Ssenari: Maliyyə Qurumunda Məlumat Elmi və Böyük Məlumat Analitikasının Təhlükəsizliyi
Məlumat elminin və böyük məlumat analitikasının risklərin qiymətləndirilməsində, fırıldaqçılığın aşkar edilməsində və müştərilərin təfəkküründə mühüm rol oynadığı bir maliyyə institutunda həssas maliyyə məlumatlarının təhlükəsizliyinin təmin edilməsi mühüm əhəmiyyət kəsb edir.

1. **Maliyyə institutunda məlumat elmi və böyük məlumat analitikasının həyat dövrü ərzində həssas maliyyə məlumatlarını qorumaq üçün hansı təhlükəsizlik tədbirləri həyata keçirilməlidir?**

Həssas maliyyə məlumatlarının qorunması, maliyyə institutları üçün ən vacib məsələlərdən biridir. İnstitutlar, məlumat elmi və böyük məlumat analitikasının həyat dövrü ərzində aşağıdakı təhlükəsizlik tədbirlərini həyata keçirməlidir:

1. Məlumatın şifrələnməsi: Bütün həssas maliyyə məlumatları, depolanma və keçidlərdən əvvəl şifrələnməlidir. Ən güclü şifrələmə protokolları istifadə edilməlidir və məlumatların yalnız şifrə açarlarına sahib olan şəxslər tərəfindən əldə edilə bilinəcək şəkildə saxlanılmalıdır.
2. Fiziki qoruma: Maliyyə institutları, məlumatların saxlanıldığı server otaqları və mərkəzləşdirilmiş sistemlər üçün fiziki qoruma tədbirləri tətbiq etməlidir. Otaqlar və serverlər, zərərli müdaxilələrə, hərəkətsizlik sensorlarına, təhlükəsizlik kameralarına və giriş nəzarət sistemlərinə malik olmalıdır.
3. Ağ təhlükəsizliyi: İnstitutlar, şəbəkələri və serverləri zərərli fəaliyyətlərə qarşı müdafiə etmək üçün ən son ağ təhlükəsizliyi protokollarını tətbiq etməlidir. Bu protokollar, ağ trafiklərini izləmə, şifrələmə, firevolların tətbiq edilməsi və zərərli proqramların müdafiə edilməsi kimi tədbirləri əhatə edir.
4. İstifadəçi məlumatlarının idarə olunması: Həssas maliyyə məlumatlarına giriş hüququ olan istifadəçilərin məlumatların idarə olunması və giriş nəzarəti üzrə qaydaları izləməsi təmin edilməlidir. İstifadəçilər yalnız lazım olan məlumatları görməlidir və sistemə qətiyyən yalnız fəaliyyətləri üçün icazə verilməlidir.
5. Fəaliyyət auditləri: Maliyyə institutları, məlumatlara əl çatan və sistemə daxil olan fəaliyyətləri izləmək və audit etmək üçün müvafiq sistemlər qurmaq üçün tədbirlər görməlidir. Bu, şübhəli fəaliyyətləri təhlil edərək potensial təhlükələri müəyyənləşdirmək və müdafiə tədbirləri almaq üçün imkan yaradır.
6. İstifadəçilərin təlimatlandırılması: Həssas maliyyə məlumatlarının qorunması, istifadəçilər arasında dəyərli təlimatlar və məlumat mənbələrinin təmin edilməsi ilə başa çıxılmalıdır. İnstitutlar, istifadəçilərə güclü şifrələr seçmək, giriş

məlumatlarını paylaşmamaq, şübhəli e-poçtları açmamaq və zərərli proqramlardan qorunmaq kimi tədbirləri nəzərdə tutan təlimatlar təklif etməlidir.

