Safety first?

Met de groei in e-commerce wordt aandacht voor veilig en betrouwbaar klantcontact steeds belangrijker. Met het toekennen van de NCCA Innovatie Award aan Teleperformance is het onderwerp fraudepreventie nu definitief op de klantcontactagenda gezet. De organisatie schenkt de meeste aandacht aan de interne organisatie van iedere eigen vestiging.

Met internet als belangrijkste driver hebben ondernemingen hun sales- en serviceprocessen de afgelopen tien jaar geleidelijk, maar ingrijpend zien veranderen. Online zaken doen – oriënteren, vergelijken, bestellen, betalen en ondersteuning krijgen – is inmiddels gemeengoed. Thuis, onderweg of op het werk zijn we als consument tamelijk onbezorgd in de weer met onze laptops, tablets en smartphones. Het aantal online transacties neemt gestaag toe en bedrijven besteden daarbij veel aandacht aan het verbeteren van de customer experience. Zaken als veiligheid, privacybescherming en fraudebestrijding horen daar onderdeel van uit te maken. Onderwerpen als informatiebeveiliging en fraudepreventie in klantcontact zijn helaas niet populair. Met onze NCCA-case wilden wij het onderwerp security op de agenda van contactcenters zien te krijgen. Door de case over onze aanpak van fraudepreventie te belonen met de NCCA Innovatie Award heeft de NCCA-jury niet alleen haar nek uitgestoken, maar ook een duidelijk statement gemaakt. Het omgaan met risico's begint namelijk bij het benoemen en erkennen van die risico's.

Bedreigingen van buitenaf of binnenuit?

Het imago van online retailers wordt steeds sterker bepaald door de mate waarin je voor consumenten een 'betrouwbare partner' bent. In de krant of online kunnen we steeds vaker lezen over DDoS-aanvallen die websites of zelfs complete bedrijven lamleggen.
Gelukkig komt informatiebeveiliging steeds hoger op de agenda van de boardroom te staan. Consumenten en hun belangenorganisaties dwingen aandacht voor informatiebeveiliging ook af met certificering en keurmerken, waarmee je als bedrijf kunt aantonen dat je maatregelen hebt getroffen om risico's in te perken. Vrijwel alle bedrijven hanteren algemeen aanvaardde normen voor informatiebeveiliging zoals ISO 27001* of PCI DSS.
Bij het nemen van maatregelen besteden bedrijven echter de meeste aandacht aan cybercrime van buitenaf. De grootste veiligheidsrisico's liggen echter op het vlak van misbruik of diefstal van data, frauduleuze transacties en bestellingen en een ongecontroleerd gebruik van externe systemen zoals internet, aldus onderzoekers van het programma Shopping2020: "Onze verwachting is dat in het jaar 2020 het winkelproces niet dramatisch zal veranderen, maar dat voornamelijk verschuiving plaats zal vinden ten aanzien van het landschap van online shopping (zowel technologisch, qua globaliteit en schaalgrootte). Door deze verschuiving zal afhankelijkheid van ketenpartners en de mogelijke schaalgrootte van onveiligheid en fraude toenemen. Technologische innovaties kunnen hierbij zowel faciliterend als bedreigend zijn." Ter illustratie: circa 1 op de 20 consumenten heeft wel eens te maken gehad met koop- en verkoopfraude, aldus onderzoeksresultaten van het programma Shopping2020.

BEDREIGINGEN VAN BUITENAF OF BINNENUIT?

Wat zijn de risico's in e-commerce?

Van bedrijven die op grote schaal te maken hebben met klantcontact en financiële transacties, mag je verwachten dat ze alle risico's goed inschatten en er ook passende maatregelen bij nemen. Daarbij is het van belang in te zien dat informatiebeveiliging geen exclusief IT-feestje is, maar iedereen aan gaat: consumenten, e-tailers, dienstverleners van uitbestedende bedrijven en het personeel.
In de klantcontactsector is het bewustzijn over de interne (fraude)risico's echter nog gering. Erkennen dat fraude van binnenuit bestaat, betekent voor menig contactcentermanager bovendien dat hij of zij zelf aan de bak moet met het creëren van veiligheid en transparantie – waar moet je beginnen? In ons land zijn we snel geneigd te denken dat als je een aantal voorzorgsmaatregelen hebt genomen om processen goed te beveiligen en af te schermen, daarmee alle risico's zijn uitgebannen. Risico's kun je niet uitsluiten; je kunt ze wel (steeds opnieuw) in kaart brengen en vooraf

Tekst: Leendert van Duijn en Hans Reuver, respectievelijk Chief Information Officer Benelux en Chief Commercial Officer Benelux en VP Business Development Eastern Europe van Teleperformance

mitigerende maatregelen bepalen. Wereldwijd wordt de top tien van fraudeoorzaken in e-commerce aangevoerd door misbruik van garantieregelingen. Het is dus niet alleen een klant die de zwakke plekken van jouw interne processen kan opzoeken. Net als in ieder contactcenter kunnen ook onze medewerkers fraude plegen in de systemen en processen van onze klanten. Medewerkers kunnen bijvoorbeeld garantiecertificaten ontvreemden en vervolgens producten naar zichzelf of anderen toesturen op basis van garantiebewijzen. Op nummer 2 staat het verkrijgen van toegang tot interne bestanden van de opdrachtgever via webadressen; op nummer 3 van het lijstje van frauderisico's staat het doen van aankopen met behulp van bestaande klantdata zoals creditcardgegevens.

