SECURITY DOSSIER 2019 | CHANNELCONNECT

Duurzame beveiligingscultuur begint bij bewustwording

Cybercriminaliteit is een groot maatschappelijk probleem en bedrijven zijn zich hier terdege van bewust. Desondanks denken nog steeds veel bedrijven dat cybercrime is te voorkomen met alleen beveiligingstechnologie. De meeste cyberincidenten worden echter veroorzaakt door menselijk handelen, waardoor organisaties ook moeten investeren in een sterke beveiligingscultuur. Securitybedrijf G DATA heeft daarom naast zijn securityoplossingen een security-awareness-training ontwikkeld. Wij spraken met Jerrel Abdoel, country manager van G DATA Nederland.

Jerrel Abdoel geeft een helder antwoord op onze eerste vraag waarom een beveiligingscultuur belangrijk is voor een organisatie. “Cybercriminelen voeren aanvallen uit met behulp van tactieken, zoals phishing, die vaak als doel hebben om mensen gevoelige gegevens te laten delen. Hierdoor zijn werknemers vaak als eerste betrokken bij een cyberaanval”, zegt Abdoel. “Computers en apps klikken tenslotte niet op phishing-e-mails en mensen wel. Bovendien hebben medewerkers dagelijks toegang tot het netwerk van de organisatie, waardoor ze een belangrijke rol spelen in de cyberveiligheid van het bedrijf.”

Loyaliteit

Abdoel vervolgt: “Daarnaast promoot een beveiligingscultuur goed gedrag en ontmoedigt het risicovol gedrag of neigingen in de richting van fraude. Bovendien zal het ook zorgen voor een sterker klantvertrouwen en loyaliteit aan je merk. De meeste klanten willen namelijk geen zaken doen met een bedrijf waarvan ze weten dat hun gegevens mogelijk niet veilig zijn. Een duurzame beveiligingscultuur op de werkplek past het gedrag van werknemers in positieve zin aan. Dit zorgt ervoor dat medewerkers zich verantwoordelijk voelen voor de veiligheid van de organisatie. Het is daarom belangrijk dat bedrijven investeren in een veilige beveiligingscultuur.”

Realisatie

Belangrijke volgende vraag aan Abdoel is hoe dan een solide beveiligingscultuur gecreëerd kan worden. “Een beveiligingscultuur realiseer je niet alleen met voorlichting over bijvoorbeeld kwaadaardige links en hoe een wachtwoord moet worden aangepast”, antwoordt Abdoel. “Dit is slechts een onderdeel van het bewustwordingsproces. Om een beveiligingscultuur te creëren zullen bedrijven een structureel bewustwordingsprogramma op moeten zetten om het gedrag van medewerkers te veranderen.”

Menselijke fout

Volgens Abdoel is het belangrijk om eerst het besef van noodzaak bij te brengen bij zowel de directie als de medewerkers. “Als eerste is het belangrijk dat het management begrijpt dat de meeste inbreuken komen door menselijke fouten. Hierdoor zal het management inzien dat training cruciaal is voor een veilige organisatie. Daarnaast zullen ook de werknemers moeten snappen dat zij doelwit zijn van cybercriminelen. Medewerkers hebben toegang tot interessante informatie die cybercriminelen graag willen bemachtigen; ze beschouwen hen dan ook als een gemakkelijke prooi. Het is daarom essentieel om ze te wijzen op hun gedrag om cybercrime te voorkomen en potentiële risico’s te verminderen.”

Confrontatie

Maar alleen het wijzen op de risico’s is meestal niet genoeg, weet Abdoel. “Het is belangrijk dat medewerkers worden geconfronteerd. Op deze manier zullen ze eerder de voordelen van gedragsverandering inzien. Denk hierbij aan een veiligere en productievere werkomgeving en de verminderde kans op diefstal van persoonlijke informatie. Een confrontatie van ‘verkeerd’ gedrag kan bijvoorbeeld worden aangekaart middels een phishingtest. Daarnaast is het een ideale nulmeting om het bewustzijnsniveau te meten van medewerkers.”

Kracht van herhaling

Nadat het besef van noodzaak is bijgebracht, is het tijd om medewerkers structureel te trainen. Abdoel geeft aan dat de kracht van herhaling hierbij cruciaal is. Door steeds opnieuw aandacht te besteden aan het gewenste gedrag blijft het onderwerp top-of-mind en wordt er toegewerkt naar een positieve beveiligingscultuur. “Een oude volkswijsheid is dat je zeven keer moet leren en zeven keer zult vergeten”, zegt Abdoel. “Er zit namelijk een groot verschil tussen het kennen en het herkennen van informatie. Als je informatie herkent, betekent het nog niet dat je iets kunt navertellen of toepassen. Door herhaling wordt informatie opgeslagen in het langetermijngeheugen en gebeuren handelingen beetje bij beetje vanzelf.”

