Cybercrime anno 2020

Slimmer dan de hacker

Cybercrime klonk een tijd als iets futuristisch, maar tegenwoordig is het aan de orde van de dag. Cybercriminelen zijn inventief en creëren, door het grote bereik van het internet, een lucratieve business. Zo bestaan er criminele organisaties gericht op ransomware (gijzelsoftware): door te klikken op een geïnfecteerde link, worden alle bestanden op je computer versleuteld. Vervolgens wordt je aangeboden om de sleutel te kopen. Meestal voor een redelijk acceptabel bedrag, zodat je in ieder geval serieus overweegt hoeveel het je waard is om je bestanden terug te hebben. In sommige gevallen levert betaling niets op. Maar in andere gevallen kun je te maken krijgen met een heuse helpdesk, die jou 'netjes' helpt je bestanden weer terug te krijgen. Ze bestaan!

Door Inge Wetzer | Fotografie: Josina van den Bosch

Inge Wetzer is gepromoveerd in de sociale psychologie. Na 10 jaar onderzoek naar gedragsbeïnvloeding bij TNO is zij sinds 2015 gespecialiseerd in cybersecurity. Ze werkt bij Secura als sociaal psycholoog cybersecurity & compliance in het team dat zich richt op gedragsverandering in informatiebeveiliging.

Willen cybercriminelen een hogere som losgeld kunnen vragen, dan versleutelen ze niet simpelweg je computer, maar leggen ze een gehele organisatie plat. Een bekend voorbeeld hiervan is de haven van Rotterdam. Daar werden twee containerterminals platgelegd. Daarop strandden vrachtwagens, vielen kranen stil en lagen schepen werkeloos aan de kant. De schade liep in de miljoenen. Maar ook de Universiteit van Maastricht maakte begin dit jaar bekend bijna €200.000 euro aan losgeld te hebben betaald, omdat het anders weken of maanden zou duren voor medewerkers en studenten weer aan de slag konden. Bovendien zouden sommige bestanden mogelijk verloren zijn gegaan.

CEO-fraude

Cybercrime gaat verder dan phishing. Bijvoorbeeld CEO-fraude, waarbij de financiële afdeling vaak per e-mail de opdracht van de CEO ontvangt om met spoed een bepaalde factuur te betalen. Hierbij wordt feilloos ingespeeld op menselijke drijfveren zoals bevestiging "dit is een gevoelige factuur en ik vertrouw alleen jou, dus houd dit stil", tijdsdruk: "ik weet dat het eigenlijk via het systeem moet, maar als dit vandaag niet wordt overgemaakt, komen we in de problemen", of gevoeligheid voor autoriteit, want in sommige organisaties durft men zich niet kritisch op te stellen tegenover de CEO. Criminelen verdiepen zich zodanig in een organisatie, haar cultuur en medewerkers, dat ze schrikbarend goed in staat zijn hier de juiste accenten te leggen. Consequenties? Negentien miljoen euro overgemaakt naar criminelen door Pathé, met ontslag van CEO én CFO tot gevolg. Maar Pathé is niet het enige bedrijf. De rest heeft alleen het geluk gehad dat ze dit uit de media wist te houden.

Beschermen en/of verzekeren?!

Nu de voorbeelden van incidenten zich opstapelen, groeit de vraag naar cyberverzekeringen. Uiteindelijk hopen we die echter allemaal zo weinig mogelijk te hoeven gebruiken. Een goede bescherming vooraf is dus noodzakelijk. Je beschermt immers ook je huis met een inboedelverzekering. Maar hoe bescherm je je nou het effectiefst tegen cybercrime? Deels zit hem dat uiteraard in veilige techniek. Zo zijn bijvoorbeeld een goede virusscanner en firewall en het draaien van updates voorwaarde nummer één. Daarnaast zijn de processen in een organisatie van belang; het beleid moet ondersteunend zijn aan het veilig werken. Alleen, met veilige techniek en processen zijn we er nog niet. Want kijk eens naar de voorbeelden hierboven. Cybercriminelen proberen juist vaak via de mens te hacken!