Bu təhlükəsizlik tədbirləri, maliyyə institutlarının həssas maliyyə məlumatlarının təhlükəsizliyini təmin etmək üçün əsasları təşkil edir. Bununla birlikdə, tədbirlərin məzmunu və intensivliyi, məlumatın cəmiyyət içində paylaşılma dərəcəsinə, yerli və beynəlxalq tələblərə, hüquqi düzənləmələrə və digər faktorlara görə dəyişə bilər. Dolayısı ilə, hər maliyyə institutu öz təhlükəsizlik qaydalarını dəqiqləşdirərək və məlumat təhlükəsizliyi üzrə mütəxəssislərin fikirlərini göz önündə tutaraq bu tədbirləri tətbiq etməlidir.

---

2. **Şifrələmə üsulları böyük verilənlərin analitikası infrastrukturunda istirahətdə və tranzitdə olan məlumatları qorumaq üçün necə tətbiq oluna bilər?**

Maliyyə institutlarında büyük veri analitiği altyapısında istirahət və tranzitdə olan məlumatların korunması üçün şifrələmə üsulları tətbiq edilə bilər. İstirahət dövründə, verilənlər mərkəzində saxlanılan məlumatların şifrələnməsi ilə qorunması vacibdir. Bu, məlumatların gizliliyini təmin edərək, yetkisiz şəxslərin verilərə girişini məhdudlaşdırır.

Aşağıdakı şifrələmə üsulları maliyyə institutlarında məlumatların güvənliyini təmin etmək üçün istifadə edilə bilər:

1. Simmetrik şifrələmə: Bu üsulda məlumatlar şifrələnmədən əvvəl bir açıq şifrə ilə şifrələnir və daha sonra eyni açıq şifrə ilə deşifrələnir. Ən yayqın simmetrik şifrələmə alqoritmləri AES (Advanced Encryption Standard) və DES (Data Encryption Standard) olaraq bilinir.
2. Asimetrik şifrələmə (həmçinin məşhur "açıq açar" şifrələmə): Bu üsulda, məlumatlar üçün iki açar istifadə olunur - biri açıq, digəri isə gizli. Açıq açar, məlumatların şifrələnməsində istifadə olunur, və yalnız gizli açarla deşifrə olunur. Bu, daha güclü bir şifrələmə üsuludur və RSA alqoritmi kimi məşhurdur.
3. Həm simmetrik, həm də asimetrik şifrələmənin bir birləşməsi: Bu metod, simmetrik şifrələmənin performans üstünlüklərini asimetrik şifrələmənin güclü gizlilik avantajları ilə birləşdirir. Məlumatlar ilk olaraq asimetrik bir açarla şifrələnir və daha sonra hər bir müştəri üçün fərdi bir simmetrik açar yaradılır. Bu simmetrik açar, müştərinin məlumatları oxumaq və yazmaq üçün istifadə etdiyi şifrələmə üsuludur. Bu, daha yüksək performans tələb edən tranzit əməliyyatlarında yararlı ola bilər.

Əsasən, maliyyə institutları, məlumatların şifrələnməsində ən məşhur və təsdiq edilmiş şifrələmə standartlarından birini və protokollardan birini tətbiq edirlər. Ayrıca, ən son təhlükəsizlik yeniliklərini izləyərək, maliyyə sektorundakı sərmayə müəssisələri, şifrələmə üsullarını güncələyərək potensial risklərdən qorunmağa çalışmalıdırlar. Şifrələmə yalnız bir təhlükəsizlik tədbiri olaraq düşünülməməlidir. Digər tədbirlər, məsələn, məlumatların giriş nöqtələrinin tənzimlənməsi, təhlükəsiz şəbəkələr, məlumat backupları və təhlükəsizlik auditləri də əlavə edilməlidir.

---

3. Yalnız səlahiyyətli personalın həssas maliyyə məlumatlarına daxil ola və təhlil edə bilməsini təmin edərək, məlumat elminə və böyük məlumat analitikası platformalarına girişi təsdiqləmək və icazə vermək üçün hansı strategiyalardan istifadə etmək olar?

