CUSTOMER CASE

A.S.F. Fischer BV normaliseert security awareness, net als brandveiligheid

“Security Awareness is meer dan een training. Het helpt ons gedrag te sturen en structuur aan te brengen in hoe we met risico’s omgaan.”

Gayana Marjani
Databeheer - A.S.F. Fischer BV

A.S.F. Fischer BV normaliseert security awareness, net als brandveiligheid

Het vergroten van het bewustzijn en het trainen van medewerkers op het gebied van cyber security, gebeurt bij A.S.F. Fischer BV niet via een eenmalige training, maar als een doorlopend proces. Gayana Marjani, verantwoordelijk voor databeheer, benadert security awareness daarom structureel als vast onderdeel van de dagelijkse praktijk.

In een organisatie waar operationele druk, logistieke complexiteit en commerciële processen samenkomen, is menselijk gedrag de belangrijkste risicofactor. A.S.F. Fischer BV koos daarom bewust voor een structurele aanpak van security awareness, ondersteund en begeleid door DTX.

In deze customer case lees je hoe A.S.F. Fischer BV security awareness heeft genormaliseerd binnen de organisatie, en hoe meetbaarheid en eigenaarschap daarbij centraal zijn komen te staan.

Over Gayana Marjani

Gayana werkt bijna een jaar bij A.S.F. Fischer BV als verantwoordelijke voor databeheer en informatievoorziening. Ze zorgt dat artikeldata kloppen, dat informatie op de juiste plek terechtkomt en dat collega's kunnen werken zonder per ongeluk gevoelige gegevens te lekken.

Haar eerdere baan was op een afdeling financial crime bij een bank. Daar zag ze hoe fraude bijna altijd begint bij één persoon die iets te snel op een link klikt of een verkeerd telefoongesprek vertrouwt. Die ervaring nam ze mee. "Security is voor mij geen los IT-thema. Het gaat over gedrag, bewustwording en weten wat je moet doen op het moment dat het misgaat," vertelt ze. Techniek helpt, maar lost het niet op.

In het kort: Security Awareness & Phished.io.

Security Awareness: De menselijke laag van cyber security: het niveau waarop medewerkers verdachte e-mails, nieuwe dreigingen en onveilig gedrag herkennen en er juist op reageren.

Phished.io: Het trainingsplatform dat DTX inzet bij klanten om medewerkers te helpen cyberdreigingen te herkennen, met gesimuleerde phishingmails, korte leermodules, informatie over actuele dreigingen en een meldknop voor verdachte e-mails. Op basis daarvan wordt een score per medewerker en voor het bedrijf bepaald.

Lees meer over Phished: **www.dtx.nl/phished**

Over A.S.F. Fischer BV.

A.S.F. Fischer BV. is een familiebedrijf dat in 1945 begon als de Amsterdamse Schroeven Fabriek (A.S.F.) met een eigen productielijn voor schroeven en draadnagels. In de decennia daarna verschoof het zwaartepunt van produceren naar importeren en distribueren, en uiteindelijk naar het samenstellen van complete bevestigingsoplossingen voor de bouw en industrie. Vanuit Lelystad bedient het bedrijf inmiddels professionele afnemers in de bouwmaterialenhandel, hout- en plaatmaterialenhandel, ijzerwarenvakhandel, elektrotechnische groothandel en industrie.

- Medewerkers: 130+
- Export: actief in meer dan 25 Europese landen
- Assortiment: meer dan 50.000 artikelen
- Marktpositie NL: circa 90% van de bouwgroothandels gebruikt producten van A.S.F. Fischer BV

Bekijk de website van A.S.F. Fischer BV.

Waarom security awareness serieus wordt opgepakt

Cyber security was bij A.S.F. Fischer BV lange tijd vooral iets wat op de achtergrond werd geregeld. Een externe IT-partij zorgt voor de technische basis, bijvoorbeeld door verdachte mails tegen te houden voordat ze bij medewerkers in de inbox belanden. Dat werk is belangrijk, maar ook onzichtbaar voor de gemiddelde medewerker. De mensen die elke dag met mail, klantdata en orders werken, stonden er eigenlijk buiten. Ze wisten dat “security belangrijk is”, maar als ze ‘s ochtends een mail van een onbekende leverancier openden met een bijlage, was er geen houvast: wat doe je dan, en aan wie meld je het?

Gayana merkte dat gat direct. Er was geen plek waar collega’s konden zien welke dreigingen op dat moment speelden, geen uitleg over wat er van hen werd verwacht, en geen manier om te meten of mensen vooruitgang boekten. “Iedereen hoorde wel dat security belangrijk was, maar het was niet concreet of meetbaar,” vat ze samen.

