Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Areas To Consider When Implementing PeopleSoft

Dirk Norman
GIAC Security Essentials Certification
Version 1.4b Option 1
October, 2003

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Areas To Consider When Implementing PeopleSoft

Abstract:

PeopleSoft is a popular ERP software application that combines all aspects of a companies business like HR, Marketing, Purchasing, AP and others. PeopleSoft uses a relational database and is web-based. When implementing PeopleSoft, IT professionals realize the importance of securing the operating system, the network and the web, but often do not secure the application properly. This paper will address some of the basic principles of securing a PeopleSoft application. It will discuss some, but certainly not all, of the security features within PeopleSoft that can help secure the data. This paper is not intended to be used as a guide to securing a PeopleSoft application, but instead, addresses some of the relevant security highlights that should be considered when implementing a PeopleSoft application.

Introduction:

Companies today are always looking for ways to save time and ultimately money. In the early 90's, these companies were looking at computer systems and applications to achieve this goal. However, the securing of these applications and systems were not always a high priority. "The FBI reports that U.S. industries suffer annual losses totaling 63 billion as a result of theft of intellectual property stored on computers. The Computer Security Institute recently polled over 500 companies who reported losses totaling 236 million to saboteurs, viruses, laptop theft, financial fraud, telecommunications fraud and theft of proprietary information. " *PeopleSoft, Inc.- Whitepaper* Today hackers have numerous options to use in order to exploit any weakness in your computer systems and apps. Companies are realizing more and more the importance of "computer" security. What companies do not realize is, just installing a few firewalls is not enough.

As was mentioned before, companies are looking for avenues to save time and money. One of the options is Internet applications. With the advent of the Internet, it has opened a whole new way of doing business. Now companies can offer their service or product directly to the customer online. It also enables companies to interact directly with each other. Companies are using Enterprise applications to achieve a competitive edge also. Enterprise applications enable

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

companies to manage all aspects of their business. One of the more popular Enterprise applications is PeopleSoft. There are others like SAP, Oracle and Microsoft. These companies are known for their Enterprise Resource Planning applications and *eB*usiness applications. What is Enterprise Resource Planning or ERP? ERP is a "business management system that integrates all facets of the business, including planning, manufacturing, sales and marketing. As the ERP methodology has become more popular, software applications have emerged to help business managers implement ERP in business activities such as inventory control, order tracking, customer service, finance and human resources." http://www.webopedia.com/term/E/ERP.html
Another definition of ERP is: "ERP is a high-end sophisticated software solution that reduces the pressure and workload off the Managers and provides accurate, timely information for taking appropriate business decisions. Managers with knowledge of ERP will be able to achieve their targets and goals by proper implementation of ERP system in their organization. In fact, Managers are expected to translate the business rules and requirements for mapping them into ERP software. Implementation of ERP solutions is one of the largest drivers of growth in the consultancy business." http://peoplesoft.ittoolbox.com

Companies using ERP applications must realize that security is an important implementation task and cannot be over looked. Management, users and customers expect the information contained in the application maintain the 3 most common security objectives; Confidentiality, Integrity and Availability, better known as CIA.

Confidentiality: Ensures the information contained in the application stays private and is not disclosed to unauthorized users.

Integrity: Is the assurance that the data or system is accurate and has not been manipulated.

Availability: Assuring the application is available or accessible when needed.

Different Layers of Security

Accessing a PeopleSoft application requires passing through several different layers of security.

Network Security
Operating System Security
Database Security
PeopleSoft Application Security

PeopleSoft is a complex application and encompasses a very broad and in-depth area of security. For the purpose of this paper, we will focus primarily on the

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

high-level application security that should be considered. But first, let's briefly define the other three areas.

Network Security

Network Security is the securing of users to hardware or software that are linked together. You can achieve this through many different ways like, access rights to files; different sign-on times and assigning separate ids and passwords. This area of security is also where you would install firewalls, SSL, application server and web server security. There are other more in-depth security features that should be considered but this paper will not focus on them.

