PCI DSS

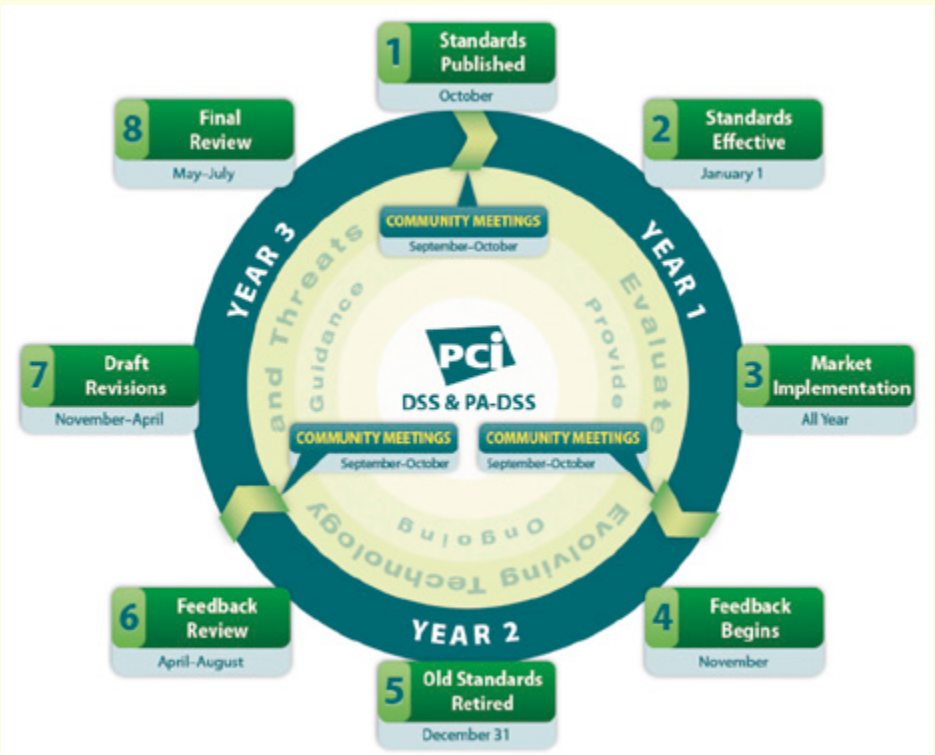
Nova verzija kartične

Kako bi se svi trgovci, banke, pružatelji kartičnih usluga i sve ostale zainteresirane strane bolje pripremili na novosti koje donosi sljedeća verzija standarda PCI DSS, vijeće mudraca izdalo je smjernice o tome što nas sve očekuje. Donosimo kratak pregled promjena

Dalibor Uremović

Nekako potiho izašle su smjernice o promjenama koje donose nove verzije standarda PCI DSS i PA DSS. Premda se po izlasku standarda traži od svih zainteresiranih strana koje rade s kartičnim podacima da odmah krenu s usklađivanjem, imat ćemo vremena za prilagodbu do kraja 2014. godine. Za one koji su već debelo u aktivnostima usklađivanja (i pokušajima da ostanu u statusu usklađenosti), ovo je dovoljno vremena da se stvari dodatno ispeglaju i doda par novih kontrola koje nova verzija donosi.

Nova verzija (3.0) slijedi uobičajeni trogodišnji ciklus ažuriranja standarda koje si je vijeće (PCI SSC) nametnulo nakon podrobnih analiza primjene prethodnog standarda, osluškivanja želja i potreba korisnika standarda te praćenja tehnoloških trendova. Ovaj se put saznanja na kojima je vijeće temeljilo promjene u standardu odnose na nedostatak svijesti o informacijskoj sigurnosti, slabo upravljanje zaporkama, slabo upravljanje zaštitom od zlćudnog koda, novim prijetnjama iz okoline te ranjivostima vezanim uz korištenje novih tehnologija. Ipak, najviše je zamjerki bilo u revizorskom pogledu na zahtjeve standarda, pri čemu su se tvrtke oslanjale na *checkbox* pristup usklađivanju, a manje na stvarnu implementaciju sigurnosnih kontrola i njihovo ažuriranje u skladu sa svakodnevnim poslovanjem i promjenama. Ono što je jasno jest da i dalje u standardu PCI DSS ostaje 12 glavnih zahtjeva uz par novih podzahtjeva.