Böyük veri analitikası altyapısında hem istirahətdə, yani depolama aşamasında, hem də tranzitdə, yani məlumatların hərəkət etdiyi zamanlarda məlumatların təhlükəsizliyini təmin etmək üçün bir neçə şifrələmə üsulu mövcuddur. İstifadə edilən konkret üsul və texnologiyalar şirkətiniz, işlənən məlumatların növü və hədəflərə bağlı olaraq dəyişə bilər. Lakin aşağıda ümumi olaraq tətbiq edilə bilən şifrələmə üsullarından bəzilərini sizinlə paylaşım:

1. Ənənəvi Şifrələmə (Traditional Encryption): Məlumatları istirahətdə şifrələmək üçün ənənəvi şifrələmə alqoritmlərindən istifadə edə bilərsiniz. Bu şifrələmə üsulu, məlumatları şifrələmək və şifrəni açmaq üçün şifrələmə və deşifrələmə açarları istifadə edir. Ənənəvi şifrələmə üsulları arasında DES (Data Encryption Standard), AES (Advanced Encryption Standard) və RSA (Rivest-Shamir-Adleman) kimi məşhur alqoritmlər mövcuddur.
2. Anonimləşdirilmə (Anonymization): Böyük verilərdəki məlumatları şifrələmək üçün anonimləşdirilmə üsulundan istifadə edə bilərsiniz. Anonimləşdirilmə, məlumatlarda şəxsi məlumatları gizlətmək və ya silmək deməkdir. Bu üsul, məlumatların müəyyən bir mərhələdə şəxsi məlumatları aşkar etməsini çətinləşdirir. Anonimləşdirilmək üçün məlumatları gizlətmə, gizlətmə, genişləndirmə və kriptografiya metodlarından istifadə edə bilərsiniz.
3. Hərəkət halındakı Şifrələmə (Transport Layer Encryption): Məlumatlar tranzitdə olduğu zaman, məlumatları təhlükəsiz bir şəkildə göndərmək üçün hərəkət halındakı şifrələmə istifadə edə bilərsiniz. SSL (Secure Sockets Layer) və ya TLS (Transport Layer Security) protokolları kimi texnologiyalardan istifadə edərək məlumatları şifrələyə bilərsiniz. Bu protokollar, verilənlərin şifrələnmiş olaraq göndərilməsini və şifrənin yalnız növbəti uçun açılmasını təmin edir.
4. Kverilərdə Poliçalar (Data-at-Rest Policies): İstirahətdə olan məlumatları qorumaq üçün, verilənlər bazalarında şifrələmədən istifadə edə bilərsiniz. Məlumatlar

depolanarkən şifrələmə tətbiq edildiyində, məlumatlara yetkisiz girişi çətinləşdirə bilərsiniz. Bu, verilənlərin istifadə olunan həddələr üzrə şifrələnməsinin təmin edilməsinə imkan verir.
5. Ağ Səviyyəli Şifrələmə (Network Level Encryption): Böyük verilərin ağ üzərində hərəkət etdiyi zaman, məlumatları ağ səviyyəsində şifrələmək üçün VPN (Virtual Private Network) kimi texnologiyalardan istifadə edə bilərsiniz. VPN, məlumatların şifrələnməsini və güvənilir bir şəkildə növbəti uca çatmasını təmin edən bir təhlükəsizlik protokoludur.

Əsas məqsədinə və tələblərinizə bağlı olaraq, fərqli şifrələmə üsullarının kombinasiyasından istifadə edərək məlumatların təhlükəsizliyini təmin edə bilərsiniz. İdeal şifrələmə həllini müəyyənləşdirmək üçün bir təhlükəsizlik mühəndisi və ya məlumat təhlükəsizliyi eksperti ilə əlaqə saxlamaq faydalı ola bilər.