Operating System Security

Operating System Security controls access to the system objects and the operating system. For instance, OS/2 or Windows. Some security controls again are assigned ID's and passwords. There are other more in-depth security features that should be considered but this paper will not focus on them.

Database Security

The PeopleSoft application uses Relational Databases to store the actual tables of data that the application uses. Database Security controls access to those tables. Database Security is very important and should not be overlooked. If you secure the application but users have wide-open access to the database, they can access the information directly through the tables. So securing the database itself cannot be forgotten. Techniques to do this but are not limited to, include assigning specific ids and passwords. Granting different degrees of access to the tables, for instance, view only access or read-write access. This type of security is done at the database level and not within the actual online PeopleSoft application. Company analysts should work with the database administrators to achieve this. Again, there are more in-depth security features for Database Security and it is recommend reviewing them when setting up a PeopleSoft application.

The PeopleSoft application can have multiple architecture designs depending on your company. For the purpose of this paper, we will use a high level diagram. The following is an example of a high level PeopleSoft architecture

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

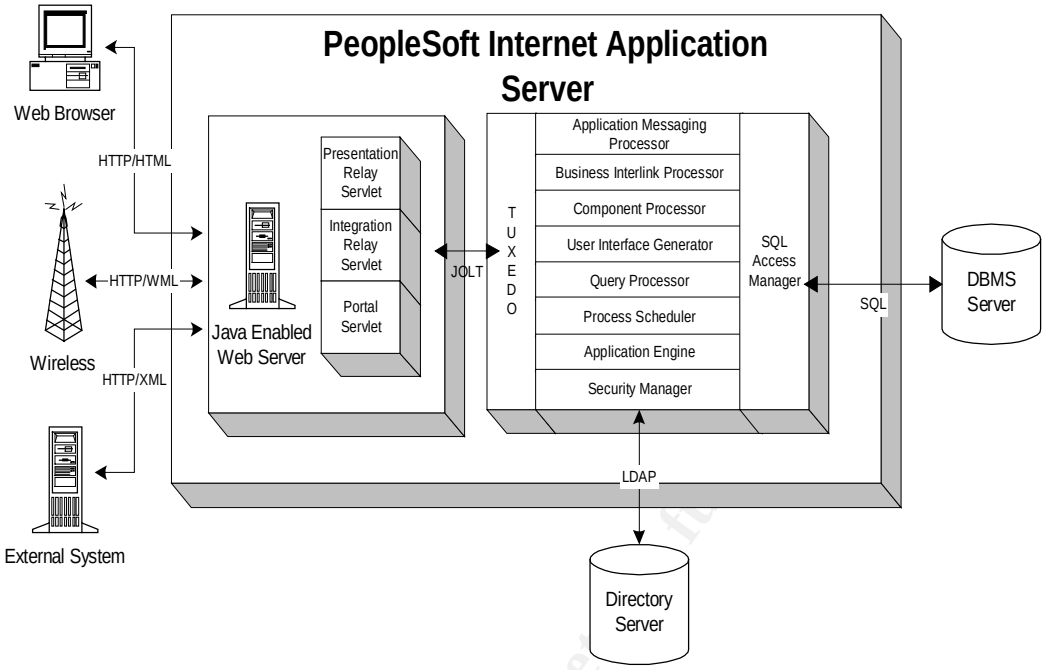

Figure 1

Within this architecture, there are several security areas that need to be addressed and secured. For instance, the database should be locked down to only those that need access to that database. The type of access to the database should also be restricted to only those that need that level of access. For example, not every user needs read/write access. All the servers should be secured and only allow access to individuals that have a business need. Each company when installing a PeopleSoft application should consider all areas with the security IT professionals. But now this paper will focus more on the PeopleSoft application and address some security features that should be considered when implementing PeopleSoft.

