«TASDIQLAYMAN»
"Biznesni rivojlantirish banki" ATB
Boshqaruv raisi o'rinbosari v.b.:
O.Voxidov

«23» fevral 2026 y.
№ 186

Texnik topshiriq

Loyiha uchun

«Biznesni rivojlantirish banki» ATB uchun PCI DSS standarti talablariga muvofiqligini tasdiqlash maqsadida sertifikatsion audit o'tkazish

Toshkent – 2026 yil

1. Xizmatlarga qo‘yiladigan talablar

1.1. Ish mavzusining to'liq nomi

PCI DSS 4.0.1 standarti talablariga muvofiqlik bo‘yicha sertifikatsion audit o‘tkazish, shuningdek «Biznesni rivojlantirish banki» ATB uchun PCI DSS 4.0.1 standarti talablariga keyingi muvofiqlikka tayyorgarlik ko‘rish bo‘yicha konsultatsiya (keyingi o‘rinlarda – Ishlar).

1.2. Ishlarni amalga oshirish chegaralari

Ishlar O‘zbekiston Respublikasi, Toshkent shahrida joylashgan Buyurtmachining 2 (ikki) tadan ortiq bo‘lmagan maydonida amalga oshiriladi.

Tashqi penetratsion test Ijrochi tomonidan 1 (bir) martadan ortiq bo‘lmagan holda amalga oshiriladi.

Ichki penetratsion test Ijrochi tomonidan 1 (bir) martadan ortiq bo‘lmagan holda amalga oshiriladi.

Tashqi zaifliklarni skanerlash (ASV-skanerlash) Ijrochi tomonidan birinchi ASV-skanerlash o‘tkazilgan sanadan boshlab 1 yil davomida kamida har chorakda, 5 ta IP-manzildan ortiq bo‘lmagan hajmda amalga oshiriladi.

Ishlar chegaralarini kengaytirish Shartnomaga tomonlar tomonidan imzolanadigan va tomonlar muhrlari bilan tasdiqlanadigan qo‘shimcha kelishuv bilan rasmiylashtiriladi.

Xizmatlar Buyurtmachining maydonida ham, masofaviy tarzda ham ko‘rsatilishi mumkin.

1.3. Ishlar tarkibi

1) Buyurtmachini PCI DSS Standarti talablariga muvofiqlikka keltirish maqsadida Ijrochi quyidagi ishlarni bajarishni ta’minlaydi:
   a) Muvofiqlikka keltirish bosqichida dastlabki audit va konsultatsiya, jumladan:
   - Buyurtmachining maydonida dastlabki audit o‘tkazish, shu jumladan PCI DSS Standartining 4.0.1 versiyasi talablariga muvofiqligini baholash;
   - Himoya vositalarini tanlash va xarajatlarni kamaytirish usullari bo‘yicha konsultatsiya berish;
   - Muvofiqlikka keltirish bo‘yicha batafsil reja ishlab chiqish;
   - Standart talablarini bajarish masalalari bo‘yicha bir yillik konsultatsion qo‘llab-quvvatlash ko‘rsatish;

   b) Zarur normativ hujjatlar paketini ishlab chiqish;
   c) Tashqi zaifliklarni skanerlashni (ASV-skanerlash) o‘tkazish;
   d) Tashqi penetratsion test o‘tkazish;
   e) Ichki penetratsion test o‘tkazish;
   f) Segmentatsiya mexanizmlarini testdan o‘tkazish;
   g) Yakuniy sertifikatsion auditni o‘tkazish.

2)

2. Ishlarni amalga oshirish bosqichlari

2.1 PCI DSS 4.0.1 Standarti talablariga muvofiq dastlabki audit

2.1.1. Standartning amal qilish doirasining dastlabki ta’rifi

Ushbu bosqichning maqsadi PCI DSS 4.0.1 Standartini «Biznesni rivojlantirish banki» ATBning yaratilayotgan va mavjud IT-infratuzilmasiga nisbatan qo‘llash sohasini aniqlash, shuningdek Buyurtmachining protsessing markazini birlamchi baholash jarayonida bajariladigan ishlar hajmini kelishishdan iborat.