De psychologie van cybercrime

Als psycholoog in de wereld van cybersecurity ben ik een beetje een vreemde eend in de bijt. Het vakgebied bestaat grotendeels uit IT'ers, informatiebeveiligingsspecialisten en techneuten. Maar ja, we hebben net gezien dat juist vaak via de mèns wordt aangevallen. Vijftien jaar geleden was dat nog een stuk minder geavanceerd dan nu. Destijds bestond de grootste aanval op de mens nog uit slecht geformuleerde e-mails over een erfenis van een Nigeriaanse prins. Daar konden de IT'ers en cybersecurityspecialisten ons prima tegen wapenen en algauw trapte haast niemand daar nog in. Tegenwoordig zijn de mensgerichte aanvalstechnieken van cybercriminelen echter een stuk vernuftiger. We zijn op het punt beland dat waarschuwen met e-mailtjes en posters niet meer volstaat. Geavanceerdere aanvallen vragen om geavanceerdere verdediging. Voer voor psychologen! Want zorg er maar eens voor dat mensen niet meer in deze aanvallen trappen...

Kans verkleinen

Om de kans te verkleinen dat mensen slachtoffer worden van cybercrime, wordt vaak informatie gezonden over de do's en don'ts. En inderdaad, het is hartstikke belangrijk dat mensen weten wat ze moeten doen. Alleen, er zit een kloof tussen wéten wat je zou moeten doen en feitelijk gedrag. Tussen begrijpen en doen. In de ideale wereld kent iedereen de regels en houdt zich daar perfect aan. De praktijk is echter wat weerbarstiger. Dit verklaart ook waarom e-learnings en bewustwordingstrainingen maar beperkt effect sorteren. Mensen zijn geen rationele wezens. Cybercriminelen weten dat en spelen daar feilloos op in. Tijd dus om daar in de bescherming aandacht voor te hebben en niet te stoppen bij het zenden van informatie. We moeten immers slimmer worden dan de hackers! Dat vergt dus niet alleen bescherming op kennisvlak, maar juist ook op de andere gebieden

Voer voor psychologen!

waar criminelen gebruik van weten te maken. Zij zorgen er namelijk vaak voor dat we – ondanks dat we weten hoe we het beste kunnen handelen – een trigger hebben om toch in hun verhaal mee te gaan. Door in te spelen op onze motivatie krijgen criminelen ons zover dat we voorbijgaan aan onze kennis. Bijvoorbeeld omdat we bang zijn dat onze bankrekening inderdaad net gehackt is, delen we tóch onze inloggegevens met die vriendelijke mevrouw aan de telefoon. Of omdat we zo vereerd zijn dat de CEO nou net precies óns in vertrouwen neemt, maken we dat geld voor hem over zonder dubbel te checken.

Veilig gedrag

Willen we dus beschermd zijn tegen cybercrime, dan zullen we ons moeten richten op veilig gedrag. Psychologie laat zien dat gedrag wordt bepaald door kennis, persoonlijke factoren (zoals motivatie en ervaring) en organisationele factoren (context en cultuur). Om een organisatie te beschermen, zullen deze factoren dan ook alle drie geadresseerd moeten worden. Net zoals criminelen doen! Zij zoeken naar het zwakste punt om op in te kunnen spelen. Zo heeft een sterk hiërarchische organisatie een grotere kans om slachtoffer te worden van CEO-fraude, omdat criminelen weten dat de machtsafstand ervoor zorgt dat mensen de CEO niet snel zullen benaderen. Tegelijk loopt een hechte organisatie met veel vertrouwen en commitment juist weer meer risico om via slimme babbeltrucs 'een collega' verder te willen helpen en daarmee meer weg te geven dan de organisatie lief is.
Tijd om het tij te keren dus! Wéét dat je uitgedaagd wordt om anders te handelen dan volgens de regels. Dus schroom niet om binnen te lopen bij een collega om te checken of die e-mail echt van hem komt, om de bank terug te bellen op het nummer dat bekend is en om die 'vriend met dat nieuwe telefoonnummer' even een berichtje op zijn oude nummer te sturen. Het is 2020. <

> Er zit een kloof tussen wéten wat te doen en feitelijk gedrag