Medewerkers de sterkste schakel in

INFORMATIEBEVEILIGING IN UW ZORGINSTELLING

Secura
A BUREAU VERITAS COMPANY

Het Cybersecurity Dreigingsbeeld Zorg 2020 dat door Stichting Z-CERT is gepubliceerd is er duidelijk over: ''De zorgsector heeft regelmatig te maken met datalekken. Deze datalekken komen voornamelijk door malware-infecties, menselijke fouten, phishing en soms door kwetsbaarheden in webapplicaties".

CREËER CYBER VEILIG GEDRAG BINNEN DE ZORG

Sturen op veilig gedrag, naast sturen op snel, efficiënt en kosteneffectief werken, vergt doorlopende aandacht van het management. Geen enkele medewerker van de zorginstelling wil een datalek, een hack of een storing veroorzaken. Toch gebeurt dat af en toe wel doordat men niet wordt beoordeeld op veilig gedrag, en omdat de beschikbare middelen niet aansluiten bij de behoefte van medewerker.

In februari publiceerde het Computer Emergency Response Team voor de Zorg (Z- CERT) het bovengenoemd Dreigingsbeeld. Daarin stelt Z – CERT meerdere malen vast dat informatiebeveiliging meer omvat dan alleen de techniek die een zorginstelling in huis heeft om hackpogingen, verstoringen of andere vormen van cyber criminaliteit het hoofd te bieden.

'' Zorginstellingen ontvangen pogingen tot financiële fraude, door bijvoorbeeld valse facturen, CEO-fraude en malafide pogingen om rekeningnummers van medewerkers en leveranciers te veranderen. Wij raden aan medewerkers van financiële afdelingen regelmatig te attenderen op dit soort fraude"

Fouten van medewerkers worden met name zorgbestuurders aangerekend. Bestuurders krijgen veel gevoelige en vertrouwelijke informatie onder ogen. Een onjuiste omgang met deze gegevens kan leiden tot (ernstige) imagoschade. Om zorgvuldig met deze gegevens om te gaan zijn er allerlei interne beveiligingsinstructies en protocollen van kracht, die bijvoorbeeld aangeven hoe er met externe gegevensdragers, smartphones, tablets en pc's moet worden omgegaan. In feite wordt er in deze instructies en protocollen vastgelegd hoe de zorginstelling wilt dat de medewerkers zich ten aanzien van informatiebeveiliging gedragen.

Toch blijkt in de praktijk dat deze instructies en protocollen lang niet altijd worden nageleefd. Waar heeft dit mee te maken? Zijn de medewerkers wel op de hoogte? Zo ja, begrijpen ze het wel? En als ze het begrijpen voeren ze het dan wel uit? Waarom wel of waarom niet? Stelt de zorginstelling de medewerker wel in de gelegenheid om de instructies en protocollen na te leven? En is het antwoord op voorgaande vragen voor alle medewerkers hetzelfde? Reguliere 'Awareness' programma's, zoals de e-learnings van het ZEKER programma van de NVZ geven antwoord op slechts een deel van bovenstaande vragen, omdat deze programma's ervan uit gaan dat de kennis van medewerkers niet op het gewenste niveau is.

Vaak ontbreekt het niet aan kennis

Hoewel kennis belangrijk is, bestaat er een kloof tussen awareness en gedrag: wéten wat je moet doen is niet hetzelfde als je daadwerkelijk zo gedragen! Voor effectieve bescherming tegen menselijk fouten is bewustwording weliswaar belangrijk, maar niet het einddoel. Dat verklaart ook het geringe effect van traditionele awarenesscampagnes. Gedrag wordt namelijk ook gestuurd door andere zaken, zoals motivatie (iemand moet het ook willen). Omdat de vraag naar de stap voorbij awareness bij zorginstellingen groeiende is, ontwikkelde Secura het SAFE programma, dat is gericht op het overbruggen van de kloof tussen awareness en gedrag. **Het doel van SAFE is dus ook het bereiken van daadwerkelijke gedragsverandering.** En dat doen we uiteraard met psychologen (gedragswetenschappers) én informatiebeveiligingsspecialisten.

Wat houdt de medewerkers van uw zorginstelling nog tegen?

Een logische stap naar gedragsverandering die vaak wordt overgeslagen, bestaat uit het **in kaart brengen van de barrières voor gedrag:** wat weerhoudt mensen ervan zich op een bepaalde manier te gedragen? Door blind te sturen op het verhogen van bewustzijn, wordt de aanname gedaan dat mensen het niet wéten. Echter, vaak weten mensen heus wel wat ze eigenlijk zouden moeten doen, maar worden ze tegengehouden door iets anders. Misschien wel het verkeerde voorbeeldgedrag? Of vindt men het niet belangrijk genoeg? Staat er misschien iets technisch in de weg? In plaats van te redeneren vanuit oplossingen ("we doen een training, we willen een escaperoom"), start SAFE met het begrijpen van het huidige gedrag. Want zodra duidelijk is welke barrière daar nog in de weg staat, kan ook gerichter worden ondersteund in het wegnemen van die barrière.

Betrek de doelgroepen binnen de zorginstelling

Succesvolle gedragsverandering kan niet zonder betrokkenheid van de medewerkers om wie het gaat. Daarom is het belangrijk om **vanaf het begin de doelgroep te betrekken.** Bij het opstellen van de belangrijkste doelen, maar ook bij het onderzoeken van de barrières. Een veelgemaakte menselijke fout is dat we vervallen in aannames; we denken al gauw te weten hoe anderen denken en zullen handelen. Vaak blijkt de praktijk weerbarstiger. In de SAFE methodiek worden vertegenwoordigers van de doelgroep betrokken vanaf het eerste moment. Zo is het een programma mèt en voor hen.

SAFE onderscheidt zich omdat het is:

- **ontworpen door psychologen en informatiebeveiligingsspecialisten**
- **gericht op veilig gedrag als einddoel** (dus het gaat verder dan bewustwording)
- **gefocust op álle facetten van gedrag:** naast kennis ook motivatie en gelegenheid (cultuur)
- **afgestemd op de aard en risico's van uw zorginstelling** (dus geen 'one size fits all')
- **ontwikkeld o.b.v. psychologische technieken** voor gedragsverandering zoals stimuleren en faciliteren (dus het gaat verder dan opleiden)
- **gebaseerd op herhaling** (dus geen 'eenmalige check-in-box-activiteit')

Secura
A BUREAU VERITAS COMPANY

Waarom SAFE?

Met SAFE investeert u in het **creëren van bewustzijn en het bereiken van gedragsverandering** die is afgestemd op de behoeften van de medewerkers in uw organisatie. Het resultaat is dat het volwassenheidsniveau van informatiebeveiliging toeneemt, waardoor de **organisatie beter bestand is tegen aanvallen van buitenaf**. Door te kiezen voor het SAFE programma is het bovendien zowel intern als extern meetbaar duidelijk dat privacy en informatiebeveiliging voor u van groot belang zijn.

Door SAFE zijn uw **medewerkers aantoonbaar bewuster en competenter** om zich gepast te gedragen bij pogingen van kwaadwillende partijen om toegang te krijgen tot systemen en informatie. Door SAFE verkleinen uw medewerkers de kans op incidenten met een grote impact en daarmee ook de bijbehorende hoge kosten en het risico op reputatieschade. Kortom:

Better SAFE than sorry!

Interesse?

Wilt u meer weten over onze services?

Neem vandaag nog contact met ons op!

088 888 3100

safe@secura.com

secura.com

Volg ons via: