Şəbəkənin valyuta konvertasiyaları və transfer sürəti bu iştirakçıların birgə fəaliyyətdən asılıdır. Ripple şəbəkəsi əvvəldə qeyd olunan valyutalardan əlavə digər rəqəmsal valyutaları və eyni zamanda fikizi mallar olan gümüş və qızılla olan ödənişləri də dəstəkləyir. Bu nəticəyə gəlmək olar ki, Bitcoin şəbəkəsi insanların bir-birləri ilə ödəniş etmələri üçün yaradılmış sosial şəbəkə olduğu halda Ripple şəbəkəsi iqtisadi institutlar üçün ənənəvi transferlərini daha da sürətli və geniş formada apara bilməsi üçün yaradılmış global blockchain şəbəkəsidir. Ripple şəbəkəsi elə formada dizayn olunmuşdur ki bu sistemdən istifadə edən iqtisadi institutlar onun imkanlarını öz qanun və normativlərinə uyğunlaşdıra bilərlər.

Beləliklə, blockchain texnologiyalarının sürətlə kapitallarının dünya bazarında artması əsasında bu texnologiyaların dünya iqtisadiyyatında daha ciddi rol alacağını söyləmək olar.

İNFORMASİYA TƏHLÜKƏSİZLİYİNİN MÜASİR VƏ KLASSİK MODELLƏRİ

Paşayeva X.C.
Azərbaycan Dövlət İqtisad Universiteti
Pashayeva-khanim@outlook.com

Müasir dünyamızı informasiya texnologiyalarsız, şəbəkələrsiz təsəvvür etmək qeyri mümkündür. Son aylar qlobal xarakter daşıyan COVİD-19 panepidemiyasının nəticəsində bir daha gördük ki, informasiya texnologiyaları, sitemləri olmazsa dünyada baş verən bütün proseslər dayana və aparıcı bir sıra sahələrdə kəskin geriləmə müşaiət olunardı. Lakin müasir dövrümüzdə informasiya texnologiyalarının sürətli inkişafı bizə bugün həyatımızı asanlaşdırmağa və vaxtımıza qənaət etməyə kömək edir. Lakin bu əməliyyatlar necə icra edilir, həmçinin icra olunarkən məlumatlarımız necə qorunur bu bizim üçün proqram təminatının işləməsində daha vacib məsələdir. Nəzərə alsaq ki, dünyada kibercinayətkarlığın geniş yayılmışdır və bütün dünyada məşhur, 40 ildən çox təcrübəsi olan öyrətmə platformalarından Reilly Medianın qurucusu Tim O'Reillynin dili ilə desək məlumatların (verilənlərin) proqram təminatlarından daha vacib olduğu yeni bir dünyaya girmişik.

Müasir proqram təminatlarında olan informasiyalara qoyulan 4 əsas tələb eyni zamanda informasiya təhlükəsizliyinin də əsasları hesab olunur. Belə ki, hər bir informasiya dəqiq, vaxtla ölçüləbilən, kontekstə uyğun (məzmunlu), müəyyən məqsədə yönəlmiş və dəyərli olmalıdır. İnformasiya mütləq bir şəkildə müxtəlif təhlükə və zərərli vasitələrdən qorunmalıdır.

Kompüter təhlükəsizliyi kontekstində tez-tez informasiya təhlükəsizliyi terminindən istifadə edirik. Son illərdə bu terminlərin siyahısına kiber təhlükəsizlik termini də əlavə edilmişdir. Kiber təhlükəsizlik terminini bir sıra ədəbiyyatlarda istənilən təşkilatın etibarlı əməliyyatlarını təmin etmək üçün texnologiya, insanlar, məlumat və proseslərin birgə əməyinin nəticəsi olan hesablama əsaslı kombinasiya kimi təyin edirlər. Buraya təhlükəsiz kompüter sistemlərinin yaradılması, əməliyyatları, təhlili və sınaqdan keçirilməsi kimi mərhələlər daxildir. Bütün bunlar informasiya təhlükəsizliyi modelləri ilə təmin edilir.

İnformasiya təhlükəsizliyi modelləri təhlükəsizlik siyasətinin identifikasiyası üçün istifadə olunan metodlardır, və təhlükəsizlik siyasətindəki əsas təhlükəsizlik anlayışlarını, proseslərini və prosedurlarını həyata keçirmək üçün kompüterin əməl edə biləcəyi dəqiq qaydalar toplusunu təmin etmək üçün nəzərdə tutulmuşdur. Bu modellər mücərrəd və ya intuitiv ola bilər.