Jerrel Abdoel

Evaluatie

Daarnaast is het volgens Abdoel belangrijk om regelmatig een evaluatie uit te voeren. Op deze manier kan er worden vastgesteld of de inspanningen effect hebben. “De conclusies van de evaluatie zijn er niet om mensen de les te lezen, maar juist om de medewerkers open en eerlijk te vertellen wat er moet gebeuren om de tekortkomingen te compenseren. Met een goede evaluatie kun je ook bepalen welke strategie wel en niet werkt binnen de organisatie. Het is daarom verstandig om vooraf al een nulmeting te doen en tussendoor metingen uit te voeren. Op deze manier kan er samen worden gewerkt aan een solide veiligheidscultuur. Een veiligheidscultuur is er tenslotte niet meteen en het duurt meestal een aantal jaar voordat er echt verandering zichtbaar is.”

Security Awareness Training

G DATA heeft enige tijd geleden de G DATA Security Awareness Training ontwikkeld. Maar kan men met deze training een solide beveiligingscultuur creëren, zo vragen we Abdoel. “Onze security awareness training is een tool om bewustwording te creëren”, antwoordt hij. “De trainingen zijn daarom ontwikkeld om menselijke fouten te voorkomen. Er is immers maar één persoon nodig die zonder nadenken een kwaadaardige e-mailbijlage opent, waardoor een compleet netwerk wordt geïnfecteerd. Je creëert met de training niet meteen een beveiligingscultuur. Hiervoor zullen organisaties zelf een plan moeten ontwikkelen. Onze partners en securityspecialisten kunnen organisaties hier uiteraard wel mee ondersteunen. De trainingen behandelen uiteenlopende onderwerpen op het gebied van IT-beveiliging, bijvoorbeeld over hoe om te gaan met phishing-e-mails of social engineering. In meer dan dertig cursussen worden de nieuwste leermethoden gebruikt om kennis over te dragen waarbij zowel video als tekst wordt gebruikt. Voordat de training begint, kunnen IT- en HR-managers een kennistest uitvoeren om te bepalen waar de meest urgente trainingsbehoeften zich bij het personeel bevinden. Dit maakt duidelijk welke onderwerpen eerst moeten worden aangepakt. Bovendien kunnen deelnemers alle cursussen in hun eigen tempo afronden.”

Updaten en patchen

Abdoel geeft aan dat de meeste fouten worden veroorzaakt door mensen. Maar welke menselijke fouten komt hij het meest tegen tijdens zijn werk? Abdoel zegt gedecideerd: “Er zijn heel erg veel soorten menselijke fouten. Bij medewerkers komt phishing en acquisitiefraude heel vaak voor; deze incidenten ontstaan meestal omdat medewerkers de signalen van een dergelijke aanval niet herkennen. Echter zie ik ook dat IT-afdelingen menselijke fouten maken. Ze vergeten bijvoorbeeld vaak hun systemen te updaten en te patchen terwijl dit een vitaal onderdeel is van je beveiliging. Het overgrote deel van alle informatiebeveiligingsincidenten vindt plaats als gevolg van misbruik van kwetsbaarheden in verouderde software. Door het installeren van updates worden de gaten in de beveiliging verholpen en wordt het risico op misbruik minder. Hoe langer je wacht met updaten, des te groter de kans op misbruik. Menselijke fouten komen overal dus voor. Echter betekent dit niet dat je er als organisatie niets aan moet doen. Om menselijke fouten zo min mogelijk voor te laten komen, zul je iedereen moeten trainen zodat incidenten voorkomen kunnen worden.”

Wat betekent deze nieuwe tool voor de partners? “Dankzij onze security awareness training kunnen partners hun klanten nog beter bedienen en een completere beveiliging bieden, aldus Abdoel. “Hierdoor kunnen ze meer omzet genereren door bijvoorbeeld totaalpakketten aan te bieden met onze beveiligingssoftware in combinatie met de security awareness training. Daarnaast trainen wij onze partners zodat zij de eindgebruiker kunnen ondersteunen met cyberbewustzijn. Want aan een veiligere online wereld werken we samen!”