

ИНФОРМАЦИОННАТА СИГУРНОСТ В СИСТЕМИТЕ ЗА ПЛАНИРАНЕ НА КОРПОРАТИВНИ РЕСУРСИ /ERP/

INFORMATION SECURITY IN ENTERPRISE RESOURCES PLANNING SYSTEMS /ERP/

P. ХРИСЧЕВ

Технически Университет-София, филиал Пловдив, ул.Цанко Дюстабанов, 25, 4000 Пловдив, hrischev@tu-plovdiv.bg

Резюме: This paper introduces Enterprise Resource Planning (ERP) systems from its evolution through architecture to its products regarding the security point of view. ERP is a technology that integrates most business processes and covers all information flows in the organization. ERP is a prerequisite and tool with which the enterprise can automate its core business activities, reduce the complexity and cost of their interaction, force the company to start reengineering business processes to optimize its work and generate a successful business. But modern business is more and more open to communication with external organizations, especially through the Internet. Therefore ERP system is becoming a system with high vulnerability and high confidentiality, in which security is a critical aspect. The main characteristics of ERP systems are presented. The largest ERP vendors have already integrated their security solutions; many vendors are using specialized hardware and software solutions. The new e-business requires the development and implementation of e-features of ERP systems (e-orders, e-shop, e-store, e-invoice, etc.), focuses on business between companies and customers. New technologies - Cloud computing, IoT, Block Chain are opportunities to make ERP highly integrated, more intelligent, more collaborative, cloud-based. Based on the literature of the biggest developers of this type of systems are presented popular security solutions for ERP systems. The standard architecture of the systems, the security policies guaranteeing secure access to the information are presented. Methods for data transfer with remote access to the systems are considered. The evolution of database development from structured /SQL/ via unstructured /NoSQL/ to blockchain is shown. The methods for ensuring secure access to user information used by the developers of ERP systems, such as permissions, roles, authentication, are summarized. The main challenges to information security and the prospects for ensuring data security are outlined.

Ключови думи: ERP systems, data security, security policy

ВЪВЕДЕНИЕ

Системите за планиране на корпоративни ресурси, познати като Enterprise Resource Planning (ERP), като подход за пълна бизнес интеграция, са широко внедрени в почти всички видове на обществената дейност – производство, услуги, администрация, отбрана, обучение. През 1990 г. Gartner Group за първи път ги определя като следващо поколение софтуер за бизнес производство и софтуер за планиране на производствени ресурси, а днес ERP системите се превърнаха в необходима предпоставка за успешното развитие на бизнеса. ERP системите са интегрирани, конфигурируеми и гъвкави информационна системи, която планират, управляват и оптимизират всички ресурси и процеси в организацията [1]. С ERP предприятието може да автоматизира основните си бизнес дейности, да намали сложността и цената на взаимодействието им, да принуди самото предприятие да започне реинженеринг на бизнес процесите, за да оптимизира работата си и да генерира успешен бизнес. В съвременния динамичен свят често успешното внедряване на ERP система е въпрос на оцеляване и просперитет. Целта на статията е да се направи преглед на състоянието на технологията на ERP системите и перспективите на развитие в светлината на информационната сигурност.

