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?

CAVAB:
1.Məlumatın şifrələnməsi: Bütün həssas maliyyə məlumatları, depolanma və keçidlərdən əvvəl şifrələnməlidir.2. Fiziki qoruma: Maliyyə institutları, məlumatların saxlanıldığı server otaqları və mərkəzləşdirilmiş sistemlər üçün fiziki qoruma tədbirləri tətbiq etməlidir.3. İstifadəçi məlumatlarının idarə olunması: Həssas maliyyə məlumatlarına giriş hüququ olan istifadəçilərin məlumatların idarə olunması və giriş nəzarəti üzrə qaydaları izləməsi təmin edilməlidir.4. Fəaliyyət auditləri: Maliyyə institutları, məlumatlara əl çatan və sistemə daxil olan fəaliyyətləri izləmək və audit etmək üçün müvafiq sistemlər qurmaq üçün tədbirlər görməlidir.5. İstifadəçilərin təlimatlandırılması: Həssas maliyyə məlumatlarının qorunması, istifadəçilər arasında dəyərli təlimatlar və məlumat mənbələrinin təmin edilməsi ilə başa çıxılmalıdır.
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?

CAVAB:
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.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.
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?

CAVAB:

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.2. Rollara əsaslanan məlumat girişi və icazələndirilmə: Məlumatların əlçatanlığını təmin etmək üçün bir rol əsaslı təhlükəsizlik modeli qurmaq faydalı olar.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.

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.

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

CAVAB:

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.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.

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?

CAVAB:

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.

1.Rəhbərlik və İdarəetmə: İnstitutun rəhbərlik tərəfindən təhlükəsizlik strategiyalarının və protokollarının düzgün şəkildə müəyyənləşdirilməsi və icrası təmin edilməlidir. 2.Əməkdaşlıq anlaşmaları: Xarici tərəfdaşlar və ya üçüncü tərəf təchizatçıları ilə əməkdaşlıq anlaşmaları hazırlanmalıdır. 3.Məlumatın emalı və paylaşılması: Maliyyə institutları, əməkdaşlıq etdikləri tərəflərlə məlumatın emalı və paylaşılması üçün təhlükəsiz kommunikasiya vasitələri və protokolları təyin etməlidir.4.Hüquqi və regulatory tələblər: Xarici tərəfdaşlar və üçüncü tərəf təchizatçıları ilə əməkdaşlıq zamanı maliyyə institutları hüquqi və regulatory tələbləri nəzərə almaq məcburiyyətindədir. 5.Təhlükəsizlik sınaqları və auditlər: Xarici tərəfdaşlar və üçüncü tərəf təchizatçıları tərəfindən təqdim edilən məlumat elmi və böyük məlumat analitikasının təhlükəsizlik səviyyəsi təhlil edilməlidir.

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.

Ssenari: Səhiyyə Təşkilatında Data Elminin və Böyük Məlumat Analitikasının Təhlükəsizliyinin təmin edilməsi edilməsi Tibbi tədqiqatlar, fərdiləşdirilmiş tibb və xəstələrə qulluq üçün məlumat elminə və böyük məlumat analitikasına əsaslanan səhiyyə təşkilatında xəstə məxfiliyinin qorunması və məlumatların bütövlüyünün qorunması təhlükəsizliyin mühüm aspektləridir.

1. Səhiyyə təşkilatı data elmində və böyük verilənlərin analitika mühitində həssas xəstə məlumatlarına icazəsiz girişin qarşısını almaq üçün möhkəm giriş nəzarətlərini və istifadəçi autentifikasiyası mexanizmlərini necə tətbiq edə bilər?
CAVAB:
1.İstifadəçi kimlik təsdiqləmə: İstifadəçilərin sistemə daxil olarkən özlərini təsdiq etmələri üçün istifadəçi adı və şifrə kimi məlumatların tələb olunması. 2.İki faktorlu autentifikasiya (2FA): İstifadəçilərin sistemə giriş zamanı, birinci faktor kimi şifrəni daxil etmələri tələb olunur və ikinci faktor kimi telefonuna göndərilən təsdiqləmə kodunu daxil etməlidirlər. 3.Ehtiyatkarlıq prinsipi: Yalnız sistemə icazəli olan istifadəçilərə məlumatlara giriş vermək. İstifadəçilərin rollara və icazələrə əsasən tənzimlənmiş bir hiearxiya sistemi ilə icazələrin idarə edilməsi.4.Girişə dair sərhədləndirmələr: Sistemə icazəsiz girişləri aşkarlamaq üçün mümkün olan bütün giriş mərhələlərində sərhədləndirmələr tətbiq edilməlidir.5.Verilənlər şifrələnməsi: Həssas məlumatların saxlanması və göndərilməsi zamanı verilənlərin şifrələnməsi tətbiq edilməlidir. Bu, məlumatların yalnız icazəli şəxslər tərəfindən oxunabiləcəyini təmin edir.// Bu tədbirlər, səhiyyə təşkilatlarının həssas xəstə məlumatlarının təhlükəsizliyini təmin etmək üçün əsaslı bir zəmin yaradacaq.

