstverwerker opsla (mijn actie), vertrouw ik erop dat het systeem daadwerkelijk mijn aanpassingen zal bewaren (actie van het IT-systeem). Wat voor mensen mogelijk onvoldoende op de voorgrond staat, is dat wanneer ze vertrouwen hebben in IT-systemen, er achter dat IT-systeem ook mensen en organisaties schuil kunnen gaan met eigen agenda's: bonafide en malafide. Dit betekent dat de vertrouwensovertuigingen niet toereikend zijn om tot accurate vertrouwensintenties en -gedrag te komen. Met andere woorden: mensen beoordelen IT-systemen met name op hun betrouwbaarheid van nut, terwijl intermenselijke, emotionele betrouwbaarheid ook mee zou moeten spelen; als ik mijn document opsla, houd ik er geen rekening mee dat het systeem wellicht door iemand is gehakt die een grapje uit wil halen.

Consequenties

Het wel of niet hebben van vertrouwen in IT-systemen is medebepalend voor hoe wij met die systemen omgaan, oftewel ons *cybergedrag*. Cybergedrag kan veilig zijn (bijvoorbeeld alleen vertrouwde Wi-Fi-netwerken gebruiken) of onveilig (bijvoorbeeld zwakke wachtwoorden kiezen). Wat de zaak rondom vertrouwen verder compliceert, is dat veel negatieve consequenties van onveilig cybergedrag abstract en ambigu zijn; de gevolgen van een virus kunnen onduidelijk zijn, mensen kunnen zelfs niet eens van de aanwezigheid ervan op de hoogte zijn. Zo is het voor veel mensen ook niet duidelijk wat de consequenties kunnen zijn van diefstal van persoonlijke data, of het gebruik van deze data door sociale media. Ons cybergedrag kan door bedrijven en overheden gemonitord of gewijzigd worden, maar kwaadwillenden kunnen dit eveneens. Bij andere risico's is de relatie tussen het gedrag en de gevolgen ervan vaak zelfs niet zichtbaar, zoals wanneer een 'achterdeur' van een website gebruikt wordt om inloggegevens te achterhalen. Het gevolg is dat men dan geen negatieve consequenties opmerkt of ervaart van het vertrouwensgedrag, en zo nog minder alert wordt op veiligheidsrisico's.

Het wel of niet hebben van vertrouwen in IT-systemen is medebepalend voor ons cybergedrag

Mensen bezitten bovendien vaak onvoldoende kennis om malafide websites en software te herkennen en zich ertegen te wapenen. Dit vermindert eens te meer de motivatie om te investeren in een kritische evaluatie van het eigen cybergedrag. Zelfs wanneer mensen wel weten wat de gevolgen van hun gedrag kunnen zijn, leggen abstracte handelingen met gevolgen op een langere termijn, zoals een veilige IT-omgeving creëren en behouden, het meestal af tegen het nastreven van concrete handelingen met een positieve beloning op de korte termijn, zoals het versturen van een e-mail via een onbeveiligd Wi-Fi-netwerk. Met andere woorden: kortetermijndoelen zijn vaak de belangrijkste redenen voor mensen om in eerste instantie online te gaan of een programma te gebruiken, en deze hebben dus meer prioriteit dan doelen op de lange termijn, zoals cyberveilig handelen.

Gewoontes doorbreken

In het relatief jonge leven van IT is er veel nadruk gelegd op de positieve kanten van technologie, automatisering en internet. Het gebruik ervan wordt al vanaf het begin gestimuleerd, door mensen bewust te maken van de voordelen, en hen deze ook te laten ervaren. Negatieve effecten en risico's lijken minder aandacht te hebben gekregen. IT en internet, plus de associatie daarvan met het nastreven van doelen (bijvoorbeeld online winkelen, sociale contacten onderhouden, online werken, communiceren, websites bezoeken) staan veiligheidsintenties in de weg die focussen op het voorkomen van problemen. Het gevolg hiervan is dat ons cybergedrag een gewoonte geworden is, sterk gebaseerd op vertrouwen, waarin cyberveiligheid slechts een kleine rol speelt. Deze gewoonte moet eerst doorbroken worden, om plaats te maken voor een nieuwe gewoonte waarin veiligheid een groter onderdeel is.