Three Main Security Components

From a high level, there are three main security components within the PeopleSoft application when setting up the users. Those three areas are:

1. User Profiles
2. Roles
3. Permission Lists

Because the PeopleSoft application has the potential to access very important data, each company will have different levels of access for the users. PeopleSoft is very flexible and should be designed to meet each company's need to allow users to do the work that needs to be done. But each user and profile should be designed with security in mind. Users should not have wide-open access; instead users should be configured according to their job description and what they will need to do within the PeopleSoft application. PeopleSoft online security provides the way to do this by using the Maintain Security feature within

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

PeopleTools. Within Maintain Security you can create different roles and permission lists that will be granted to the varying user's profiles within the application.

User Profiles

Each individual of the PeopleSoft system will have a unique user profile. This user profile will allow a user to sign into the system and perform the granted level of access that will allow them to perform tasks. A user of the system can be anyone from an employee, a customer, vendor, or supplier. Each user is assigned one or more roles. Defining a user within PeopleSoft is done through the Maintain Security Menu. This is where you define the values that are specific to the user. For instance, user password, employee id, email address, primary permission lists, etc. Below is a screenshot of a user profile page within PeopleSoft.

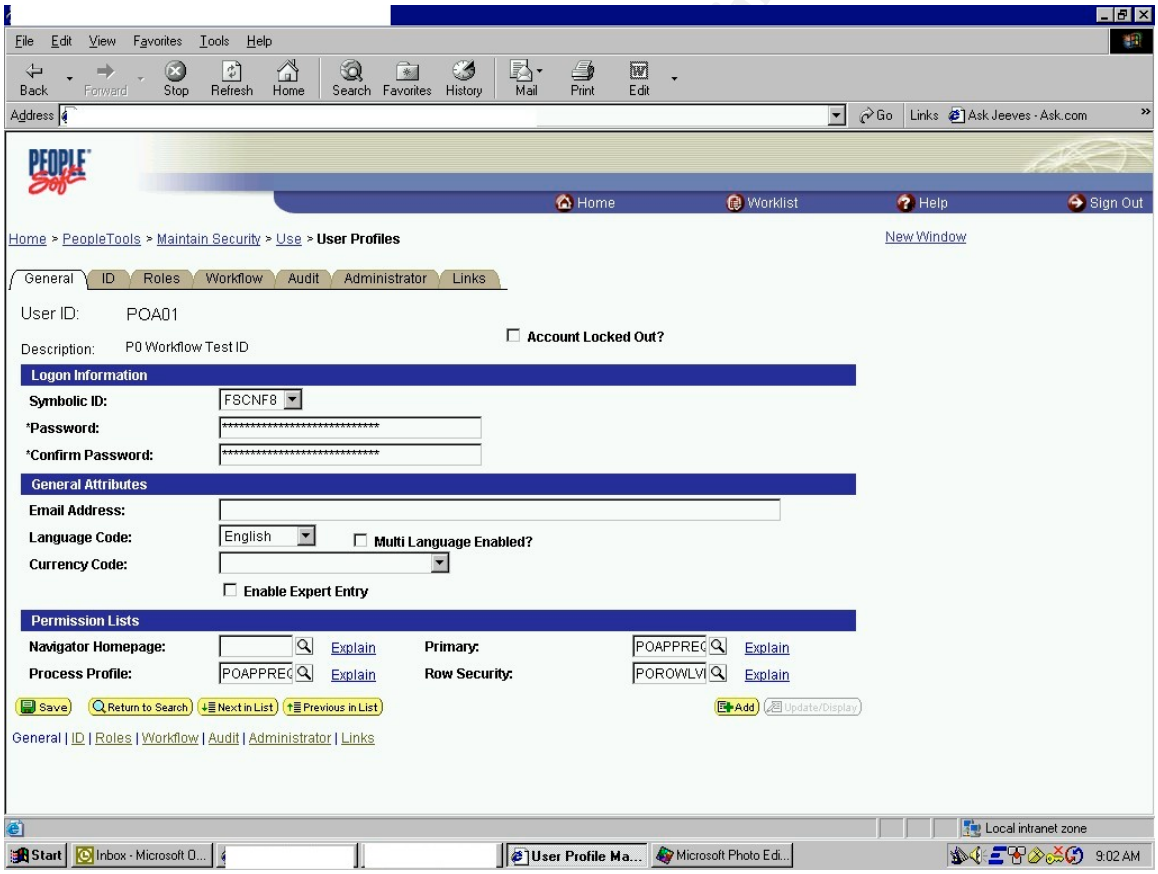

Figure 2

The user profile page is where each company will set up or configure the actual users for the PeopleSoft application. The company system administrator and security analyst are the only individuals who should have the ability to configure users. This paper will not go into the actual steps of setting up a user profile.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