ПРЕГЛЕД НА ERP ТЕХНОЛОГИЯТА

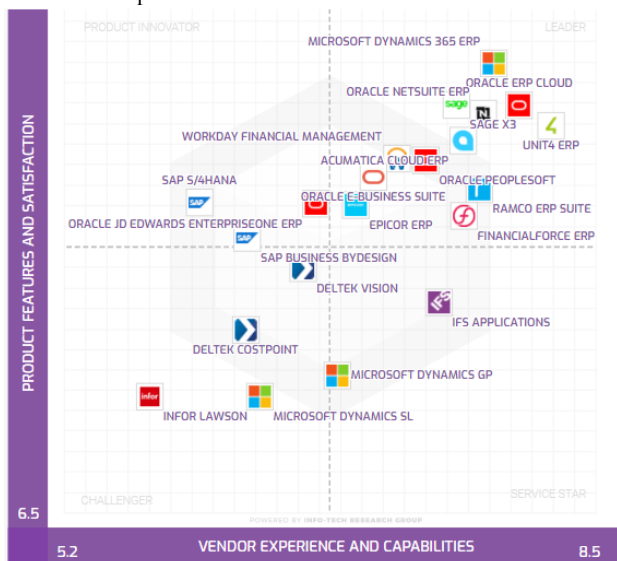
ERP системите обхващат всички или почти всички информационни потоци в организацията. Те представляват най-високото ниво на развитие на информационните системи. В основата на ERP системите е клиент-сървърната технология. Най-разпространените ERP системи са от типа централизирани информационни системи и в основата им са централизираните приложения и бази данни. ERP системите се развиват стремително през годините. Първоначално системи с такива функционалности се разработваха на местно ниво от ИТ специалистите в организацията и/или външни фирми за управление на базови бизнес функции като счетоводство, планиране, управление на складовете и на човешките ресурси. Използваха се различни технологии, програмни езици и бази данни, което затрудняваше интегрирането им. Разработваха се сложни и не винаги стабилно работещи интерфейси. Освен това, отделните системи се различаваха технологично една от друга, което затрудняваше неизмерно ефективното адаптиране към промените и надграждането на бизнеса. Масовото внедряване на ERP системите започна, когато компании като IBM, SAP и BAAN разработиха набор от типични приложения като компоненти за ERP системи, обособени в относително самостоятелни модули.

С изграждането на устойчива ИКТ инфраструктура и ERP функционалности, капсулирани в типични стандартни компоненти - модули, ERP системите вече не само отстраняват тетнологичните проблеми пред интеграцията, но и отговарят на новите динамични изисквания на бизнеса. Не само това, внедряването на унифицирани системи за управление на бизнеса, доведе до оптимизиране на бизнес процесите, особено в големите и сложни компании и организации.

Технологии като Web Services оказаха голямо влияние върху ERP системите. Новите системи използват защитени бази данни и приложения, базирани в Интернет. Вече сме в етап на внедряване на нови, облачно базирани ERP системи, такива като SAP S/4 HANA. Те предоставят нови мощни инструменти за управление на база проблемно ориентирана обработка на огромни бази от данни. Това е резултат от революционното навлизане във всички сфери на човешката дейност на нови концепции и технологии като Cloud Computing, IoT, Big Data.

Все повече фирми представят на пазара свои разработки с подобни функционалности, някои от тях с отворен код [2]. Български компании успешно разработват и внедряват свои продукти, например българската bgERP предлага пълна функционалност на платформа с отворен код [3].

През октомври 2019 година списание Форбс [4] публикува проучване на SoftwareReviews относно удовлетвореността на потребителите на ERP системи, резултатите от което са показани на фиг.1.



Фиг.1 Проучване на удовлетвореността на потребителите на ERP системи в световен мащаб

Един от критериите за формиране на тази удовлетвореност е информационната сигурност. Фокусът върху този критерий е една от причините четири големи компании да доминират в този бързорастящ сектор на информационните технологии - SAP, Oracle, PeopleSoft и JD Edwards с повече от половината пазарен дял.

Типичната съвременна ERP система носи следните типови характеристики [5]:

1. Компонентност или модулност, т.е. всички различни бизнес функции трябва да бъдат проектирани като различни относително самостоятелни компоненти.
2. Интегрираност. Компонентите са интегрирани и безпроблемният поток от данни между компонентите

им позволява да взаимодействат като една функция. Компонентите са свързани чрез стандартни интерфейси.