Həssas maliyyə məlumatlarının güvənliyini təmin etmək və yalnız səlahiyyətli personalın buna daxil ola biləcəyi təhlil və analitik platformalarına icazə vermək üçün aşağıdakı strategiyalardan istifadə edə bilərsiniz:

1. Ehtiyatlı məlumat əldə etmə sistemi: Bu sistem, yalnız həssas məlumatlara ehtiyacı olan səlahiyyətli personalın məlumatlara daxil ola biləcəyi bir istifadəçi identifikasiya və autentifikasiya prosesi təklif edir. Bu, bir istifadəçinin məlumatlara giriş üçün doğru kimlik və səlahiyyətlərinə malik olduğunu təsdiqləmək üçün parol, ikinci faktor doğrulama (məsələn, SMS kodu və ya məlumat işləmədən əvvəl parol tələbi) və ya biometrik məlumatlar (məsələn, parmak izi və ya yüz təsdiqi) kimi əlavə məlumatlar istəyə bilər.
2. Rollara əsaslanan məlumat girişi və icazələndirilmə: Məlumatların əlçatanlığını təmin etmək üçün bir rol əsaslı təhlükəsizlik modeli qurmaq faydalı olar. Hər bir istifadəçiyə bir rol təyin edərək, o istifadəçinin giriş icazələrini və yetkiləndirmələrini nəzərdə tutan bir sistem yaradırsınız. Bu, yalnız həssas maliyyə məlumatlarını təhlil etməyə və icazə verməyə səlahiyyətli olan rollara sahib istifadəçilərə məhdudiyyət qoyacaq.
3. Verilənlərə giriş auditləri: Platforma daxil olan bütün istifadəçilərə aid giriş və icazələndirmə hadisələrini qeydə ala bilən bir audit sistemi qurmaq faydalıdır. Bu, məlumatlara kimin giriş etdiyini, hansı tədbirləri həyata keçirdiyini və hər hansısa yanlışlığı aşkar etmək üçün istifadə edilə bilər. Auditlər, məlumatların güvənliyini

təmin etmək və həssas məlumatlara yetkisiz girişi aşkar etmək üçün əhəmiyyətlidir.
4. Əlçatanlıq tədbirləri: Əlavə təhlükəsizlik tədbirləri də əlavə edə bilərsiniz, məsələn, məlumatlara giriş üçün VPN (Virtual Private Network) istifadə etmək, səlahiyyətli personala yalnız təhlükəsiz və şifrələnmiş bağlantılarla məlumat əldə etməyi təmin etmək və həssas məlumatların qorunduğu fiziki server otağını sərhədən çıxarmaq kimi addımlar atmaq.

Bu strategiyalar, həssas maliyyə məlumatlarının güvənliyini təmin etməyə və yalnız səlahiyyətli personalın məlumatları təhlil etməsi və platformalara girişi təsdiqləməsi üçün kömək edəcəkdir. Bunlar sadəcə bazalardır və təcrübəniz və təhlükəsizlik tələblərinizə əsasən daha çox tədbir görməyə ehtiyac duya bilərsiniz.

---

4. **Məxfiliyi qorumaq üçün məlumatların anonimləşdirilməsi və identifikasiya üsullarından necə istifadə etmək olar, eyni zamanda effektiv məlumat təhlili və anlayışların yaradılmasına imkan verir?**

Məxfiliyi qorumaq və məlumatların anonimləşdirilməsi, istifadəçilərin şəxsi məlumatlarını gizlətməyə və anonim olaraq qalmağa imkan verir. Bu, məlumatları təhlil etmək və anlayış yaratmaq üçün əhəmiyyətli bir addımdır. Aşağıda, məlumatların anonimləşdirilməsi və identifikasiya üsullarından bəzilərini təqdim edirəm:

