Business essays – common business applications flashcard

ASSIGN BUSTER

Contents

Common Business Applications

Procuring Common Business Applications

Research Undertaking

Losing 1000000s of dollars because Bank of America’s recognition card database was vulnerable to a default login and watchword should merely be a bad dream for the alone security decision maker and ne’er the alibi you give the foreman after happening out 1000000s of dollars has been falsely charged to your clients recognition cards.

Procuring common concern applications is one of the most of import determinations any size company will of all time hold to do in the 21 st century. To to the full understand the thought of procuring common concern applications we will discourse the different types of concerns and their common concern applications. Next we will reply the inquiry of why we need to procure common concern applications and the common methods used to procure them in each type of concern.

The constructs behind procuring concern applications to include web, database, electronic mail, and de-militarized zone (DMZ) services will besides be presented. Following up behind the current constructs of procuring concern applications will be the tendencies to today in the industry of security as related to concern applications.

By analyzing Security Software Development Life Cycle (SecSDLC) we can understand the procedure and processs used to procure common concern applications along with the Enterprise Information Security Policy (EISP) . Finally we will research the functions of security in the hereafter and predict the function of security related to concern applications.

- What types of concerns are out at that place?
- What are common concern applications?
- Why do we necessitate to procure common concern applications?
- What are the common methods to procure common concern applications in each type of concern?
- What are the constructs of procuring concern applications for web, database, electronic mail, and DMZ waiter services?
- What are the current tendencies in procuring concern applications?
- What are SecSDLC and EISP?
- What is the function of security in the hereafter?
- What anticipations can be made of the function of security related to concern applications for the hereafter?

Any lawfully recognized organisational entity which provides goods and services to consumers or a corporate group like authoritiess, non-profit charities is a concern. The chase of concern is to gain a net income, to which most are in private owned to increase the net incomes to the proprietors. The proprietors and operators of a concern must bring forth a fiscal return in permutation of work and possible accepted hazard. Because a concern needs to accept some hazard security is enacted to guarantee the concern survives.

The types of concerns are classified in many ways. A common method of categorization is that of primary profit-generating activities. For case, makers produce merchandises, from natural stuffs, and so are sold for a net income. Companies that make physical goods, such as autos or pipes, are considered makers. Service concerns offer intangible goods or services and typically bring forth a net income by bear downing for labour or other services provided to authorities, other concerns or consumers.

Organizations runing from house interior designers to confer withing houses to eating houses and even to entertainers are types of service concerns. Retailers and distributers act as middle-men in acquiring goods produced by makers to the intended consumer, bring forthing a net income as a consequence of supplying gross revenues or distribution services. Most consumer-oriented shops and catalogue companies are distributers or retail merchants. Agriculture and excavation concerns are concerned with the production of natural stuff, such as workss or minerals.

Fiscal concerns include Bankss and other companies that generate net income through investing and direction of capital. Information concerns generate net incomes chiefly from the resale of rational belongings and include film studios, publishing houses and packaged package companies. Utilities produce public services, such as heat, electricity, or sewerage intervention, and are normally authorities chartered. Real estate concerns generate net income from the merchandising, leasing, and development of belongingss, places, and edifices.

Transportation system concerns deliver goods and persons from location to location, bring forthing a net income on the transit costs. What ties these sorts of concern together? As you will see in the following paragraph it is all about the sections in which the concern uses to finish the concerns demands.

What do all of these different types of concern have in common? The sections that maintain and operate the overall concern units on a uninterrupted graduated table. For illustration, accounting which is typically responsible for fiscal coverage, fiscal controls and the elevation of the capital necessary to run the concern. Human resources section which is typically responsible for hiring, fire, paysheet, benefits, etc. The following are more illustrations of what all concern normally have in common:

- Selling and gross revenues – responsible for selling the concern ' goods or services to the client and for pull offing the relationships with the client
- Marketing – Typically responsible for advancing involvement in, and bring forthing demand for, the concern ' merchandises or services, and positioning them within the market
- Gross saless – happening likely buyers and obtaining their understanding (known as a contract) to purchase the concern ' merchandises or services.