3. Гъвкавост. Системата трябва да е разширяема и съвместима със старите системи, промяната в бизнес процесите и стратегиите е лесна за изпълнение.
4. Мащабируемост. ERP системата трябва лесно да се конфигурира и преконфигурира според нуждите на предприятието. Това е особено важно при работа в корпоративна среда.
5. Компонентите на системата трябва да работят в реално време, като трябва да са достъпни онлайн.
6. ERP системата трябва да има потенциал да минимизира разходите и увеличаване печалбата. Това е основно изискване за функциониране на организацията и основа на мотивацията на компанията.
7. Сигурност. Най-ефективните методи за сигурност в информационните системи трябва да бъдат прилагани и постоянно актуализирани.
8. Ефективно внедряване и поддръжка. Доставчикът на системата трябва да разполага с механизми и структура за бързо, оптимално и гарантирано внедряване на системата.
9. Трябва да бъдат разработени и инструменти за контролиране на ефективността на работата, отстраняване на възникващи проблеми и постоянно обновяване на инсталираните модули.

Структурата на ERP системата и тези особености определят методите за повишаване на информационната сигурност.

ИНФОРМАЦИОННА СИГУРНОСТ В ERP СИСТЕМИТЕ

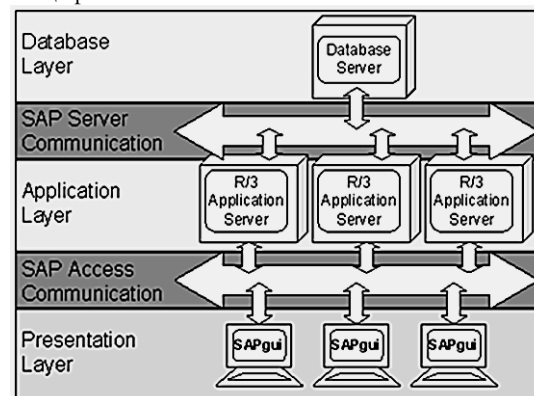
Информационната сигурност е от решаващо значение за ERP системите, тъй като те се използват и в редица опасни в глобален мащаб индустрии, например химическо производство, енергетика, металургия; в медицината, финансовите услуги и отбраната.

Първостепенна задача е разработката на адекватна и детайлна политика и модел на сигурност за ERP системите. Ще разгледаме методите на обезпечаване на информационната сигурност започвайки от архитектурата, през трансфера на данните до политиките и функциите за разрешаване и гарантиране достъпа до информация.

В основата е архитектурата на системите.

Трислойна архитектура на ERP системи

ERP системите използват клиент/сървър архитектура, за да създадат разпределена изчислителна среда. Използва се архитектура, която съдържа три логически слоя. Този тип архитектура дава възможност за гарантиране на сигурността на информацията, използвайки различни специфични за всеки слой технологии.



Фиг.2 Трислойна архитектура на SAP R / 3 [6]

На фиг.2 е представена трислойната архитектура на SAP R/3. Тя съдържа:

1. Презентационен слой (FrontEnd). Това е отдалечен /дистанционен/ терминал, хардуерен или виртуален; унифициран графичен потребителски интерфейс (GUI) или браузър /или приложение за браузър/, който събира входящата информация, генерира заявки и връща резултатите от обработката на потребителя или машината.
 2. Приложен слой. Тук са приложните програми, които събират заявките от презентационния слой и обработват данните въз основа на правилата, функциите или логиката на бизнеса.
 3. Слой на базата данни (BackEnd). Системата за управление на базите данни /DBMS/, която управлява оперативните и бизнес данни в организацията и достъпа на потребителя до тази информация, съгласно дефинираните и конфигурирани разрешения за достъп и работа. Този слой включва и операционната система и свързания хардуер, локален или облачен, като базови елементи на системата. Това е основата на ERP системата, платформата за обмен на информация и винаги се внедрява преди имплементирането на модулите на ERP системата. Например, за SAP R/3 това е SAP Net Weaver [6].
- Проблеми със сигурността съществуват във всеки слой на ERP системата. Презентационният слой се отнася до графичния потребителски интерфейс, браузърите и устройствата за достъп – компютри, смартфони, терминали и др. Тъй като предаването на GUI пакети е невъзможно да се ограничи, защитата се реализира като се регламентира достъпа на потребителя до GUI с роли, профили, пароли. По-добрият начин за осигуряване на сигурност може да бъде поставянето на CITRIX сървър между потребителя и ERP системата [7]. Същността на използване на CITRIX се състои в създаване на CITRIX виртуална десктоп инфраструктура /VDI/.

