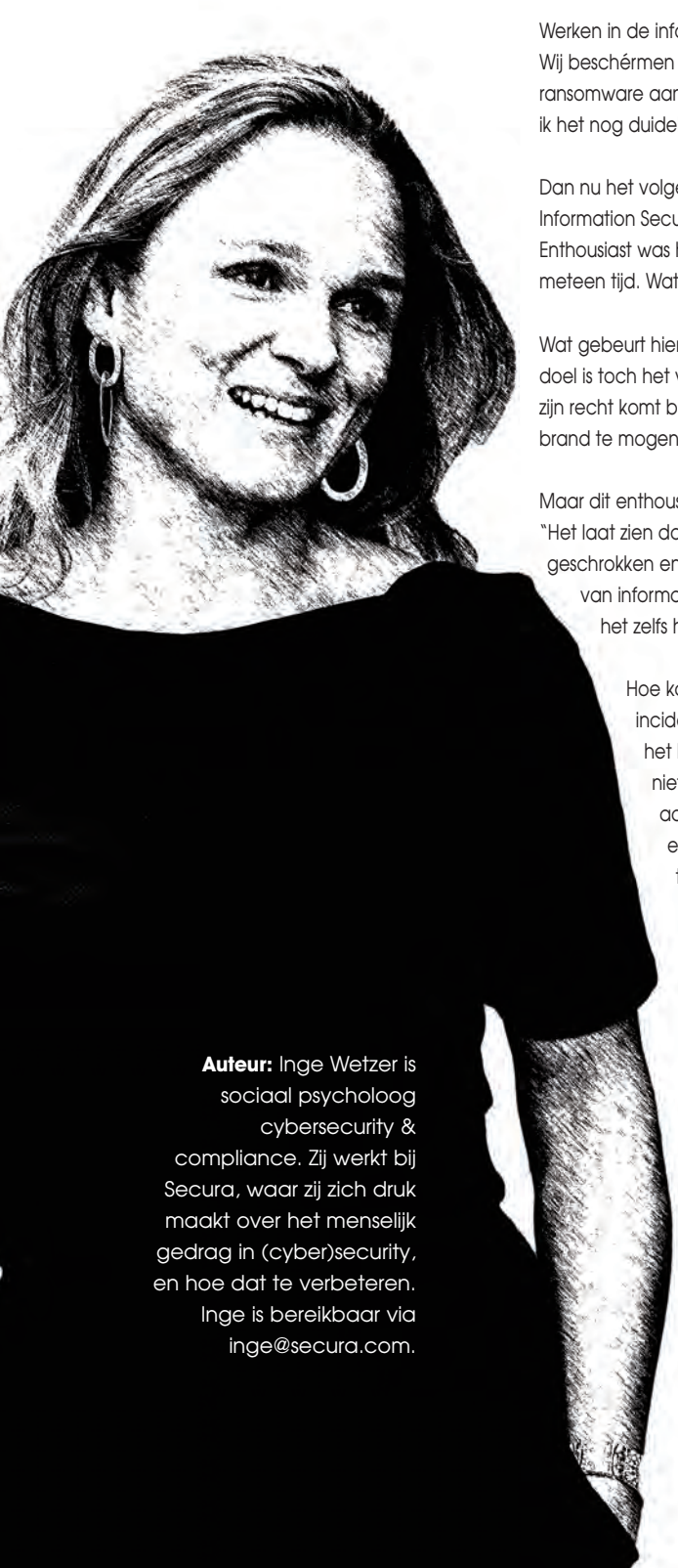
Yes! Een incident!



Werken in de informatiebeveiliging betekent dat je je bezighoudt met het voorkómen van incidenten. Wij beschérmen organisaties. Wij zorgen ervoor dat organisaties niet het slachtoffer worden van een ransomware aanval. Wij zijn ervoor verantwoordelijk dat er géén datalek komt. Oké? Ik weet niet hoe ik het nog duidelijker kan omschrijven. Wij willen géén incidenten! Eens? Ja toch?!

Dan nu het volgende: vorige week ontving ik een zeer enthousiast berichtje van de CISO (Chief Information Security Officer) van een organisatie die ik ondersteun bij hun informatiebeveiliging. Enthousiast was hij, goed nieuws had hij, of ik snel even kon bellen. Nieuwsgierig geworden maakte ik meteen tijd. Wat bleek het goede nieuws? Er was een incident! Euh...

Wat gebeurt hier nou, dacht ik (ja, met het stemmetje van juf Ank: "Ik vind dit héél bijzonder"). Ons doel is toch het voorkómen van incidenten? Is het misschien dat onze passie voor dit vak het best tot zijn recht komt bij een incident? Brandweerlieden vinden het immers toch ook mooi om naar een brand te mogen om daar te kunnen helpen?

Maar dit enthousiasme was toch van een andere soort. Dat bleek uit het vervolg van het telefoontje: "Het laat zien dat het dus écht kan gebeuren! Het is niet uit de hand gelopen, maar we zijn wel geschrokken en nemen het serieus. Hopelijk kan ik nu eindelijk...." Het incident maakte het belang van informatieveiligheid duidelijk. Het onderstreepte de reason to be van de CISO. Misschíen zou het zelfs helpen om eindelijk eens een `1' op zijn rekest te krijgen.

Hoe kan het toch dat wij – voorkómers van incidenten – regelmatig toch blij zijn met een incident? Omdat we het nodig hebben! Voor draagvlak, budget en ondersteuning van het bestuur. Helaas is het risico van slechte informatiebeveiliging voor veel bestuurders niet tastbaar, helder of reëel genoeg om er prioriteit aan te geven. Er is iemand voor aangewezen in de organisatie en daarmee is het onderwerp afgedekt. En eerlijk is eerlijk, het is een stuk lastiger uitleggen aan de board dat je investeert om dingen níet te laten gebeuren. Zeker als die dingen de afgelopen periode ook niet zijn gebeurd, dan denkt men al gauw dat het zo toch prima gaat. Risico is kans × impact. De kans wordt graag onderschat en de impact gebagatelliseerd. Dan valt het risico best mee.

Met enige regelmaat heb ik CISO's horen verzuchten dat ze eigenlijk een incident nodig hebben. Let wel, dit incident moet natuurlijk wel aan onze voorwaarden voldoen: het mag niet té groot zijn, want dan zijn de consequenties te omvangrijk. En niet te klein, want dan maakt het nog geen indruk. We willen dus graag een precies goed incident. En dan niet gesimuleerd, want dan krijgen we weer te horen dat het toch nep was en in het echt nooit zou gebeuren. En niet bij een ander, want dan wordt gezegd dat wij een heel ander type organisatie zijn en dat risico niet lopen. En met impact, zodat men even schrikt van de mogelijke gevolgen. Vandaag hadden wij geluk. Wat een geluk! Wij hadden precies het goede incident. Yes!

Inge

Auteur: Inge Wetzer is sociaal psycholoog cybersecurity & compliance. Zij werkt bij Secura, waar zij zich druk maakt over het menselijk gedrag in (cyber)security, en hoe dat te verbeteren. Inge is bereikbaar via inge@secura.com.