1. Şəxsi məlumatların anonimləşdirilməsi: İstifadəçilərin şəxsi məlumatları, adlar, e-poçt ünvanları, telefon nömrələri kimi şəxsi məlumatları gizlətmək üçün anonimləşdirilməlidir. Məsələn, adları və e-poçt ünvanları yerinə təsadüfi yaratılmış identifikatorlar istifadə edilə bilər.
2. Agregasiya: Məlumatların anonimləşdirilməsi üçün məlumatlar toplanaraq cəmiyyətləşdirilə bilər. Bu, hər bir istifadəçinin məlumatlarının cəmiyyətləşdirilməsi deməkdir və bu yolla təhlil etmək üçün əhəmiyyətli məlumatlar əldə edilə bilər.
3. Məlumatların sahələrə bölünməsi: Məlumatları anonimləşdirmək və təhlil etmək üçün məlumatları sahələrə bölə bilərsiniz. Bu, müxtəlif məlumatlara sahib olan bir sənədin bəzi hissələrini anonimləşdirmək və bu sahələr üzərində təhlil aparmağa imkan verir.

4. De-identifikasiya: Şəxsi məlumatları anonim hala gətirmək üçün de-identifikasiya texnikalarından istifadə edilə bilər. Bu prosesdə adlar, ünvanlar, rəqəmlər və digər şəxsi məlumatlar çıxarılaraq, məlumatlar daha çox anonimləşdirilir.

Bu tədbirlər məxfilik təmin etmək və məlumatların anonimləşdirilməsini dəstəkləmək üçün əlverişli addımlardır. Bununla birlikdə, bu tədbirlər əvvəlcədən planlaşdırılmalı və məxfilik təhlili və anlayışları təşkil etmək üçün yaxşı bir mənbə koddur. Məlumatları anonim hala gətirmək üçün məlumatların sahələrə bölünməsi və de-identifikasiya, effektiv məlumat təhlili və anlayışların yaradılmasını təmin edəcək effektiv addımlardır.

Maliyyə institutlarının müştərilərin məlumatlarını anonimləşdirmək və identifikasiya üsullarından istifadə etməklə məxfiliyi qorumaq, effektiv məlumat təhlili və anlayışların yaradılmasına imkan verir. Aşağıda bu məsələlərə dair əsas prinsiplərə qısaca toxunacağam:

1. Anonimləşdirmə: Müştərilərin şəxsi məlumatlarını anonim hala gətirmək, məlumatların şəxslə əlaqələndirilməsinə imkan verərək, məlumatların məxfiliyini təmin edir. Bu, müştərilərin adını, doğum tarixini, sosial təyinatını və digər şəxsi məlumatları anonim məlumatlara çevirməyi içərir.
2. Identifikasiya: Müştərilərin anonim məlumatlarını onların kimliklərinə əsasən təyin etmək, məlumatların səlahiyyətli şəxslər tərəfindən idarə edilməsini və qorunmasını təmin edir. Bu, müştəri kimlik təyinatı prosesində şəxsiyyət, ünvan, bank hesabı və digər identifikasiya məlumatlarının istifadəsini əhatə edir.
3. Risk qiymətləndirməsi: Müştərilərin anonim məlumatları və identifikasiya məlumatları, məlumat təhlili və anlayışların yaradılması üçün risk qiymətləndirməsinə əsas təşkil edir. Bu, məxfiliyi risklərin təyin edilməsinə və potensial məxfiliyin səbəblərinin və nümayəndələrinin müəyyən edilməsinə kömək edir.
4. İntelligent analitika və texnologiyalar: Anonimləşdirmə və identifikasiya üsulları, effektiv məlumat təhlili üçün istifadə olunan intellektual analitika və texnologiyaların təməlini təşkil edir. Bu, verilərə tətbiq edilən maşın öyrənməsi, analitika alqoritmləri və digər texnologiyaların istifadəsi ilə məxfiliyi risklərini daha yaxşı qiymətləndirməyə imkan verir.

Bu prinsiplər maliyyə institutlarının müştəri məlumatlarının məxfiliyini təmin etmək, məlumat təhlili və anlayışların yaradılmasına imkan verir. Anonimləşdirmə və identifikasiya, məxfiliyi qoruma tədbirləri ilə birgə istifadə olunmalıdır və tətbiqi proses, yerli və beynəlxalq məxfiliyi qaydalarına və tədbirlərinə riayət edilməsi ilə əlaqəlidir. Hər

bir maliyyə institutu, məxfiliyi qoruma və effektiv məlumat təhlili üçün özünə xüsusi bir strateji və proses qurmağa ehtiyac duyacaq.