- Operationss – makes the merchandise or delivers the service.
- Production – produces the natural stuffs into the delivered goods, if they require processing.
- Customer service – supports clients who need aid with the goods or services
- Procurement – responsible for geting the goods and services necessary for the concern.
- Buying – processes the purchase orders and related minutess.
- Research and Development – trials to make new merchandises and to find their viability (e. g. pilot workss) .
- Information Technology – manages the concern ' computing machine and informations assets
- Communications/Public Relations – responsible for pass oning to the outside universe
- Administration – provides administrative support to the other sections (such as typewriting and filing)
- hypertext transfer protocol: //en. wikipedia. org/wiki/Business

As you can see there are many specific maps concerns need to hold in order to run. Each map needs some sort of computing machine application resource to utilize. Without procuring those applications the concern jeopardizes its net incomes. As stated in the following subdivision we will discourse the types of concern applications that each section might utilize or meet as portion of the day-to-day work rhythm.

The sort of common concern applications we are speaking about in the above subdivisions can be categorized by the concern functionality from an endeavor position and it can besides be categorized based on how and where they run.

Application classification based on the concern functionality

Business to Customer (B2C) Applications. These are in general client facing applications. Most of these are web/browser based applications. It includes dynamic content based web sites. Some of these applications can be client based application that needs to be installed on client ' s computer science device (laptop/desktop) .

Examples include telling system, client support system, net sites supplying merchandise information, applets/Active-X lightweight clients, and clients that are installed on client devices.

Business to Business (B2B) Applications. These applications are used between concern spouses like providers, resellers etc. Traditionally these applications are accessed utilizing dedicated lines between concern spouses.

Recently many of these applications straight use Internet with security characteristics such as VPNs. Many of these applications are based on SOA (service oriented architecture) and leverage web-services. Examples include parts telling and position system, and bulk order entry web service.

Internal Applications. These applications are used within the organisation (Intranet) and are non exposed or available to the outside endeavor. These include web based applications every bit good as desktop applications such as electronic mail and instant messaging. Examples include HR systems, internal fiscal, IT Desktop support system, and email clients.

Application classification based on how and where they run

Front-End Applications. These are the applications that interact with users through GUI such as browser, desktop client etc. Examples include order position look intoing system and email clients.

Background Applications. These applications do non straight interact with the user. These are typically background procedures and occupations. Examples include background order proof and occupation every night data synchronism books. hypertext transfer protocol: //www. owasp. org/index. php/Definition_for_common_business_applications

As these types of common concern applications addition in industry standardisation and go more widely used the strong our security execution will hold to be. So why do we necessitate so much security in our common concern applications if they are merely traveling to be used for good? Well as the following subdivision will turn out common concern applications are non ever used for good in fact more so non they are used for bad.

External hackers, malicious employees (internal menace) , organized offense, concern competition, along with stolen informations, individuality larceny, informations breach, hijacked personal information are merely some of the ingredients needed to back up grounds why we should procure common concern applications.

In an article by Ray Martin called “ Preventing Identity Theft” he explains how consumer fraud is the most common ailment in the United States. “ Last twelvemonth, more than 750, 000 Americans had their individualities hijacked — including high-profile victims like Oprah Winfrey and Tiger Woods.” It costs the mean victim more than $ 1, 000 to clean up the muss left by individuality stealers, harmonizing to the Federal Trade Commission.

Martin inside informations that, highjacking of personal information for fraud or larceny made up 42 per centum of the 204, 000 fraud ailments filed with the Federal Trade Commission (FTC) last twelvemonth. Ailments of individuality larceny increased 23 per centum of the FTC ‘ s Consumer Sentinel database in 2000 ; this besides translated into the top consumer fraud concerns (which is no surprise) . Equipped with societal security Numberss, bank history Numberss and other confidential personal information, felons can so use for recognition cards or bank loans, set up cell phone service or base on balls bad cheques under the victims name and recognition history.

hypertext transfer protocol: //www. cbsnews. com/stories/2002/05/21/earlyshow/contributors/raymartin/main509691. shtml

Why do we necessitate to procure common concern applications? To reply this inquiry we look to one of the most well-thought-of studies on the information engineering main road, “ The 2008 Data Breach Investigations Report” . This study spans four old ages and more than 500 forensic probes affecting 230 million records, and analyzes 100s of corporate breaches including three of the five largest 1s of all time reported.