For more information and how to configure user profiles contact PeopleSoft at www.peoplesoft.com .

Roles

Roles are assigned within PeopleSoft to the individual user profiles. Roles are objects that are similar in nature that allows or links user profiles to permission lists. For instance, a manager, within your company may perform the same type of activities or tasks within PeopleSoft no matter if they are in the Marketing or the Purchasing department. So you might create a role called Manager that would be assigned to all managers within your company. Another example might be all the employees within a company may be allowed to access certain pages within PeopleSoft, so a role called Employee might be created and granted to all users, since all users would need access to those pages.

You can assign multiple Roles to a user profile. For example, a manager of a company may get the Manager role and would also get the Employee role since he is an employee too. Roles are assigned permission lists and each role can have multiple permission lists. Permission lists defines the authorization or the level of access a role can access.

It is important for companies when implementing a PeopleSoft application to define their users and develop the security through roles. If a company implements an ERP application, but does not identify their roles and just uses delivered roles or an ALLUSR type role, users may potentially have access to data or manipulate data that they should not be able to. Companies open themselves to a security weakness if careful consideration of the roles is not taken. Each implementation project should design the security around the roles to protect the company's assets and data. The implementation team should gather all the business requirements and business processes then configure the roles to meet those requirements. Below is an example of a Role page within a PeopleSoft application. From the diagram, you can see this is the page, within Maintain Security, where the permission lists that are unique to a specific role are assigned.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

