Kaardiandmete turvalisus

PCI Data Security Standard (PCI DSS)
PCI standard on rahvusvaheliste kaardiorganistasioonide poolt väljatöötatud standard, et reguleerida kaardiandmete käitlemist ja hoidmist vastavalt andmekaitsele. Nõuded on kohustuslikud nii kaupmeestele, protsessoritele, pankadele kui ka kõikidele maksesüsteemi osadele (n. võrgud, serverid, kassasüsteemid, terminalid)
Täpsem info pangast ning lugeda saab ka
https://www.pcisecuritystandards.org

Account data compromise juhtum ehk kaardiandmete leke

Kaardiandmete leke võib leida aset tänu volitamata isikute lubamatule juurdepääsule kaardi andmetele. Sensitiivsed andmed on kaardinumber, kehtivusaeg, CVC1, CVC2, kaardiomaniku nimi, magnetriba info, pin kood, kiibi info, isikukood, e-maili aadress, kodune aadress, sünniaeg jne.

Kaitske arvutit ja selle tarkvara

Tähelepanelik tasub olla kui märkate järgmist:
- Avuti viirusetõrje poolt on tekitatud alert võimalikust ohust arvutile
- Arvuti tulemüüri alert
- Kui arvuti poolt on tuvastatud tundmatu kasutaja
- Kui on tuvastatud volitamata isiku juurdepääs arvutile või volitamata käsud
- Tuvastatud kahtlased failid süsteemis
- Vasturääkiv info arvuti auditi logides
- Kui arvuti on tuvastanud mõne kahtlase nuhktarkvara nagu - key logger, memory scraper jne.
- Arvutisüsteemi kokkujooksmine teadmata põhjustel
- Arvuti logi näitab ebatavalist tööajavälist sisselogimist
- Seletamatuid failinimede muutmisi, lisamisi, katseid faile muuta või kustutatada
- Tundamatud võrguühendused IP addressidega, mis ei ole kaupmehe tööks vajalikud

Kelmid võivad kasutada järgmisi võtteid andmete kättesaamiseks:

Phishing ehk andmepüük/õngitsemine
On moodus arvutikasutajatelt välja petta isiklikku või finantsalast teavet petturlusega seotud meilisõnumit avades (tavaliselt manusena kaasa lisatud faili avades või meilis oleval lingil klikates, mis suunab kasutaja osavalt võltsitud veebisaidile). Tavaline võrgus tegutsev andmepüüki kasutav kelm alustab meilisõnumi saatmisega, mis sarnaneb usaldatud allikast (pank, krediitkaardiettevõte või lugupeetud veebikaubitseja) pärineva ametliku teatega. Meilisõnumis suunatakse adressaadid

petturlusega seotud veebisaidile, kus kasutajatel palutakse sisestada isiklikku teavet nagu panga kontonumber või –paroole, isikukoode, telefoninumbreid, elukoha aadressi jne. Seda teavet kasutatakse tavaliselt identiteedi varguseks.

Andmete väljapetmiseks või kasutaja arvuti viirustega nakatamiseks kasutatakse vahel ka õngitsuslehte (inglise keeles pharming).

Tasub meeles pidada, et pank ei küsi kunagi maili teel kaardinumbrit, pin koodi või muud isiklikku teavet. Vajalik info on pangal juba olemas.

Social engineering ehk suhtlusosavus, manipuleerimisrünne
Manipuleerimisrünne ehk social engineering kasutab ära inimlikke nõrkusi selleks, et pääseda ligi kaitstud informatsioonile või süsteemile. Niisugust tüüpi ründed on väga levinud, kuna inimlike nõrkuste ärakasutamine on lihtsam kui süsteemi sisse tungimine. Näiteks kas otsene manipuleerimine või telefoni teel info hankimine.

Jällegi tasub mõelda, kellele ja millist infot väljastada. Lisaks tasub kaaluda, kas telefoni teel tehtud tegelikkusest palju soodsam pakkumine on realistlik või mitte.

Hacking ehk süsteemi häkkimine, sissemurdmine
Autoriseerimata isiku süsteemi tungimine nagu näiteks SQL rünnak, pahavara süsteemi sokutamine, administraatori õiguste väärkasutamine. Ohus on kaugjuurdepääsu rakendused, mis nõuavad vaid ühe teguriga autentimist. Samuti ebaturvalised traadita võrgud ja traadita krüptimisprotokollid.

MALWARE ehk- pahavara
Tarvara või pahatahtlik kood, mida kasutatakse süsteemi tungimiseks, andmete saamiseks – sealhulgas ka salasõna hankimiseks.

Kuna suur enamus toimunud infovargustest saab võimalikuks tänu puuduvale või nõrgale turvalisusele nagu näiteks teenusepakkuja vaikimise seaded, juurdepääsud, siis toome siinkohal mõned soovitused turvalisuse tagamiseks.

Soovitused interneti kaupmeestele:

- teadaolevate kuritahtlike Internet Protocol (IP) aadresside blokeerimine
- süsteemi teadlik monitooring, identifitseerimaks süsteemi administraatori nõrka salasõna
- kasutaja salasõna regulaarse muutmise nõue
- erilist tähelepanu pöörata kasutajate käitumisele, kellel on suuremad õigused andmetele ligipääsemiseks, tugevdades nende kasutajate parooli muutmise poliitikat
- sulgeda kõik mittevajalikud üldised kontod/kasutajad
- pidevalt täiendada/uuendada süsteemi turvalisust

- pidevalt jälgida kõiki kaugjuurdepääsu taotlusi ja eemaldada mittevajalikud aplikatsioonid
- kaugjuurdepääsu taotluse korral alati nõuda kahefaktorilist autentimist
- süsteemi tulemüüri reeglite pideva jälgimine
- analüüsida veebirakenduste haavatavust
- anti-virus programmi regulaarne täiendamine
- süsteemi alertide järjepidev monitoorimine ja probleemi korral eskaleerimiprotseduuride loomine, et info ikka õige inimeseni jõuaks

Turvanõuded terminalidele

Skimming ehk kaardiandmete kopeerimine
Kaardil olevate elektroonsete andmete (magnetribal oleva info) kopeerimine mingile andmekandjale hilisema pettuse teostamise eesmärgil. Kriminaalid võivad üritada panna elektroonilist andmete lugejat ehk skimmerit terminali ja see võib olla väga väikene ning jääda kaupmehele märkamatuks. Seepärast on oluline, et müüja kontrolliks igapäevarutiini käigus üle ka terminali, et see oleks alles ja et ei oleks muukimise jälgi.

Terminali vahetus või parandamine

Alati kui tullakse kauplusesse terminali parandama või välja vahetama, peab müüja küsima tehnikult töötõendit veendumaks, et tegu on terminali vahetamiseks volitatud isiku või koostööpartneriga.

NB! ***Kui kaupmees avastab terminalis muukimise jälgi või on terminal varastatud, tuleb sellest koheselt teavitada panka ja politseid. Muukimisjälgede või lisaseadme olemasolu korral terminali mitte puutuda. Sama nõue kehtib ka internetikaupmeeste puhul, kui arvutis avastatakse pahavara. Korduvad kaardiomanike pöördumised kaupmehe poole seoses valetehingutega võivad olla indikaatoriks, et andmed on lekkinud.***