Not merely did this study cover the right countries of concern but it is one if the first-of-its-kind, conducted by Verizon Business Security Solutions fact-finding experts. This survey found that 73 per centum of breaches resulted from external beginnings versus 18 per centum from insider menaces. Insider menaces are still really common to put on the line appraisal for common concern applications.

Most breaches resulted from a combination of events instead than a individual drudge or invasion. Procuring common concern applications is a really of import occupation and as we find out more on why we need to procure these engineerings we will besides put the tone for common methods used to procure concern applications.

The cardinal findings examine basic security dogmas that will besides be discussed in the following subdivision, the common methods used to procure common concern applications? Researching this universe of menaces many people will state that the insider is responsible for most security breaches. The 20080 Data Breach Investigations Report will turn out otherwise.

First cardinal determination is that most informations breaches investigated were caused by external beginnings. 39 per centum of breaches were attributed to concern spouses, a figure that increased five times during the class of the period studied. More breaches resulted from a combination of events instead than a individual action of the interloper. 62 per centum of breaches were attributed to important internal mistakes that either straight or indirectly contributed to a breach. These internal mistakes point in the way of the development life rhythm which will be discussed in a ulterior subdivision.

For breaches that were consider, 59 per centum were the consequence of hacking and invasions. Of the breaches ensuing or arising by agencies of hacking, 39 per centum were aimed at the application or package bed. This is a direct ground why information proprietors need to procure common concern applications. Even more of a ground is the facet of onslaughts to the application, package and services bed were much more ordinary than runing system platform feats, numbering 23 per centum.

Less than 25 per centum of onslaughts took advantage of a known or unknown exposure. Well, 90 per centum of known exposures exploited had spots available for at least six months prior to the breach. Nine of 10 breaches involved some type of unidentified systems, informations, web connexions and/or account user privileges. Recently, 75 per centum of breaches are discovered by a 3rd party instead than the exploited organisation and travel undetected for a drawn-out period.

The breaches investigated in this study denote a wide scope of industries. The retail, nutrient and drink industries account for more than half of all instances investigated by Verizon Business Security Solutions fact-finding experts. By comparing, the fiscal concern services, where you cover with great pecuniary assets that have to be well-protected more so so other sectors, accounted for 14 per centum of breaches studied. To get the better of condemnable pudding stones that maintain entree to hackers, fraudsters and other organized offense groups we must foremost hold upon why we must procure common concern applications!

hypertext transfer protocol: //www. net-security. org/secworld. php? id= 6213

Now after understanding why we must procure common concern applications we will discourse common methods used to procure common concern applications. Many organisations have the critical issue of developing those secure concern applications. The high-ranking solution to the issue might include one if non all of the undermentioned common ways to procure concern applications:

First, unafraid substructure such as routers, firewalls, and runing systems. Secure applications, including secure scheduling patterns for linguistic communications like Java and Perl, and specific application-level security controls such as application firewalls. Second, security policies and processes including information engineering policy and procedures, for case, secure system design and development patterns, sound constellation and alteration direction, exposure testing, menace appraisals, and ongoing exposure and incident monitoring and response. Recently, business-level policy and procedures, such as secure methods for conveying new clients on board, and extenuating the security issues that result from insecure client service and assist desk activities.

The common subject throughout the security industry is most security activity has emphasized on procuring the information engineering substructure. Without uncertainty procuring web and systems substructures are critical to the release of a secure concern application. This might include decently and firmly configuring the base substructure elements such as waiters, routers, switches, etc. , and establishing alterations and spots over clip to take new exposures.

It besides might necessitate seting in topographic point protective steps such as fixed firewalls, guaranting web, system, and local degree entree controls, and right protecting informations and communications through practical private webs (VPNs) or other cryptanalytic protocols. This substructure bird's oculus position of security besides involves such steps as monitoring for potentially malicious activity or for denial of service conditions as appropriate.

Important to see non merely substructure but organisations need to set every bit much attempt into procuring the whole system, non merely the base substructure constituents like waiters and routers, and switches but integrated application-level mechanisms as good, for case, plans, databases, and middleware elements, and those nucleus concern applications.

