Nõuded e-Kaubanduse lahenduse vahendusel kaarte aktsepteerivale Teenindajale

Interneti keskkond on väga mugav ja kiire e-Tehingute tegemiseks. Kuna tegemist on suhteliselt anonüümse keskkonnaga ja kaarti füüsiliselt ei esitata, kätkeb see ohtu e-Tehingute turvalisusele. Selleks, et nii Teenindaja kui ka kaardivaldaja (edaspidi Klient) e-Tehingust kasu saavad, on kahju vältimiseks väga oluline jälgida teatud nõudeid.

1. Üldnõuded kodulehele

1.1. Kliendiandmete küsimisel on soovitav kasutada turvatud ühendust (SSL – Secure Socets Layer). Turvalise ühendamise kasutamisel peab selle sertifikaat olema väljastatud tunnustatud sertifikaadi väljastaja poolt (mitte ise genereeritud).
Kaardiandmete edastamine toimub Nets Estonia AS-i serveri kaudu ja sellisel juhul kasutatakse Teenindaja ja Nets Estonia AS-i vahel alati turvalist ühendust.
Andmeedastuse turvalisuse tagamiseks kasutatakse Teenindaja ja E-Commerce Payment Gateway interneti liikluse vahel 128-bitist krüpteeringut (SSL- Secure Socket Layer turvaprotokolli) ning andmed, mis liiguvad Teenindaja ja E-Commerce Payment Gateway vahel, allkirjastatakse elektrooniliselt, mis kokkuvõttes välistab selle, et kõrvalised isikud saaksid neid andmeid pealt kuulata või muuta.
Teenindajal on juurdepääs kaarditehingute aruandlusele, kuid puudub juurdepääs täielikule kaardinumbrile.
1.2. Maksekaarte aktsepteeriv internetikaubamaja peab sisaldama:
1.2.1. Privaatsuspoliitika/andmete turvalisus.
1.2.1.1. Viide, et kaardiandmete küsimisel kasutatakse SSLi, MasterCard SecureCode, Verified by Visa.
1.2.1.2. Kliendi poolt ettevõttele esitatud personaalsete andmete kasutamine/mitte kasutamine.
1.2.1.3. Info selle kohta, et Teenindaja sisestatud kaardi andmeid ei näe, kaarditehingu tegemiseks suunatakse Klient Nets Estonia AS-i turvalisse keskkonda. Maksmise hetkel toimub Kliendi kaardiandmete sisestus Kliendi poolt Nets Estonia AS-i serveris paiknevasse andmebaasi ning andmeid säilitatakse samuti Nets Estonia AS-is paiknevas serveris.
1.2.2. Teenindaja täielik ärinimi.
1.2.3. Asukoha riik ja postiaadress.
1.2.4. Kaupade/teenuste täielik nimekiri, hinnakiri. Kauba/teenuse võimalikult täpne kirjeldus, võimaldamaks Kliendil saada piisav ülevaade pakutavast, pöörates erilist tähelepanu sellele, kas need on legaalsed või kasutatavad ka väljaspool Teenindaja asukohariiki.
1.2.5. Aktsepteeritavate kaartide (Visa/Mastercard) logod ja kaubamärgid (SecureCode, VbV). Logod ja kaubamärgid peavad olema esitatud samades mõõtmetes ja ühtegi kaubamärki ei tohi teisele eelistada.
1.3. Kaarditehingu sooritamise valuuta. Tehingute teostamisel eurodes on soovitav ära näidata ka euro ja teiste tuntumate valuutade (sõltuvalt sihtturust) ristkursid. Kurssidejuures peaks olema viide nende allikale ja uuendamise sagedus.
1.4. Kauba üleandmise/saatmise kord, lisanduvad postikulud ja nende määramine ja Kliendi teavitamine. Piirangud kaupade saatmisel (Eestist välja ei saadeta, suuregabariidilisi kaupu saadetakse ainult mingi kindla teenuse kaudu, kaupu on võimalik saata ainult teatud riikidesse jms.)
1.5. Tellimuse lõplik maksumus koos postikuludega, viide võimalikele lisamaksetele sh. võimalike tollide ja käibemaksude tasumise kohustus Tellija poolt.
1.6. Kliendi teavitamine taganemisõigusest. Kauba tagastamise kord, ajapiirid. Kauba garantiitingimused ja ümbervahetamise kord.
1.7. Tagasiside Kliendile tellimuse kinnitusega.
1.8. Kliendi teavitamine võimalikest tõrgetest kauba käitlemisel.
1.9. Klienditeeninduse telefon ja e-posti aadress ning tagasiside andmise kord. Telefoni puhul tööaeg kohaliku aja järgi ja ajavööndi tähis (GMT+2), e-posti aadressi korral e-kirjadele vastamise kiirus. Kasutatavad keeled.
1.10. Teenindaja on vastutav kodulehel oleva info ja pakkumiste õigsuse eest. Oluliste muutuste korral pakutava kauba/teenuse olemuses või sortimendis on Teenindaja kohustatud sellest Panka eelnevalt informeerima.

2. Kviitungile esitatavad nõuded

2.1. Peale maksetehingule positiivse vastuse saatmist peab Kliendile kuvama kokkuvõtte tellimusest. Kokkuvõte peab olema vormis, mis võimaldab seda lihtsasti välja printida või salvestada. Soovitav oleks sama kokkuvõte saata ka Kliendile e-postiga kui aadress on teada.
2.2. Kviitung peab sisaldama järgmisi andmeid
2.2.1. Nõuded vastavalt Eestis kehtivatele seadustele.
2.2.2. Info, et Tehingu eest on tasutud kaardiga.
2.2.3. Tehingu unikaalne identifitseerimise number, mis aitab nii Kliendil kui ka Teenindajal tellimuse üle arvestust pidada ning võimalikke probleeme lahendada.
2.2.4. Interneti kaubamaja veebiaadress.
2.2.5. Kviitungi lõpus peab olema teade, et Klient prindiks või salvestaks kviitungi säilitamiseks.