Tegelijk kwam het onderwerp steeds dichterbij. Phishingmails werden geraffineerder, berichten over gehackte Nederlandse bedrijven verschenen bijna wekelijks in het nieuws en in de eigen branche circuleerden verhalen over bedrijven die dagen stillagen na één verkeerde klik. In een omgeving waar orders en leveringen geen uur kunnen wachten, was de conclusie snel getrokken: techniek alleen is niet genoeg.

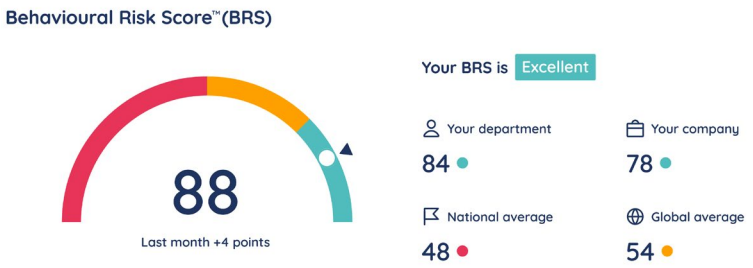
Security awareness als continu proces, niet als training

A.S.F. Fischer BV heeft bewust geen “awareness-training” ingekocht met een begin, en einddatum. In plaats daarvan krijgen collega’s het hele jaar door prikkels die hen scherp houden: gesimuleerde phishingmails die onaangekondigd in hun inbox verschijnen, korte leermodules van een paar minuten, een meldknop in Outlook voor verdachte berichten, en waarschuwingen over nieuwe dreigingen in de apps en devices waar ze mee werken. Gayana vult dat aan met bijna wekelijks een kort advies, bijvoorbeeld over een actuele phishingtruc of veilig privégebruik van de mobiel, plus een vaste rubriek in de interne maandelijkse nieuwsbrief. Zo hoort het onderwerp bij het gewone ritme van het bedrijf, en niet bij een losse campagne.

Het Phished.io-platform is daarvoor de basis. Het stuurt gesimuleerde phishingmails, biedt leermodules aan en laat per afdeling zien wie welke berichten herkent en wie erin trapt. Maar, zegt Gayana, een platform op zichzelf werkt niet. Het zijn de gesprekken eromheen, in de kantine, op de werkvloer en in de nieuwsbrief die het onderwerp levend houden. En die gesprekken gaan vaak verder dan het werk. Phishing op je privémail, een valse sms van “de bank”, een nepbericht van een bezorgdienst: het zijn dezelfde trucs. “Wat medewerkers leren, kunnen ze ook thuis toepassen. Dat maakt het persoonlijker en daardoor serieuzer,” legt ze uit. Zodra mensen merken dat het ook hun eigen gezin raakt, wordt het geen bedrijfsregeltje meer.

Behavioral Risk Score

De BRS-score (Behavioral Risk Score, een bedrijfsbrede indicator voor digitaal gedrag) versterkt dat: omdat het één centrale score is waar iedereen aan bijdraagt, voelt elke collega dat zijn gedrag meetelt in het gezamenlijke resultaat.



Voorbeeld BRS-Score – Geen A.S.F. Fischer BV score.

Security awareness normaliseren, de vergelijking met brandveiligheid

De kern van Gayana's aanpak is een simpele vergelijking: brandveiligheid. Iedereen weet bij een brand waar de nooduitgang is en wie er belt met 112. Dat is niet omdat mensen er graag over nadenken, maar omdat het is ingesleten. Datzelfde wil ze bereiken voor digitale incidenten: een verdachte mail? Meldknop. Per ongeluk een bijlage geopend die niet klopt? Direct even melden bij IT, geen paniek, geen schaamte. "Bij brand weet iedereen wat hij moet doen en waar hij moet zijn. Maar weten mensen dat ook bij een datalek? Dat moet je normaliseren."

Die normalisering krijgt steun van bovenaf. Tijdens bijeenkomsten op kantoor heeft de directie zelf toegelicht waarom A.S.F. Fischer BV met het programma is gestart en wat er van collega's wordt verwacht. Daardoor krijgt security awareness het gewicht van een bedrijfsbrede keuze, en niet van een IT-project.

Dat maakt gesprek over de score en onderwerp security makkelijker, zonder dat Gayana hoeft te preken. Wie een paar keer in dezelfde val trapt, krijgt geen standje, maar wel persoonlijke aandacht.