Standartni qo‘llash sohasini aniqlash uchun Buyurtmachi «Biznesni rivojlantirish banki» ATBning ishlab chiqilayotgan (mavjud) arxitekturasi, to‘lov kartalari ma’lumotlarini qayta ishlash, saqlash yoki uzatish jarayonlarida ishtirok etuvchi tizimlar ro‘yxati, shuningdek mavjud axborot xavfsizligini ta’minlash jarayonlari bo‘yicha hujjatlarni taqdim etadi.

Mazkur bosqich natijasi sifatida ishlar o‘tkazish chegaralariga kiritiladigan tekshiriladigan jismoniy, dasturiy va axborot resurslari hamda funksional quyi tizimlar ro‘yxati shakllantiriladi.

2.1.2. Protsessing markazi bo‘yicha tashkiliy va texnik ma’lumotlarni yig‘ish

Ushbu bosqichning maqsadi yaratilayotgan protsessing markazining arxitekturasi, to‘lov kartalari ma’lumotlari oqimlari, axborot xavfsizligini ta’minlashning joriy darajasi, protsessingni rivojlantirish va modernizatsiya qilish rejalari, shuningdek PCI DSS Standarti talablariga muvofiqlikni baholash hamda muvaffaqiyatli sertifikatsion auditga tayyorgarlik ko‘rish bo‘yicha tavsiyalar bilan Tadbirlar rejasini ishlab chiqish uchun zarur bo‘lgan boshqa ma’lumotlar haqida dolzarb va ishonchli axborotni olishdan iborat.

Mazkur ishlarni bajarish jarayonida quyidagi ma’lumotlar yig‘iladi:

- tashkiliy tuzilma haqida;
- foydalanilayotgan dasturiy-texnik vositalar majmuasi tuzilmasi haqida;
- tarmoq topologiyasi va qo‘llanilayotgan segmentatsiya usullari (shu jumladan foydalanilayotgan aloqa kanallari va aloqa tarmoqlari hamda Internet tarmog‘iga ulanish nuqtalari tavsiflari, simsiz kirish nuqtalari);
- lokal tarmoqda xavfsizlikni ta’minlash tartib-taomillari haqida;
- to‘lov kartalari ma’lumotlarini himoya qilish mexanizmlari haqida;
- zaifliklarni boshqarish tartib-taomillari haqida;
- kirishni boshqarish tizimini joriy etish haqida;
- kirishni monitoring qilish va nazorat qilish tartib-taomillari (tarmoq va ilovalar darajasida);
- axborot xavfsizligi siyosati haqida.

Barcha zarur ma’lumotlarni yig‘ish Buyurtmachi tomonidan taqdim etilgan hujjatlarni o‘rganish, Buyurtmachi xodimlari bilan intervyu o‘tkazish, dasturiy va dasturiy-texnik tizim komponentlarining konfiguratsiya fayllarini tahlil qilish, shuningdek Buyurtmachi xodimlari tomonidan bajariladigan tartib-taomillarni namoyish etish orqali amalga oshiriladi.

Shuningdek, Buyurtmachining xohishiga ko‘ra, ushbu bosqichda aniqlangan zaifliklarni bartaraf etish bo‘yicha tavsiyalar berilgan holda bir martalik ichki zaifliklarni skanerlash o‘tkazilishi mumkin.

2.1.3. PCI DSS Standarti talablariga muvofiqlikni baholash

Ushbu bosqichning maqsadi Buyurtmachining to‘lov shlyuzi PCI DSS Standarti talablariga muvofiqligining joriy darajasini aniqlashdan iborat.

Mazkur bosqichda, avval olingan ma’lumotlar asosida, Buyurtmachi infratuzilmasining PCI DSS Standarti talablariga muvofiqligi tahlil qilinadi, buning uchun quyidagi ishlar amalga oshiriladi:

- tarmoq tuzilmasi va segmentatsiyasini tahlil qilish;
- faol tarmoq uskunalari konfiguratsiyalari hamda mavjud kirishni cheklash qoidalarini tahlil qilish;
- qo‘llanilayotgan tarmoq protokollarini xavfsizlik nuqtai nazaridan tahlil qilish;
- axborot tizimida qabul qilingan xavfsizlik siyosatlarini tahlil qilish;
- to‘lov kartalari ma’lumotlarini qayta ishlash jarayonlarini tahlil qilish;
- va boshqa zarur ishlar.