3. Pettuse ennetamine
Internetikaubanduse iseloomust tulenevalt, kus Teenindaja ei näe kaarti ega Klienti, on internetikaubamajade pettuste hulk suurem kui tavalistel müügikohtadel.
3.1. Teenindaja peab väga tähelepanelikult suhtuma kõikidesse e-Tehingutesse, sest ta vastutab kõikide e-Tehingute eest, mis on tema veebilehel tehtud.
3.2. Võimalike pettuste ennetamiseks tuleb:
3.2.1. Töötajaid koolitada ja riskidest teavitada. Enne tellimuse täitmist ja kauba väljasaatmist peab tellimuse andmed üle vaatama.
3.2.2. Tähelepanu pöörata ebatavalisele ostutegevusele. Kahtluse korral võtta ühendust Pangaga.
3.2.3. Võrrelda andmeid varem toimunud pettustega.
3.2.4. Jälgida aadresse, kuhu kaubad toimetatakse. Kahtlust peaks äratama samale aadressile erinevate kaartidega või Klientide nimedega tehtud tellimused.
3.2.5. Jälgida ebatavaliselt suuri ostusummasid. Kaubamajale ebatavaliselt suurtes summades tehtud tellimused peaksid olema erilise tähelepanu all.
3.2.6. Jälgida tellijate IP aadresse, tellimusi samalt IP-lt erinevate kaartidega või erinevatele saajatele.
3.2.7. Pettuse kahtluse korral peab Teenindaja koheselt kontakteeruma Pangaga. Pettuse kahtluse korral jääb Pangal õigus uurimise ajaks e-Tehingu töötlemine peatada või e-Tehing tühistada. Kusjuures Pank teavitab Teenindajat e-Tehingu kontrollist ja Teenindaja ei tohi kaupa välja saata enne vastava uurimise lõppemist

4. e-Tehingu tühistamine
4.1. e-Tehingu ainuvõimalikuks tühistuse viisiks on avalduse saatmine Panka koos e-Tehingu andmetega. Avalduses peab olema ära toodud ka tühistamise põhjus. Muid kanaleid raha tagastamiseks kasutada ei tohi.
4.2. Tellijat, kes on kauba tagastanud ja soovib e-Tehingu summa tagastamist, tuleb teavitada kui tühistamine on teostatud.

Nõuded Teenindajale Kaardivaldaja andmete turvalisuse tagamiseks

1. Teenindaja peab tagama oma arvutisüsteemide kaitsmise volitamata ligipääsu eest, installeerides ja hoides korras tulemüüri konfiguratsioone ja tehnilisi vahendeid, mis kontrollivad ühendusi ettevõtte arvutivõrku väljastpoolt ja tundlikumatesse piirkondadesse ettevõtte sisevõrgus.
2. Teenindaja ei tohi kasutusele võtta arvutisüsteemi(de) tootja(te) poolt määratud vaikeparoole ja muid turvalisuse parameetreid.
3. Teenindaja peab tagama oma süsteemides talletatud andmete kaitse. Säilitavate andmete hulga ja alleshoidmise aja määramisel tuleb piirduda minimaalselt äriks vajalike andmetega.
4. Teenindaja peab kasutama krüpteerimist kaardivaldaja (edaspidi Klient) tundlike andmete edastamisel üle avaliku arvutivõrgu.
5. Teenindaja peab kasutama ja regulaarselt uuendama viirusetõrje tarkvara.
6. Teenindaja peab arendama, hoidma töökorras ja regulaarselt uuendama kasutatavaid turvasüsteeme ja rakendusi.
7. Teenindajal tuleb kehtestada meetmed, millega tagatakse ligipääs ainult nendele andmetele, mida on tööks vaja ja ainult neile, kellel on seda tööks vaja
8. Kindlustamaks volitatud kasutajate poolt arvutisüsteemides tehtud toimingute jälgimine, peab Teenindaja määrama igale arvutikasutajale unikaalse kasutajatunnuse ning kaitsma seda saladusega, mida teab või saab kasutada ainult nimetatud kasutaja.
9. Teenindaja peab piirama füüsilist ligipääsu kaardivaldaja (Kliendi) andmetele
10. Teenindaja kohustuseks on jälgida kõiki ligipääse arvutivõrgu ressurssidele ja Kaardivaldaja (Kliendi) andmetele. Äärmiselt vajalik on süsteemi loodud logide abil olla suutlik jälgida süsteemis kasutaja tegevusi.
11. Teenindaja peab regulaarselt testima turvasüsteeme ja protsesse, kohandatud tarkvara jne, et oleks tagatud turvalisuse säilimine.
12. Teenindaja peab kehtestama sisepoliitika, mis tegeleb informatsiooni turvalisusega töötajate ja lepingupartnerite jaoks. Tugev turvalisuse poliitika tagab turvalise olukorra kogu ettevõtte jaoks ja laseb töötajatel teada, mis neilt oodatakse. Kõik töötajad peavad olema teadlikud tundlike andmete töötlemise korrast ja nende kohustusest andmeid kaitsta.
Täiendavat infot saate www.danskebank.ee või helistades infotelefonile 6 800 800.