Методи за сигурен трансфер на данни в ERP системите

Първите ERP системи работеха в затворена среда и най-използваната технология за сигурност беше изолиране, отначало физическо, а после и логическо, и сегментиране на мрежите. Големите компании използваха наети линии за свързване на клиентите със системите. С разработването на Web-базирани ERP системи започнаха да се използват и съвременни методи за защита на информация, като например протокола за мрежова сигурност IPsec (Internet Protocol Security). IPsec, известен още като IP Security протокол, определя архитектурата на услугите за сигурност за мрежовия трафик. IPsec описва рамката за осигуряване на сигурност и набор от протоколи, създадени да осигурят тази сигурност, чрез удостоверяване и криптиране на IP мрежови пакети. IPsec се използва за защита на преноса на данни в ERP системите чрез настройка на свързаност с помощта на тунелиране, при което всички данни, изпращани между две крайни точки са кодирани. Установява се пренос на данни във виртуална частна мрежа (VPN). VPN технологията е ефективен начин за защитен трансфер на данни през жични и безжични мрежи.

Политики на сигурност и методи за обезпечаване на сигурен достъп до информация

Гарантирането на сигурността на данните в ERP включва следните аспекти:

1. Политики на сигурност /Security policy/. Политиките за сигурност регламентират правилата за достъп и трансфера на данни. Администраторите на системата разрешават/блокират разрешенията на потребителите.

2. Удостоверяване /Authentication/. Основната цел на удостоверяването на потребителя е да се провери дали потребителят е едно и също лице с предоставено разрешение за достъп до данни.
3. Разделяне /Separation/. Задачите могат да се изпълняват само от определени потребители.
4. Авторизацията /Authorization/. Разрешението за употреба проверява дали потребителят има достъп до съответните ресурси.
5. Ограничаване на времето /Time restriction/за достъп. Разрешаването на работа е допустимо само през определеното работно време.
6. База данни Сигурността на данните обезпечава точността на данните и проследява и записва тяхната промяна във времето. Данните трябва да бъдат архивирани с възможност за бързо възстановяване в случай на аварии. Съвременните информационни технологии обезпечават онлайн бекъп на данните.

Като цяло се нуждаем от пълна сигурност за ERP системите на всички етапи на събиране, съхранение и обработка на информацията на всички нива на системата.

Политика за сигурност за ERP системите

Голяма част от акцентите върху сигурността на ERP бяха поставени върху поверителността на информацията. Трябва обаче да включим и други видове политики, защото основната цел на ERP системите е интегриране и споделяне на информация. Например:

1. Need-to-know policies – политики за необходимост от знание. Това са политики, при които се предоставя достъп до данни въз основа на изискването потребителят да знае или не някаква информация.
2. Need-to-share policies – политики за необходимост от споделяне. Тези политики определят нивото на обмен на данни в една организация.
3. Trust policies - политики за доверие. Тези правила гарантират, че данните се споделят само между доверени организации или потребители.
4. Integrity policies - политики за интегритет. Това означава, че данните се променят само от оторизирани потребители.

По същество ERP системата трябва да имплементира и налага различните политики. В зависимост от конкретното приложение на ERP системата, то и политиките за сигурност и методите за реализирането им са различни.

Автентикация - удостоверяване на потребителя и роли

Много от съвременните системи са базирани на ролево контролиран достъп - Role-Based Access Control /RBAC/.

Ролево контролираният достъп се състои от следните компоненти:

1. Разрешения /Permissions/. Разрешението е достъпът до един или повече обекти в системата. За базата данни разрешението се отнася до правата за събиране, избор, актуализиране, изтриване или вмъкване на запис.
2. Роли /Roles/. Ролята е определена работна функция в организацията - йерархична или не.
3. Потребители /Users/. Потребителят е човек, устройство, система, на когото може да бъде възложена една или повече роли. При това потребителите наследяват политиките на всяка отделна роля.
4. Ограничения /Constraints или Restrictions/. Отговорни за ограниченията на потребителите са администраторите, които настройват правата в зависимост от таблицата на отговорностите.