Životni ciklus izdanja novih verzija standarda PCI DSS i PA DSS

Edukacija i "awareness"

Kao jedan od ključnih razloga daljnjeg povećanja broja napada na kartične podatke navodi se nedostatak edukacije zaposlenih, kako za poslove koje obavljaju tako i uže za područje informacijske sigurnosti. U nas često prevedeno kao osvješćivanje o informacijskoj sigurnosti (*security awareness*), provodi se rijetko, nesistematično te uz zastarjele materijale i tehnološka pomagala. Kao revizor, ovu tvrdnju mogu potvrditi jer se u mnogim tvrtkama edukaciji o sigurnosti daje malo pažnje. I dalje prevladava mišljenje da je za sigurnost isključivo zadužen CISO

sigurnosti

(engleski termin za voditelja informacijske sigurnosti), a ostali samo rade svoj posao te se na njih ova tema ne primjenjuje. I dok se IT stručnjaci donekle i osposobljavaju u predmetnoj temi, ostali su vrlo rijetko uključeni u razne oblike sigurnosnog osvješćivanja koje danas pruža moderna tehnologija. Nova verzija standarda daje smjernice o uključivanju vanjskih partnera u skrb oko informacijske sigurnosti te npr. raspoređuje 12. poglavlje (politika sigurnosti) na ostala poglavlja. Tako ćemo odsad imati više politika (pravilnika, procedura) za pojedina područja standarda PCI DSS.

Nove tehnologije

U tri se godine svašta može promijeniti, pa tako i tehnologije koje su bile u začetku mogu postati *mainstream*. PCI SSC vijeće posebnu je pažnju posvetilo sada već standardnim tehnologijama i načinu poslovanja poput e-poslovanja, korištenja raznih varijacija mobilnih platformi, oblačnog računalstva, *point-to-point* enkripcije te tzv. tokenizacije. Dio kontrola detaljiziran je u poglavljima samog standarda, a dio je već izdan ili će biti izdan u zasebnim dokumentima koji pobliže opisuju predmetna područja (v. okvir sa strane).

Izmjene u standardima odnose se na potrebu izrade detaljnog dijagrama toka kartičnih podataka (1. poglavlje), izrade i održavanja registra informacijske imovine za PCI DSS opseg (2. poglavlje), zahtjeve za sigurnošću POS terminala, čitača kartica, tokena i certifikata (8. i 9. poglavlje) te detaljnije zahtjeve vezane uz penetracijska testiranja (11. poglavlje). Od općih zahtjeva valja posebno izdvojiti smjernice o implementiranju sigurnosnih praksi u svakodnevno poslovanje kako bi se postigla kontinuirana usklađenost s PCI DSS zahtjevima, a ne kao dosad u trenutku revizije, najčešće putem neke *checkliste*. Što se tiče standarda PA DSS, u 5. poglavlju detaljnije se propisuju kontrole tijekom razvoja proizvoda (povremena sigurnosna testiranja, metode verzioniranja, upotreba *threat-modelling* tehnika i sl.) te držanje ažurne OWASP ili neke druge liste najčešćih prijetnji aplikacijama. U ostalim poglavljima radi se samo o sitnijim promjenama (npr. važnost treninga o uporabi aplikacija, puštanje *release notesa* prije implementacije i sl.).

Fleksibilnost i podjela odgovornosti

U modernim sustavima koji koriste nove tehnologije i u kojima postoji mnoštvo pristupnih točaka prema kartičnim podacima nemoguće je izbjeći problem definiranja odgovornosti za zaštitu kartičnih podataka. Nova verzija pomaže organizacijama da lakše shvate koje su njihove obaveze te kako da podijele odgovornost među raznim pružateljima usluga i vanjskih partnera. Zgodan dodatak vezan uz ovaj problem jest i poseban dokument PCI DSS Cloud Computing, koji već postoji te daje matricu odgovornosti primjenjivu za većinu organizacija.

Osim podjele odgovornosti, za niz postojećih zahtjeva - poput upravljanja zaporkama, autentifikacijom i zlođudnim kodom - daje se više slobode oko odlučivanja koje kontrole primijeniti, ali se zato pojačavaju zahtjevi nad načinom testiranja implementacije onih kontrola na koje se organizacije odluče.