İnformasiya təhlükəsizliyinin ilk hərtərəfli modeli 1991-ci ildə McCumber tərəfindən hazırlanmışdır. McCumber's Cube kimi də tanınan bu model peşəkarlar üçünm informasiya sistemləri təhlükəsizliyi üçün Milli Təlim Standartının bir hissəsidir. McCumber kubu üç hər birində 3 komponent olan 3 blokdan ibarətdir: 1-ci blok informasiya prosesləri (ötürülmə, saxlama, emal), 2-ci kritik məlumat xüsusiyyətləri (məxfilik, bütövlük və mövcudluq) və 3-cü təhlükəsizlik tədbirləri (texnologiya, siyasət və təcrübə, təhsil, təlim və maarifləndirmə).İnformasiya təhlükəsizliyinin əsas konsepsiyasından danışarkən klassik model olan CİA (Confidentiality, Integrity, Availability) modeli baza model qəbul edilir. Bu model informasiyanın məxfiliyini, bütövlüyünü və yararlılığını özündə təcəssüm etdirir.

İnformasiyanın məxfiliyi dedikdə o informasiya nəzərdə tutulur ki, həmin informasiya yalnız giriş icazəsi olan istifadəçilər üçün əlçatan olsun. İnformasiyanın bütövlüyü dedikdə isə informasiyanın bütövlüyünün pozulmasından mühafizəsi də başa düşülə bilər. Sistem eyni zamanda elə qurulmulıdır ki, istifadəçilər üçün yararlı informasiyalardan təşkil olunsun.

İnformasiya təhlükəsizliyinin klassik modeli ilə yanaşı müasir dövrümüzdə istifadə olunan və CİA metodundan daha geniş tətbiq olunan RMİAS (Reference Model of Information Assurance & Security)

modeli də bugün bütün informasiya sistemlərində mühafizə üsullarından biri kimi istifadə edilir. Bu model dilimizə "Məlumat Təminatı və Təhlükəsizliyinin İstinad Modeli" kimi tərcümə edilir. Bu modelin konsepsiyası 2013-cü ildə İngiltərənin Kardif və Kranfild univesitetlərinin professorları Yulia Cherdantseva və Jeremy Hilton tərəfindən irəli sürülmüşdür. RMİAS modeli 4 hissənin qarşılıqlı fəaliyyəti nəticəsində qurulur. Bunlar aşağıdakılardır:

- İnformasiya Sistemlərinin Təhlükəsizlik Ömrü
- İnformasiya taksonomiyası
- Təhlükəsizlik Məqsədləri
- Təhlükəsizlik əleyhinə tədbirlər

İnformasiya Sistemlərinin Təhlükəsizlik Ömrü - müvəqqəti bir aspekti və iş / təşkilat kontekstində bir məlumat sistemini / həllini yaradan, yerləşdirən, ölçən, təmizləyən və nəhayət istifadə edəcək bir inkişaf metodologiyasının tətbiqini göstərir.İnformasiya taksonomiyası - qorunan məlumatı və yaradılandan məhv edilənədək ömrünü təsvir edir. Burada məlumatların hər bir kateqoriyasını forma, vəziyyət, həssaslıq və yerləşmə ilə nəzərdən keçiririk.

Təhlükəsizlik Məqsədləri - bir təşkilat, iş və ya sistem kontekstində tətbiq oluna biləcək məqsədlər toplusunu müəyyənləşdirin. Buradakı model, misal üçün hesabatlılıq, rədd etmə və məxfilik əlavə edərək "IAS octet" olmaq üçün CIA Triadının genişləndirilməsidir. Razılaşdırılmış hədəflər, maraqlı tərəflərə daha sonra texniki, iş, proses və insan perspektivləri ilə müqayisə oluna biləcək anlayışları başa düşməyə imkan verir.