2. Məlumat elmində və böyük məlumat analitikası infrastrukturunda saxlama, ötürmə və emal zamanı xəstə məlumatlarını qorumaq üçün hansı şifrələmə üsullarından istifadə edilə bilər?
CAVAB:
1.Simmetrik şifrələmə: Simmetrik şifrələmədə eyni açıq mətn şifrəyə çevrilmək üçün istifadə edilir. Şifrələmə və deşifrələmə üçün eyni gizli açar (şifrələmə açarı) istifadə olunur. Səhiyyə təşkilatları AES kimi güclü simmetrik şifrələmə alqoritmlərindən istifadə edə bilər.2.Asimetrik şifrələmə: Asimetrik şifrələmə, şifrələmə və deşifrələmə üçün fərqli açarlar istifadə edən bir şifrələmə metodudur. Bu metodda, məlumatı şifrələmək üçün bir açıq açar (şifrələmə açarı) və şifrəni deşifrə etmək üçün fərqli bir gizli açar (deşifrə açarı) istifadə olunur. 3.Hash funksiyaları: Hash funksiyaları, verilənlərdən sabit uzunlukda bir məlumat qüvvətlənməsi üçün istifadə edilir. Məlumatın daxil olunan məlumatlarından asılı olaraq sabit uzunlukda bir hash dəyəri yaradır. Hash funksiyaları, məlumat tam təsdiqlənməsində və bir məlumatın orijinalliğinin yoxlanılmasında istifadə olunur. \\Səhiyyə təşkilatları, məlumat elmində və böyük məlumat analitikası infrastrukturunda məlumatların qorunması üçün şifrələmə üsullarından bir və ya bir neçəsindən istifadə edərək məlumatların gizliliyini və məlumat tamamlığını təmin edə bilərlər. Bu, səhiyyə məlumatlarının istifadəsi və paylaşılması üçün təhlükəsiz bir mühit yaratmağa kömək edəcək.

3. Səhiyyə təşkilatı məlumatların məxfiliyini və təhlükəsizliyini qoruyarkən müxtəlif qurumlar üzrə xəstə məlumatlarını təhlil etmək üçün təhlükəsiz çoxtərəfli hesablama və ya federasiya edilmiş öyrənmə yanaşmalarından necə istifadə edə bilər?
CAVAB:
Səhiyyə təşkilatları, məlumatların məxfiliyini və təhlükəsizliyini qoruyarkən müxtəlif qurumlar üzrə xəstə məlumatlarının təhlilini həyata keçirmək üçün təhlükəsiz çoxtərəfli hesablama və federasiya edilmiş öyrənmə yanaşmalarından istifadə edə bilərlər. Təhlükəsiz çoxtərəfli hesablama, fərqli təşkilatlar arasında məlumatları bölüşmək və əməliyyatları həyata keçirmək üçün bir yoludur. Bu yanaşmada, hər bir təşkilat öz məlumatlarını şifrələyir və digər təşkilatlara göndərir. Digər təşkilatlar gələn məlumatları deşifrə edərək üçüncü tərəflərə məxfi məlumatları ifşa etmədən təhlil etmək üçün işləmələri icra edir. Bu yolla, təşkilatlar arasında əlaqələr təhlükəsiz və məxfi qalır.Federasiya edilmiş öyrənmə isə bir başqa yanaşmadır ki, fərqli təşkilatlar üçün məlumatların bir araya gətirilməsini və birgə öyrənməni təşkil edir. Burada, hər bir təşkilat öz məlumatlarını öyrənmə modelində təhsil edir və sonra bu modeli bir birinə verməklə digər təşkilatlar da öz məlumatlarını əlavə edir. Beləliklə, birlikdəki məlumatlar bir araya gəlir və daha geniş bir öyrənmə modeli formalaşır. Bu yanaşma, təşkilatlar arasında məlumat paylaşımını minimal səviyyəyə endirir və hər bir təşkilatın məlumatlarının məxfiliyini qoruyur.