Kortom

Samengenomen zorgen positieve ervaringen met IT voor vertrouwen in de toepassingen ervan, zonder een gezond wantrouwen jegens de personen en organisaties achter de IT-systemen. Dit wordt versterkt doordat negatieve gevolgen vaak op de lange termijn spelen, moeilijk te herkennen zijn, geen duidelijk verband houden met specifiek gedrag, abstract van aard zijn, en het voor de leek onduidelijk is hoe hij/zij zich ertegen kan verweren. Dit maakt het voor gebruikers van een IT-systeem weinig aantrekkelijk om actief in te zetten op het creëren en behouden van een veilige omgeving. Om mensen te motiveren kritischer om te gaan met hun cyberomgeving, en cybergedrag veiliger te maken, zul je positieve ervaringen en een zekere mate van voorwaardelijk vertrouwen in IT-systemen aan moeten vullen met een gezond wantrouwen. Daarmee kunnen mensen cyberrisico's beter herkennen en – nog belangrijker – ernaar handelen.

DOELEN

Zoals gezegd leggen abstracte belangen of doelen op de lange termijn (cyberveiligheid) het dus meestal af tegen concrete beloningen op de korte termijn (snel dat ene fotootje op Facebook posten). Mensen hebben een concreet doel voor ogen, waar ze prioriteit aan geven boven andere belangen – en ze hebben er veel voor over om dat doel te halen. Of het nu gaat om snel inloggen, een foto van je vakantiebestemming versturen, een rapport op tijd inleveren of je telefoon opladen; als je belemmerd wordt in het behalen van je doel, zul je zoeken naar omwegen om toch in je doelbehoefte te voorzien. Je kiest dan een makkelijk in te typen wachtwoord, gebruikt de lokale, openbare Wi-Fi-netwerken, je verstuurt het rapport via je privémail, of je laadt je telefoon op aan de laptop van je maat. Of de oplossing die je kiest veilig is – of de IT te vertrouwen is – is even minder van belang als het moment daar is, en er geen voor de hand liggend alternatief beschikbaar is.

Als je cybergedrag veiliger wilt maken en het vertrouwen in IT wilt vergroten, zul je mechanismen moeten aanwenden die cyberveilig gedrag bevorderen, én het nastreven van een doel ondersteunen, in plaats van het in de weg te staan. Je gebruikt in dat geval multifactorauthenticatie (bijvoorbeeld een wachtwoord en een code via een sms om in te loggen), je stuurt de foto via het 4G-netwerk, je versleutelt het rapport voor het versturen, je gebruikt een 'datablocker' om je telefoon op te laden (dit is een soort USB-sluis die alleen stroom doorlaat, en geen data).

Figuur 2. Belemmeringen van cyberveilig gedrag.

Kennis en kunde

- Mensen bezitten vaak de kennis en kunde niet om te beoordelen of iets wel of niet te vertrouwen is.
  Hoe kan ik zien of een bijlage een virus bevat?

Nadenken

- Mensen willen niet uitgebreid nadenken over de veiligheid van IT, en of ze hier wel of niet vertrouwen in kunnen hebben.
  De mail is van mijn bank, zegt dat niet genoeg?

Oordelen

- Samengenomen zorgen de eerste twee punten ervoor dat het moeten vormen van een oordeel over de vertrouwenswaardigheid van een IT-systeem mensen frustreert in het nastreven van hun doel, wat de kans op veilig handelen verkleint.
  Ik heb geen tijd om uit te zoeken of de mail van mijn bank bonafide is; ik geloof het wel.

Alternatieven

- Er zijn op dit moment te weinig makkelijke en 'hassle free' alternatieven voorhanden om de eerste drie obstakels te ondervangen; mensen zijn vaak aan hun lot overgelaten waar het gaat om het daadwerkelijk inschatten van het gesignaleerde risico en het kiezen van een vervolgactie.
  Ook al zou ik tijd hebben om het risico van de mail en bijlage te checken, weet ik toch niet hoe dat moet.