Mazkur bosqich yakunida «Buyurtmachining yaratilayotgan va mavjud infratuzilmasining PCI DSS Standarti talablariga muvofiqligini baholash to‘g‘risida hisobot» tayyorlanadi. Ushbu hisobot to‘lov shlyuzining taklif etilayotgan arxitekturasi tavsifini, PCI DSS Standarti talablariga aniqlangan

nomuvofiqliklar ro‘yxatini, Standart talablarining joriy qo‘llanish sohasi (joriy audit sohasi) va unga kiruvchi tizim komponentlari tavsifini o‘z ichiga oladi.

2.1.4. PCI DSS standarti talablariga muvofiqlashtirish bo’yicha tavsiyalar ishlab chiqish

Mazkur bosqichda PCI DSS Standarti talablarini amalga oshirishning mumkin bo‘lgan variantlari ishlab chiqiladi, bunda tashkiliy tadbirlar majmuasini shakllantirish va zarur texnik yechimlarni joriy etish ko‘zda tutiladi. Shuningdek, ushbu bosqichda muvaffaqiyatli sertifikatsiyaga tayyorgarlik xarajatlarini kamaytirish maqsadida audit (sertifikatsiya) sohasini qisqartirishning mumkin bo‘lgan variantlari ham ishlab chiqiladi, ya’ni joriy etiladigan himoya vositalari soni va bajariladigan ishlar hajmini kamaytirish hisobiga.

Aniqlangan nomuvofiqliklarni bartaraf etish bo‘yicha tavsiyalarni shakllantirishda quyidagi yo‘nalishlar inobatga olinadi:

• PCI DSS Standarti talablarining qo‘llanish chegaralarini qisqartirish;

• mavjud himoya vositalari konfiguratsiyalarini o‘zgartirish;

• axborot xavfsizligini ta’minlash sohasida mavjud hujjatlarni takomillashtirish va qo‘shimcha hujjatlar ishlab chiqish;

• qo‘shimcha axborot himoya vositalarini (ommabop va tijorat yechimlari) joriy etish va sozlash.

Mazkur bosqich yakunida Buyurtmachiga tashkiliy va texnik tadbirlarni amalga oshirish rejasi taqdim etiladi, uning bajarilishi PCI DSS Standarti barcha talablarining bajarilishini ta’minlaydi. Reja, shuningdek, PCI DSS 4.0.1 versiyasi talablariga muvofiqlikka erishish bo‘yicha tadbirlarni ham o‘z ichiga olishi lozim.

2.1.5. PCI DSS Standarti talablarining asoslari bo‘yicha o‘qitish

Mazkur bosqich doirasida Ijrochi Buyurtmachi mutaxassislariga PCI DSS standartiga muvofiqlikni ta’minlash asoslari bo‘yicha bir martalik o‘quv mashg‘ulotini o‘tkazadi.

Buyurtmachi bilan kelishilgan holda o‘qitish 1-bosqich doirasida QSA-auditor tashrifi vaqtida Toshkent shahrida, Buyurtmachi ofisida bevosita shaklda yoki vebinar ko‘rinishida o‘tkazilishi mumkin.

O‘qitish 5 (besh) soatdan ortiq bo‘lmagan muddatda o‘tkaziladi.

Kurslar quyidagi dastur bo‘yicha o‘tkaziladi:

1. PCI DSS standarti bilan tanishtirish
1.1. PCI SSC va standartga umumiy sharh
1.2. To‘lov industriyasi terminologiyasi
1.3. Savdo-xizmat ko‘rsatish korxonalari va servis-provayderlar tasnifi
1.4. PCI DSS standarti hayotiy sikli
1.5. Standart doirasida ishtirokchilar o‘rtasidagi munosabatlar
2. PCI DSS standartidagi rollar va unga tutash sertifikatsiyalar
2.1. To‘lov brendlari rollari
2.2. VISA va MasterCard tomonidan ma’lumotlar xavfsizligi dasturlari
2.3. SAQ va ROC
2.4. SSF standartiga umumiy sharh
2.5. PCI PIN Security Requirements standartiga umumiy sharh
2.6. Ishtirokchilarning rollari va majburiyatlari
3. To‘lov kartalari ma’lumotlarini aniqlash va audit sohasi
3.1. O‘z infratuzilmangizda to‘lov kartalari ma’lumotlarini qanday aniqlash
3.2. Tarmoq segmentatsiyasi. Uni qanday to‘g‘ri amalga oshirish
3.3. Audit sohasini qanday aniqlash
4. PCI DSS standarti talablari
5. PCI DSS muvofiqligini joriy etish va qo‘llab-quvvatlash
5.1. Standart talablariga muvofiqlikka keltirish xususiyatlari
5.2. Davriy nazorat talab qilinadigan talablar
5.3. Doimiy nazorat talab qilinadigan talablar
5.4. PCI DSS talablarini autsorsing qilish. Qanday to‘g‘ri tashkil etish

