Building security on trust

ISSE

Building Security on Trust

Any enterprise moving its business to the Web is inevitably faced with an increase in data security risks. Doing e-business usually entails the migration to the Internet of entire processes and their associated data – confidential data that must not under any circumstances be allowed to fall into the hands of competitors.

PAULUS SACHAR

All possible security risks must therefore be identified as early on as possible and appropriate measures taken. In many countries this is already a legal requirement. Germany, for example, passed a law in 1998 – the KonTraG ("Gesetz zur Kontrolle und Transparenz im Unternehmensbereich") – that requires companies to implement a monitoring system for giving early warnings of any threatening developments. Across-the-board risk management may not be popular, but it has become indispensable.

Guaranteed security

Crucial factors

Your information is a valuable commodity – not only for your own enterprise but also for your competitors'. Four crucial factors determine the security of sensitive data:

- Integrity: data cannot be manipulated.
- Authenticity: the originator of the data can be identified with 100% certainty.
- Confidentiality: data is accessible only to the "right" persons.
- Availability: data is always accessible when required.

E-business security demands that each of these properties be guaranteed.

Risk analysis

The cost of security measures must be commercially justifiable, however. Risk analysis is essential in order to estimate both the value of the information and the likelihood of a security leak. This analysis provides a guideline for the size of investment that can be justified for protective mechanisms. After risk analysis the next step is to investigate each of the mechanisms under consideration, and in particular to assess their practicability. Since any given mechanism is likely to have unavoidable side-effects on certain business processes, each specific proposal should be communicated within the corporate hierarchy, in order to ensure that senior management is aware of and agrees to the consequences of any decision taken. The investigations need to be repeated at regular intervals in order to ensure continuous data protection. The final result of this process ought to be a fairly detailed security policy.

Security policy

The security policy needs to take account of every possible aspect of security within an enterprise, because an absolutely water-tight concept is an essential prerequisite for the trust-based relationships that are central to e-business. Processes must first be documented and then implemented in the form of a comprehensive security architecture, paying particular attention to four key areas: efficient user and role management, secure system management, and realisation of the trust relationships and of security mechanisms at the application level (fig. 1).

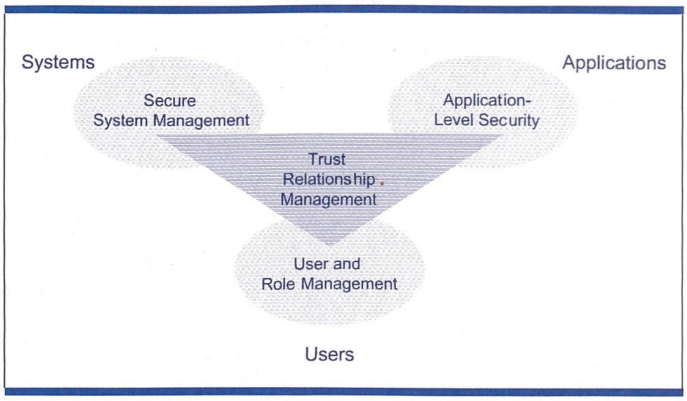

Fig. 1. Trust relationships in e-business.