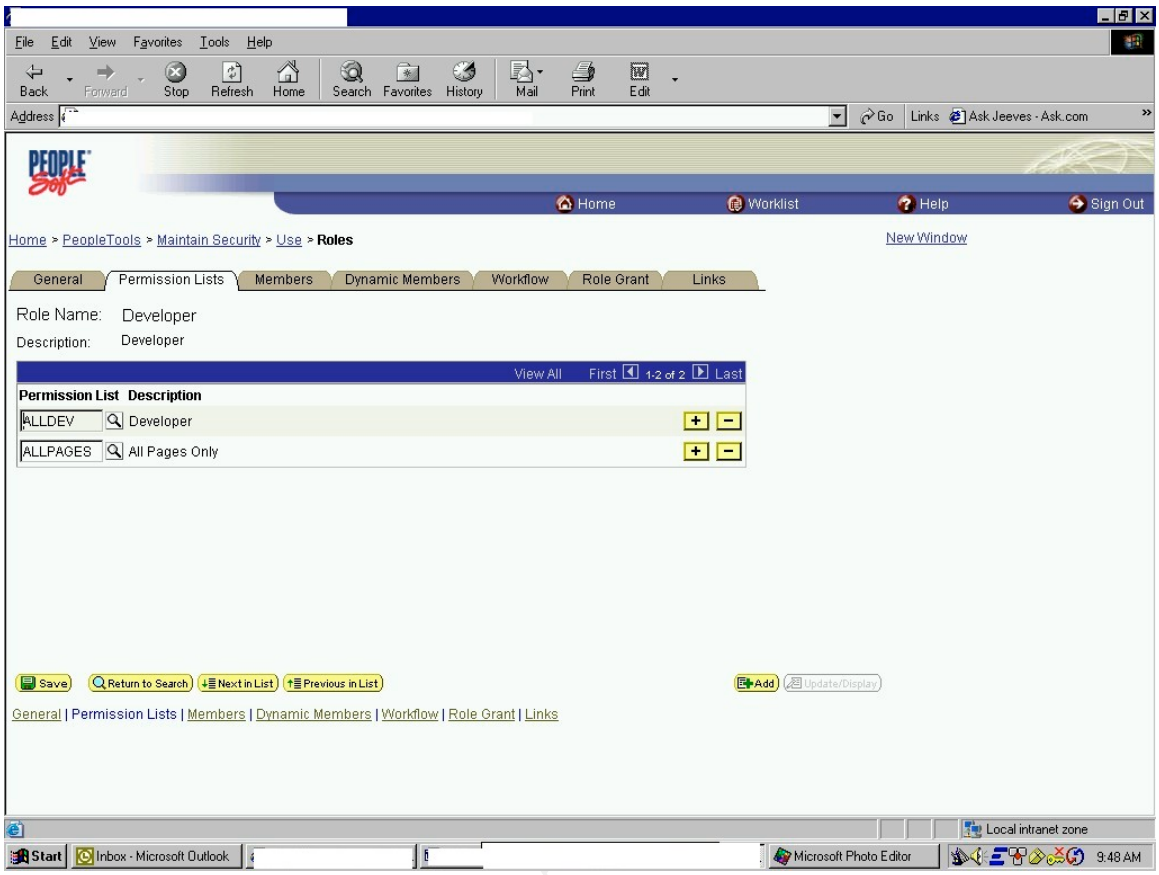

Figure 3

Permission Lists

Once the users are identified and the Roles are identified Permission lists need to be created and assigned to the Roles. Multiple Permission lists can be assigned to multiple roles. Permission lists are the groups or combined authorizations that allow roles or users to perform tasks within PeopleSoft. Permission lists allows what type of access each role will have to a page, for example, display only or update display. There are multiple actions that can be granted to pages. Permission lists control sign-on times for users. The process that a certain role can perform is also defined within the Permission list. Query access and what type of queries that a user can run is set up within the permission list menu. Essentially this is where you build your security for the user profiles and roles. When implementing a PeopleSoft product, a company will want to gather all the business requirements and processes so that the permission lists can be configured properly. This ensures the roles and users are only accessing data and pages that are needed to perform their job. Again, if a company does not take the time to consider securing the permission list and build those permission lists from the requirements, users could potentially have access that is not authorized.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

PeopleSoft allows companies to get as granular as they would like with the building permission lists. This allows for ease of use and maintenance for administrators. It also allows large companies to secure the application depending on the business processes and organization. For example, a small company with only six employees might only need two roles and permission lists, but a large company with 80,000 employees my need 40 or different roles and 100 permission lists. The important thing to remember is only assign access to the permission list to individuals that need that particular access. Far too often companies take the simple approach by assigning ALLUSR to individuals and this opens up a huge security risk. Access should only be granted based on a user's business requirement and need.

Below is an example of a Permission list page within PeopleSoft. It shows the different tabs that can be used to configure each permission list. This paper's purpose is not designed to describe how to build a permission list or build a particular security design, but just make companies aware that the permission list is a very important part of implementing a secure PeopleSoft application. For more information on how to build a permission list go to www.PeopleSoft.com.