Making certain the application itself is protected is every bit of import as protecting the base substructure. Chiefly, application-level security is achieved by utilizing secure coding patterns to make suitably hardened applications. Nevertheless, even in smaller concerns, it is hard to guarantee that all application developers are sufficiently trained in secure cryptography patterns, processs, and techniques which must be kept up on new exposures. In larger concerns, it is a challenge.

It is vitally of import to set non-technical security controls on an equal terms with proficient controls. Using non-technical security controls, like security policy, preparation and instruction, and procedures and processs, are of import as proficient controls, this might include strong watchwords and firewalls. The non-technical controls pertain to such points as implementing a secure systems development life rhythm and doing the determination to set security into systems from the start instead than after its development.

hypertext transfer protocol: //www. cgisecurity. com/lib/ProtectingWebBasedApplications. pdf

Included in the common methods of procuring concern applications are constructs of procuring web, database, electronic mail, and demilitarized zone (DMZ) waiter services. The constructs to web security can be found in understanding the picks and schemes available as edifice blocks of web security. These include implementing user hallmark, utilizing proxy waiters and firewalls, puting up DMZs, and taking advantage of port and package filtering engineerings.

Procuring web based services starts with vetting the web content and codification. User interaction of this web interface would be without vulnerable cross-side scripting or codification based onslaughts. Vulnerability analysis of web content and web engines travel a long manner in procuring your web services. Email services can be applied to the construct of leting and forbiding users the right to hold entree to direct and have electronic mail.

The construct of procuring your electronic mail services lies in the patching of exposures and supervising control of use. DMZ waiter service do include web and electronic mail but besides include file transportation protocol (FTP) . Any DMZ service should be applied the construct of a bastion host. Procuring all unneeded ports and protocols of the host except it intended map. These constructs of procuring the concern applications can travel along manner as many menaces are of mispatched or unpatched waiters and services.

hypertext transfer protocol: //www. net-security. org/news. php? id= 5750

Net-Security. org gives us a really good thought of how to utilize constructs of procuring web, database, electronic mail, and DMZ services by first:

Align procedure with policy. In 59 per centum of informations breaches, the organisation had security policies and processs established for the system, but these steps were ne’er implemented.

Implement, implement, implement. Make a informations keeping program. With 66 per centum of all breaches affecting informations that a company did non even know was on their system, it ‘ s critical that an organisation knows were informations flows and where it resides. Identify informations and prioritise its hazard to the organisation.

Control data with dealing zones. Research workers concluded that web cleavage can assist forestall, or at least partly extenuate, an onslaught. In other words, palisade off informations when and where appropriate.

Monitor event logs. Evidence of events taking up to 82 per centum of informations breaches was available to the organisation prior to existent via media. Data logs should be continually and systemically monitored and responded to when events are discovered.

Create an incident response program. If and when a breach is suspected, the organisation must be ready to react, non merely to halt the informations via media but to roll up grounds that enables the concern to prosecute prosecution when necessary.

Increase consciousness. Merely 14 per centum of informations breaches were discovered by employees of the exploited organisation, even though employees are the first line of defence in safeguarding informations.

Educate them to be cognizant. Engage in mock-incident testing: Making certain employees are well-trained to react to a breach. Run drills and trial people ' s abilities, judgements and actions during a mock crisis.

hypertext transfer protocol: //www. net-security. org/secworld. php? id= 6213

What are the current tendencies in procuring concern applications?

Parag Shiralkar and Bindiganavale S. Vijayaraman have talked about many tendencies in concern. None every bit of import as the digital signatures. Shiralkar and Vijayaraman are from the University of Akron working in the direction section which utilizes digital signatures everyday for concern maps.

In their study, “ Digital Signature: Application Development Trends In E-Business” they talk about applications of digital signature engineering and the rise because of legal and technological developments, along with strong market demand for secured minutess on the Internet.

The survey of current tendencies of digital signature requires a comparative survey via assorted signifiers of concern indexs that the bulk of digital signature applications have been developed for the Business-to-Business (B2B) manner of e-business. Governments and the potency for their rapid growing in the Business-to-Consumer (B2C) manner of e-business is besides a really strong tendency of today.