EEN GEZOND WANTROUWEN

Uiteindelijk is het wenselijk dat mensen verstandig omgaan met IT en de daarmee gepaard gaande risico's, dus dat mensen niet onverstandig of onveilig handelen. Figuur 2 presenteert vier belemmeringen van cyberveilig gedrag. Deze staan niet los van elkaar, maar volgen elkaar op en versterken elkaar.

Een ander voorbeeld is het downloaden van nieuwe software. Je computer geeft dan een seintje dat de software mogelijk schade kan toebrengen. Hoewel veel mensen weten dat dit een risico is, hebben ze vaak te weinig kennis om in te schatten wat dit nu precies betekent, of het in dit geval van toepassing is, wat de alternatieven zijn en welk alternatief op dat moment het beste is. Om dat te achterhalen, zouden ze na moeten denken over hoe ze de benodigde informatie kunnen vinden, zich moeten verdiepen in de relevante risico's, consequenties en alternatieven, een mening erover vormen en ten slotte een weloverwogen keuze maken. Dit frustreert het behalen van hun doel, namelijk het downloaden van de software, en doet een ongewenst beroep op schaarse mentale middelen. Wanneer de software echt nodig of gewenst is, krijgt het downloaden prioriteit boven cyberveiligheid, en zal dit analyseproces overgeslagen worden; het risico wordt voor lief genomen en de software gewoon gedownload.

IT-systemen informeren de eindgebruiker vaak slechts met de mededeling dat er risico's gepaard kunnen gaan met het openen van een bestand of bezoeken van een website, niet hoe de gebruiker kan zien of *dit* bestand of *deze* website problematisch is. Leken-eindgebruikers ontbreekt het aan kennis en kunde om a priori een mening te vormen over hoe ze de risico's moeten afwegen. Hoe kan ik weten of er *nu* een dreiging is? Hoe kan ik beoordelen of downloads van *deze* site te vertrouwen zijn of niet? Hoe kan ik weten of *deze* USB-stick gevaarlijk is?

Het is niet zo dat mensen zich niet bewust zijn van de aanwezigheid van risico's; veel van ons weten dat allerlei digitale handelingen risico's met zich meebrengen, soms ook zelfs welke specifieke risico's ([Bark17]). Het bewustzijn alleen is gewoon niet voldoende om een gedragsverandering te bewerkstelligen ([Aite12], [McGr12], [Schn13]). Het ontbreekt ons echter aan manieren om de vertrouwenswaardigheid van iets te beoordelen. Alleen een waarschuwing dat een download een gevaar met zich mee kan brengen is niet informatief: dat weet men al. De vraag is: hoe kan iemand weten of *deze download* wel of niet veilig is?

HOE DAN?

Uiteindelijk wil je dit proces doorbreken, een gezond cyberwantrouwen creëren en mensen in staat stellen de risico's en alternatieven op waarde te schatten. Mensen hebben hulp nodig waar de technische signalering van risico's ophoudt, om zo zelf een mening te kunnen vormen over de vertrouwenswaardigheid van IT; hetzij van software, een bestand, device, netwerk of website.

Mensen kritischer maken, en daarmee blind vertrouwen te lijf gaan, kan alleen als mensen de middelen in handen hebben waarmee ze de vertrouwenswaardigheid kunnen beoordelen. Figuur 3 geeft een aantal voorbeelden van hulpmiddelen.

Dergelijke hulpmiddelen zijn niet per se gericht op het veranderen van een blind vertrouwen in IT. Ze helpen echter wel degelijk om veilig cybergedrag te vergroten en de gevaren van blind vertrouwen in IT te lijf te gaan. Door ervaring op te bouwen met wat wel en niet veilig is, en hoe met risico's om te gaan, wordt misplaatst vertrouwen in IT getemperd.

Wasstraten voor URL's en bestanden bestaan al, zowel tegen betaling (bijvoorbeeld Microsoft ATP Safe Links of Norton Safe Web) als gratis (bijvoorbeeld URL Void of Scan URL). Dergelijke programma's ondersteunen bij de beoordeling of een website bonafide is of niet. Voor bijlagen zijn er vergelijkbare oplossingen, zoals Virustotal.com. Verder kun je bijvoorbeeld ook klantbeoordelingen controleren op echtheid, dankzij sites zoals Review Skeptic (zie ook [Böhm17]).