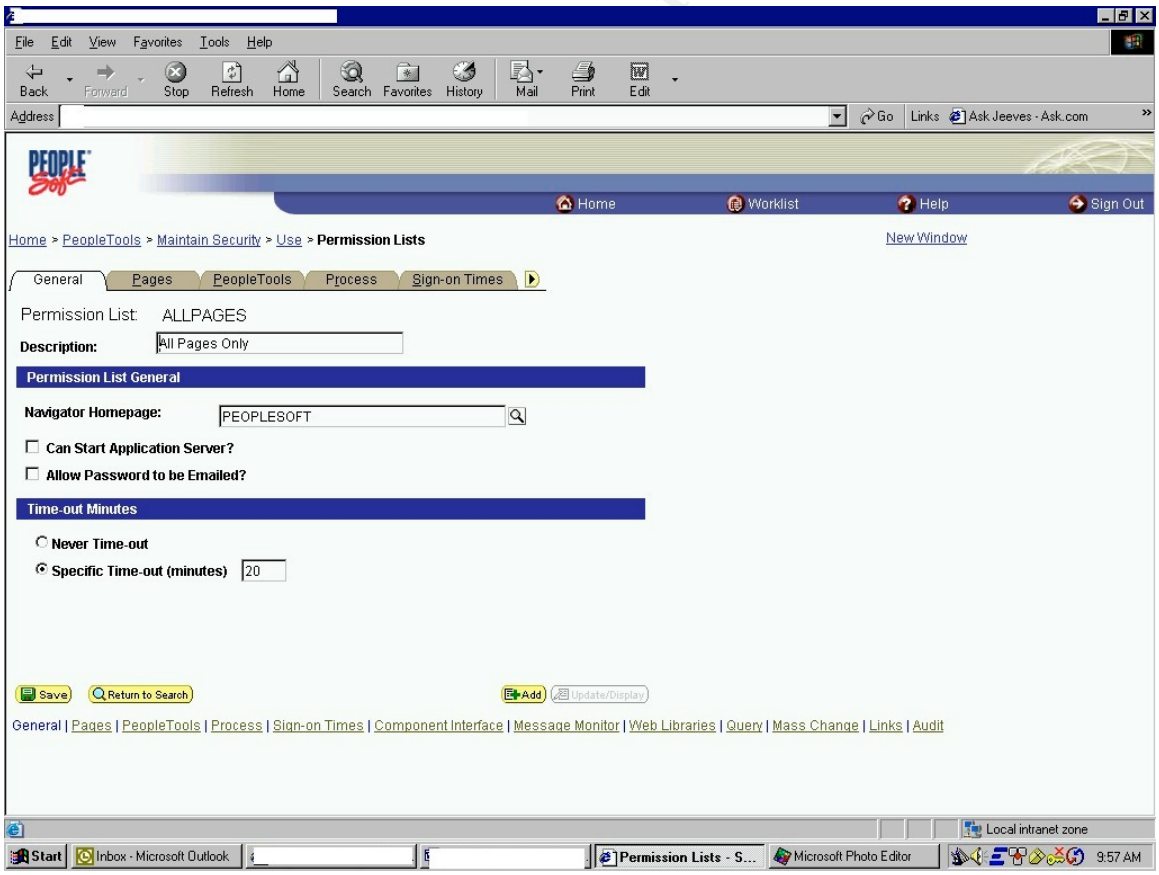

Figure 4

The three main components of PeopleSoft security are User Profile, Roles and Permission lists. These three components are all setup with the PeopleSoft

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

application under Maintain Security provided within a development tool called PeopleTools. It is important for companies, when implementing an ERP application like PeopleSoft, to recognize the business requirements and develop the security configuration of the profiles, roles and permission lists from those requirements. Often time's companies will secure the network, operating systems and databases, but forget about the application itself. Actual employees or insiders often times will present the most high risk or unauthorized access. With the proper setup and configuration of the profiles, roles and permission lists, companies can limit their exposure.

There are numerous ways that companies can secure its PeopleSoft application. It depends on the size of the company and the information that the PeopleSoft application contains. The important thing is to secure it. As mentioned earlier, the User Profile, Roles and Permission Lists are the nuts and bolts of securing the application at a high-level. There are other security features that should also be considered.