Digital signature engineering involves coding messages so merely echt parties are able to read the message. Two divided but interconnected keys carried out this procedure of encoding and decoding. One party in the communicating holds the secret key, or the private key, and the other party holds the public key.

Shiralkar and Vijayaraman explain that digital signatures satisfy all maps, such as genuineness, non-repudiation, and security of a hand-written signature. A signature can be viewed as a agency of hallmark and can be owned by an single electronically. This engineering must be verified or approved by a 3rd party in order to manage the liability issues that may be raised by bilateral minutess.

The tendency began with the Utah Digital Signature Act which introduced the construct of a Certifying Authority (CA) . CA is an organisation that acts as a sure 3rd portion. Many other provinces implemented really similar digital signature acts and/or had some association with security and online hallmark which was added to their province Torahs. These technologically impersonal Acts of the Apostless were advancing concern applications in all its manners such as business-to-business (B2B) , business-to-consumer (B2C) , and business-to-government (B2G) .

Puting together treatments about the different types of concerns and their common concern applications, why we need to procure common concern applications, the common methods used to procure them in each type of concern, constructs behind procuring concern applications to include web, database, electronic mail, and de-militarized zone (DMZ) services, and constructs of procuring concern applications have all lead to how it can wholly be done to bring forth a secure concern application.

The Security Software Development Life Cycle (SecSDLC) is the methodological analysis used to take each concern application and secure, implement, and maintain. Understand the procedure and processs used to procure common concern applications are the SecSDLC to include the Enterprise Information Security Policy (EISP) .

Many information system security professionals believe the SecSDLC to be the best attack for implementing the information security system in concern applications. The SecSDLC Begin with the widely acknowledged Systems Development Life Cycle (SDLC) , a theoretical theoretical account for general information systems undertakings. Like the SDLC, the SecSDLC is usually composed of six stages: probe, analysis, logical design, physical design, execution, and care and alteration.

The phases are portion of a progressive theoretical account in which each stage begins with the consequence and information gained from the last stage. The probe stage inspects the current position of your concerns information security. The analysis stage consists of documenting your concerns information assets and associated menaces, every bit good as legal demands affecting information security.

The logical design stage creates and/or develops your information security programs while the physical design stage develops the peculiar engineerings needed to use the logical design. Execution puts into pattern what is determined in the physical design stage, and the care and alteration stage includes life clip proving and alteration of the security system.

Probe

The probe stage of the SecSDLC serves as a starting topographic point for any new information security-driven undertaking. The first measure of the probe stage should be to closely analyze current information security patterns. You should be able to reply the undermentioned inquiries: Do you hold an information security policy, and if so, what does it include? What types of hardware and package do you utilize for security intents? Do you hold virus protection for all workstations? What types of firewalls are in topographic point to protect your concerns applications and webs from people with malicious purposes? Are wireless webs used, and if so, are they encrypted? Are backups performed on all indispensable systems? Can employees easy put in package onto computing machines? What sort of physical security is in topographic point? What monies, if any, are set aside entirely for information security intents? The replies to these and related inquiries should be documented for comparing intents subsequently in the SecSDLC.

Another cardinal component of the probe stage is to specify direction functions within the information security kingdom. Person must be responsible for doing information security determinations, and that individual should hold the backup of senior direction such as the Chief Executive Officer (CEO) . Some companies frequently have a dedicated Chief Information Security Officer (CISO) to head information security.

Support is yet another cardinal component of the probe stage. While Open Source options can assist lower package costs, hardware costs and manpower costs can non be ignored. The execution stage will assist the concerns information security professionals estimation costs, but budgetary affairs should be planned in front of clip. Possibly the undertaking should get down near the beginning of the financial twelvemonth so more monies could be spent. These sorts of determinations should be considered in the probe stage.

Analysis

The analysis stage of the SecSDLC surveies your information assets and likely menaces to them. An plus is an “ organizational resource” that has value, while a menace includes an object, individual, or other entity that represents a changeless danger to an plus.