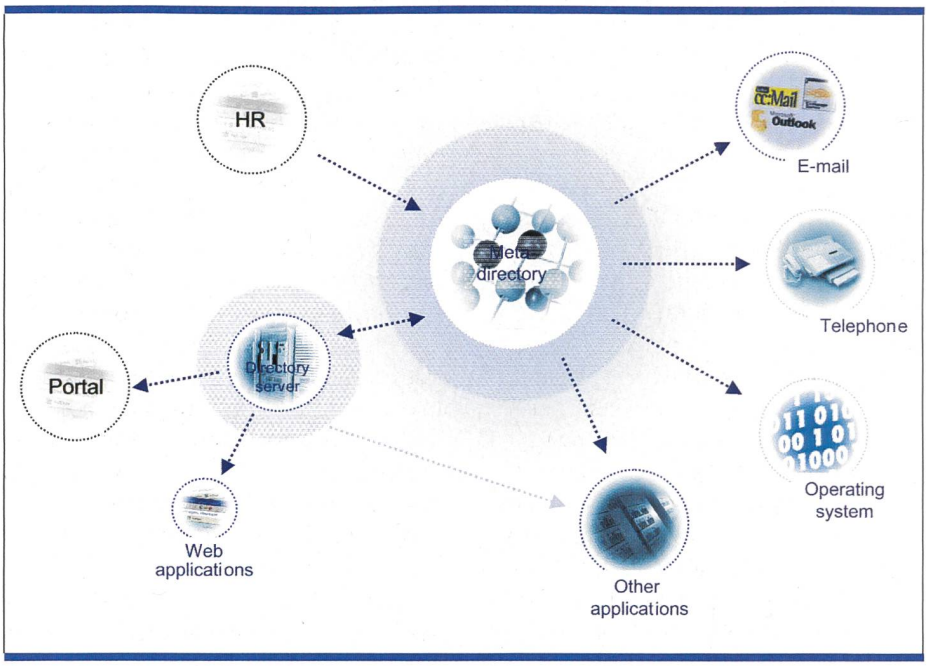

Fig. 2. User management based on a directory service.

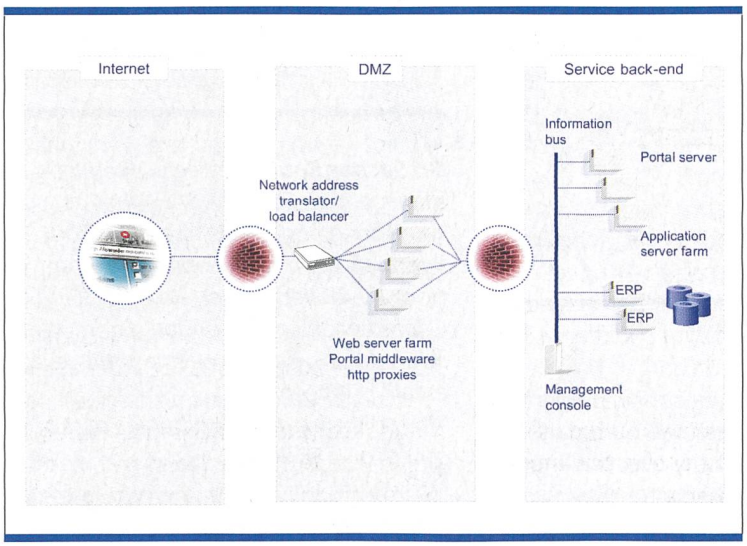

Fig. 3. A secure network architecture.

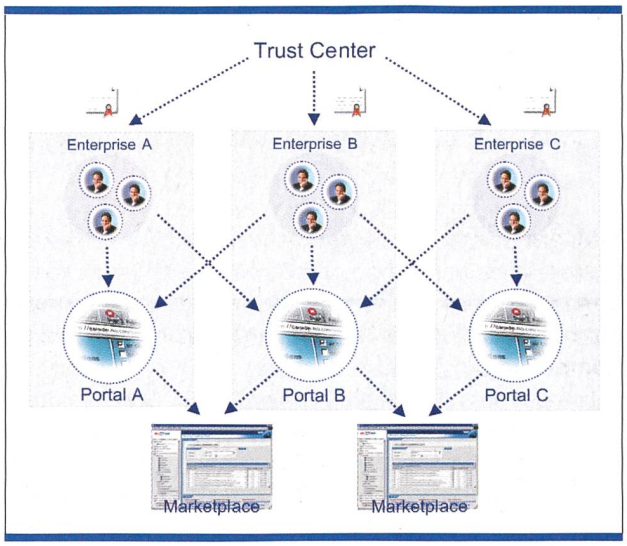

Fig. 4. Secure access to external and internal web sites.

User and role management

The business processes typical of e-business are creating exciting new opportunities for enterprises: Customers and business partners can be integrated seamlessly into business processes, while employees can be granted significant levels of responsibility within these processes. But – how do you make sure that users, whether internal or external, cannot gain access to information that they should not see? And how can employees' roles and authorisations be managed in a way that is secure, efficient and application-independent?