De grote vraag is hoe je ervoor moet zorgen dat mensen daadwerkelijk ook de tijd nemen om dergelijke middelen te zoeken, bekijken en de adviezen toe te passen. Duurzame verandering zal moeten gebeuren via het afbreken van oude, onveilige gewoontes en het opbouwen van nieuwe, veilige gewoontes. Dit heeft tijd nodig, maar wordt ondersteund wanneer het gebruik van de tips en tools zo makkelijk en toegankelijk mogelijk wordt gemaakt. Geef dus niet alleen een waarschuwing dat een bijlage misschien gevaarlijk kan zijn, maar geef tegelijkertijd ook een lijst van kenmerken van gevaarlijke bijlagen (of nog beter: een link naar de digitale wasstraat).

CONCLUSIE

Mensen willen kunnen vertrouwen op IT. Gezien de technologische verzadiging van onze maatschappij is dit ook goed, maar het moet nooit om blind vertrouwen gaan. Mensen kritisch laten nadenken over de mate waarin ze IT-systemen kunnen – of moeten – vertrouwen begint met hen bewust te maken van de risico's, consequenties en alternatieven. Om gebruikers vervolgens ook veilig en met gezond wantrouwen te laten handelen, vereist meer dan alleen bewustzijn.

Figuur 3. Mogelijke hulpmiddelen om de vertrouwenswaardigheid van een IT-systeem te beoordelen.

Met een terugblik van de economische context die we in de inleiding aanhaalden, zijn er onafhankelijke bedrijven die beoordelingen bij betalende klanten verzamelen over webshops, en zo dus inzicht bieden in de mogelijke risico's ([eKom18], [TRUS18]).

Ook handig zijn lijsten van risicovolle websites ([QUTT18]). Hierbij is het echter wel de vraag hoe up-to-date deze zijn, of deze handig zijn voor gebruik door leken en of die dergelijke overzichten snel en makkelijk kunnen vinden.

Er zijn op internet handige en concrete tips te vinden om te controleren of een website/webshop bonafide is ([Veen14]).

Helemaal handig is een soort wasstraat waar je digitale zaken kunt controleren.

In de weg staat dat:

1. veel mensen niet de juiste kennis bezitten om de vertrouwenswaardigheid van een IT-systeem in te schatten;
2. mensen bij het gebruik meer na moeten denken dan ze willen;
3. dergelijk denkwerk mensen frustreert bij het halen van hun doel.

Een belangrijk onderdeel van de oplossing is dat, naast het verhogen van het bewustzijn, er ook hulpmiddelen moeten zijn om afwegingen en keuzes transparanter, makkelijker en dus hopelijk beter te maken. Deze middelen moeten vervolgens bekend worden bij de mensen. Ze moeten ook makkelijk en snel te gebruiken zijn, en op zichzelf te vertrouwen (doordat ze bijvoorbeeld van een betrouwbare bron komen, zoals een overheidsinstantie).

Vertrouwen in IT is noodzakelijk, maar kan cyberveiligheid in de weg zitten. Om hier een goede balans in te vinden, moet vertrouwen gepaard gaan met een kritische houding en de middelen om een weloverwogen inschatting te maken van het risico en alternatief. Bewustzijn alleen is niet afdoende. Gelukkig zijn er veel manieren om mensen hiermee te helpen, zodat ze niet hoeven te kiezen tussen vertrouwen en veiligheid.

Disclaimer

De websites en tools genoemd in dit artikel zijn bedoeld als voorbeelden en 'used (good) practices'. Ze vormen geenszins een organisatieadvies voor aanschaf c.q. gebruik.

Literatuur

[Aite12] D. Aitel, *Why you shouldn't train employees for security awareness*, CSO Online, http://www.csoonline.com/article/2131941/security-awareness/why-you-shouldn-t-train-employees-for-security-awareness.html, 2012.