Упълномощаване /Authorization/ като процес

Процесът на упълномощаване е различен за различните фирми, разработчици на ERP системи и е важна част от сигурността. Например, процесът на разрешаване на достъпа в SAP R/3 се състои от следните понятия:

- Главен запис за потребителя /user master record/, който дефинира ролята на потребителите в процеса на работа с транзакциите и данните;
- Обект за упълномощаване, който представлява формализирана рамка на концепцията за разрешение и съдържа полета на разрешение;
- Профил за ауторизация, който съдържа разрешения, които са назначени на потребителя от администратора;
- Проверка на ауторизация, която се използва за защита на избраните транзакции или данни и е вградена в логиката на програмата.

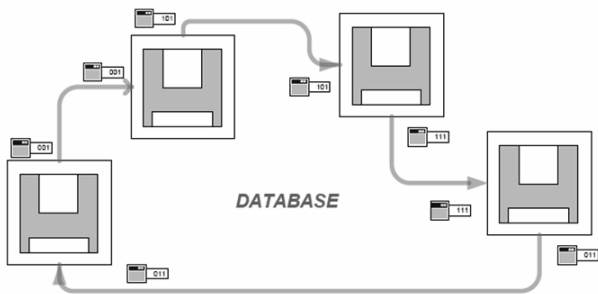
Друга важна концепция в разрешението на достъпа в SAP R/3 е начина на администриране на разрешенията, което означава създаването, генерирането или възлагането на разрешение. Може да е централизирано или децентрализирано (с един или повече администратори). Контролирането и записването на влизанията в системата също е необходим компонент за сигурността на приложния слой на ERP системата.

Бази данни на ERP системите – еволюция и сигурност

Повечето ERP системи в момента използват централизиран бази данни. Според организацията на данните могат да бъдат класифицирани два типа бази данни - релационни и нерелационни. Повечето ERP системи използват SQL /Structured Query Language/ релационни бази данни. Поддръжката на дадения модел за съхранение, структурата и управлението на данните се извършва от системата за управление на бази данни (СУБД). Използват се най-вече Microsoft SQL Server и Oracle релационни бази данни.

NoSQL бази данни се появиха в началото на 21 век. Те са резултат от необходимостта от управление на големи обеми информация в съвременните Web и мобилни приложения. NoSQL бази данни се използват при работа с Web приложения в реално време. Най-новите версии на ERP системите използват NoSQL бази данни, например, SAP HANA.

В момента най-големите доставчици на ERP системи на SAP [6] и IBM [8] работят по използването на нови бази данни, базирани на технологията blockchain. Blockchain е растящ последователен списък на криптирани документи, които се наричат блокове, свързани помежду си, но разположени на различни места и носители. Всеки блок съдържа криптографски хеш на предишния блок, времева марка и данни за транзакциите - фиг.3.



Фиг.3 Илюстрация на blockchain технологията

С такъв дизайн, blockchain е технология за изграждане на бази данни с високо ниво на сигурност. Това може да бъде бъдещето на организацията на базите данни на ERP системите. Възникват обаче юридически въпроси, свързани особено с националното законодателство.

БЪДЕЩЕТО НА ERP СИСТЕМИТЕ И ИНФОРМАЦИОННАТА СИГУРНОСТ

В наши дни ERP системите се превръщат в ядрото на бизнеса в много компании. Големите и сложни бизнес системи не могат да съществуват ефективно без ERP системи. Затова и сигурността на ERP системите ще бъде условие за съществуването и развитието на бизнеса.