5.5. Kompensatsion choralarni qanday qo‘llash
6. PCI SSC yordamchi hujjatlari va Xalqaro to‘lov tizimlari (MPS) bilan ishlash
6.1. PCI SSC tomonidan chiqarilgan yordamchi hujjatlarga umumiy sharh
6.2. PCI DSS muvofiqligiga erishishda ustuvor yondashuv
6.3. ROC va AOC
7. Yakuniy xulosa
Kurslar dasturi Ijrochi tomonidan o‘zgartirilishi mumkin.

2.2. Normativ hujjatlar paketini ishlab chiqish

Mazkur bosqichning maqsadi PCI DSS Standarti talablarini bajarish uchun zarur bo‘lgan normativ hujjatlar loyihalari paketini ishlab chiqishdan iborat, jumladan:

• Operatsion tizimlar va MBBT (ma’lumotlar bazasini boshqarish tizimlari)ni konfiguratsiya qilish standartlari;
• To‘lov kartalari ma’lumotlari xavfsizligini ta’minlash siyosatlari;
• Axborot xavfsizligi hodisalariga javob berish tartib-taomillari;
• Reglamentlar va yo‘riqnomalar;
• Boshqa zarur hujjatlar.

Ishlab chiqiladigan hujjatlarning yakuniy tarkibi Ijrochi auditorlari tomonidan «PCI DSS Standarti talablariga muvofiqlikka keltirish bo‘yicha tavsiyalarni ishlab chiqish» bosqichi natijalari asosida belgilanadi.

Mazkur bosqich yakunida Buyurtmachiga PCI DSS Standarti talablarini bajarish uchun zarur bo‘lgan normativ hujjatlar loyihalari paketi topshiriladi.

2.3. Tashqi zaifliklarni skanerlash (ASV-skanerlash)

Ishlarni bajarish jarayonida Ijrochi ASV-sertifikatlangan yechimdan foydalangan holda Buyurtmachining ommaviy tarmoqlarda mavjud bo‘lgan tarmoq tugunlarida faoliyat yuritayotgan tarmoq xizmatlaridagi zaifliklar va xavfsiz bo‘lmagan konfiguratsiyalarni aniqlaydi.

Tashqi zaifliklarni skanerlash (ASV-skanerlash) Ijrochi tomonidan Buyurtmachining so‘roviga ko‘ra, birinchi skanerlash o‘tkazilgan sanadan boshlab 1 yil davomida har chorakda, 5 ta IP-manzildan ortiq bo‘lmagan hajmda amalga oshiriladi.

Ishlarni PCI DSS Standarti talablariga (skanerlash tartib-taomillariga) muvofiq bajarishda xizmat ko‘rsatishni rad etish (DoS) hujumlari, parollarni tanlash (brute force) kabi xavfli tekshiruvlarni o‘z ichiga olmaydigan profillardan foydalaniladi, hamda aniqlangan zaifliklar ularning kritikligi darajasi bo‘yicha tasniflanadi.

Buyurtmachining xohishiga ko‘ra, birinchi skanerlash o‘tkazilgan sanadan boshlab 1 yil davomida cheklanmagan miqdorda mustaqil skanerlashlarni amalga oshirish uchun unga skanerlash tizimiga kirish huquqi taqdim etilishi mumkin.

Ishlar natijasi sifatida har bir o‘tkazilgan skanerlash yakuni bo‘yicha Buyurtmachiga hisobotlar taqdim etiladi.

2.4. Penetratsion test

Potensial tajovuzkor harakatlarini modellashtirish bo‘yicha ishlar ikki turga bo‘linadi:

• Tashqi penetratsion test. Internet tarmog‘i orqali amalga oshiriladi va Buyurtmachining korporativ kompyuter tarmog‘i tashqi perimetri axborot tizimlaridagi texnik zaifliklarni aniqlash va tahlil qilishni o‘z ichiga oladi.