Hoe gaan bedrijven om met risico's?

Wanneer klantcontact wordt uitbesteed, gaan (klant)data 'op reis' en ontstaan nieuwe touchpoints waarbij de veiligheidsrisico's in kaart moeten worden gebracht. Hiervoor zijn veel richtlijnen, regels en (wettelijke) voorschriften ontwikkeld, zoals ISO 27001, PCI DSS, HIPAA en Safe Harbour. Ook het personeel moet aan allerlei eisen voldoen: denk aan gecertificeerde auditors en securityanalisten of aan gedragscodes voor medewerkers. Wij zien dat security vaak en op diverse manieren in outsourcingcontracten aan de orde komt. Maar de verschillen zijn groot: sommige bedrijven stellen zeer uitgebreide en doordachte eisen, anderen willen dat er 'iets' geregeld wordt. Uitbestedende bedrijven beschikken zelden over specifieke programma's en systemen die de frauderisico's structureel in kaart brengen en beperken. Vaak ontbreekt ook een audit- en monitoringcultuur, met name op het vlak van fraudepreventie. Als het gaat om fraudepreventie wordt er meestal voor gekozen om procedures zo te ontwerpen dat de agent niet te veel beslissingsbevoegheden heeft. Dat gaat niet alleen ten koste van de mogelijkheden om optimale service te verlenen; je ziet met die keuze ook over het hoofd dat aandacht voor security meer omvat dan het opheffen van de meest in het oog springende risico's.

Securitybeleid van Teleperformance

Omdat de toegevoegde waarde van een compleet securitybeleid op voorhand vaak lastig hard te maken is, vergt het enige moed om op het vlak van veiligheid en fraude de juiste analyses te durven maken. Je moet conclusies durven trekken over mensen, middelen en systemen en vervolgens passende maatregelen nemen. Veiligheid en zaken als one-stop-service of empowered agents hoeven elkaar echter niet uit te sluiten, zo is onze ervaring.
Door de grote volumes aan transacties die bij veel van onze klantcontactprocessen horen, is Teleperformance behoorlijk 'dataintensief'. We nemen dus ook relatief veel maatregelen. Dat begint bij onze eigen internationale community: wereldwijd zijn er bijna 200 professionals betrokken bij security. Dat die kennis binnen onze wereldwijde organisatie gebundeld wordt, is voor iedereen binnen onze organisatie prettig; het onderstreept dat security geen bijkomstigheid is, maar een wezenlijk onderdeel is van onze bedrijfsvoering waarbij iedereen van elkaar kan leren. Deze expertgroep drijft het securitybeleid aan: er wordt doorlopend gekeken

HANS REUVER

LEENDERT VAN DUIJN

naar standaarden en ontwikkelingen op het gebied van encryptie en compliancysystemen.
Binnen Teleperformance lichten we onze processen en die van onze klanten steeds opnieuw en nauwgezet door aan de hand van ons Fraud Risk Assessment. Dat Fraud Risk Assessment vormt een belangrijk onderdeel van ons securityprogramma, waarbij mogelijke frauderisico's worden geïdentificeerd en vervolgens ingeperkt door het nemen van gerichte maatregelen. Het securityprogramma van Teleperformance heeft wereldwijde erkenning gekregen van Secure Computing Magazine (2012: best security team) en van Frost & Sullivan (2008, 2012: best security practice).

Fraudepreventie is mensenwerk

De meeste aandacht voor security gaat echter uit naar de interne organisatie van iedere Teleperformance-vestiging. Wij controleren en monitoren onze processen intensief en gestructureerd aan de hand van meer dan 500 meetpunten. We houden hiervoor verschillende systemen in de lucht en ook het uitvoeren van audits kost tijd en geld. Ons securityframework is meer dan een systeem; veel onderdelen zijn gericht op het sturen en controleren van dagelijks gedrag. Onze medewerkers weten bijvoorbeeld dat ze niet overal naar binnen kunnen en mogen. Ze hebben alleen toegang tot hun eigen vloer en hun eigen projectsystemen. Ze weten ook dat deze regels gecontroleerd worden, bijvoorbeeld door de inzet van camera's, en begrijpen dat ze hun smartphone moeten inleveren voordat ze aan het werk gaan. Supervisors krijgen bij ons op hun kop als ze controles overslaan of niet goed uitvoeren. Elkaar op gewenst en ongewenst gedrag aanspreken is één van de belangrijkste onderdelen van security. Binnen Teleperformance worden alle medewerkers in trainingen en via posters actief aangemoedigd om (los van de auditors die alle processen regelmatig en gestructureerd doorlichten) zelf findings te rapporteren. Dat kan binnen Telepeformance op een veilige manier – dus met respect voor de 'melder'.
Doordat iedereen binnen Teleperformance weet dat veiligheid en fraudepreventie hoog op de agenda staan, zijn dit 'normale onderwerpen' binnen onze organisatie. Iedereen is het er over eens dat het naief is om af te wachten totdat het misgaat. Juist deze openheid brengt mensen minder in de verleiding en draagt bij aan het besef dat fraude uiteindelijk voor iedereen schade oplevert. Het is het vertrekpunt voor een duidelijke cultuur met een heldere set aan normen en waarden.