Бъдещите ERP системи добавят към традиционните и нови функции:

1. Хетерогенност. Това означава, че компонентите от различни доставчици работят в единна ERP система. За тази цел доставчиците разработват сигурни комуникационни платформи и стандартни защитени интерфейси за пренос на данни.
 2. Колоборативност или сътрудничество. Можем да класифицираме бизнес процесите в две основни групи. Първите са вътрешно-ориентирани процеси, например счетоводство, или управление на веригата на доставки. Втората е основана на взаимодействието в Интернет, например електронната търговия, а сигурността е основното изискване за всички Интернет базирани или свързани системи.
 3. Интелигентност. ERP системата в бъдеще ще включва повече компоненти, които правят анализи, проучвания или дори съвети и предложения за стратегическа трансформация на бизнеса. Елементите на Изкуствен Интелект /Artificial Intelligence/ ще бъдат интегрирани в ERP системите.
 4. Безжична свързаност в ERP системите. Наблюдаваме три различни аспекта:
 - Достъп до ERP системата от мобилни устройства;
 - Трансфер на данни с помощта на бързи безжични мрежи, например 5G, част от концепцията Интернет на нещата /IoT/;
 - Разпределени облачно базирани и с динамична организация бази данни и приложения.
 - Облачно базирани приложения за обработка на огромни масиви данни с цел анализ и генериране на оптимални решения по зададен критерий.
- Но за всички аспекти има едно общо изискване - сигурност.

ЗАКЛЮЧЕНИЕ

Планиране на ресурсите в предприятието е технологията, която задвижва реформацията в сферата на икономиката и влияе положително върху живота на хората. ERP системата сега се трансформира в система с повече координация, висока хетерогенност и интегритет, по-интелигентна, работеща на ниво знания, базирана на облачни технологии и бърза безжична връзка.

Системите и политиките за сигурност на ERP системите се развиваха паралелно с развитието на системите за управление, но повечето от решенията се основаваха на предположението, че ERP системата е затворена информационна среда. Настоящите тенденции са към отваряне на ERP системите и работа в Интернет. Ето защо се нуждаем от нови решения, нови технологии и инструменти за обезпечаване сигурността на системите.

Можем да очертаем перспективите на развитие на информационната сигурност на ERP системите:

1. Разработка на нови политики, модел и дизайн на архитектурата за обезпечаване сигурността на информацията.
2. Проучване на сигурността на интерфейсите между различни компоненти - операционните системи, базите данни, приложенията, модулите и комуникационните платформи.
3. Развитие на технологиите за защита на обменяните данни и документи.
4. Защита на управлението и споделянето на знания.
5. Защита на Web базираните услуги и приложения чрез разработка на нова web ориентирана архитектура.
6. Нови методи за автентикация и ауторизация на потребителя в отворена Интернет среда.
7. Осигуряване на безопасен трансфер на данни в жични и безжични комуникации.
8. Разработване на методи, базирани на Изкуствен интелект, за актуализиране на технологиите за защита на данните.

ЛИТЕРАТУРА:

1. Bakry, A. H. and Bakry, S. H. (2005). "Enterprise resource planning – a review and a STOPE view," International Journal of Network Management 15. pp. 363-370.
2. Stoilov T., K.Stoilova. Functional Analysis of Enterprise Resource Planning Systems. Proceedings of International Conference Computern Systems and Technologies "CompSysTech 2008", Gabrovo, Bulgaria, 2008, ISBN 978-954-9641-52-3, p.IIIВ.8-1 – IIIВ.8-6.
3. bgERP official site <https://bgerp.com/>
4. Forbes, Oct 22, 2019 <https://www.forbes.com/sites/louiscolumbus/2019/10/22/which-erp-systems-are-the-most-popular-with-their-users/?sh=3f88050d19da>
5. R.Hrishev, Planning and implementation of the ERP system in packaging production, Seventh International Scientific Conference "Engineering, Technologies and Systems", TECHSYS 2018, 17-19 May, Plovdiv, ISSN Online: 2535-0048.
6. SAP official site <https://help.sap.com/>
7. CITRIX official site <https://www.citrix.com/>
8. IBM official site <https://www.ibm.com/blockchain>