• Ichki penetratsion test. Ijrochining Buyurtmachining lokal hisoblash tarmog‘iga ulangan mobil ishchi stansiyasi orqali amalga oshiriladi va ichki axborot tizimlaridagi texnik zaifliklarni aniqlash hamda tahlil qilishni o‘z ichiga oladi.

Har bir bosqichda penetratsion testning tarkibi va bajarilish jarayoni Ijrochining ichki metodikalari asosida belgilanadi. Ushbu metodikalar muntazam qayta ko‘rib chiqish va tahlil qilish orqali, ishlarni amalga oshirish davomida to‘plangan tajriba hamda axborot xavfsizligi sohasidagi joriy o‘zgarishlarni inobatga olgan holda doimiy ravishda yangilanib boriladi.

Shuningdek, penetratsion test davomida Ijrochi bunday ishlarni o‘tkazish bo‘yicha umumqabul qilingan xalqaro amaliyotlardan, jumladan OSSTMM v3.0 va OWASP Testing Guide v3 metodikalaridan foydalanadi.

Har bir bosqichdagi ishlar oldindan Buyurtmachining mas’ul vakillari bilan kelishiladi. Maqsadli tizimlar faoliyatining buzilish ehtimoli yuqori bo‘lgan taqdirda yoki Buyurtmachining maxfiy ma’lumotlariga muvaffaqiyatli kirish aniqlanganda, Ijrochi ishlarni davom ettirish uchun Buyurtmachidan rasmiy ruxsat olmaguncha keyingi ishlarni to‘xtatadi.

Ishlar davomida Ijrochi xizmat ko‘rsatishni rad etish bo‘yicha taqsimlangan hujumlarni (DDoS) amalga oshirmaydi.

Ishlar yakunlari bo‘yicha Buyurtmachiga bajarilgan ishlar tavsifi, aniqlangan muammolar (zaifliklar) va ularni bartaraf etish bo‘yicha tavsiyalarni o‘z ichiga olgan hisobot hujjatlari taqdim etiladi.

2.4.1. Hujumchi modeli tafsilotlari

Penetratsion test ishlari doirasida quyidagi modellarga mos keluvchi potensial tajovuzkorlar harakatlarini modellashtirish taklif etiladi:

- • «Internet-xaker» – Internet tarmog‘idan harakat qiluvchi, Buyurtmachining axborot tizimlarida mantiqiy huquqlarga ega bo‘lmagan hamda korporativ tarmoq va Buyurtmachi axborot tizimlari haqida ma’lumotga ega bo‘lmagan tajovuzkor;
- • «Tashrif buyuruvchi» – Buyurtmachining lokal hisoblash tarmog‘iga nazoratsiz ishchi stansiyani ulash imkoniyatiga ega bo‘lgan (masalan, tashqi konsultant), Buyurtmachining axborot tizimlarida mantiqiy huquqlarga ega bo‘lmagan va korporativ tarmoq tuzilmasi hamda qo‘llanilayotgan himoya vositalari haqida batafsil ma’lumotga ega bo‘lmagan tajovuzkor.
- Har bir tavsiflangan modelga mos keluvchi potensial tajovuzkorlar umumfoydalaniladigan maxsus dasturiy ta’minotdan foydalanadi va axborot tizimlari hamda ularning komponentlaridagi zaifliklarni mustaqil tadqiq etish ko‘nikmalariga ega emas, shuningdek zararli dasturiy ta’minotni mustaqil ishlab chiqish uchun yetarli malakaga ega emas.

- Potensial tajovuzkorlarning asosiy maqsadlari quyidagilardan iborat:
- • Buyurtmachining korporativ tarmog‘iga kirish imkoniyatini qo‘lga kiritish;
- • Buyurtmachining axborot tizimlariga mantiqiy kirish huquqini qo‘lga kiritish;
- • Buyurtmachining axborot tizimlarida qayta ishlanayotgan maxfiy ma’lumotlarga kirish;
- • Qayta ishlanayotgan ma’lumotlar yaxlitligini buzish yoki faoliyat yuritayotgan servislar mavjudligini buzish orqali Buyurtmachining ma’lumotlarni qayta ishlash markazi (MQM/ЦОД) ish faoliyatini buzish imkoniyatini aniqlash.
-

2.4.2. Tashqi penetratsion test

3)Tarmoq tashqi perimetri himoyalanganligini tahlil qilish bo'yicha ishlar Buyurtmachining korporativ tarmog'i va protsessing markazi haqida batafsil ma'lumotga ega bo'lmagan potensial tashqi tajovuzkor harakatlarini modellashtirishdan iborat.