[Bark17] Jessica Barker, *The Human Nature of Cyber Security*, Cyber.uk, http://cyber.uk/humancyber/, 2017.

[Böhm17] Iris Böhm, *Online reviews: wat zijn de regels en hoe herken je neprecensies?*, Radar, https://radar.avrotros.nl/columns/detail/online-reviews-wat-zijn-de-regels-en-hoe-herken-je-neprecensies/, 2017.

[eKom18] eKomi, http://www.ekomi.nl/nl/, 2018.

[HSBC17] HSBC, *Trust in technology*, HSCB.com, https://www.hsbc.com/trust-in-technology-report, 2017.

[IBM15] IBM, *IBM Cyber Intelligence Index; analysis of cyber-attack and incident data from IBM's worldwide security services operations*, 2015.

[Kame13] Anya Kamenetz, The Four Things People Can Still Do Better Than Computers, FastCompany, https://www.fastcompany.com/3014448/the-four-things-people-can-still-do-better-than-computers, 2013.

[McGr12] G. McGraw en S. Migues, *Data supports need for security awareness training despite naysayers*, Search Security, http://searchsecurity.techtarget.com/news/2240162630/Data-supports-need-for-awareness-training-despite-naysayers, 2012.

[Paul17] S. Paul en C. Roi, *The Role of Trust in an Information Technology Milieu: An Overview*, Canadian Journal of Applied Science and Technology, 2017/5.

[Pien16] D. Pienta, H. Sun en J.B. Thatcher, *Habitual and Misplaced Trust: The Role of the Dark Side of Trust Between Individual Users and Cybersecurity Systems*, 37th International Conference on Information Systems, Dublin, 2016.

[Quis18] B. Quist, *De regels van online winkelen*, Consumentenbond, https://www.consumentenbond.nl/online-kopen/regels-online-shoppen#no5, 2018.

[QUTT18] Quttera Labs, *Data Feed*, Quttera.com, https://quttera.com/lists/malicious, 2018.

[ReSk13] ReviewSkeptic, http://reviewskeptic.com/, 2013.

[Schn13] B. Schneider, *Security Awareness Training*, Schneider on Security, https://www.schneier.com/blog/archives/2013/03/security_awaren_1.html, 2013.

[SUCU12] Security.nl, *Chrome dwingt cyberboef tot social engineering (interview)*, Security.nl, https://www.security.nl/posting/37063/Chrome+dwingt+cyberboef+tot+social+engineering+(interview), 2012.

[TRUS18] TrustPilot, https://nl.trustpilot.com/, 2018.

[Veen14] N. Veenstra, Hoe controleer je de betrouwbaarheid van een website?, Letterzaken, https://letterzaken.nl/betrouwbaarheid-website-controleren/, 2018.

De icoontjes in Figuur 1 zijn gemaakt door Smartline van www.flaticon.com en die in Figuur 3 zijn gemaakt door Freepik en Becris van www.flaticon.com.

Over de auteurs

Dr. H. Young is trekker van het Human Factors in Cybersecurity-programma bij TNO. Ze is gepromoveerd in de sociale psychologie. Haar werk is gefocust op een nieuwe approach voor het vergroten van cyberveilig gedrag. Hierbij staat nadrukkelijk niet cyberbewustzijn centraal, maar het begrijpen van de aard van onveilig gedrag, het bieden van praktische alternatieven voor onveilige handelingen en het faciliteren van cybergedrag. Zij publiceert en spreekt hierover bij diverse gelegenheden, onder andere het Congres IT & Information Security en de conferentie van de Nederlandse Vereniging voor Criminologie.

Dr. R. Wijn is gedragsonderzoeker bij TNO. Hij is gepromoveerd in de sociale psychologie en richt zich in zijn werk op het begrijpen en voorspellen van het gedrag van individuen als consument, eindgebruiker, burger, et cetera. Zijn kennis van gedrag en onderzoeksmethodieken past hij toe op diverse onderzoeksthema's, zoals online gedrag, duurzame economie en criminaliteitspreventie. Hij beschrijft dit onderzoek in populaire en wetenschappelijke outlets, en adviseert organisaties bij de toepassing van deze kennis.