5. Maliyyə institutunda məlumat elmi və böyük məlumat analitikasının təhlükəsizliyi kontekstində xarici tərəfdaşlar və ya üçüncü tərəf təchizatçıları ilə əməkdaşlıq edərkən hansı mülahizələri nəzərə almaq lazımdır?

Maliyyə institutlarının məlumat elmi və böyük məlumat analitikası ilə əməkdaşlıq edərkən xarici tərəfdaşlar və üçüncü tərəf təchizatçıları ilə işləmələrində təhlükəsizlik məsələlərini nəzərə almaq son dərəcə önəmlidir. Aşağıdakı mülahizələr bu əməkdaşlıq zamanı gözlənilən təhlükəsizlik tədbirləri və məhdudiyyətlər haqqında fikir verə bilər:

1. Rəhbərlik və İdarəetmə: İnstitutun rəhbərlik tərəfindən təhlükəsizlik strategiyalarının və protokollarının düzgün şəkildə müəyyənləşdirilməsi və icrası təmin edilməlidir. Bu, təhlükəsizlik siyasətlərinin müəyyənləşdirilməsi, təhlükəsizlik üzrə məsuliyyətin təyin edilməsi, məlumatın emalında və paylaşılmasında məhdudiyyətlərin qoyulması və yoxlanış tədbirlərinin həyata keçirilməsi kimi məsələləri əhatə edir.
2. Əməkdaşlıq anlaşmaları: Xarici tərəfdaşlar və ya üçüncü tərəf təchizatçıları ilə əməkdaşlıq anlaşmaları hazırlanmalıdır. Bu anlaşmalarda məlumatın paylaşılması, gizlilik, məlumatın saxlanılması və imhası, təhlükəsizlik tədbirlərinin öhdəsində olan tərəflərin məsuliyyətləri kimi məsələlər əhatə edilməlidir.
3. Məlumatın emalı və paylaşılması: Maliyyə institutları, əməkdaşlıq etdikləri tərəflərlə məlumatın emalı və paylaşılması üçün təhlükəsiz kommunikasiya vasitələri və protokolları təyin etməlidir. Bu, şifrələmə, müşahidə, yetkiləndirmə və məlumatın təhlükəsiz saxlanılması tədbirləri ilə əlaqədar olmalıdır.
4. Hüquqi və regulatory tələblər: Xarici tərəfdaşlar və üçüncü tərəf təchizatçıları ilə əməkdaşlıq zamanı maliyyə institutları hüquqi və regulatory tələbləri nəzərə almaq məcburiyyətindədir. Bu, verilənlərin mühafizəsi, məlumatın gizliliyi, müştərilərə aid olan məlumatın qorunması və digər məhdudiyyətləri əhatə edir.
5. Təhlükəsizlik sınaqları və auditlər: Xarici tərəfdaşlar və üçüncü tərəf təchizatçıları tərəfindən təqdim edilən məlumat elmi və böyük məlumat analitikasının təhlükəsizlik səviyyəsi təhlil edilməlidir. Maliyyə institutları, bu tərəflərin təhlükəsizlik tədbirlərinə uyğunluğunu yoxlamaq üçün müvafiq auditləri və sınaqları təşkil etməlidir.

Bu məmulatlar maliyyə institutlarının məlumat elmi və böyük məlumat analitikası ilə əməkdaşlıq etdikləri xarici tərəfdaşlar və üçüncü tərəf təchizatçıları ilə təhlükəsizlik tədbirlərinin yerinə yetirilməsini təmin etmək üçün nəzərə alınmalıdır. Bu, məlumatın təhlükəsizliyini, gizliliyini və müşahidə altında saxlanılmasını təmin etməyə yardım edəcəkdir.