The Internet economy – characterised as it is by the complex system environments required by electronic business processes and by corporate networks that are necessarily open to outside access – is changing the way that user and authorisation management is done. More than ever, a high priority is being attached to such things as simple, centralised administrative processes, the integration of external users into authorisation processes, a universal role concept that can be applied to every application used in the enterprise and the integration of directory services via enterprise portals.

In many system environments, user information is dispersed across several different systems: e-mail, telephone and application systems are typical examples. Thus, a single enterprise will often have a number of directories containing the same or at least similar data. One way of avoiding this kind of data redundancy is to effectively combine each of these user data directories into a central meta-directory for the whole enterprise. This central directory obtains user data directly from the HR system and passes it on to all other connected systems as required – e.g. to messaging, telephone and application systems. Information about roles and responsibilities can also be stored in this way. Implementing a directory service creates a "single point of administration" for user management. Minimizing data redundancy and centralizing administrative processes allows the highest levels of both efficiency and security to be achieved (fig. 2).

The role concept needs to make a clear distinction between roles and authorisations. This will help keep the concept independent of specific applications and will simplify administration. A role consists of a number of logical services – for example, the creation of customer orders or order billing – which together define an employee's activity profile. These logical services are then allocated to physical services such as those for enabling access to transactions or to reports in application systems. Thus roles are defined according to relevant activities, in other words "bottom-up", and on a department-by-department basis. Combining employee authorisations into the same roles would result in a very complex administrative process, since authorisations are usually defined along the lines of the organisational structure and according to the user's position in the organisation – in other words "top-down". It is, moreover, common for authorisations to be assigned either centrally, for example in the HR organisation management, or in individual applications, in Controlling or in Financial Accounting, for example.

Secure system management

The creation of secure network configurations is a well-understood science, based on the principles of defining network segments and configuring firewalls. The trend toward opening up corporate networks to outside access, however, has made the elimination of all security gaps increasingly tricky. A network should consist of a set of security zones together with a small number of connections between these zones, each protected by a firewall. External access to the corporate network is provided by means of so-called demilitarised zones (DMZ), which use a combination of external and internal firewalls. This ensures that access to the information systems is only possible from certain zones and using specified services and protocols.

Together with appropriate mechanisms for authenticating system components and for encrypting communications between servers, this provides a good level of protection. For this reason the use of HTTP on the standard Internet protocol known as Secure Sockets Layer (HTTPS = HTTP on SSL) is strongly recommended for all Internet communication. HTTPS is now supported together with strong encryption by all commonly used web servers and browsers worldwide. It is also possible to integrate intrusion detection systems into system management. These record all unusual system activity and detect attempts at unauthorised access (fig. 3).

Building trust on reliable authentication

Authentication mechanisms are becoming increasingly hard to manage in com-

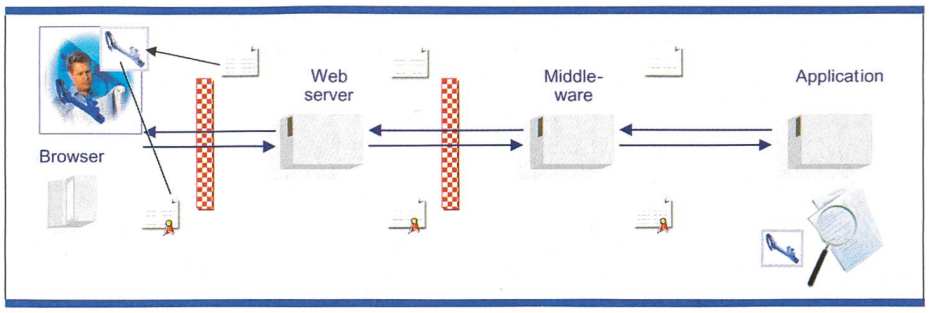

Fig. 5. Transaction security based on digital signatures.