Ze werkt in twee stappen: eerst een korte herinneringsmail dat de training klaarstaat, en pas als dat niet helpt pakt ze de telefoon om rustig uit te leggen waarom het belangrijk is. "We zien bijvoorbeeld dat het gebruik van de rapporteerknop duidelijk is toegenomen zodra we dit actief zijn gaan uitleggen en benadrukken," merkt ze op.

Gezamenlijke verantwoordelijkheid: hoe erkenning security awareness versterkt

Met de introductie van de Teamtrofee moedigt A.S.F. Fischer BV medewerkers aan om actief bij te dragen aan security awareness. Maandelijks worden de drie meest betrokken collega's bekendgemaakt, wat gezonde competitie en motivatie stimuleert. De nummer één ontvangt de trofee als erkenning voor hun bijdrage.

Doordat de trofee binnen het team rouleert, blijft de focus liggen op groei, ontwikkeling en gezamenlijke verantwoordelijkheid. Het is een manier om niet alleen prestaties te vieren, maar ook om het belang van digitale veiligheid te benadrukken.

De rol van DTX

Elke maand zit Gayana aan tafel met DTX om de cijfers van de afgelopen periode door te nemen: welke oefenmail werd vaak aangeklikt, welke afdeling loopt voorop, waar zit juist een knelpunt? Die analyses vertalen de ruwe data naar gerichte vervolgstappen: een extra oefenronde voor een specifiek team, een nieuwsbrief over een dreiging die actueel is, of een gesprek met iemand die extra hulp kan gebruiken.

Door dat overleg komt Gayana niet alleen te weten wat er gebeurt, maar ook wat ze ermee kan. "Door de maandelijkse analyses begrijp ik niet alleen wat we zien, maar ook wat ik ermee kan doen in de organisatie," zegt ze. Dat laatste is voor haar het verschil tussen een rapport dat in een la verdwijnt en een programma dat meebeweegt met het bedrijf.

Een belangrijk hulpmiddel daarbij is het Power BI-dashboard (ontwikkeld door onze Data & AI eXperts) dat voor A.S.F. Fischer BV is ingericht. Waar Gayana in het Phished.io-platform zelf veel informatie handmatig bij elkaar moet klikken, brengt het dashboard de belangrijkste cijfers in één scherm samen: de BRS-score, het gebruik van de meldknop, de voortgang per afdeling, en de actuele dreigingen in apps en devices waar collega's mee werken. **Frank Bakkum**, CISO bij DTX, gebruikt datzelfde dashboard om zijn maandelijkse advies op te bouwen, en Gayana kan er op elk moment zelf in kijken. Dat scheelt werk en maakt het gesprek scherper: in plaats van te hoeven zoeken in losse rapportages, ligt het beeld klaar.

Binnen de samenwerking noemt ze Frank als belangrijke sparringpartner. Zijn rustige manier van uitleggen en zijn vermogen om technische signalen terug te brengen tot een simpele keuze, helpt Gayana om snel te schakelen en collega's mee te nemen zonder het onderwerp zwaarder te maken dan nodig.

Wat er op de werkvloer is veranderd

De verschuivingen en ontwikkelingen zijn duidelijk zichtbaar:

- Collega's kijken twee keer voordat ze een bijlage openen
- De meldknop in Outlook wordt steeds vaker gebruikt
- Twijfel wordt eerder uitgesproken in plaats van weggeklikt
- Security komt spontaan ter sprake in gesprekken tussen collega's

Het onderwerp heeft zijn plek gevonden in het dagelijks werk, en voor een deel van de medewerkers ook thuis. Dat A.S.F. Fischer BV een familiebedrijf is, helpt daarbij: de lijnen zijn kort, collega's kennen elkaar, en een gezamenlijk belang zoals samen veilig blijven landt sneller dan in een anonieme organisatie.

Slotadvies van Gayana

Voor organisaties die nog twijfelen of ze hiermee aan de slag moeten, houdt Gayana het kort: "Behandel het net als brandveiligheid. Je oefent niet omdat het leuk is, maar omdat je wilt weten wat je moet doen als het misgaat. Met cyber security is dat niet anders."

Dankwoord

DTX bedankt A.S.F. Fischer BV en Gayana Marjani voor de openheid waarmee ze dit verhaal hebben willen delen. Hun aanpak laat zien dat digitale weerbaarheid begint bij mensen en gedrag, ondersteund door kennis, inzicht en samenwerking.

www.dtx.nl/contact

SECURE TODAY
ACCELERATE TOMORROW