Password Controls

One security feature many companies forget to enforce is Password controls. Within the PeopleSoft application, a company can apply password controls that will help mitigate the possibility of unauthorized use. Password controls are highly recommended. The PeopleSoft application allows the enforcement of a minimum length for passwords. Typically a strong password is 6-8 characters. The password should contain upper and lower case alpha characters. It should also contain numeric and special characters. For instance, ? $ @ ! ^ & + etc. The PeopleSoft application allows all of these controls to be enforced. The application also allows for a maximum amount of login attempts, once the maximum attempts is reach without success, the user would be locked out. It is recommended to set company policy to less then 5 attempts. This prevents hackers from trying multiple times to gain access to the application.

Sign-On Times

Another way to secure the application is by using sign-on times within PeopleSoft. Each time a user signs into PeopleSoft, the id is authenticated and the password is verified. This ensures the id is valid. PeopleSoft allows the configuration of different sign-on times for each id using sign-on times within the permission lists. Different sign-on times can be set for different permission lists. For example, if managers are not allowed in the system after 5:00 o'clock on Friday and not allowed back in until 8:00 o'clock Monday, companies can configure the manager permission lists to not allow the ability to log in after 5:00 o'clock and then be able to log in after 8:00 Monday. In essence, this would lock out the managers over the weekend. If a user tries to log in and does not have a valid sign-on time, they will not get access to the system. Also, if a user is in the system and their sign-on time expires while logged in, their active session will

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

expire. The sign-on tool is configured within the Permission list menu in Maintain Security. This option is very helpful if companies have blackout periods like payroll processing and they do not want any access into the system. PeopleSoft Permission lists can be configured to accommodate any sign-on time needed.

Process Security

The granting of pages and the actions a user can access is accomplished through configuring Roles and Permission Lists. But often time's companies neglect to configure the security for the processes that run within PeopleSoft. Like payroll processing or accounts payable processing. You can configure this type of security through the Process Scheduler within the PeopleSoft application. Companies should group Process groups by similar groups or departments. For example, the payroll for a company might be under the Process group HR_PAYROLL. A user must have the Permission to access that page that holds the process, but they also must have the access to the actual Process Group. If they don't have the access to the Process Group, that user cannot run the process. This is another good security feature within PeopleSoft. It provides an extra layer from unauthorized access to the processes running within PeopleSoft.

Object Security

Just as importantly has securing the access of users, companies must also consider who can access the PeopleTools objects. PeopleTools objects are record definitions, page definitions, menu definitions that reside within the PeopleSoft tables. This access is usually limited to developers and should not be given to the business end user. PeopleSoft allows companies to create object groups and associate them to certain permission lists. A user as to have that object security access to be able to access those objects. Object security is used a lot of times with the General Ledger module within PeopleSoft to lock down certain ledgers.

Query Security

Another area when implementing PeopleSoft that should be locked down is queries. PeopleSoft allows users the ability to retrieve data and create queries or reports. Companies should not allow all users the access to query and users should only be allowed to run queries that are associated to their job. For instance, a company would not want all end users to have the ability to run a query on payroll data. Therefore, query security should be used to control this access. Access groups contain the record definitions that hold the data for the queries. Companies can control access to the query by limiting access to the query access groups. If a user has access to the query tool, but does not have access to the query access groups, they cannot run that particular query. Query security is very important and should be considered when implementing PeopleSoft.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Row-Level Security

Row-Level Security is another way to control access to certain information within the application. "Row-level security consists of several views attached to components, records, or menus." http://www.vp1online.com/samples/v1i1a2.pdf Security views can be designed to control access to individual rows of data within the database. PeopleSoft allows row-level security for departments and locations. For example, the HR module for PeopleSoft allows companies to secure data in departments according to the region they are located. If a manager in the West region is only allowed to see his information in the West region, then you could implement row-level security to restrict the access to any other region. Row-level security is a good option to consider when implementing PeopleSoft and should not be left out.

Rename or Remove Delivered Roles or Permission Lists

Another consideration when implementing PeopleSoft is the removal or renaming of delivered roles, permission lists or Operator ID's. If these known ids are left in the system, someone that knows PeopleSoft could potentially hack into your application. It is recommended to delete or rename and change the passwords of the delivered ids. For a listing of delivered roles, permission lists and ids, please contact PeopleSoft at www.peoplesoft.com .