4. Məlumat elmi və böyük məlumat analitikası təhlükəsizliyi kontekstində HIPAA kimi səhiyyə qaydalarına uyğunluğu təmin etmək üçün hansı siyasət və prosedurlar müəyyən edilməlidir?
CAVAB:
Məlumat elmi və böyük məlumat analitikası təhlükəsizliyi kontekstində HIPAA (Health Insurance Portability and Accountability Act) tələblərinə uyğunluğu təmin etmək üçün aşağıdakı siyasət və prosedurlar müəyyən edilməlidir:1.Məlumatların müstəqil olması: Müəyyən bir sistemə daxil olan səhiyyə məlumatları, digər sistemlərdən asılı olmayan və təmsil edən şəxs və ya təşkilatın məlumatına əsaslanan müstəqil bir formada saxlanılmalıdır.2.Məlumatların şifrələnməsi: Səhiyyə məlumatları və böyük məlumat analitikası təhlükəsizliyi üçün ən yaxşı təhlükəsizlik tədbirlərindən biri məlumatların şifrələnməsidir. Məlumatlar, əgər zərər görülərsə onlardan yararlanmaq imkanını məhdudlaşdıran şifrələnmə metodu ilə təhlükəsiz bir şəkildə saxlanılmalıdır.3.İstifadəçi hüquqlarının idarə edilməsi: Səhiyyə məlumatlarına girişin idarə edilməsi, yalnız icazəli və tələb olunan şəxslərin bu məlumatlara giriş etməsinə imkan verən siyasət və prosedurlar təyin edilməlidir. Bu, məlumatların yalnız lazım olan personel tərəfindən istifadə olunması və müəyyən bir məqsədə xidmət etməsi məqsədilədir.

5.Səhiyyə təşkilatının məlumat elmi və böyük məlumat analitikası mühitində məlumat pozuntularını və ya icazəsiz fəaliyyətləri aşkar etmək və qarşısını almaq üçün məlumatların auditi və monitorinq mexanizmləri necə həyata keçirilə bilər?

CAVAB:

Səhiyyə təşkilatları məlumat elmi və böyük məlumat analitikası ilə məlumat pozuntularını və icazəsiz fəaliyyətləri aşkar etmək və qarşısını almaq üçün bir neçə məlumat audit və monitorinq mexanizmlərindən istifadə edə bilərlər. Aşağıda bu mexanizmlərə nümunələr verilmişdir:

1.İstifadəçi hüquqlarının nəzarəti: Məlumat pozuntularını aşkar etmək üçün, səhiyyə təşkilatları məlumat sistemlərində istifadəçilərə verilən hüquqları nəzarət altında saxlamaq üçün uyğun tədbirlər almalıdır. Hər bir istifadəçiyə yalnız lazım olan məlumatlara giriş imkanı verilməli və bu girişlərə nəzarət edilməlidir.2.İcazə və hesabatlılığın təminatı: Məlumat pozuntularını aşkar etmək üçün, səhiyyə təşkilatları məlumat sistemlərində icazələr və hesabatlılıq qaydalarını tətbiq etməlidir. Hər bir istifadəçiyə yalnız lazım olan məlumatlara icazə verilməlidir və hər hansı bir məlumat pozuntusu hallarında hansı istifadəçilərin hansı məlumatlara giriş etdiyi izlənə bilər olmalıdır.3.Müəyyən edilmiş monitorinq və audit prosedurları: Məlumat pozuntularını aşkar etmək və qarşısını almaq üçün, səhiyyə təşkilatları monitorinq və audit prosedurları təyin etməlidir.