4)

5) Potensial tajovuzkor harakatlarini modellashtirish ikki asosiy bosqichga bo'linadi:

1. Dastlabki ma'lumotlarni yig'ish. Ushbu bosqichda Buyurtmachining korporativ tarmog'i tuzilmasi va komponentlari haqida ma'lumotlar to'planadi, jumladan: domen nomlari va zonalari, tarmoq adresatsiyasi, tarmoq komponentlari, qo'llanilayotgan himoya vositalari.

2. Faol tashqi penetratsion testni o'tkazish. Ushbu bosqichda zaifliklar "qo'lda" usulda hamda maxsus dasturiy ta'minotdan foydalangan holda aniqlanadi. Ushbu bosqichdagi ishlar tarkibiga quyidagilar kiradi:

- Tashqi ta'sirga javob reaksiyasi asosida qurilmalar turlari va versiyalari, operatsion tizimlar, tarmoq servislar hamda ilovalarni aniqlash;
- Serverlar, tarmoq uskunalari va tarmoq himoya vositalaridagi zaifliklarni identifikatsiya qilish. Zaifliklarni aniqlash ishlar chegarasiga kiruvchi va Internet tarmog'idan kirish

mumkin bo'lgan (yoki ishlar davomida kirish imkoni paydo bo'lgan) barcha xostlar uchun amalga oshiriladi (jumladan HTTP va DNS servislar, VPN-servislar, veb-ilovalar, elektron pochta xizmati, tizimli va amaliy servislar). Noto'g'ri realizatsiya bilan bog'liq zaifliklar hamda tarmoq servislar, operatsion tizimlar, ilovalar, tarmoq qurilmalari va himoya vositalarining noto'g'ri konfiguratsiyasi bilan bog'liq zaifliklar aniqlanadi;

- Himoyalanganlikni ekspert tahlili (penetratsiya). Bu maxsus vositalar va ma'lum zaifliklar haqidagi ma'lumotlardan foydalangan holda maqsadli tizimlarga nisbatan hujumlarni modellashtirishni anglatadi. Zarurat bo'lganda, ushbu bosqichdagi ishlar ishlar chegarasiga kiruvchi o'zaro bog'liq axborot tizimlariga ta'sir ko'rsatish maqsadida iterativ ravishda takrorlanishi mumkin.

6)

2.4.3. Ichki penetratsion test

7)Mazkur bosqichdagi ishlar potensial ichki tajovuzkor harakatlarini modellashtirishdan iborat. Ishlar tarkibiga quyidagilar kiradi:

8) Buyurtmachining lokal hisoblash tarmog'i (LHT) haqida ma'lumotlarni tarmoq ichidan yig'ish;

9) Tashqi ta'sirga javob reaksiyasi asosida qurilmalar turlari va versiyalari, operatsion tizimlar, tarmoq servislar hamda ilovalarni aniqlash;

10) Tarmoq darajasida hujumlarni modellashtirish;

11) Foydalanuvchilarning ishchi stansiyalari, axborot tizimlari komponentlari, tarmoq uskunalari va tarmoq himoya vositalaridagi zaifliklarni identifikatsiya qilish;

12) Aniqlangan tizimlarga nisbatan ma'lum zaifliklar haqidagi ma'lumotlar va maxsus vositalardan foydalangan holda ilovalar, tarmoq servislar hamda operatsion tizimlar darajasida hujumlarni modellashtirish.

13)

3.5. Segmentatsiya mexanizmlarini testdan o‘tkazish

Mazkur bosqichdagi ishlar tarmoq segmentatsiyasi bo'yicha qo'llanilgan choralar samaradorligini (sertifikatsiya chegaralarini qolgan tarmoqdan ajratish) tekshirishdan iborat. Ishlar tarkibiga quyidagilar kiradi:

1. Buyurtmachining lokal hisoblash tarmog'i (LHT) haqida ma'lumotlarni tarmoq ichidan yig'ish;
2. Sertifikatsiya chegaralaridan tashqaridan turib tashqi ta'sirga javob reaksiyasi asosida tarmoq servislar va ilovalarni identifikatsiya qilish;
3. Sertifikatsiya muhiti chegarasida tarmoqlararo ekran (firewall) qoidalarini tanlab tekshirish.