Nema sumnje da nove verzije standarda PCI DSS i PA DSS unose niz novih stvari, i to prvenstveno kao odgovor na zahtjeve korisnika standarda, nakon podrobne analize novih tehnoloških trendova te samim tim i novih prijetnji i ranjivosti u informacijskim sustavima. Nije realno očekivati neku revoluciju, pogotovo jer trenutni standard sadrži većinu kontrola čije se postojanje temeljem dobrih praksi i očekuju u modernim i dobro zaštićenim informacijskim sustavima. Promjene su dobrodošle, a kao i u raznim drugim slučajevima, i ovdje se potvrđuje činjenica da je jedan od većih uzroka nesigurnih sustava upravo ljudski faktor, odnosno neznanje i nemaran rad samih zaposlenika. Ako ne žele zakasniti s usklađivanjem prema novim zahtjevima, tvrtke već sada, i prije nego što izađe službena verzija, znaju što ih očekuje te kojim putem trebaju krenuti. @

Pomoć pri implementaciji standarda

Kako bi pomoglo tvrtkama pri implementaciji oba standarda (PCI DSS i PA DSS), vijeće je izdalo i niz popratnih dokumenata kojima se detaljnije objašnjavaju razlozi uključivanja pojedinih kontrola u standarde i daju smjernice kako je najbolje implementirati pojedinu kontrolu, ali i jasno ukazuju kako revizori daju ocjenu usklađenosti s njima. Dokumenti se sekvencijalno izdaju već par godina, a niže u tablici pojašnjeni su neki od njih. Za detaljniji je popis potrebno otići na službene stranice vijeća (https://www.pcisecuritystandards.org/security_standards/documents.php).

DOKUMENT	NAPOMENA
PCI DSS Risk Assessment Guidelines	Pobliže opisuje metodologiju procesa upravljanja rizikom (procjena rizika, profiliranje rizika, obrada rizika), oslanjajući se pritom najviše na metodologijeISO 27005, NIST i OCTAVE. Posebnu pažnju daje rizicima poslovanja s vanjskim partnerima.
PCI DSS Wireless Guideline	Ovaj je dokument izdan među prvima, između ostalog, zbog velikog interesa zainteresiranih strana o tumačenju standarda u poglavljima vezanim za (ne)korištenje bežičnog pristupa na mrežu. Dokument je koristan svim vrstama organizacija, bez obzira na to rade li s kartičnim podacima.
PCI DSS Virtualization Guidelines	Virtualizacija je donijela mnoge razlike u odnosu na dosadašnji način kreiranja arhitekture te upravljanja i održavanja IT sustava u tvrtkama. Pritom su se pojavili novi rizici koji se pobrojavaju u ovom dokumentu te se daju smjernice za njihovo umanjivanje. Posebno je koristan dodatak A koji detaljnije objašnjava zahtjeve 12. poglavlja PCI DSS-a u odnosu na virtualna IT okruženja.
PCI Mobile Payment Acceptance Security Guidelines for Developers	Uzimajući u obzir mnoge vrste uređaja kojima se pristupa aplikacijama za kartično poslovanje (računala, prijenosnici, tableti, smartfoni), ovaj dokument daje smjernice razvojnim inženjerima za arhitekturu, dizajn i programiranje aplikacija za te uređaje. Može se smatrati dodatkom standarda PA DSS, ali ga naravno ne zamjenjuje. Ovaj je dokument koristan svim razvojnim inženjerima, pa i onima koji ne razvijaju aplikacije vezane uz kartično poslovanje.
PCI Mobile Payment Acceptance Security Guidelines for Merchants as End-Users	Za razliku od prethodnog dokumenta, ovaj se bavi istim područjem, ali je namijenjen krajnjim korisnicima mobilnih uređaja (tableta, smartfona, prijenosnika i sl.) te daje upute kako ih zaštititi i sigurno koristiti.
PCI DSS E-commerce Guidelines	Uz shematski prikaz entiteta koji uobičajeno sudjeluju u e-poslovanju, navode se tipične ranjivosti e-poslovanja, preporuke za smanjivanje rizika te veza tih preporuka s poglavljima standarda PCI DSS.
PCI DSS Cloud Computing Guidelines	Detaljizira modele oblačnog računalstva i stavlja naglasak na odgovornosti CSP-ova (Cloud Service Provider) u odnosu na tvrtku. Kako bi se to postiglo, potrebno je jasno definirati opseg i granice sustava između CSP-a i tvrtke. Osim toga, u posebnom se poglavlju daju i tehnološke smjernice pri upotrebi oblačnog računalstva. U dodacima dokumentu (Appendix) moguće je pronaći zanimljive predloške matrica, tablica i upitnika vezanih uz predmetno područje.