Companies should besides look into menaces that plague all industries. If you concluded in the probe stage that your company does non hold equal virus protection, so viruses are decidedly a menace to your school’s web, as they can do injury to computing machine systems and take attempt to take.

Worms are another menace that plagues all industries. Worms are different from viruses in that they are self-replicating, and frequently spread by means other than feasible files. As assets and their associated menaces change so must be alteration of security patterns and policies.

Logical Design

The primary end of the logical design stage of the SecSDLC is “ to “ design an information security plan. The creative activity of an information security plan begins with an information security blueprint” . An information security design must include an information security policy. Information security policy is defined as the written regulations that users of engineering must detect, as it provides regulations for the protection of the information assets of the organisation.

The individual in charge of information security should develop a thorough information security policy that defines what web behaviour is and is non allowed. The policy should besides specify what effects will be enforced if policy is broken, with way from upper direction.

Finally, the policy must be seen by all users of computing machine web engineering, including employees, contractors, housemans, and clients. All users should be forced to subscribe an recognition of and hold to follow the information security policy, besides known as acceptable usage policy.

From the information gathered in the first two stages, you should hold an thought of what security demands should be addressed. The logical design stage describes out in composing what should be done to turn to security demands. For illustration, if viruses pose a job to machines on your company's web, so virus protection should be specified as a solution to the job. Install anti-virus package on all workstations and likely on the email gateway as good.

The email gateway should likely forbid certain types of fond regards that traditionally carry viruses. If hackers are a concern, so you must stipulate a firewall and/or web invasion sensing system. Address the job of worms by necessitating workstations to update operating system spots.

Address physical security for company computing machine systems as good. What kinds of door locks need to be installed to the computing machine room, and who needs transcripts? If backups are unequal, stipulate a backup system. Take steps to do certain employees can non short-circuit security controls. There should be some type of hallmark strategy in topographic point so that employees must hold a login and watchword to entree any school computing machine system, and besides prevent users from holding decision maker authorization over any computing machine system.

Physical Design

The physical design stage of the SecSDLC develops generic thoughts from the local stage into a certain program of action. It specifies which peculiar engineerings to utilize to turn to information security concerns.

Execution

The execution stage of the SecSDLC carries out the programs designed in earlier stages. This happens through a undertaking program, a written program that delivers instructions to the persons who are put to deathing the execution stage. These instructions focus on the security control alterations needed to the hardware, package, processs, informations, and people that make up the organization's information systems. It is besides of import to make mileposts or specific points in the undertaking program when a undertaking and its action stairss are complete. You will find costs in the probe stage, followed by implementing the undertaking recommended in the physical design stage.

Care and Change

The care and alteration stage of the SecSDLC is the last stage and will go on throughout the security project's life-time. Penetration and exposure testing should be an on-going undertaking to prove for new exposures. Nmap and Nessus are free Open Source public-service corporations utile in this phase.

Nmap is a port scanner that detects unfastened TCP and UDP ports, while Nessus studies exposures for any web services running on your computing machines. Your company will doubtless put in new engineerings, and those engineerings will convey more hazards. Flaws will be found in bing engineerings every bit good, doing more exposure in the information systems. By maintaining a stopping point oculus on security, hopefully your information security plan will stand for several old ages.

hypertext transfer protocol: //www. techlearning. com/showArticle. php? articleID= 60401696

The intent of this Enterprise Information Security Policy is to make an environment withinstate of Iowa bureaus that maintains system security and handiness, informations unity and single privateness by forestalling unauthorised entree to information and information systems and by forestalling abuse of, harm to or loss of informations. If there is a difference between this policy and other needed policies, those with the more rigorous control take precedency.

This papers describes an enterprise degree policy. Enterprise criterions, procedures and processs will be developed to help in the execution. Each bureau is responsible for developing policies, criterions, procedures and processs to run into this policy. If it is determined that more rigorous steps are needed, the bureau is responsible for developing the policies, criterions procedures and processs to run into that higher degree of security.

hypertext transfer protocol: //www. iowa. gov/standards/documents/IowaEnterpriseSecurityPolicy050128. pdf

What is the function of security in the hereafter?

hypertext transfer protocol: //www. cio. com/article/32033/_The_Future_of_Security

Predict the function of security related to concern applications in the hereafter.