Managing the security of data flow

Customer Relationship Management (CRM) systems are cited as one of the major technology successes of the last decade. These ‘super databases’ enable the real-time sharing of information across global organisations, increasing the visibility of the sales pipeline and providing a central control of the customer experience. A far cry from the early databases which were supported in the locally networked environment, CRM systems have pushed database capabilities into the enterprise arena, providing accurate monitoring of customer information and enabling corporations to sell and market to customers through a centrally managed delivery mechanism.

This increased fluidity of information across multiple interfaces effectively brings customers and suppliers closer together. By its very nature, however, such free-flowing information introduces inherent risks in system security; a fact which many developers and users of these web-facing enterprise systems are now being forced to address.

Globally accessible CRM systems are built on the principal that they can be operated in real time by the user and, subject of course to locally determined permissions, allow the read and write functionality of shared information. The CRM package itself is responsible for the transfer, processing and storage of this data. As a system, it is made up of several applications that sit on top of standard web servers and database platforms, feeding information to and retrieving it from the massive database that lies behind.

It is this web interaction and multi component composition which introduces the possibility of increased security risk, even if the server (or servers in a load balanced situation) upon which the CRM is installed may be hosted in a secure and regularly tested network environment.

Many of the applications which constitute the packaged CRM solution, such as chart servers and search engines, may in fact be third party items which the CRM manufacturer has bundled with its product. Obviously it is entirely possible that these individual products have been tested thoroughly and configured in such a way that the dataflow between them is secure. But this is not what security experts are finding.

On the one hand, each component is susceptible to and must be secured against all the individual vulnerabilities which that product may possess. Coupled with this is the interaction with the CRM software itself. If the software does not have inbuilt checks and regulations to secure the data flowing through it from each of its component products then it is conceivably possible that the system may be compromised should such a weakness occur. And it only takes one ‘rogue’ product.

Furthermore, if these component products were bundled into the package with their default installations, then these vulnerabilities would remain, even if patches and updates were applied.

The packaged nature of these solutions means that the corporation which is operating the CRM system may have unwittingly relinquished control of some of its system administration procedures. Although they may be aware that the complete solution or package is of multi-vendor origin, they may not realise the possible security risk associated with this bundling. Indeed some may even believe that they have increased the protection of their network by adopting the multi-layered security that a mixed-vendor system can offer. One of the most common vulnerabilities that security experts are finding with the multiple component bundling is that some of the gateways between the applications are deliberately left open in order that the transfer of data is expedited. As such, some of the default accounts and passwords used by the system itself (as opposed to those at the user interface) may be removed from the normal procedures stipulated by the organisation’s security policy. Password rotation, or indeed procedures to disable certain passwords, is an integral part of any good security policy. If these static system passwords are cracked for example, an attacker could then have administrative access to the CRM’s settings and of course the underlying database.
Managing the security of data flow

Another security risk, and one that can by no means be ignored, is from the intended users of the system themselves. If the read/write permissions have not been thoroughly checked then an employee may find that they have unauthorised access to what should be a closed area of the system. Whether maliciously intended or accidental, there is then the potential that a security breach could occur from within the organisation.

The CRM systems themselves offer massive business benefits in streamlining the sales process, efficiently connecting suppliers and customers in a global environment and allowing a central control of the customer experience. With the increased data share though comes the increased risk. From ‘holes’ created in the installation and customisation processes through to other errors made by the software vendor, the permutations in the possibility of weaknesses within the system then become abundant. It is only through a vigilant and regular testing of the application itself, both in isolation from and within the network environment, that these risks can be truly mitigated.

By Diane Seddon
Industry Analyst, Corsaire Ltd

About Corsaire
With over 6 years experience in providing network security solutions to the private, public and non-profit sectors, including the FTSE 100, Corsaire is considered a leading specialist in the delivery of network security design, implementation and management. Whilst offering a broad range of bespoke solutions that are based on industry standards & guidelines, Corsaire adopt a consultative approach and combine a vendor neutral policy with knowledge-share to deliver impartial, up-to-date advice. Corsaire is respected for its contribution to R&D, its consistent, high-level service delivery and an ability to combine technical and commercial excellence within the workplace.

Corsaire Contact:
Jane Frankland
Tel: +44 (0) 1483 226 000
Fax: +44 (0) 1483 226 001
Email: jane.frankland@corsaire.com