plex e-business system environments. In environments with a large number of systems, users can no longer be expected to remember the multiplicity of passwords needed. Procedures such as single sign-on and authentication delegation have become practically indispensable for an e-business environment. Because systems are increasingly designed for internal use by a company's own staff as well as external use by customers and partners, the mechanism used for identifying and logging on users must be both secure and easy to use. Digital certificates, issued by a recognised "trust center" and embodying standardised authentication processes, offer a very high level of security for electronic transactions. A trustworthy registration authority is set up, with which all users must register. Ideally, this is integrated directly into the user management and can pass user data straight to the trust center. For each user the trust center creates a digital identity consisting of two keys, one public and the other private. The digital certificate contains the name of the user and the public key of the digital identity, while the private key is known only to the owner of the certificate. The certificate can now be used to perform the authentication required at portals or at virtual marketplaces (fig. 4).

Security mechanisms at the application level

Collaborative business processes are frequently distributed across a number of interlinked systems. For this reason, detailed authorisation management alone cannot guarantee a secure, audit-proof environment. When processes are executed in distributed system environments, the trust relationship information must be attached directly to the data so that records can be kept to prove that the data was used correctly. Companies can achieve this by using digital signatures. Collaborative transactions are allocated a number of electronic properties, and these help guarantee both data integrity and authenticity over the entire lifespan of the transaction.
Since the technology required for this cannot be made available centrally, it is integrated into the application processes. A digital signature equips data – for example, the details of an online order – with additional information that helps guarantee the integrity of the transaction. Each system through which the data passes and which has the functions required for verifying digital signatures can check this information. Verification can be performed at a number of different levels. Factors such as the type of certificate or the issuing trust center, for example, can be used to determine whether or not the signature is accepted. The validity of the certificate at the time the signature was made can also be checked. Business processes involving digitally signed transactions require a fall-back configuration for instances where a transaction is aborted following a negative verification (fig. 5).
The application itself is responsible for security in other areas too, for example in the statutory forms of digital signatures for bid invitations and contracts, in electronic payment procedures, e-mail encryption or steganography.

The security challenge

The growth of Internet usage has made the protection of corporate systems and data – no trivial task even back in the days of closed system environments – into a highly significant challenge. Whereas system-oriented security mechanisms were generally adequate in the past, the mechanisms must now be implemented at the level of individual transactions. However, if an enterprise ensures that its security policy takes adequate account of the four areas of security architecture described here, the exciting new opportunities offered by e-business can be exploited while avoiding unnecessary security risks. [4]

Dr. Sachar Paulus, *Director Product Management Security, SAP who are sponsoring and speaking at ISSE 2001 – Information Security Solutions Europe, from 26-28 September 2001 at QEII Conference Centre, London. For more information visit www.eema.org/isse or email: isse@eema.org*
This article has been written as part of a series for ISSE 2001.

Zusammenfassung

Sicherheit auf Vertrauen aufbauen

Jedes Unternehmen, das seine Geschäfte in das Internet bringt, steht unausweichlich erhöhten Sicherheitsrisiken für seine Daten gegenüber. E-Business erfordert normalerweise die Verlagerung kompletter Prozesse und der zugehörigen Daten in das Internet, wobei es sich um vertrauliche Daten handelt, die unter keinen Umständen in die Hände der Konkurrenten gelangen dürfen. Alle möglichen Sicherheitsrisiken müssen daher so früh wie möglich erkannt werden, und die erforderlichen Massnahmen müssen in die Wege geleitet werden. In vielen Ländern ist dies bereits gesetzlich vorgeschrieben. Lineares Risiko-Management mag nicht beliebt sein, aber es ist unumgänglich geworden. Durch die zunehmende Internet-Nutzung ist der Schutz von Unternehmenssystemen und -daten – schon in den Tagen der geschlossenen Systemumgebungen keine einfache Aufgabe – zu einer bedeutenden Herausforderung geworden. In diesem Artikel werden vier Bereiche der Sicherheitsarchitektur beschrieben. Wenn ein Unternehmen dafür sorgt, dass seine Sicherheitsrichtlinien diese Bereiche angemessen berücksichtigen, können die spannenden neuen Chancen, die E-Business bietet, genutzt werden, ohne unnötige Sicherheitsrisiken einzugeben.