From:

Bodo Kother, Von-Bruchhausen-Str. 17, D-45657 Recklinghausen (bkother@gmx.de ,
Tel: ++49 2361 9397-0, Fax: ++49 2361 9397-43)

and

Daniel Hamburg, Augustastr. 23, D-45879 Gelsenkirchen (dhamburg@genion.de ,
Tel: ++49 179 5383825)

Date: 28. Feb. 2002

To: International Society for Environmental Protection, Marxergasse 3/20, A-1030 Vienna

Paper Presentation: ENVIROINFO Vienna 2002 September 25-27, 2002

We want to submit a paper with the following title:

Security related aspects of environmental web portals

Because of the increasing international competition (liberalization of markets) and new technologies, public utilities face the problem to offer different applications for various user groups with a uniform GUI (graphic user interface). A possible solution for this are web portals.

Closely connected with this is the necessary differentiation of the different user groups regarding authentification and authorization and the implementation of content security and content management.

To implement efficient and safe web portals all applications and the related security risks must be defined. This definitions determine the necessary technical infrastructures and needed security solutions.

In this paper the described problems and solutions are pointed out by the example of a power supplier.

Applications in critical infrastructures e.g. “Power Suppliers”

On principle applications are developed for the use in administration and engineering or a combination. In the historical application development the fact that user with different rights access data and information wasn’t taken into consideration. Connected to the building of web portals the differentation and the protection against abuse of applications and information is of highest interest.

In general applications can be assigned into the following categories depending on user groups:

Category	User Groups
Internet	Public – Everyone
Extranet	Restricted – External Users
Intranet	Private – Internal Users

Table 1: Categories and User Groups

Internet applications

Possible internet applications are : customer specific combination of the gas, water and energy supply. A concret example is the mix of nulcear -, solar and regenerative power offered by power suppliers.

Extranet applications

Inside the extranet public utilities and authorities can exchange information concerning emission and water quality measurement.

Intranet applications

Intranet applications are: process supervising, visualization and control, SAP, system administration.

Endangering – Information Warfare

Information warfare admits of the concept of superiority. One side has more sensors in better places, more collection and analytical capabilities, and a more reliable process for turning data into information and information into decisions.

Today the forms of information warfare are: command-and-control (C2W), intelligence-based warfare (IBW), electronic warfare (EW), psychological warfare (PSYW), hacker warfare (HW), economic information warfare (EIW), and cyberwarfare (CW). [1]

All used information systems enter into information warfare only if and when an opponent targets to degrade them and they are subject to attack.

The certain forms are used to reach information denial (or distortion) by the enemey and protect the own systems in conflicts. Many organisations develop and use weapons and concepts for this.

Programming knowledge is not needed any more because many tools which offer a graphic interface and can even be used by beginners are available from the internet. Some examples are: Trinoo, Stacheldraht (Denial of Service), Back Orifice, Nuke (Trojan Horses) etc.

In this paper we combine the economic related different forms of information warfare into EIW.

EIW (economic information warfare)

The different methods of EIW may be: e-spionage, information denial or blockade.

e-spionage is the most often used way of EIW with the aim to obtain secret information about products, concepts and customers. The most efficient way is to gain access and control over systems inside the opponents infrastructure. Either this systems contains sensitive data or it can be used to attack other systems. The most difficult task in e-spionage is to hack target systems inside the network.

There are different possibilties to invade the opponents infrastructure. The first one is to use the gaps in the electronic systems which protect the target. Another is to use internal personal e.g. to install a trojan horse or get information about user and passwords.

The aim of information denial (or distortion) attacks is not to gain information but to stop the communication of the opponent e.g. to disable mail communication, http or database traffic. One possibility are “Denial of Service” attacks.

Security Solutions

There are many tools and methods that protect data and information in critical infrastructures.

The first step to implement security into an organization is to analyse the existing environment and to define security policies according to the organizational need. It is necessary that employees understand the need of this policies. There is no working security system without acceptance.

Firewall- and Intrusion Detection Systems

Mostly used and often not really secure because overestimated are firewall systems. Firewall systems can be compared to a doorman who decides who is allowed to enter the building and who not. Like a doorman a firewall has to be instructed. In contrast to the doorman the firewall can not ask anyone about undefined events and act properly. So the most important task when configuring a firewall is to have all rules implemented for a given application. One single gap endangers the system integrity. In complex environments multistage firewall systems are needed.

Intrusion Detection Systems (IDS) are used to detect and eliminate intruders inside the companies infrastructure. To ensure this the network traffic is scanned, collected and compared with known attack patterns.

Information Warfare Attack Assessment System (IWAAS)

A key problem in Information Warfare is in formulating collection and analysis methodologies which will enable corporations to assess the threat of attack, detect an Information Warfare attack , assess the nature, extent and origin of the attack and predict likely enemy actions.

IWAAS is a conceptual architecture from King´s College London that aims to identify solutions to these problems. IWAAS is a decision support system with three purposes: first, to evaluate the IW threat posed by a variety of actors; second, to provide Indicators and Warnings (I&W) of an IW attack; third, to predict enemy Courses of Action (COA). [2]

The system is based on a short term knowledge base (Attack Detection System, ADS) and a long term knowledge base (Threat Assessment System, TAS).

ADS responds not only to software warfare attacks like IDS but to a broader range of possible IW events (deception operations, preparation of IW, physical attacks on critical nodes).

TAS components are an Intelligence Fusion System (IFS) and a Threat Data Base (TDB). The IFS is a rule-based expert system that enables the operator to ask high level questions concerning IW threats and mines the TDB to provide structured answers.

Authentication Systems

To ensure that only authorized persons can access applications, authentication systems are needed. There are several different authentication types e.g biometric, two factor, simple password and combinations. The use of a special authentication method depends on the need of protection for the application.

Biometric authentication uses natural differences between human beeings like fingerprint, voice or proportion of faces. Today this methods don't offer a high level of security. In the near future this systems will probably be the most often used.

The problem of simple password authentication is that most employees use passwords that are easy to guess for intruders e.g. names of family members, birthdays.

Two factor authentication is based on the fact that in addition to a password a hardware token is needed. This token may be a key fob or a smart card which contain information needed for successfull authentication.

Public key infrastructure (PKI)

PKI´s use encryption and signing funcionality to provide different security aspects like authentication, authorization, non repudiation and integrity.

A digital signature can be compared with a handwritten signature. It ensures that the sender of a document can be clearly identified and that the document hasn't been changed. Encryption is used to prevent that the document is accessed by unauthorized persons.

Keywords used in this context are certificate, certificate authority (CA), private and public key and smart card.

Summary

Within critical infrastructures web portals allow the integration of several applications with external and internal user groups. Therefore different security policies and mechanism are needed to ensure the system integrity. General several security solutions must be combined to secure the use of web portals (PKI, IDS or IWAAS, Firewall, Directory Services and others).

---

1 Institute for National Strategic Studies, USA, Martin Libicki – What is Information Warfare ?

[2] ICSA, King´s College London, UK, Dr. Andrew Rathmell, Dr. Richard Overill, Mr. Lorenzo Valeri – IWAAS, Information Warfare Attack Assessment System