Summary

In review, PeopleSoft is a complex application that can house some very critical information for a company and should be secured. There are several different areas to secure when implementing PeopleSoft. The common levels are Network Security, Operating System Security, Database Security and the area that is often overlooked, Application Security. Each area should have a design that ensures the confidentiality of the data, integrity of the data and the availability of the data.

To often a company will do an effective job in securing the architecture of PeopleSoft, but neglect to effectively secure the application. PeopleSoft provides many different tools and segments within the application to ensure a solid security design. The main way to secure users of the application is by setting up the user profiles, roles and permission lists correctly. Users should only have the access that is needed to perform their job duties efficiently and effectively. No more, no less.

Other areas to consider are implementing password controls. PeopleSoft provides the flexibility to create strong passwords and this policy should be enforced through the enable password controls within PeopleSoft. Sign-on

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

times are another effective way to limit unauthorized access to the application. Process Security ensures only those individuals who have the business need will have the ability to run your processes. Object security is another effective option, within PeopleSoft, that allows only those users that have the business need to access certain objects. The ability to run certain queries or any queries at all should also be considered. Query security provides the ability to grant query security to only those individuals that need it. Row-level security can also be incorporated into a security design to ensure only authorized users have access to the data. Delivered ids, roles and permission lists should also be removed or renamed to protect the possibility of intrusion. Passwords of those delivered ids should also be changed.

When protecting a company's infrastructure, the common areas are almost always secured properly by a solid network, operating system and database security. But the area that often does not get the attention needed is the application itself. This can present a hole that hackers or unauthorized individuals can exploit. But if companies take the time to use what PeopleSoft provides and configure a security design based on business need, that security risk can be minimized effectively. PeopleSoft is very flexible and each company's need is different. So there is no "cookie cutter" security design that can be implemented. The main thing to remember is, **secure the application**.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Works Cited

1. Bajwa, Fouad Riaz. “ERP Rising: The Enterprise Resource Planning Guide” 1 August 2003 http://sap.ittoolbox.com/documents/document.asp

2. Bossong, Julian. “Managing ERP Applications for Strategic Advantage” 8 August 2003 http://peoplesoft.ittoolbox.com

3. Brain Tree Security Software Inc., “Securing PeopleSoft Data” URL: www.sqlsecure.com 1999

4. Entellus Technology Group, Inc. “PS8 Overview & How Does this Impact My Audit Approach?” – White Paper, Lyons, Frank W and Hamilton, Brad W, CPA-Hamilton@talgov.com (2000)

5. MIS Training Institute “Controlling and Securing PeopleSoft Applications” URL: www.misti.com 2000

6. Permeo Technologies Inc. “Permeo Absolute Application Security, Application Security DataSheet” www.permeo.com 2003

7. PeopleSoft, Inc. “PeopleSoft 8 PeopleTools Peoplebooks: Security” www.peoplesoft.com 2001

8. PeopleSoft, Inc. “PeopleSoft Security- PeopleSoft PeopleTools 8.1” Contributors Rich Eusebio, www.peoplesoft.com 2000

9. PeopleSoft, Inc. “Security Features of the PeopleSoft Internet Architecture” – White Paper, www.peoplesoft.com 2000

10. Whitley, Shannon. “Customizing HRMS Security-Don’t settle for security that doesn’t meet your business needs.” Jan 2003, http://www.vp1online.com/samples/v1i1a2.pdf

Other websites used:

11. www.knowledgestorm.com

12. www.webopedia.com

13. Information Technology Toolbox, Inc. www.peoplesoft.ittoolbox.com

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Figures Used:

Figure 1 is a common PeopleSoft Architecture diagram from the PeopleSoft Architecture.

Figures 2-3 are screenshots from a development configuration environment within Peoplesoft.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.