Mazkur bosqich yakunida qo'shimcha ichki segmentatsiya testlari natijalari bo'yicha hisobot tayyorlanadi. Hisobot bajarilgan ishlar, aniqlangan barcha kamchiliklar va ularni bartaraf etish bo'yicha tavsiyalarni o'z ichiga oladi.

2.6. PCI DSS 4.0.1 standarti talablariga muvofiqlik bo‘yicha sertifikatsion audit

2.6.1. Sertifikatsiya sohasini aniqlash

Mazkur bosqichda Ijrochining auditorlik guruhi tomonidan auditning dolzarb sohasi aniqlanadi va kelishiladi. Buning uchun Ijrochi protsessing markazining axborot tizimlari tuzilmasi hamda axborot xavfsizligini ta’minlash jarayonlari bo‘yicha mavjud ma’lumotlarni so‘raydi, shuningdek PCI DSS Standarti talablariga muvofiq audit sohasiga kiritiladigan tizim komponentlari, ma’lumotlarni uzatish kanallari va boshqa tizimlarni belgilaydi.

Mazkur bosqich natijasi sifatida auditdan o‘tkazilishi lozim bo‘lgan tizim komponentlari ro‘yxati shakllantiriladi.

2.6.2. Muvofiqlik dalillarini yig‘ish

Mazkur bosqichda Ijrochining auditorlari Buyurtmachining mas’ul xodimlari bilan zarur intervyular o‘tkazadi, audit sohasiga kiruvchi tizim komponentlarining xavfsizlik parametrlarini tekshiradi hamda yakuniy hisobot hujjatlarini shakllantirish uchun zarur bo‘lgan audit dalillarini hujjatlashtiradi.

Barcha zarur ma’lumotlarni yig‘ish normativ hujjatlarni o‘rganish, intervyular o‘tkazish, konfiguratsiya fayllarini tahlil qilish, shuningdek Buyurtmachi xodimlari tomonidan axborot xavfsizligini ta’minlash bo‘yicha bajariladigan tartib-taomillarni namoyish etish orqali amalga oshiriladi.

2.6.3. Hisobot hujjatlarini shakllantirish

Mazkur bosqichda Ijrochining auditorlik guruhi yig‘ilgan audit dalillari asosida PCI DSS Standarti talablarining bajarilishini tahlil qiladi, ular oltita guruhga ajratilgan:

a) Himoyalangan hisoblash tarmog‘ini qurish va qo‘llab-quvvatlash;
b) To‘lov kartalari egalarining ma’lumotlarini himoya qilish;
c) Zaifliklarni boshqarish dasturini amalga oshirish;
d) Qat’iy kirish nazorati choralarini amalga oshirish;
e) Hisoblash tarmoqlarini muntazam monitoring qilish va testdan o‘tkazish;
f) Axborot xavfsizligi siyosatini qo‘llab-quvvatlash.

hamda zarur hisobot hujjatlarini shakllantiradi.

Mazkur bosqich yakunida Buyurtmachiga va Xalqaro to‘lov tizimlariga yuboriladigan hisobot hujjatlari shakllantiriladi:

- Report on Compliance (Ingliz tilida);
- Attestation of Compliance (Ingliz tilida);
- PCI DSS 4.0.1 muvofiqlik sertifikati (rus va ingliz tillarida);

2.7. PCI DSS Standarti talablarini bajarish masalalari bo‘yicha konsultatsion qo‘llab-quvvatlash

Mazkur bosqichdagi ishlarning maqsadi Buyurtmachi mutaxassislariga PCI DSS Standarti aniq talablari mazmunini tushuntirish va ularni bajarish usullari bilan bog‘liq yuzaga keladigan savollar bo‘yicha konsultatsiya berishdan iborat.

Buyurtmachiga konsultatsion qo‘llab-quvvatlash shartnoma tuzilgan kundan boshlab 1 yil davomida amalga oshiriladi. So‘rovlar elektron pochta va telefon orqali qabul qilinadi. Har bir kelib tushgan so‘rovga javob berish muddati so‘rov murakkabligiga qarab, qabul qilingan kundan boshlab 1 dan 5 ish kunigacha bo‘lishi mumkin.

kelishuvchilar: J.Alimov, B.Shamsiev