Riskin təhlili prosesində müəlliflər təhlükəsizlik məqsədlərinin prioritet sayıla biləcəyini və təhlükəsizlik tədbirlərini təyin etmək üçün istifadə edilə biləcəyini qeyd edirlər.Təhlükəsizlik əleyhinə tədbirləri - tələb olunan təhlükəsizlik məqsədlərinə çatmaq üçün istifadə olunan bir texnika və ya bir proses olaraq təyin edə bilərik. IAS baxımından təhlükəsizlik tədbirlərinin seçimi səmərəlilik və iş səmərəliliyi baxımından həyata keçirilir. Bu əks tədbirlər dəsti texniki iş, hüquqi və insan amillərini əhatə edir, Məsələn, insan aspekti işçilərin iş tələblərinə cavab verməsi üçün təhlükəsizlik siyasətinin qurulmasını əhatə edir. İşçilərin məlumatlılıqlarını və uyğunluğunu təmin etmək üçün təlimlər və sınaqlar keçirilə bilər, məsələn, bir çox müəssisələrdə təhlükəsizlik mütəxəssisləri kimin açdığını və nişanlandığını görmək üçün saxta fişinq xarakterli elektron poçtları işçilərə göndərir və bununla risk qrupunu müəyyən edirlər. Təhlükəsizlik əleyhinə tədbirlərin effektivliyini izləmək və ya yoxlamaqla informasiyanın mühafizəsi yüksək səviyyədə təmin edilə bilər.Bu modellərdən əlavə digər modellər də mövcuddur.

Dövlət maşın modeli, işlədiyi əməliyyat vəziyyətindən asılı olmayaraq həmişə etibarlı rejimdə olan bir sistemə aiddir. Dövlət maşın modelinə görə, dövlət müəyyən bir anda bir sistemin görüntüsüdür. Dövlət maşın modeli, analiz edənlər, dekoderlər və tərcüməçilər də daxil olmaqla, bütün növ sistemləri modelləşdirmək üçün xarici bir girişi daxili bir maşın vəziyyəti ilə birləşdirən sonlu bir dövlət maşınının kompüter elmləri tərifindən gəlir. Bir giriş və bir dövlət nəzərə alınmaqla, bir dövlər maşını başqa bir dövlətə keçir və bir nəticə yarada bilər. Giriş qəbul edilərkən və ya məhsul istehsal edilərkən bir keçid baş verir və həmişə yeni bir vəziyyətlə nəticələnir.

Bütün dövlət keçidləri nəzərdən keçirilməlidir və dövlətin bütün komponentləri təhlükəsizlik siyasətinin tələblərinə cavab verirsə, dövlət etibarlı sayılır. Hər bir dövlət başqa bir təhlükəsiz vəziyyətə keçəndə sistem etibarlı bir dövlət maşını şəklində göstərilir. Bir çox digər təhlükəsizlik modelləri etibarlı dövlət konsepsiyasından təsirlənmişdir.

Digər model isə Bell-LaPadula Modelidir. Bell-LaPadula Modeli ABŞ Müdafiə Departamentinin çox səviyyəli təhlükəsizlik siyasətini rəsmiləşdirmək üçün hazırlanmışdır. ABŞ Müdafiə Departamentinin resursları dörd fərqli səviyyəyə təsnif edir.Ən az həssasdan ən çox həssasına qədər artan səviyyələrə daxildir: ümumi, konfidensional, gizli və çox gizli. Bell-LaPadula modelindən istifadə edərək, hər hansı bir rəsmiləşdirmə səviyyəsi digərlərinə mənbələrə daxil ola bilər. Bununla birlikdə, yalnız bir insanın əldə etməsi lazım olan qaynaqlar mövcuddur. Məsələn, "gizli" səviyyə üçün təmizlənmiş şəxsin yalnız "gizli" etiketli giriş sənədləri var. Bu məhdudiyyətlərlə Bell-LaPadula modeli obyektlərin məxfiliyini qoruyur. Bell-LaPadula modeli dövlət maşın modelinə əsaslanır. Bu modeli informasiya sistemlərinə tətbiqini istifadəçi növlərinə görə sistemdə icra icazələrinin verilməsi mexanizmində görə bilərik.

Yekun olaraq deyə bilərik ki, informasiya təhlükəsizliyi modelləri təhlükəsizliyin vacib tərəflərini və onların sistem davranışı ilə əlaqələrini dəqiq təsvir edir. İnformasiya təhlükəsizliyi modellərinin əsas məqsədi əsas təhlükəsizlik tələblərinin müvəffəqiyyətlə yerinə yetirilməsi üçün zəruri əsas səviyyələri təmin etməkdir.